Současné útoky na osobní počítače k narušení bezpečnosti informací

Lukáš Navrátil

Bakalářská práce
2019

Univerzita Tomáše Bati ve Zlíně
Fakulta logistiky a krizového řízení

Univerzita Tomáše Bati ve Zlíně
Fakulta logistiky a krizového řízení
Ústav ochrany obyvatelstva
akademický rok: 2018/2019

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

Jméno a příjmení:	**Lukáš Navrátil**
Osobní číslo:	**L16185**
Studijní program:	**B2825 Ochrana obyvatelstva**
Studijní obor:	**Ochrana obyvatelstva**
Forma studia:	**prezenční**
Téma práce:	**Současné útoky na osobní počítače k narušení bezpečnosti informací**

Zásady pro vypracování:

1. **Zpracujte rešerši současného stavu vztahující se k dané problematice s důrazem na monografie a analytické materiály.**
2. **Seznamte se se současnými útoky na osobní počítače k narušení bezpečnosti informací.**
3. **Realizujte útok na osobní počítač za účelem narušení bezpečnosti informací.**
4. **Navrhněte opatření pro snížení rizika spojeného s realizovaným útokem.**

Rozsah bakalářské práce:

Rozsah příloh:

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

Seznam odborné literatury:

[1] JIRÁSEK, Petr, NOVÁK, Luděk a POŽÁR, Josef. Výkladový slovník Kybernetické bezpečnosti: Třetí doplněné a upravené vydání. 3. Praha: Policejní akademie České republiky v Praze, 2015. ISBN 978-80-7251-436-6.

[2] KOLOUCH, Jan. CyberCrime. Praha: CZ.NIC, z.s.p.o., 2016. CZ.NIC. ISBN 978-80-88168-15-7.

[3] NEZMAR, Luděk. Zákon o kybernetické bezpečnosti pro organizace – Implementace nových povinností do praxe. Grada, 2018. ISBN 978-80-271-0899-2.

Další odborná literatura dle doporučení vedoucího bakalářské práce.

Vedoucí bakalářské práce: **Ing. Petr Svoboda**
Ústav ochrany obyvatelstva

Datum zadání bakalářské práce: **30. listopadu 2018**

Termín odevzdání bakalářské práce: **15. května 2019**

V Uherském Hradišti dne 30. listopadu 2018

doc. Ing. Zuzana Tučková, Ph.D.
děkanka

prof. Ing. Dušan Vičar, CSc.
ředitel ústavu

PROHLÁŠENÍ AUTORA BAKALÁŘSKÉ PRÁCE

Beru na vědomí, že:

- bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému a dostupná k nahlédnutí;
- na moji 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;
- 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;
- podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – 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);
- pokud bylo k vypracování bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tj. k nekomerčnímu využití), nelze výsledky bakalářské práce využít ke komerčním účelům;
- pokud je výstupem 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 bakalářské práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze bakalářské práce a verze elektronická nahraná do IS/STAG jsou obsahově totožné.

V Uherském Hradišti, dne: 15.5.2019

Jméno a příjmení studenta: Lukáš Navrátil

.....

podpis studenta

ABSTRAKT

Tato bakalářská práce se zabývá možnými útoky na osobní počítače, kdy je v teoretické části popisováno několik obecných pojmů, jako je bezpečnost, informační a komunikační technologie a zabezpečení. Prostor je věnován také názvosloví z oblasti bezpečnosti informací a další související pojmy. Následně jsou popsány přímo základní typy útoků dělených podle způsobu provedení. Praktická část se plně věnuje přípravě virtuálního počítače a instalaci vybraných operačních systémů. Následují samotné analýzy bezpečnosti systémů při použití různých vybraných útoků. V poslední části práce lze nalézt opatření proti analyzovaným útokům.

Klíčová slova: Útok, bezpečnost, počítač, operační systém, data, informace

ABSTRACT

This bachelor thesis deals with possible attacks on personal computers, where several general terms such as security, information and communication technologies and security are described in the theoretical part. The space is also devoted to the terminology of information security and other related concepts. Subsequently, the basic types of attacks divided according to their execution are described. The practical part is fully devoted to the preparation of a virtual machine and installs selected operating systems. Following are security system analyses themselves using various selected attacks. In the last part of the thesis, measures against analyzed attacks can be found.

Keywords: Attack, safety, computer, operating system, data, information

Rád bych poděkoval hlavně svému vedoucímu Ing. Petru Svobodovi za čas, který mi věnoval. Za veškeré rady a ochotu. Dál bych chtěl poděkovat své rodině, která mi umožnila studovat a vždy mě podporovala. Rád bych taky poděkoval kamarádům za pomoc při anglickém překladu a matce za gramatickou kontrolu.

Prohlašuji, že odevzdaná verze bakalářské práce a verze elektronická nahraná do IS/STAG jsou totožné.

V Uherském Hradišti, 14. 5. 2019

Lukáš Navrátil

OBSAH

ÚVOD

Rozvoj informačních a komunikačních technologií je v současnosti výrazný. Se stále větší dostupností mobilních telefonů, osobních počítačů a dalších různých technologií je samozřejmě spjato větší bezpečnostní riziko. Mnoho uživatelů těchto technologií nebere bezpečnost moc vážně, většinou ani nemají přehled o hrozbách a už vůbec na ně neumí reagovat. Nyní se útočníkem může stát téměř kdokoliv. Hlavním důvodem je anonymita a to, že se nástroje pro útoky dají sehnat na internetu zcela běžně. Uživatelé mnohokrát slepě důvěřují výrobci operačních systémů, že výrobek, který vlastní, je zabezpečen proti nejnovějším útokům, ale většinou to není pravda.

V teoretické části práce je hlavně vysvětleno několik základních pojmů. Nejen informační a komunikační technologie, ale také bezpečnost, data a informace, útok, kyberterorismus a zabezpečení. Kapitola je dále zaměřena na názvosloví z oblasti bezpečnosti informací a dalšími souvisejícími pojmy, které jsou zmiňované napříč celou prací. Druhá kapitola je již zcela zaměřena na útoky, které jsou rozděleny podle způsobu provedení. Jsou zde popsány principy fungování těchto útoků.

Praktická část je ukázkou analýzy náročnosti provedení útoku na osobní počítač. V současnosti jsou útoky na počítače více pravděpodobné kvůli dostupnosti těchto technologií snad už v každé rodině. „I obyčejný člověk s nějakým programem dnes může napadnout něčí počítač a ukrást mu z něj data a informace, pokud je nebude mít chráněná.“ A důležité je zmínit, že nemusí mít vystudovanou žádnou školu se zaměřením na informační bezpečnost. Na začátku praktické části je příprava virtuálního počítače, kde se vše realizovalo. V další kapitole jsou už samotné průběhy analýz vybraných způsobů útoku. A na závěr opatření, která mají chránit data a informace uživatele počítače.

I. TEORETICKÁ ČÁST

1 TERMÍNY Z OBLASTI ICT

První kapitola se zabývá základními pojmy z oblasti informačních a komunikačních technologií. Názvosloví z bezpečnosti informací a dalšími pojmy, které jsou zde použity.

1.1 Obecné pojmy

V této podkapitole jsou vysvětleny pojmy, které se nepoužívají pouze v informatice, ale i v jiných oborech. Jedná se o slova, která jsou používána v každodenním životě.

1.1.1 Informační a komunikační technologie

Informační a komunikační technologie označující se ICT (dále jen ICT) v sobě zahrnují dva pojmy. Souvisí s tím veškerá technologie určená ke komunikaci a práci s daty i informacemi. ICT je rozšíření zkratky IT, která se používala dříve a znamenala jen informační technologie. Rozšíření o komunikaci bylo díky komunikaci mezi počítači a jinými sítěmi. Patří sem veškeré hardwarové a softwarové vybavení, které tvoří právě celek ICT. Bez jedné části by totiž nemohla probíhat buď komunikace, nebo by nefungovaly informační technologie. V současné době je pojem ICT velmi používaný. Je to i z důvodu velké komunikace mezi lidmi skrze různé sociální sítě a víc než kdy jindy probíhá sdílení informací hodně rozšířeně. I ve školách se již nevyučuje informatika, ale ICT. [1,2]

1.1.2 Bezpečnost

Tento termín se používá v mnoha oblastech a to od bezpečnosti státu, přes firemní bezpečnost až po kybernetickou bezpečnost a mnoho jiných. Přesný význam se tedy odvíjí od toho, s kterou oblastí je spojen. Je tudíž velmi složité definovat pojem samotný. Naštěstí se o jednu definici, o kterou se opírá mnoho materiálů, postaral stát, který zpracoval terminologický slovník právě kvůli vysvětlení bezpečnosti a jiných zásadních termínů. Terminologický slovník pojmů z oblasti krizového řízení, ochrany obyvatelstva, environmentální bezpečnosti a plánování obrany státu definuje bezpečnost takto: *„Stav, kdy je systém schopen odolávat známým a předvídatelným (i nenadálým) vnějším a vnitřním hrozbám, které mohou negativně působit proti jednotlivým prvkům (případně celému systému) tak, aby byla zachována struktura systému, jeho stabilita, spolehlivost a chování v souladu s cílovostí. Je to tedy míra stability systému a jeho primární a sekundární adaptace.“[3]* [3]

1.1.3 Data vs. Informace

Data a informace jsou v oblasti ICT velmi používané. Jedná se o dvě rozdílné věci, i když si jsou také velmi blízké.

V Úmluvě o počítačové kriminalitě jsou hned na začátku zmíněna počítačová data. Tento dokument je definuje jako *„jakékoli vyjádření faktů, informací nebo pojmů ve formě vhodné pro zpracování v počítačovém systému, včetně programu způsobilého zapříčinit provedení funkce počítačovým systémem“[4]*. Pokud se, ale zaměříme na data jako samotný pojem, tak význam je jiný. Data *„jsou fakta, čísla, události, grafy, mapy, transakce atd., které byly zaznamenány. Jsou základním materiálem, surovinou pro informace.“[5]* Jde tedy důležité skutečnosti, které jsou uloženy na datovém nosiči, což může být hardware (Harddisk, USB Flash Disk,…), ale také to může být papír.[5]

Informace je předávání dat mezi příjemcem a informátorem, která mají určitou hodnotu. Neznamená to ale, že data musí tvořit informaci vždy. Data jsou skutečnosti, které sami o sobě nemusí dávat žádný smysl a nejsou tudíž informací. Ale když se data dají do souvislosti, tak utvoří plnohodnotnou informaci. [5]

1.1.4 Útok

Jde o jakýkoliv pokus o poškození, zničení, či jakékoliv ohrožení chráněného zájmu. Útok je v různých souvislostech chápán různě, ale hlavní charakteristika je ohrožení chráněného zájmu, čili aktiva. Aktivem je chápán život, zdraví, majetek nebo cokoliv, co má pro majitele hodnotu. [3]

1.1.5 Kyberterorismus

Kyberterorismu je založen na práci v utajení, finanční nenáročnosti, překvapivém útoku a samozřejmě nekonvenčnosti. Můžeme ho chápat v širším a užším smyslu. V širším smyslu jde o využití dostupných prostředků ICT k terorismu za účelem informování svých členů, propagaci nebo zveřejňováním získaných informací. V užším smyslu tím jsou chápány útoky na ICT, získání dat a informací a jejich využití. Cílem může být šíření strachu, zviditelnění organizace nebo také obohacení.

V současné době se jedná o zcela aktuální pojem, jelikož se ICT využívají více než kdy dřív. Nyní jde o běžnou věc téměř pro každého člověka. Přes internet se dnes nakupuje a posílá mnoho informací a dat. Lidé mají své osobní údaje už nejen na svých dokladech,

ale právě třeba v počítači a na různých účtech na internetu. Mohou to být nejen údaje jako rodné číslo, číslo účtu, adresa, ale také fotky, videa, dokumenty a podobné osobní věci. Pro „kyberteroristy“ jsou takové cíle velmi lákavé. Důvody: malá ochrana, nižší vzdělanost v oblasti ICT a anonymita. [6]

1.1.6 Zabezpečení

Tento pojem má více významů, podle toho v jakém kontextu se použije. Při použití „zabezpečit dodávku potravin“ znamená zaopatřit. Ale u „zabezpečit majetek“ jde o ochranu.

V souvislosti s počítačem jde o zajištění ochrany před vpádem či útokem na jeho obsah nebo také na fyzický hardware. Máme tedy více druhů zabezpečení, které se dá dělit podle objektu zabezpečení.

Fyzické

Zabezpečit fyzicky počítač jde většinou ruku v ruce se zabezpečením celého objektu, ve kterém je počítač umístěn. Jedná se například o dům nebo místnost. Ale může jít i o zabezpečení počítačové skříně (obal, ve kterém je zdroj, základní deska, procesor a ostatní komponenty) a to různými způsoby. Většinou jsou umístěné v uzamykatelné skříni nebo mohou být připevněny ke stolu ocelovým lanem. Ale jsou i speciální stoly s kovovou konstrukci, která má místo pro počítačovou skříň uzamykatelnou a nejde z ní počítačová skříň vyndat.

Obrázek 1 – Speciální stůl s kovovou konstrukcí a uzamykatelnou skříní pro počítačovou skříň [Zdroj: 7]

Softwarové

Nejčastěji používané je softwarové zabezpečení z důvodu možné ztráty nebo odcizení dat z počítače. Zabezpečení může být několikanásobné. Mohou to být antivirové programy, heslo uživatele počítače, šifrování dat v počítači a další. Většina způsobů je bezplatná, mívají ji všichni (heslo uživatele počítače, antivirový program – bezplatný). Následně jsou i placené jako plnohodnotné antivirové programy a zálohovací úložiště hlavně využívané podniky. A další způsob je spíše pro odborníky nebo někoho, kdo se zajímá o tuto problematiku a to je šifrování dat, kterému musíte rozumět. [8]

1.2 Názvosloví z oblasti bezpečnosti informací

Tato podkapitola vysvětluje pojmy, které mají vztah se zabezpečením počítače, dat a informací v něm. Jsou to informační bezpečnost, počítačová bezpečnost, narušení bezpečnosti informací a bezpečnostní zranitelnost.

1.2.1 Informační bezpečnost

V současné době velmi používané slovní spojení. Ne každý zná jeho význam. Především jde o zabezpečení všech informací po dobu jejich existence. Kdyby nebyly zabezpečeny, mohlo by dojít k jejich ztrátě nebo krádeži a majiteli by vznikla škoda. Jelikož se data uchovávají v elektronické podobě, je třeba je chránit, ať už jsou uložena v počítači, online úložištích a podobně. Touto oblastí se zabývá mnoho firem, které nabízejí kurzy pro zaměstnance zaměřené na to, jak se o data starat, bezpečně je používat, uchovávat a také možnost vzdělání zákonem o kybernetické bezpečnosti. Pro firmy a společnosti pracujícími s daty a informacemi by to mělo být samozřejmé, ale i obyčejný člověk zacházející s daty by měl znát základy zacházení s nimi, kvůli ztrátě. [9]

Pro informační bezpečnost jsou důležité tři základní pilíře. Označují se CIA. Každé písmeno představuje jeden pilíř. Jsou to:

- **C** (Confidentiality) – důvěrnost
- **I** (Integrity) – integrita
- **A** (Availability) – dostupnost

Útoky mohou být namířeny na každý pilíř. Dopad útoku na kterýkoliv z nich bývá velmi závažný. Majitel může o svá data přijít, mohou být pozměněna nebo v případě důvěrných dat s nimi může být vydírán. Proto je důležité vysvětlit význam každého pilíře.

Důvěrnost znamená, že k datům mají přístup pouze jejich majitelé a oprávněné osoby.

Integrita zase zajišťuje správnost a úplnost dat. Nikdo je nesmí poškodit nebo pozměnit. Ať už útočník nebo zaměstnanec firmy.

Dostupnost zajišťuje, že jsou data a informace k dispozici v potřebný čas. [10]

1.2.2 Narušení bezpečnosti informací

Samotná definice není nikde přesně určena, proto není lehké toto sousloví přesně vystihnout. Dalo by se také napsat jako „narušení informační bezpečnosti“. Zde je použit pojem, který je už rozebrán v této podkapitole. Můžeme ho tedy popsat tak, že vysvětlíme zvlášť pojmy narušení a informační bezpečnost. Poté významy spojíme a zkusíme je logicky zformulovat do jedné definice. Samotné narušení se dá popsat jako ohrožení, poškození, změnu nebo zničení něčeho. Informační bezpečnost (nebo také bezpečnost informací) znamená zabezpečení informací po dobu jejich existence. Definice by mohla znít: „Naru-

šení bezpečnosti informací znamená neoprávněné či nezákonné ohrožení, poškození, změnu nebo zničení zabezpečení informací, které může vést k jejich odcizení."

V zákoně o kybernetické bezpečnosti je pojem „narušení bezpečnosti informací" použit takto v souvislosti s definicí kybernetické bezpečnostní události a kybernetického bezpečnostního incidentu.

*„Kybernetickou bezpečnostní událostí je událost, která může způsobit **narušení bezpečnosti informací** v informačních systémech nebo narušení bezpečnosti služeb anebo bezpečnosti a integrity sítí elektronických komunikací." [11, § 7, odstavec 1]*

*„Kybernetickým bezpečnostním incidentem je **narušení bezpečnosti informací** v informačních systémech nebo narušení bezpečnosti služeb anebo bezpečnosti a integrity sítí elektronických komunikací v důsledku kybernetické bezpečnostní události." [11, § 7, odstavec 2]*

1.2.3 Bezpečnostní zranitelnost

Je chyba, nedostatek nebo závada, kterým oplývá software nebo firmware. Toto slabé místo může být zneužito útočníkem, který může způsobit škodu. Je to jedna z bezpečnostních hrozeb nejen pro počítače. Po vývoji softwaru a jeho spuštění může kdokoliv najít právě nějakou chybu či nedostatek. Výrobce ještě před plným spuštěním sice software testuje, ale i tak nemusí objevit vše. Záleží, kdo chybu nakonec objeví, protože podle toho se rozhodne, jestli vznikne škoda či nikoliv. Pokud nedostatek nahlásí uživatel nebo bezpečnostní analytik přímo výrobci, ten musí sjednat nápravu. Útočník může chybu zneužít pro své účely. [12]

1.3 Definice souvisejících pojmů

Následující pojmy jsou důležité z hlediska ICT. V této práci jsou mnohokrát zmiňované a to zejména v praktické části, kdy jsou podstatné při analýze a hlavně při opatřeních proti útokům.

1.3.1 Počítač

V obecném pojetí tohoto slova se jedná o jakýkoliv stroj, který zpracovává data a provádí rozličné aritmetické a logické operace. Počítač obecně může být i kalkulačka, mobilní telefon a podobně. Většině lidí se ihned vybaví PC, které je v dnešní době už všem známé

a má ho snad každý doma a tráví u něj svůj veškerý volný čas. Zkratka PC pochází z anglického „Personal Computer“, což znamená osobní počítač. PC můžeme dělit na nepřenosné a přenosné. Nepřenosné jsou stolní počítače, které se skládají z počítačové skříně („case“), monitoru, klávesnice, myši a dalšího rozšiřujícího vybavení. Zato přenosné mají tyto komponenty vestavěné. Jsou to notebooky, které mají monitor připevněný ke zbytku. Klávesnice a myš jsou integrované. A myš je ve formě touchpadu, který je dotykový.[13,14]

Počítač ve smyslu nám známých stolních počítačů nebo notebooků se skládá ze dvou hlavních částí a těmi jsou hardware a software.

1.3.2 Hardware

Tento pojem, který se občas zkracuje na HW, označuje v podstatě celý počítač. Nejedná se však jen o počítač a jeho komponenty, ale i o rozšiřující vybavení jako tiskárnu, skartovací stroj, mikrofon, reproduktory a jiné. Celkový výčet veškerého hardwaru je velmi dlouhý. Hardware je tedy oproti softwaru hmatatelný. Při pořizování počítače se právě nejvíce utratí za hardware, který obstarává chod počítače a další rozšiřující funkce. Další důvod, proč se za hardware musí utrácet je ten, že oproti softwaru, který často lze sehnat zadarmo z internetu, to s hardwarem udělat nejde. Součástky k počítači nelze získat jinak, než si je koupit. [15]

1.3.3 Software

Obecně tak lze nazvat počítačový program, ale to není přesná definice softwaru. Přesnější vymezení pojmu je programové vybavení PC. Software zahrnuje celou baterii programů, které jsou využívány v počítači. Software lze rozdělit na několik skupin, a to na:

- Systémový software – programy zajišťující chod počítače.
- Aplikační software – programy, které využívá uživatel.
- Firmware – program, který ovládá hardware (BIOS).

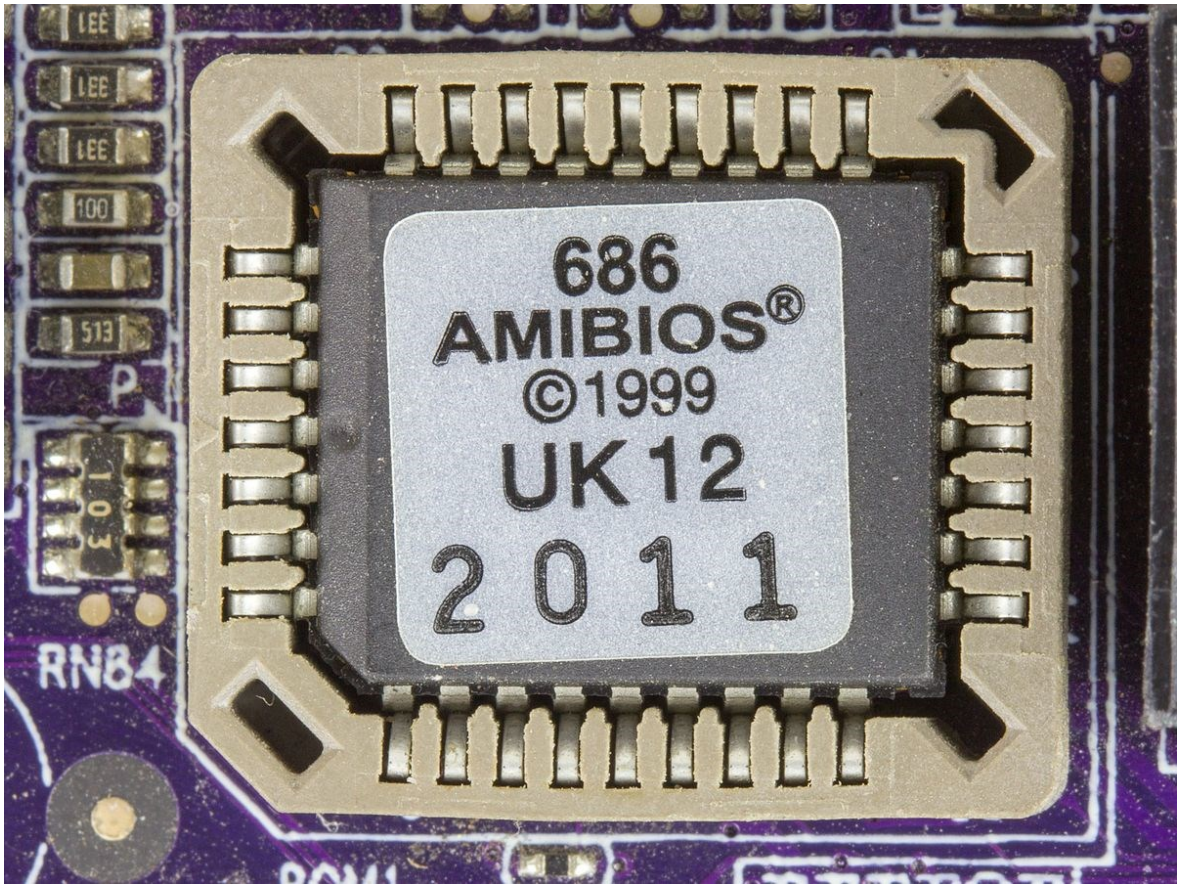
Software je nehmotný, nemůže existovat a fungovat bez hardwaru, kde je i uložen. A to konkrétně na záznamovém médiu nebo v paměti.

Z důvodu používání dalších významných pojmů v této práci je potřeba je vysvětlit. Jde o základní softwarové nástroje počítače, které mají velký význam nejen pro chod počí-

tače, ale také pro bezpečnost dat uživatele počítače. Jsou to BIOS a operační systém. [12,15,16]

BIOS

Celým názvem Basic Input-Output System (česky „základní vstupně-výstupní systém“) slouží jako prostředník mezi základní deskou (anglicky „motherboard“) a operačním systémem. Tento software se nachází na malém paměťovém čipu typu ROM na základní desce. V BIOSu jsou uloženy informace o základní desce, rozšiřujících slotech a umožňuje základní nastavení počítače. V podstatě při instalaci nového PC se při prvním spuštění objeví právě BIOS, který funguje, i když není nainstalován operační systém. V BIOSu se poté nastaví, odkud se bude instalovat operační systém (CD-ROM, DVD-ROM, USB Flash Disk). [17,18]



Obrázek 2 – Paměťový čip, na kterém je uložen BIOS [Zdroj: 19]

BIOS také provádí při každém spuštění PC kontrolu, takzvanou POST (Power-On Self-Test). Při tomto testu v podstatě BIOS zkontroluje všechny hlavní komponenty PC, zda pracují, tak jak mají. Pokud je vše v pořádku, spouští samotný operační systém. Je to nepostradatelný díl PC, bez kterého by nešel zapnout. Výrobou BIOSů se zabývá několik firem

a mezi nejznámější patří Phoenix Technologies, IBM, Dell, Gateway, BYOSOFT, American Megatrends Inc. (AMI) a Insyde Software. [20]

Operační systém

Je to základní softwarový nástroj, který musí mít každý počítač, aby uživatel mohl používat jeho další funkce: aplikace, hry, internet, práce se soubory apod. I když jsou i takové aplikace, které umějí komunikovat přímo s hardwarem, tak převážná většina je vytvořená pro operační systém (dále jen „OS“). OS je velmi komplexní nástroj, který spravuje nejen software, ale také hardware pro ovládání počítače (např. klávesnici, myš, monitor, paměťová zařízení, síťová zařízení, tiskárnu a další). Nejde jen o osobní počítače, ale také o mobily, které mají také OS. [21,22]

Tyto systémy mají mnoho komponentů a funkcí a každý OS se ovládá jinak. Ty nejzákladnější komponenty jsou:

Jádro (Kernel) vykonává několik úkolů. Mezi hlavní patří čtení dat z paměti a jejich zápis do paměti. Dále zpracovává prováděcí příkazy, určuje způsob přijímání dat, které pak posílá do monitoru, myši a klávesnice. Řídí činnost procesů OS. [22,23]

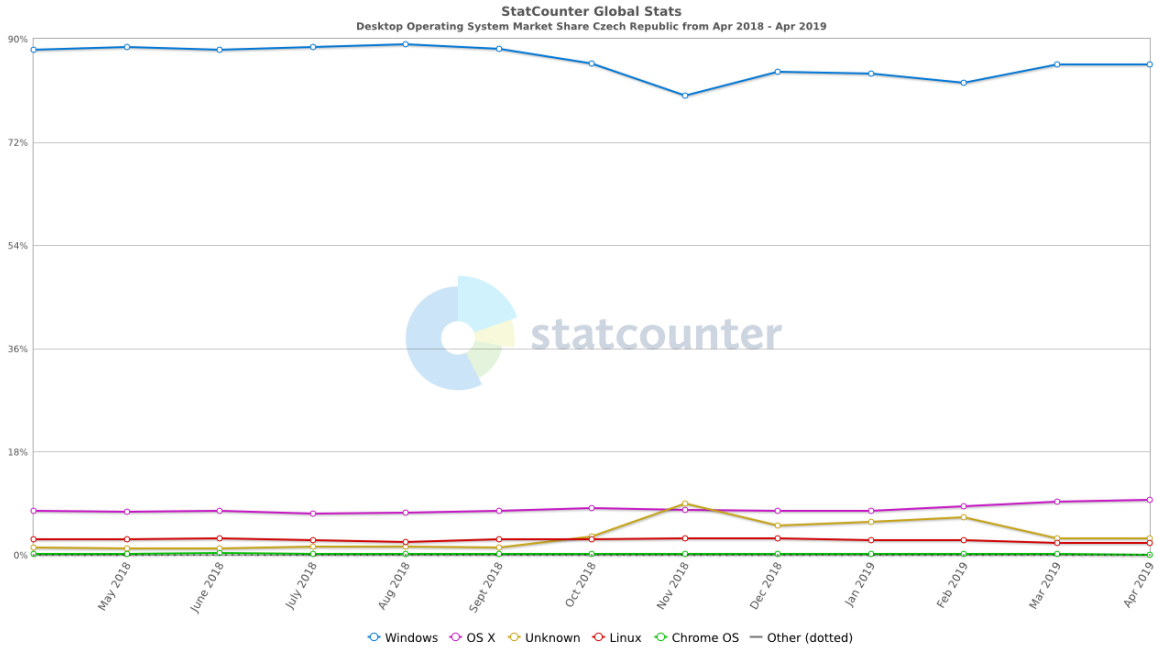
Uživatelské rozhraní (User Interface) slouží k interakci mezi OS a uživatelem ve formě grafické ikony, plochy či příkazového řádku. Jde tedy o to, co vidíme na monitoru. [22]

Programovací rozhraní (API = Application Programming Interfaces) je jazyk nebo také zdrojový kód, který slouží jako komunikační prostředník mezi OS a programem, programy či částí programu. [24]

OS je tedy jeden z nejdůležitějších nástrojů v ICT. Mezi nejrozšířenější OS patří Microsoft Windows, Mac OS X a Linux. U mobilních telefonů to je Android a iOS. [22]

Obrázek 3 – Loga nejznámějších OS na počítače [Zdroj: 25]

Pro názornou ukázku popularity výše zmíněných OS jsou zde přiloženy statistiky používání OS v České republice. Nejvíce používaný je Windows a to 85,45%, následuje Mac OS (zde označený OS X) s 9,56% a Linux má 2,04%. Neznámé OS 2,88%, Chrome OS 0,07% a neznámé 0%. Statistiku prováděla internetová stránka gs.statcounter.com. [26]



Obrázek 4 – Statistika používaných OS v ČR [Zdroj: 26]

2 ÚTOKY NA OSOBNÍ POČÍTAČE

Snad každý někdy na něco zapomene. Ať už se jedná o heslo do e-mailu, mobilu nebo v našem případě do počítače. Při takové příležitosti je na místě otázka: „Co teď s tím?“. Odpovědí je několik. Můžete počítač odvést do servisu, kde vám heslo „prolomí“, ale zaplatíte za to. Nebo zavoláte kamaráda, který umí s počítačem a pomůže Vám. Pokud člověka baví technika a rád se něco přiučí, jde to zkusit svépomocí. Jednoduše zajdete na internet, do vyhledávače zadáte „program na vyhledání hesla od počítače“ a okamžitě Vám vyjede několik výsledků. Po pročtení pár návodů a stažení příslušného programu je možné za několik minut heslo vyhledat nebo smazat a je možné se dostat opět do počítače.

Výše popsaná situace je právě důvod, proč jsou takové programy na internetu k dispozici, ale vždy to není jen o „správném“ použití tohoto programu. Při nesprávném používání/zneužívání programu může dojít ke krádežím dat a obohacování útočníků.

Cílem těchto útoků jsou data a informace, které si v počítači uživatel uchovává. Jsou to osobní věci, které mají pro něj cenu. Ne každý člověk je doceňuje. To je důvod útoku na osobní počítače. Útočník proniká do počítače a hledá osobní věci či informace. Při nalezení zásadních dat a informací (rodné číslo, číslo účtu, adresa apod.) se může obohatit nebo oběti způsobit škody a nepříjemnosti. Může se také spoléhat na osobní věci oběti (fotky, videa a dokumenty), se kterými může oběť vydírat.

K útoku na počítač potřebuje útočník nějakou „zbraň“. V ICT se jedná o program či vir, kterým se dostane do počítače, získá potřebná data z něj, nebo ho zablokuje. Z důvodu mnoha způsobů napadení je lepší útoky dělit podle různých kritérií. Pro naše využití je dělení podle způsobu provedení.

2.1 Fyzické

Mnoho programů se dá použít, jen když jste přímo u počítače. Fyzický kontakt je podmínkou, jelikož jde o programy, které jsou umístěny na CD nebo na USB Flash Disku. Úložná zařízení se vkládají do počítače, kde samotný proces zjišťování či mazání hesla může začít. Útočník musí být přímo u počítače, to je nevýhoda, musí jednat rychle. V současnosti to dokáže zřejmě kdokoliv, kdo alespoň trochu umí s počítačem. Programů pro „nabourání“ hesla do počítače je na internetu mnoho a většinou nic nestojí. Dají se rozdělit na dvě skupiny podle toho, na jakém základě fungují.

2.1.1 Linux Live CD

Mnoho z nich funguje na technologii Linux Live CD. Co je Live CD? Je to samostatný disk, kde je plně funkční OS. Tímto diskem může být CD, DVD nebo USB. OS na Live CD funguje odděleně od OS počítače, tudíž se může používat právě k takovým úkonům jako mazání hesla, obnovu souborů a podobně. Tyto programy si jsou velice podobné a mnohokrát používají stejné nástroje. Jen část programu je jinak přepracovaná. [27]

Na tomto principu funguje mnoho programů. Jedním z nich je Trinity Rescue Kit, který funguje na všech známých systémech Windows. Druhý je Offline NT Password & Registry Editor, který je stejný jen s rozdílem menšího využití, protože nemá tolik funkcí.

2.1.2 Rainbow tables

Druhá početná skupina funguje na tzv. „rainbow tables“, česky také „duhové tabulky“. Co to je? Když se využije českého překladu, tak to jsou tabulky s velkými sadami přednastavených hodnot hash pro možná hesla. Každé heslo je totiž převedeno do speciální číselné formy, tedy hashe. Je to „otisk“ hesla a právě rainbow tables ho porovnává a zjišťuje shodu. Samozřejmě čím delší a složitější heslo je, tím déle dešifrování trvá. Vše záleží na různosti použitých znaků (od normálních písmen, přes čísla až po speciální znaky). Takových programů, které používají rainbow tables je celá řada. Jsou dost používané a oblíbené u uživatelů. [28,29]

Hlavními představiteli, kteří používají rainbow tables jsou Ophcrack, John The Ripper a Cain & Abel. Ophcrack je zároveň asi nejvíce používaný a známý program pro zjištění hesla, který funguje pouze ve Windows, ale nefunguje ve Windows 10. John The Ripper musí mít přístup do systému, jinak nezjistí heslo. Funguje ve všech systémech, ale jen v příkazovém řádku. Cain & Abel funguje ve starších OS, takže dnes není používaný, ale je velmi známý.

2.2 Vzdálené

Tento typ útoku je prováděn, jak už název napovídá, dálkově. Vzdálený útok může nejčastěji poškodit či změnit data uživatele napadeného počítače. Některé dálkové útoky se oproti tomu neprovádí přímo na počítač, ale slouží ke zjištění přihlašovacích údajů na internetu (do bankovnictví, e-mailu,…). Zde budou zmíněny pouze ty, které mohou nějak ovlivnit data přímo v počítači. Jsou to sociální inženýrství, malware a hacking.

Sociální inženýrství

Tento pojem má dva významy. První je společenskovědní disciplína. A druhá je ve spojení s ICT. Techniky sociálního inženýrství jsou založeny na chybném rozhodnutí člověka. Člověk je více chybující článek než počítač. Útočník může ze své oběti vymámit data a údaje, které zneužije k nějaké činnosti, která oběť poškodí. Důvěřivá oběť poté může skončit s poškozenými daty v počítači, prázdným bankovním účtem či jinou škodou. [30]

Malware

Pravý význam tohoto slova je škodlivý software. Do kategorie malware patří veškerý škodlivý kód. Jsou to kódy jako ransomware, viry, červy,…. Je velmi nebezpečný a v případě, že napadne počítač, je jeho úkolem získávat a poškozovat data a způsobit co nejvíce škody v napadeném počítači. **Ransomware** šifruje data napadeného počítače a požaduje výkupné. **Spyware** zase získává a odesílá data z počítače, kde je nainstalován. A **adware** způsobuje zobrazování reklam na internetu v jakékoliv podobě. Různé **viry** mají například za úkol poškodit co nejvíc dat. [31]

Spam

Neboli spamming je nevyžádané rozesílání elektronické pošty. Nejvíce se to týká e-mailů, ale může také napadnout různé blogy, fóra a messengery. Rozesílání není cílené, ale masové. Často obsahuje malware, který od napadeného uživatele získává data a odesílá je útočníkovi. [31]

Hoax

Hoax je falešná nebo poplašná zpráva. Klade důraz na přeposlání zprávy dalším osobám. Účelem bývá zastrašení osob, šíření zprávy, poškození osoby nebo organizace falešnými informacemi a podobně. [31]

Phishing

Technika phishingu se snaží oklamat osoby a získat od nich data a přihlašovací údaje od internetového bankovnictví, e-mailu a dalších internetových účtů. Při phishingu se využívá napodobenina oficiální internetové stránky. K rozesílání odkazu se používá e-mail nebo jiná sociální síť. Cílem je „donutit“ osoby k zadání přihlašovacích údajů, které se tak dostanou do rukou útočníka. Internetové stránky jsou nerozeznatelné od skutečných. Poznat, že jde o podvrh lze jen z webové adresy, která není stejná jako u oficiálních stránek. [31]

Pharming

Pharming je formou phishingu, ale je sofistikovanější a mnohokrát nebezpečnější. Útočí se na DNS servery, kde se přepíše IP adresa. Výsledek je takový, že podvodná stránka je nerozeznatelná od skutečné. IP adresa je zaměněna za útočníkovu. Funguje to tak, že osoba zadá skutečnou webovou adresu, ale načte se podvodná stránka. Takže na webové adrese nelze poznat, že se jedná o podvrh. Útočník může využít i jinou formu a to u OS Windows. Windows obsahuje soubor „Hosts“. Ten obsahuje IP adresy různých navštívených internetových stránek. Útočník tedy přepíše IP adresu přímo v souboru. Pro útočníka je snazší druhá forma, protože zabezpečení DNS serverů je velice dobré. [31]

Hacking

Při hackingu útočník využívá slabiny systému a překonává je. Ať už za účelem obohacení, poškozování nebo zábavy. Hacking může být bez použití škodlivých programů, ale také je použít může. [32]

DoS/DDoS

DoS je zkratka z anglického sousloví „Denial of Service“. Cílem útoku DoS je vyřadit určitou službu z provozu. Dosáhne toho tím, že službu přehltí poslanými požadavky nebo využije jinou chybu třeba k restartu či vypnutí služby. DDoS (anglicky Distributed Denial of Service) je formou útoku DoS. Ale oproti útoku DoS využívá celou síť robotů, kteří rozesílají příkazy za účelem přehlcení služby. Síť robotů se nazývá botnet. Mnoho tvůrců botnetů je pronajímá. [33,34]

2.3 Kombinované

Tento způsob útoku kombinuje dálkově použitý program, který zjistí heslo a fyzický přístup k počítači. Tímto způsobem se dá použít jakýkoliv keylogger, pokud na něj uživatel nepřijde. Útočník musí mít svou oběť vybranou, což je pro něj výhoda. Nevýhodou je, že se útočník musí dostat přímo k počítači, aby z něj mohl ukrást data.

2.3.1 Keylogging

Je užití programu, který dokáže monitorovat a zaznamenávat znaky napsané klávesnicí. Umí i zachycovat snímky ze sledovaného počítače, rozpoznat zda byl k počítači připojen nějaký externí nosič dat (USB Flash Disk), vložen do něj CD či DVD a pokud má počítač

mikrofon či webkameru, dokáže využít i tyto věci k pořízení záznamu. Nejdříve se samozřejmě musí nainstalovat do cílového počítače. A to odesláním e-mailu, kde je příloha se skrytým programem. Uživatel si ji musí nejdříve stáhnout a tím nainstalovat software. Další způsoby jsou, že keylogger může být přibalen k nějakému užitečnému softwaru, zaměněn za užitečný program a podobně. Spousta keyloggerů je určena spíše k instalaci přímo na cílovém počítači, ale pokud je útočník zběhlý, zvládne to i vzdáleně. [35,36]

Neexistují jen softwarové keyloggery, ale také hardwarové. Ty jsou ale finančně náročné oproti softwarovým, které se dají sehnat zadarmo. Některé jsou ve formě propojky u klávesnice, přímo součástí klávesnice nebo propojka z monitoru. Hardwarové keyloggery útočníci nevyužívají z důvodu finanční a vizuální stránky. [36]

Antivirus může odhalit softwarový keylogger, ale měl by mít k tomu příslušné nástroje. Obyčejný antivirus by ho nedokázal odhalit. Zato hardwarový keylogger antivirus neodhalí vůbec. Dřív ho může odhalit uživatel, který ho odhalí. Mohou být i určité indicie přítomnosti keyloggeru v počítači, a to: pomalejší načítání webových stránek, občasné zasekávání kurzoru myši, zpožděné zobrazování písmen při psaní. Odstranit jej lze buď ručně, což je zdlouhavá forma (odstraňování všech podezřelých souborů) nebo za pomoci antiviru. [36]

3 CÍLE A ZVOLENÉ METODY ZPRACOVÁNÍ

Cílem teoretické části bylo shromáždit co nejvíc materiálů, které souvisejí s danou problematikou. Na základě použitých materiálů bylo dalším cílem seznámit se se současnými útoky na osobní počítače k narušení bezpečnosti informací.

V praktické části byla uskutečněna analýza náročnosti provedení útoku na osobní počítač. K analýze bylo vybráno několik druhů útoků. Analýza probíhala v určeném prostředí. Tímto prostředím byl v našem případě virtuální počítač. Následná instalace vybraných operačních systémů a realizace útoků na ně. Vybrány byly nejnovější systémy, které mají být připraveny na bezpečnostní ohrožení. Po analýze vybraných útoků, které jsou popsány, byla navrhnuta opatření, která by měla zabezpečit data a informace v počítači.

Metody použité při zpracování práce

V teoretické části byla použita metoda indukce, kdy po nastudování materiálů byla vyvozena podstata řešeného pojmu či názvosloví.

Praktická část bakalářské práce se věnovala provádění vybraných útoků na vybrané operační systémy. Při této činnosti byla použita metoda analýzy. Pro navržení opatření se využila komparace. Na základě poznatků z analýzy se volila opatření proti útokům, které jsou bezpečnostní hrozbou pro uživatele počítačů.

II. PRAKTICKÁ ČÁST

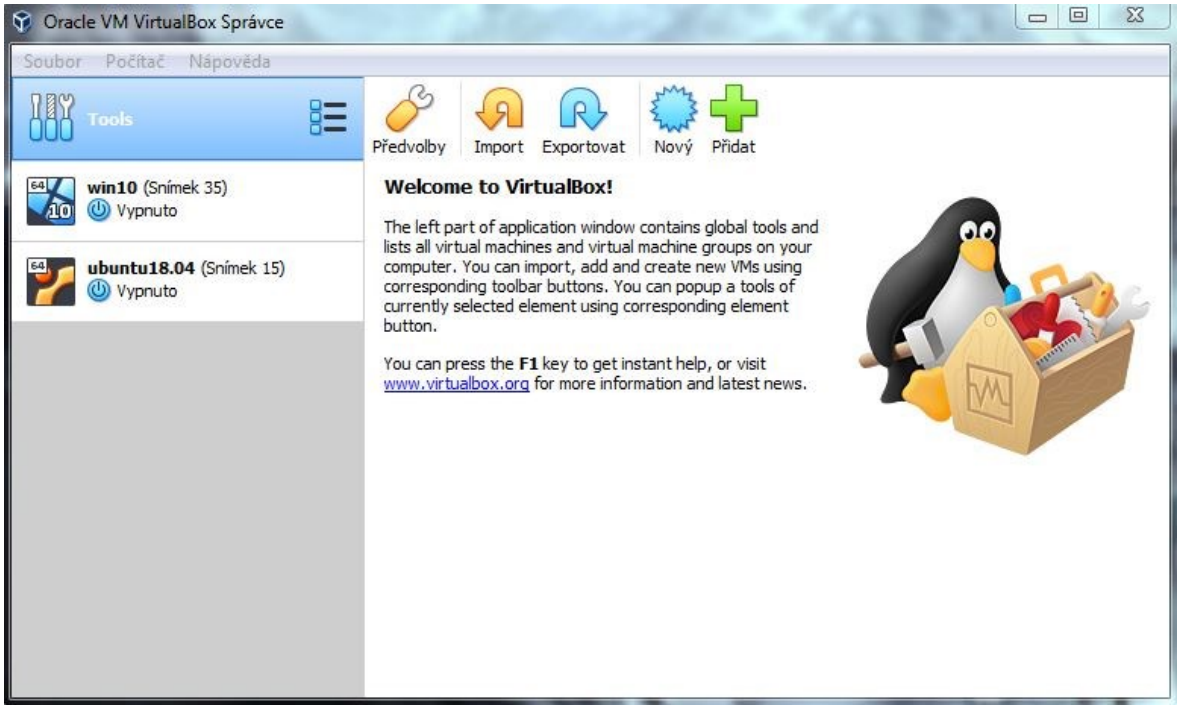
4 PŘÍPRAVA TESTOVACÍHO PROSTŘEDÍ

Důležité bylo vybrat a připravit testovací prostředí. Testovací prostředí je stejně důležité jako samotná analýza, která dále probíhala. Byl vybrán virtuální počítač, který je vhodný pro instalaci několika OS.

Virtuální počítač je program, který umožňuje uživateli na jeho počítači nainstalovat jakýkoliv jiný OS. Člověk může mít na jednom PC mít tolik OS, kolik chce nebo kolik mu dovolí velikost paměti. Bývá označován jako „image“ a funguje jako skutečný počítač. Nejde jen o jakýsi simulátor, ale opravdový počítač se vším, co má kterýkoliv jiný počítač a umožňuje mu na něm pracovat. Tento virtuální počítač je izolován od zbytku OS a díky tomu je velice vhodný jako prostředí pro různé testování. Testování může probíhat u ještě nevyzkoušených OS, antivirových programů nebo čehokoliv jiného, co by nebylo zrovna bezpečné testovat na normálním počítači. Jde to za pomocí harddisku, ze kterého by nemělo nic proniknout do hostitelského systému. Výhoda je v tom, že uživatel pro vyzkoušení jiného OS, nemusí kupovat nový PC a vše může udělat na jednom, což mu ušetří nemalou finanční částku za nákup nového počítače. [37]

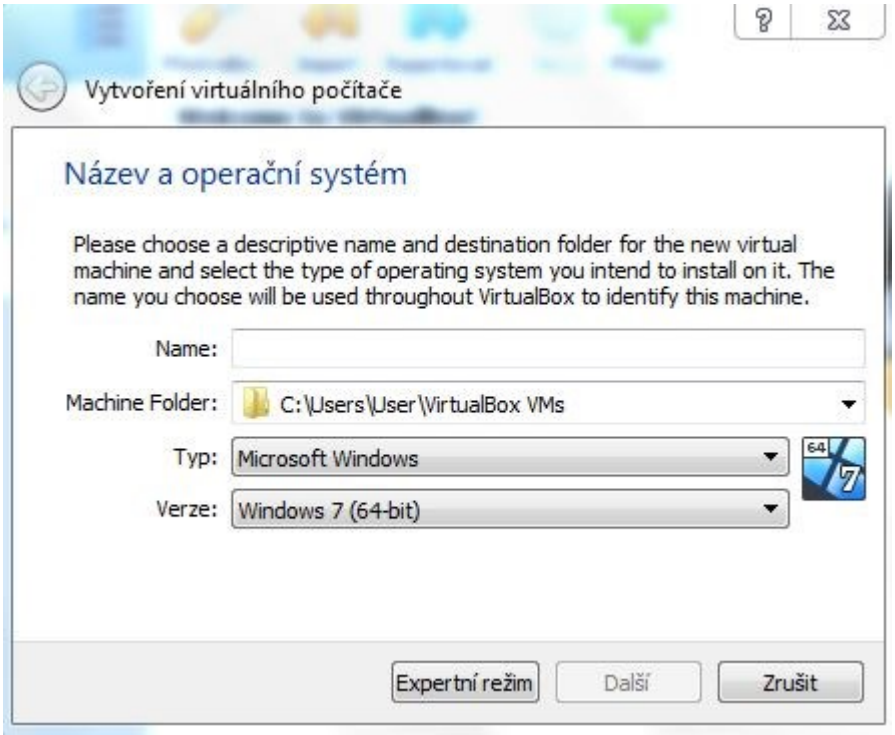
Pro účel testování byl tedy vybrán program Oracle VM VirtualBox. Je přístupný na internetu zcela zdarma, což je velká výhoda, kde si ho může vyzkoušet každý. Další výhodou je rychlá a snadná instalace. V následující části je popsán postup při instalaci spolu s obrázky.

Nejprve byl tedy nainstalován samotný program VirtualBox, následně po jeho spuštění se začal vytvářet nový virtuální počítač, což můžete vidět na obrázku 5.



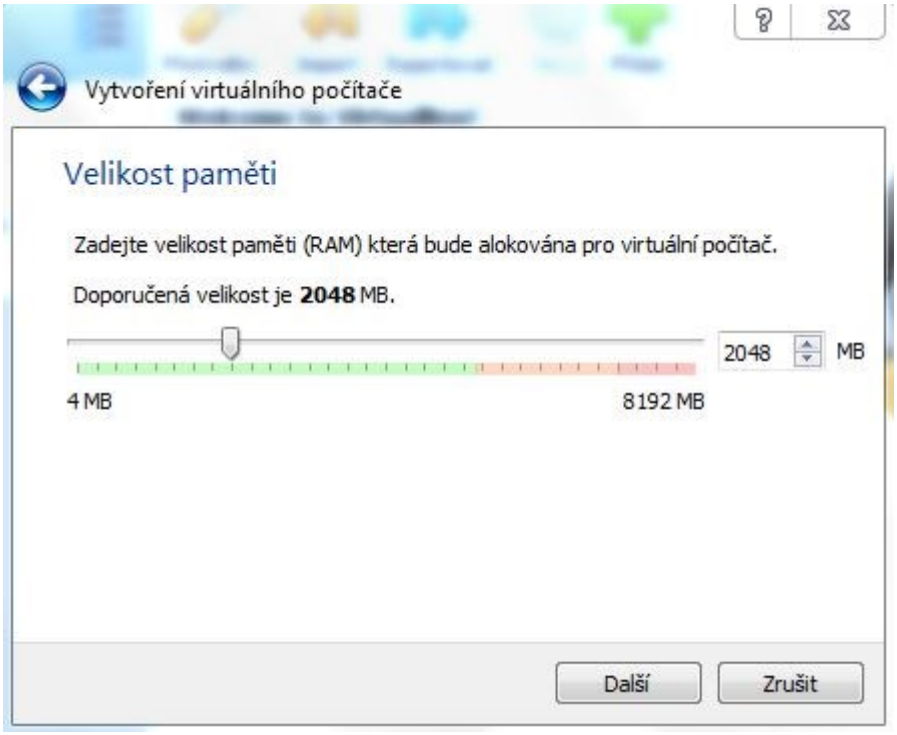
Obrázek 5 – Spuštěný program Oracle VM VirtualBox [Zdroj: vlastní]

Název byl zvolen podle dále instalovaného OS. Dále byl vybrán přesný typ systému, který byl po vytvoření virtuálního počítače instalován. Na obrázku níže můžeme vidět okno, kde se uvádí název, umístění virtuálního počítače a přesný typ systému.



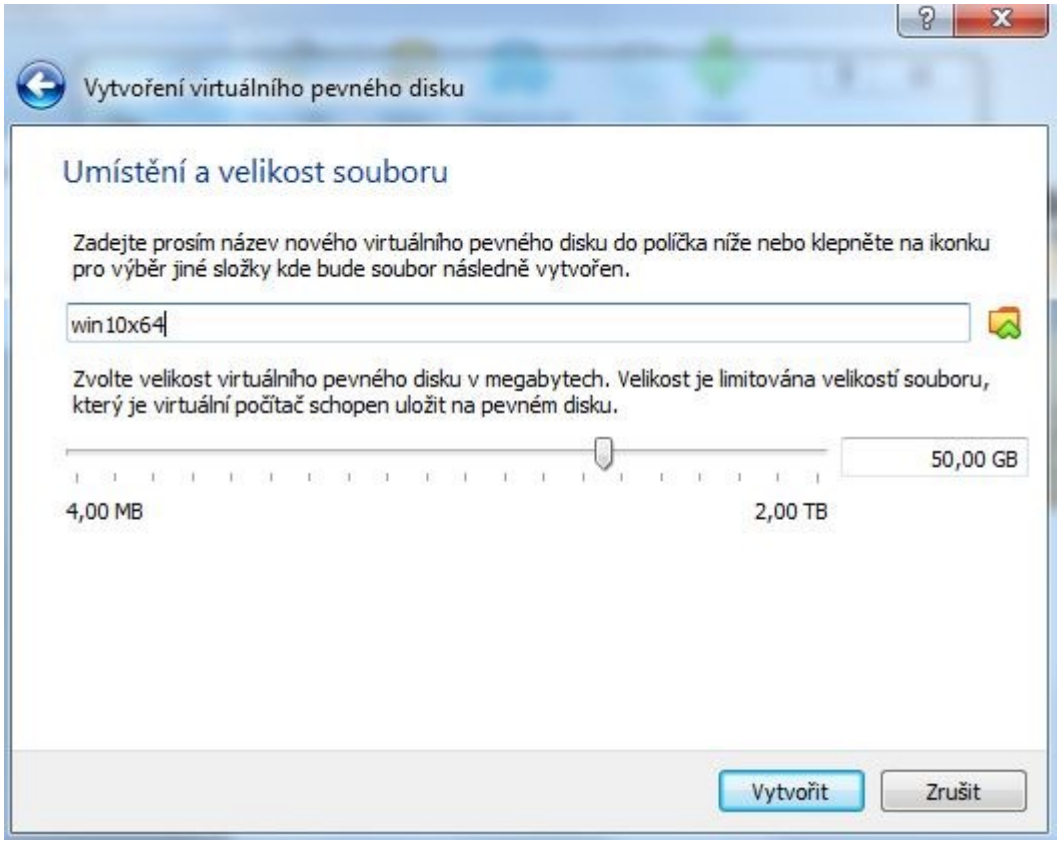
Obrázek 6 – Nevyplněné okno se základními údaji [Zdroj: vlastní]

Paměť RAM byla ponechána podle doporučené hodnoty (u Windows 10 na 2048 MB, u Ubuntu na 1024 MB), jak je vidět na obrázku 7. Byla zvolena možnost „Vytvořit nyní virtuální pevný disk“ a dále typ souboru a to VirtualBox Disk Image (VDI). Následně bylo vybráno, že virtuální disk bude dynamicky alokovaný, což znamená, že disk bude zaplňovat tolik místa, jak velký bude.



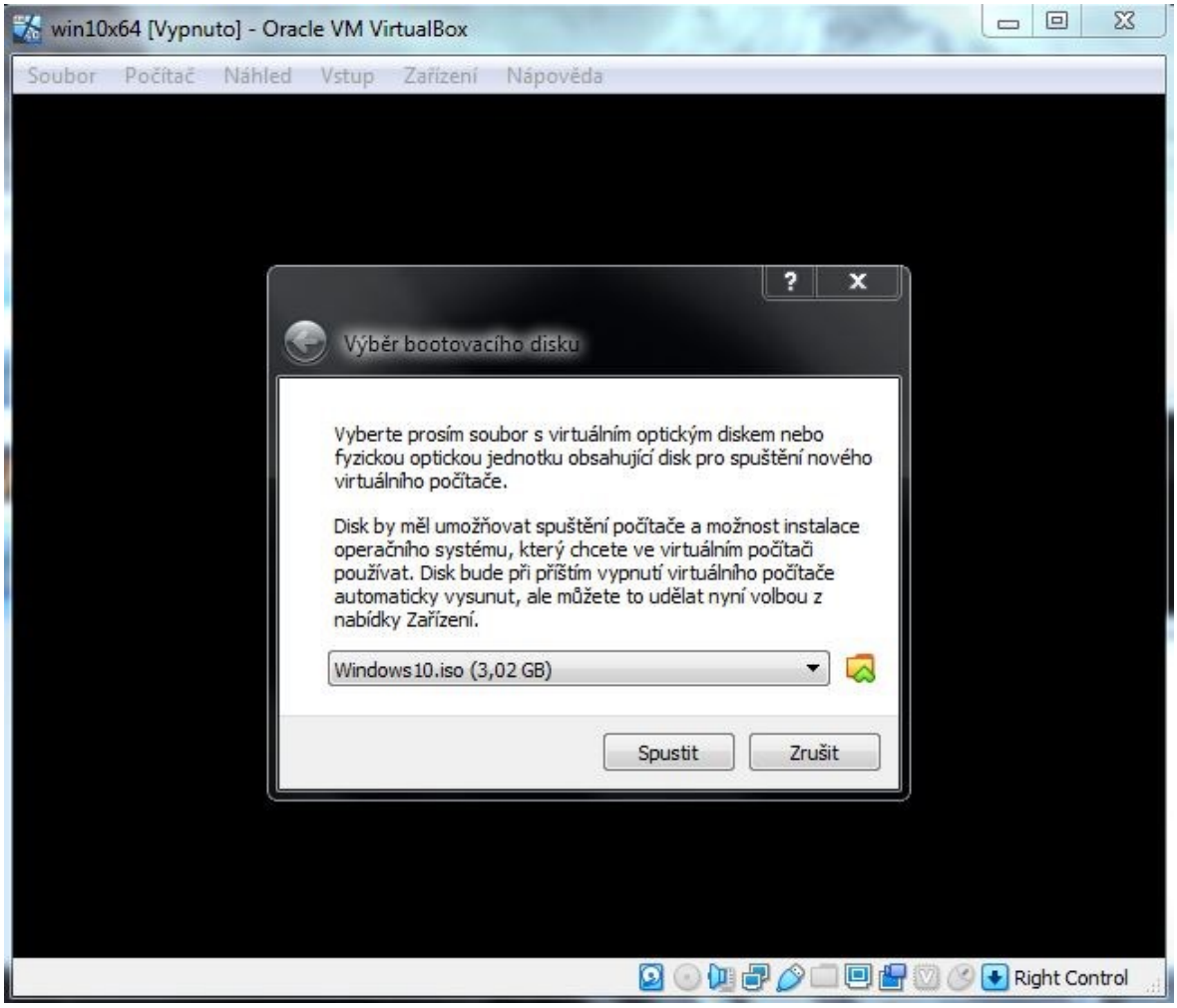
Obrázek 7 – Nastavení paměti RAM [Zdroj: vlastní]

A jako poslední krok byla volba velikosti virtuálního disku, kde bylo ponecháno podle doporučení (u Windows 10 na 50 GB, u Ubuntu na 10 GB). Tento krok je vidět na obrázku níže.



Obrázek 8 – Umístění a velikost virtuálního pevného disku [Zdroj: vlastní]

Po spuštění virtuálního počítače stačilo nainstalovat odpovídající OS. Vybrána byla složka, kde byl umístěn instalační soubor systému. Pokud by byl systém na CD či DVD vybrala by se mechanika. Po instalaci, která byla jednoduchá, ale poněkud delší bylo vše připraveno na analýzu.



Obrázek 9 – Výběr bootovacího disku pro instalaci OS [Zdroj: vlastní]

4.1 OS Windows 10

Prvním vybraným OS byl dnes dobře známý Windows 10. Tento systém je poslední verze od firmy Microsoft a byl vydán v roce 2015. V dnešní době je to hlavní podporovaná verze OS od Microsoftu. Od roku 2020 už nebude podporovaná verze Windows 7. Windows 10 je pouze upravená předchozí verze, čili Windows 8.1. Microsoft jen vylepšuje nynější Windows 10 a už by neměl plánovat tvořit jinou verzi. Je to univerzální OS, který používají od počítačů, přes mobily až po Xbox. [38]

Obrázek 10 – Windows 10 logo [Zdroj: 39]

4.2 OS Ubuntu

Druhý OS je Ubuntu, který běží na linuxovém jádře. Jde tedy o jednu z několika verzí Linuxu. Tento systém stejně jako všechny jiné linuxové je zdarma. První verze byla vydána již v roce 2004, ale instalována byla verze 18.4, tedy z roku 2018. Ubuntu funguje nejen na počítačích, ale také na smartphonech, tabletech, robotech či dronech. Tento systém používají i některé celosvětově známé školy jako Harvard University a Oxford University. Na vývoji se podílí open source experti z celého světa a finance pochází z komerční sféry. Jde tedy o jeden z velice oblíbených OS. [40,41]

Obrázek 11 – Ubuntu logo [Zdroj: 42]

4.3 OS Kali Linux

Kali je open source projekt, který je financován pod záštitou firmy Offensive Security. Open source znamená, že zdrojový kód je poskytnut dalším lidem a to zejména vývojářům k prostudování. Systém Kali vychází z OS Debian, který je jeden je známějších verzí od Linuxu. Dá se říct, že programátoři vzali Debian, podrobili ho testování a začali ho přepracovávat do podoby, jakou má dnes systém Kali. Projekt začal v roce 2012 a první verze vznikla v březnu 2013. Systém je určen hlavně k provádění různých bezpečnostních analýz a penetrací. Je k dispozici mnoho nástrojů právě k jejich zkoušení. [43,44]

Obrázek 12 – Kali logo [Zdroj: 45]

5 PROLOMENÍ ZABEZPEČENÍ HESLEM

V této kapitole byly pro účel analýzy zabezpečení vybraných OS použity nejen programy zmíněné v teoretické části, ale také jiné metody, které fungují pro vniknutí do systému počítače. Většinou jde o jednoduché způsoby, při kterých není třeba nic kupovat, a jsou rychlé.

5.1 OS Windows 10

Mnoho programů na vymazání hesla je vytvořeno hlavně pro systém Windows. Nejen pro nejnovější verzi, ale také pro verze předešlé, jako je Windows 8, 7 a XP. Analyzovány byly dva programy, ale jelikož jsou v podstatě stejné, tak je zde uveden pouze jeden, který je všestrannější a jednodušší. Druhý analyzovaný program se jmenuje Offline NT Password & Registry Editor.

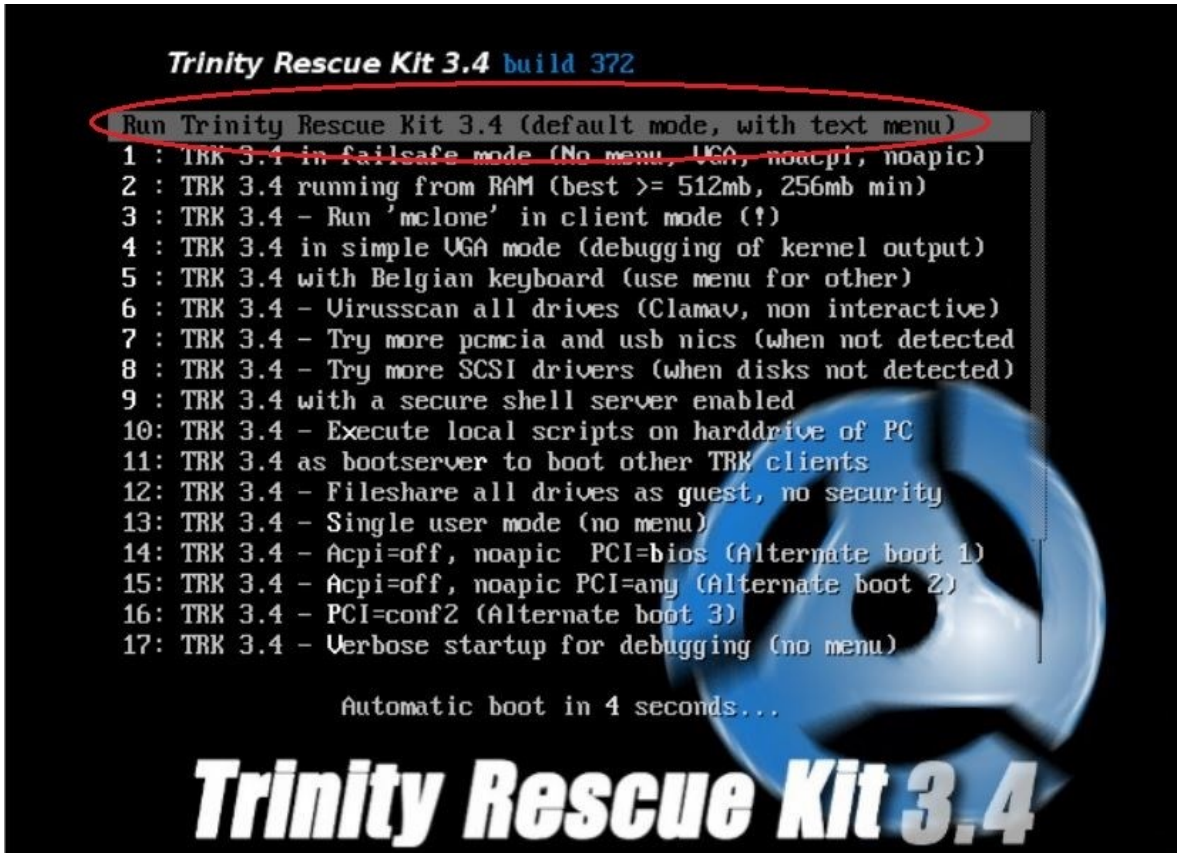
Při prvním útoku byl využit Trinity Rescue Kit. Tento program funguje na Linuxovém systému. Lze spustit z CD nebo USB Flash Disku a je okamžitě připraven k použití. Nedokáže zjistit heslo uživatele či administrátora, ale umí ho smazat.

Druhý způsob proniknutí do počítače je za pomoci Live CD/USB. V případě CD se na něj vypálí vybraný OS. U USB se za pomoci příslušného programu vytvoří bootovací USB. Funguje to tak, že program naformátuje USB a vytvoří na něm „obraz“ OS, takže se USB chová jako CD. OS se spustí a zobrazí HDD, které jsou v počítači. Takže lze získat či jinak manipulovat se soubory.

5.1.1 Trinity Rescue Kit

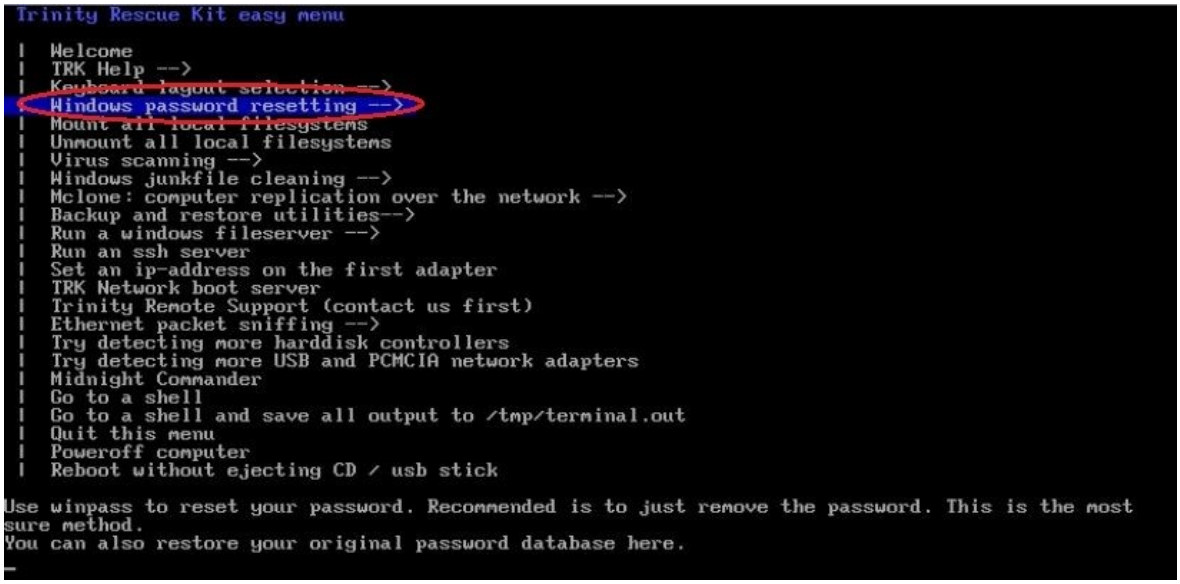
Zkráceně TRK je bezplatný program na bázi Linuxu. Je určen k operacím obnovy a pro opravy na OS Windows. Nejnovější verze 3.4 je jednodušší k použití díky rolovacímu menu, které se dá snadno ovládat klávesnicí jednoduchým anglickým frázím a celkové přehlednosti. S tímto nástrojem lze kromě resetování hesla také čistit disk nebo provádět antivirovou kontrolu. Je to víceúčelový nástroj na rozdíl od jiných programů na zjištění hesla. [46]

Nyní přejdeme k průběhu testu. Nejprve je třeba si program stáhnout z internetu. Dostupný je na oficiálních stránkách (http://trinityhome.org/). Po stažení byl vytvořen za pomoci programu UNetbootin bootovatelný USB Flash Disk. Program lze také vypálit na CD. Následně byl USB Flash Disk zaveden do počítače, ten se zapnul, ihned poté se stiskem DEL (popřípadě tlačítka F1-F12) přešlo do BIOSu, kde se nastavilo bootování z USB. Objevilo se TRK menu, kde se zvolila první možnost, což je vidět na obrázku 13.



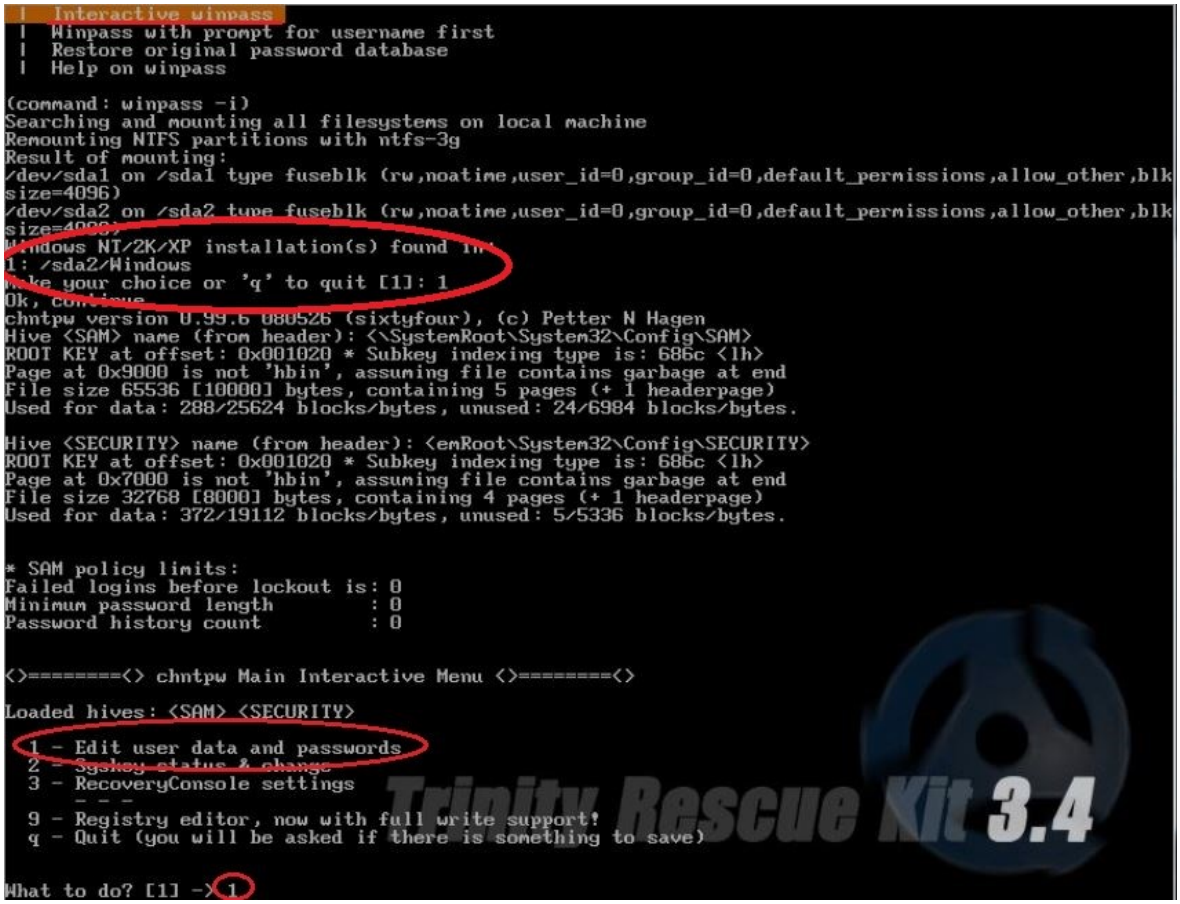
Obrázek 13 – Úvodní obrazovka TRK [Zdroj: vlastní]

Po načítání se objevilo hlavní menu, kde byl výběr z možných nástrojů. Zde se pokračovalo volbou možnosti „Windows password resetting“ (česky resetování hesla Windows), jak je vidět na obrázku 14.



Obrázek 14 – Hlavní menu TRK [Zdroj: vlastní]

Dál se pokračovalo volbou „Interactive winpass“, která umožňuje spravovat hesla. Následně byl vybrán oddíl, kde se nachází systém. Další byla vybrána možnost 1 a potvrzeno klávesou „Enter“. Postup je vyznačen na obrázku 15.

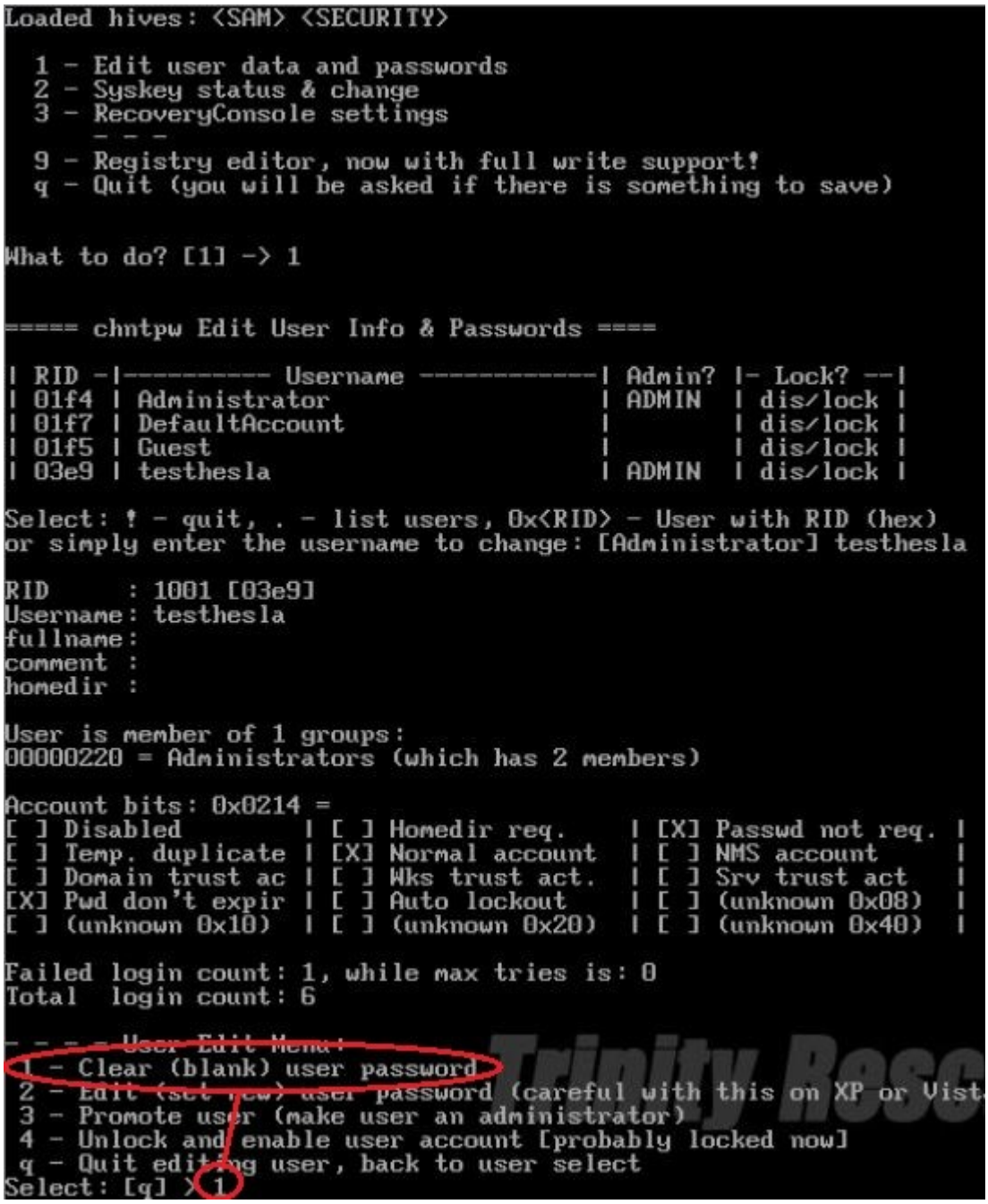


Obrázek 15 – Kroky vedoucí ke správě hesel [Zdroj: vlastní]

Nyní již výběr uživatele, u kterého chceme vymazat heslo. Jméno vybraného uživatele bylo napsáno do požadovaného pole a potvrdili jsme výběr. Na obrázku 16 můžete vidět výběr uživatele.

Obrázek 16 – Výběr uživatele [Zdroj: vlastní]

Předposledním krokem byla volba vymazat heslo, což byla volba číslo 1, jak je vidět na obrázku 17.



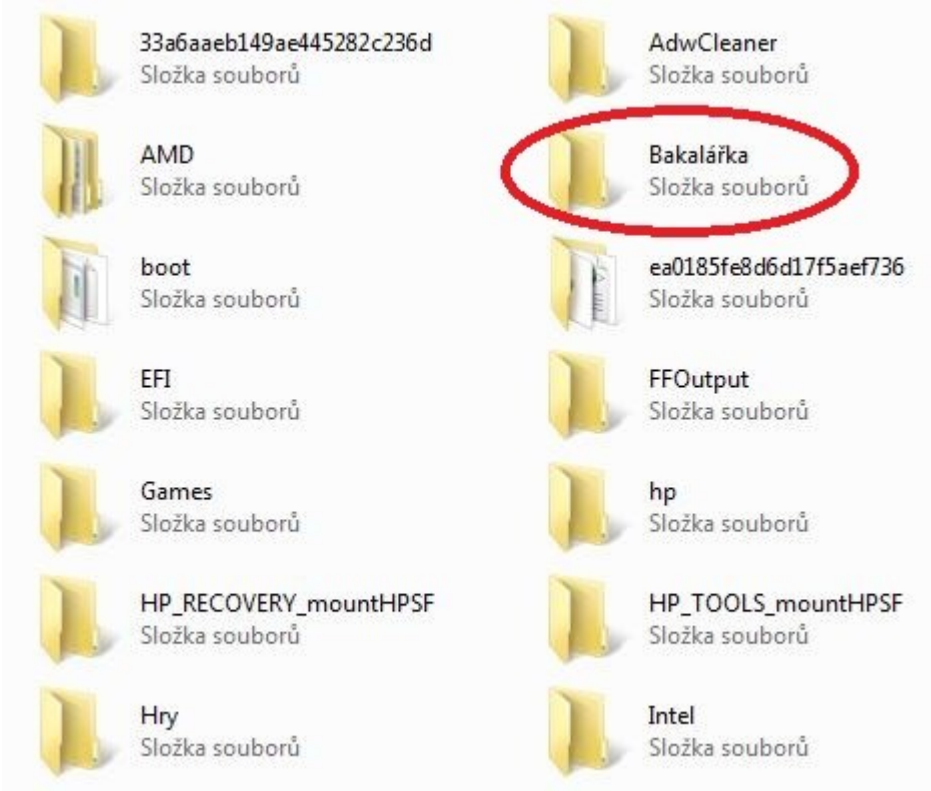
Obrázek 17 – Výběr možnosti smazání hesla [Zdroj: vlastní]

Nakonec, když bylo vše hotovo, tak stačilo napsat „quit“ (česky opustit) a počítač restartovat, popřípadě zvolit bootování z pevného disku (načte se systém Windows) a heslo je odstraněno. Je to jednoduchý způsob, jak přechytračit počítač asi za pět minut, podle toho, jak je uživatel zběhlý v tomto programu.

Obrázek 18 – Kroky pro opuštění programu [Zdroj: vlastní]

5.1.2 Použití Live CD

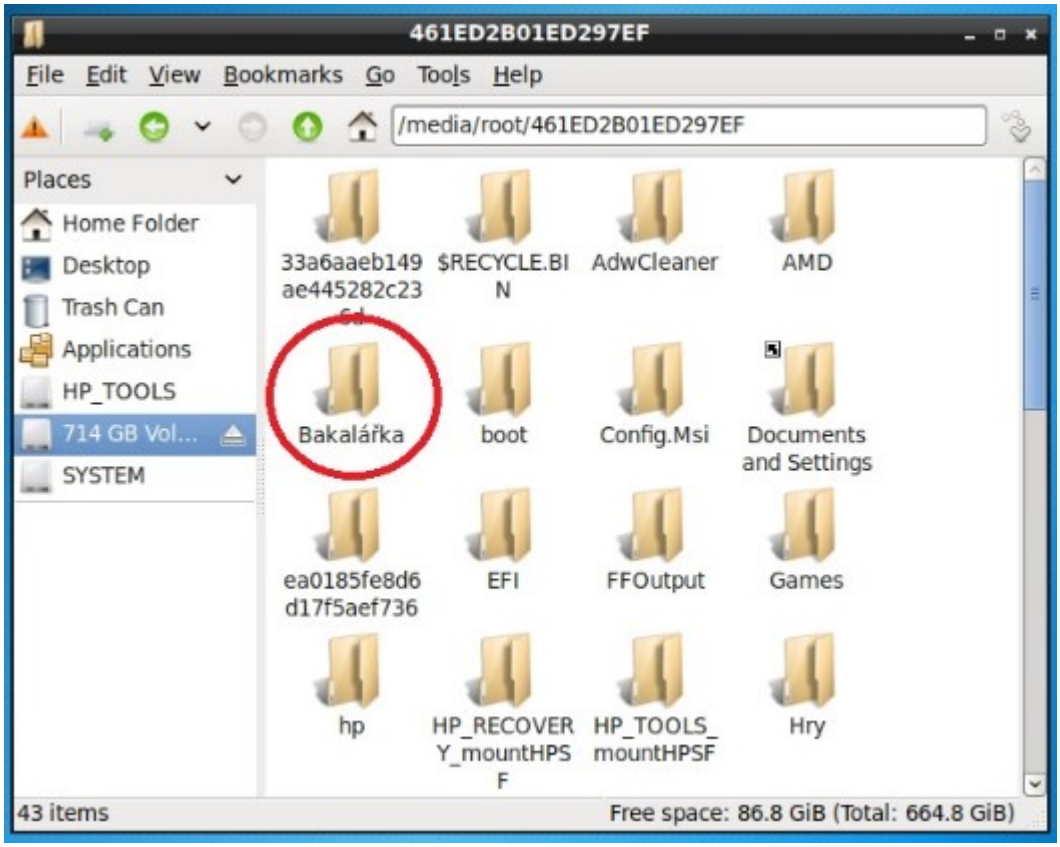
V tomto případě spíše Live USB, jelikož byl OS vložen na USB Flash Disk. Jedná se o jednoduchý útok na obsah počítače, který je chráněn heslem. Nejprve se musí vytvořit Live systém, který se buď vypálí na CD, nebo se pomocí programu vloží na USB Flash Disk. Zde byl použit program Rufus, který dokáže vytvářet bootovací USB. Program je bezplatně ke stažení na internetu (https://rufus.ie/). Byl vybrán systém Kali Linux. USB Flash Disk byl vložen do počítače a v BIOSu se nastavilo bootování z USB. Následně se načetlo menu, kde se zvolila možnost „Live“. Ještě bylo třeba se přihlásit. Na oficiálních stránkách Kali Linux byly nalezeny „výrobní“ přihlašovací údaje (jméno: root a heslo: toor). Poté se systém načetl a přístup k datům z počítače byl přístupný. Na přiložených obrázcích je vidět složka v počítači z pohledu Kali a Windows. Tento útok byl jeden z nejjednodušších a nezanechává po sobě stopy, protože nijak nemanipuluje s heslem uživatele.



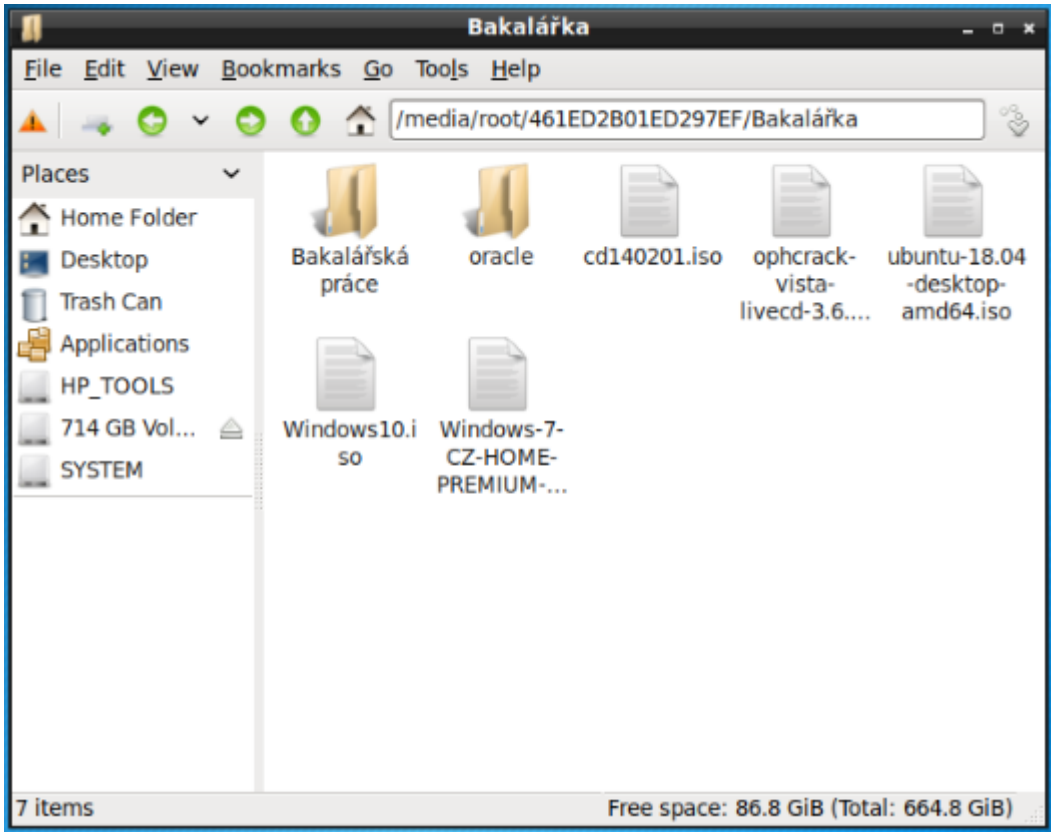
Obrázek 19 – Složka ve Windows [Zdroj: vlastní]

Bakalářská práce	7.4.2019 13:11	Složka souborů	
oracle	7.4.2019 10:18	Složka souborů	
cd140201	1.2.2014 17:35	Soubor ISO	17 522 kB
ophcrack-vista-livecd-3.6.0	19.4.2019 10:11	Soubor ISO	664 576 kB
ubuntu-18.04-desktop-amd64	7.4.2019 19:37	Soubor ISO	1 876 800 kB
Windows-7-CZ-HOME-PREMIUM-PROF...	6.4.2019 22:03	Soubor ISO	3 887 910 kB
Windows10	7.4.2019 19:31	Soubor ISO	3 168 640 kB

Obrázek 20 – Obsah složky ve Windows [Zdroj: vlastní]



Obrázek 21 – Složka v Kali Linux [Zdroj: vlastní]



Obrázek 22 – Obsah složky v Kali Linux [Zdroj: vlastní]

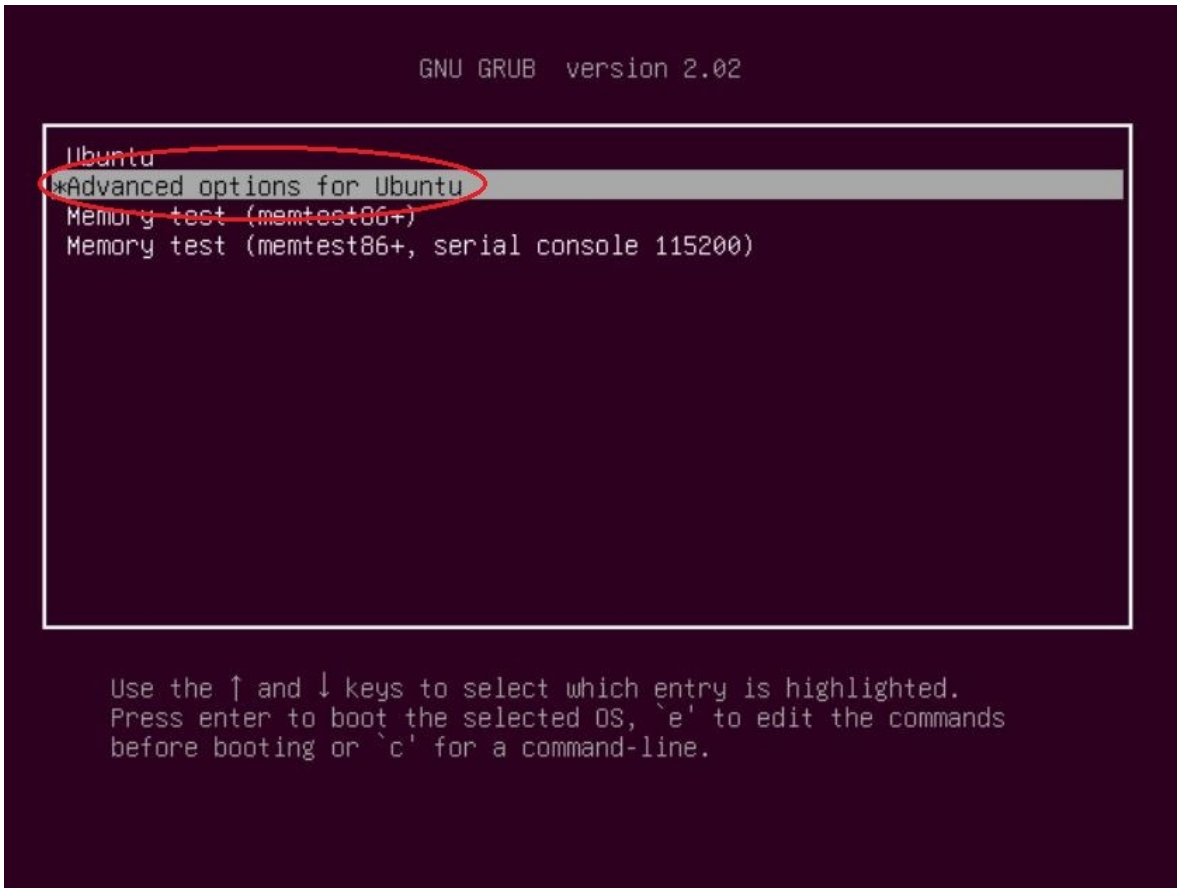
5.2 OS Ubuntu

Ubuntu je jeden ze známějších Linuxových OS, které jsou k dispozici. Pro uživatele počítačů má hned několik výhod, kterými jsou bezplatnost, každých šest měsíců nová verze, podpora většiny aplikací, které má i Windows a možnost používání v mobilu, tabletu a podobně. Zabezpečení není dostatečné. Následně je popsán samotný průběh analýzy.

U systému Ubuntu byl použit postup bez jakéhokoliv programu. Stačilo se dostat do „záchranného módu“, do kterého má běžně přístup kdokoliv. Poté za pomoci několika příkazů bylo možné změnit heslo uživatele.

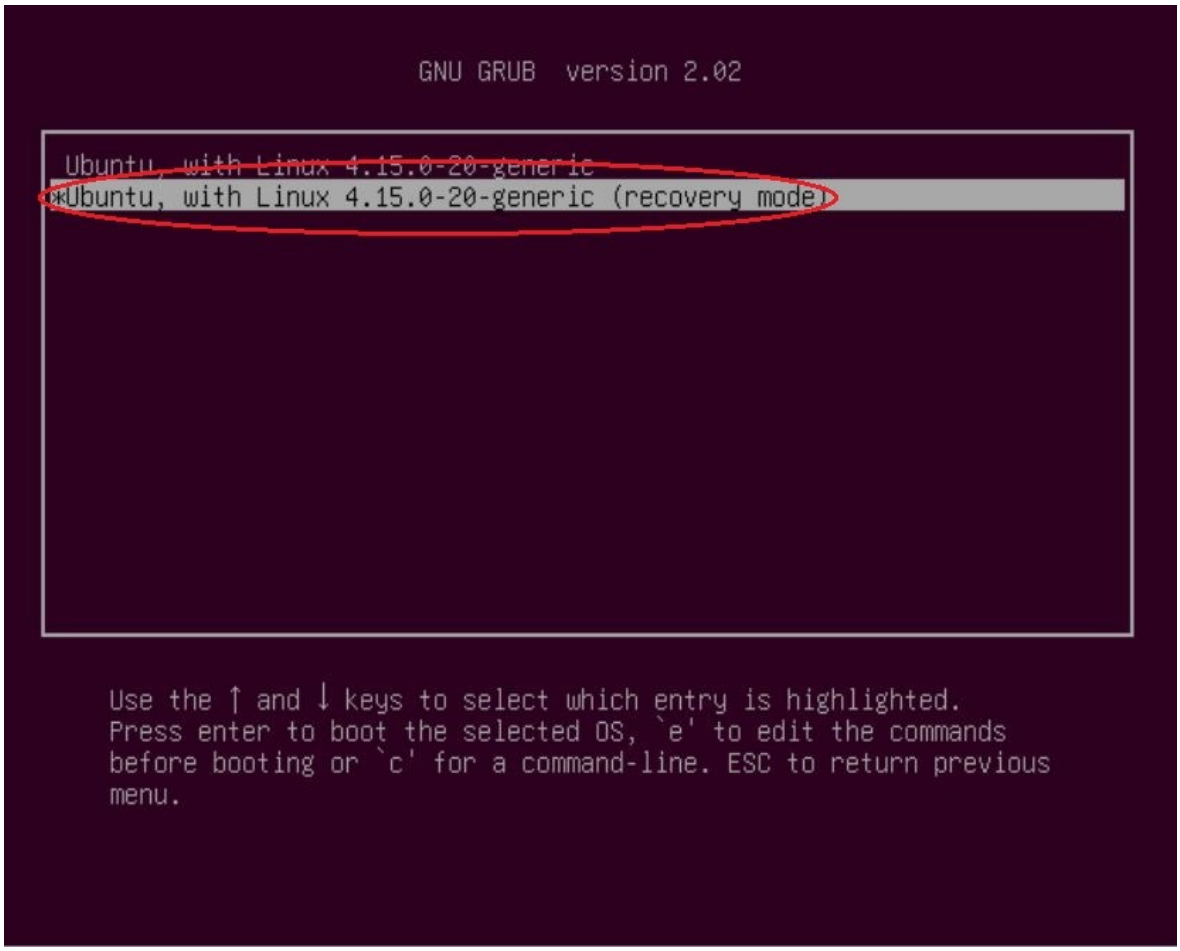
5.2.1 Změna hesla

U této analýzy nebyl použit žádný pomocný program jako u předchozích. Zde byl využit pouze návod z internetových stránek (https://www.psychocats.net/ubuntu/resetpassword), který byl vyzkoušen, zda funguje. Analýza začala spuštěním počítače, následným stiskem klávesy „Shift“ – spuštěním GNU GRUB menu. Na obrázku 23 se znázorněn postup.



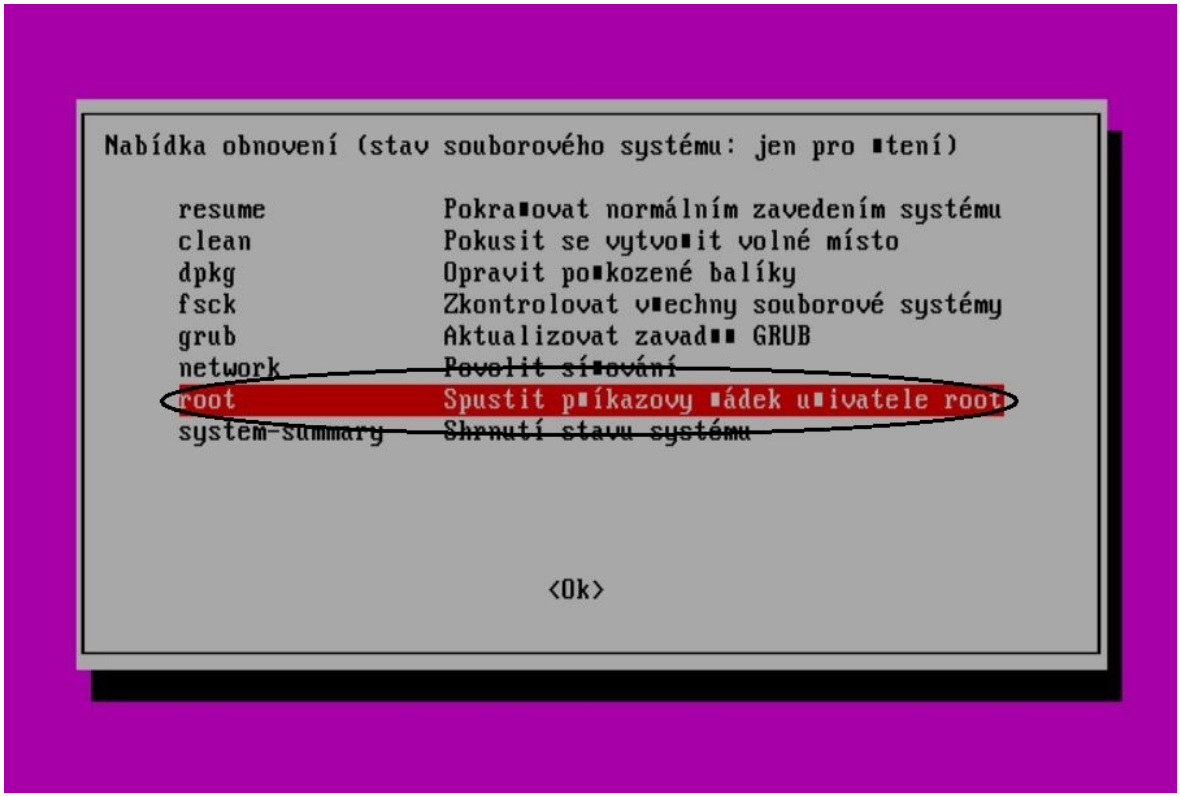
Obrázek 23 – Zavaděč GNU GRUB [Zdroj: vlastní]

Dále byl vybrán „recovery mode“, kde se odehrává vše ostatní, od zvolení uživatele až po změnu hesla.



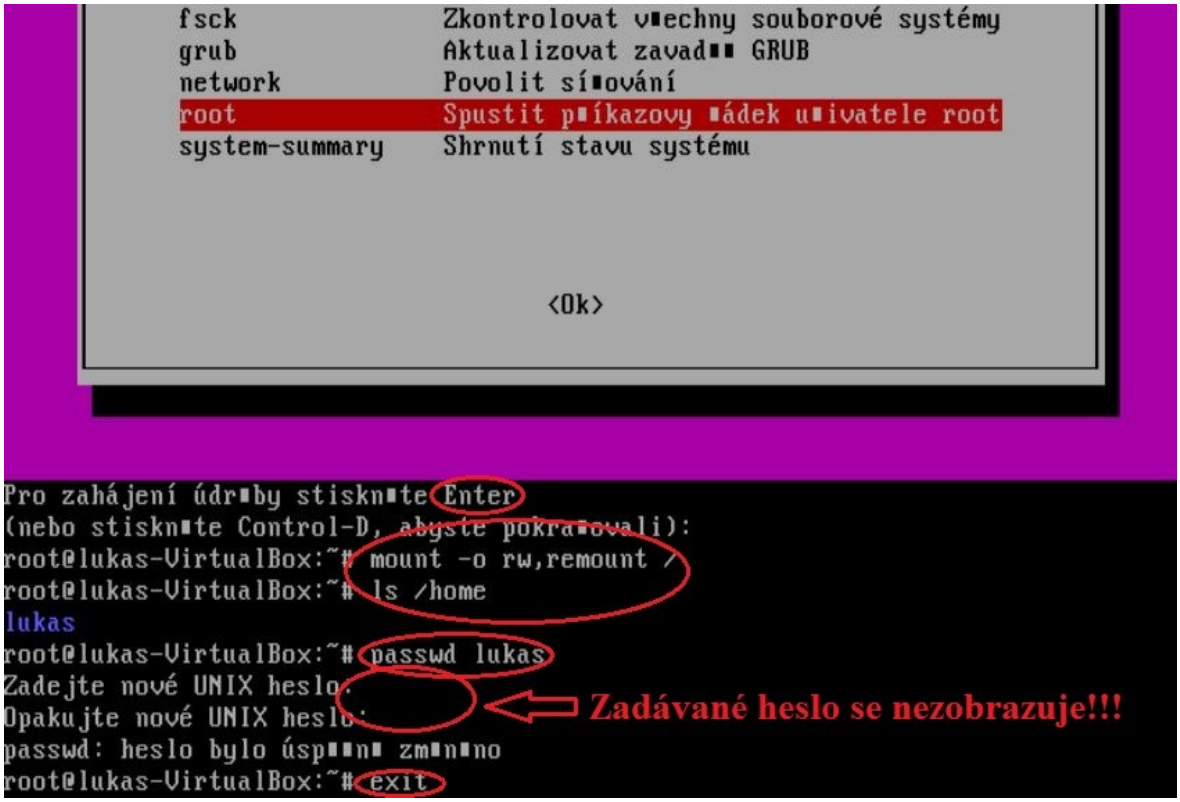
Obrázek 24 – Výběr tzv. záchranného módu [Zdroj: vlastní]

Nyní je již na obrázku 25 vidět „recovery mode“ a vybraná možnost „root“. Česky nebyla písmena s diakritikou zobrazena, ale slova se dala přečíst, jak je vidět na obrázku.



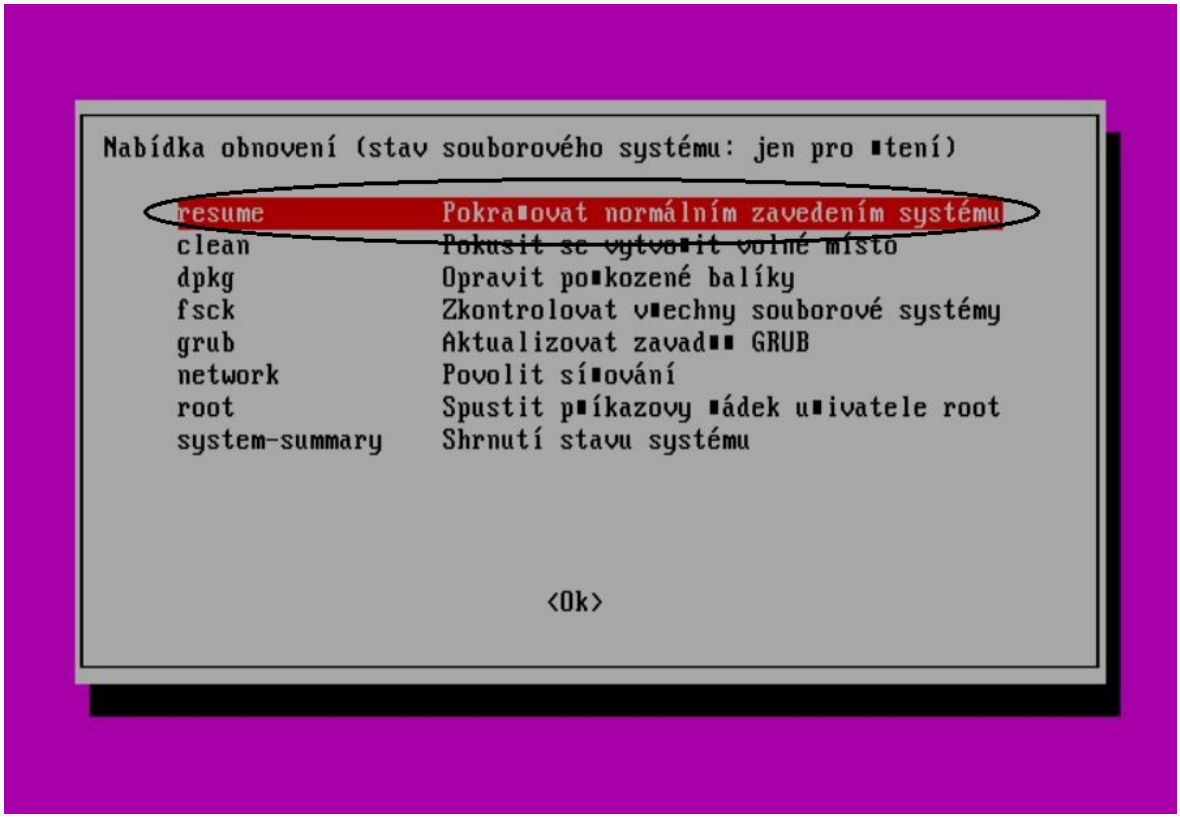
Obrázek 25 – „Záchranný mód“ s výběrem příkazového řádku [Zdroj: vlastní]

To hlavní probíhalo v černém poli, kde se nejdříve podle pokynu stiskl „Enter“. Poté se napsal příkaz „mount –o rw,remount /“ a potvrdil. Další příkaz „ls /home“ a opět potvrdit. Následně se objevil modře napsaný uživatel počítače. Příkazem „passwd jménouživatele“ a potvrzením se objevila možnost zadat nové heslo. Zadávané heslo se nezobrazuje, ale o nic nejde. Heslo opakujeme a po potvrzení je oznámen úspěch. Ukončuje to příkazem „exit“.



Obrázek 26 – Postup pro změnu hesla [Zdroj: vlastní]

K ukončení stačilo pokračovat a heslo bylo změněno. Po zadání nového hesla byl systém zpřístupněn. Tento způsob byl jednoduchý a zabezpečení téměř žádné, jelikož se návod našel jednoduše na internetu.



Obrázek 27 – Pokračování k přihlášení do systému [Zdroj: vlastní]

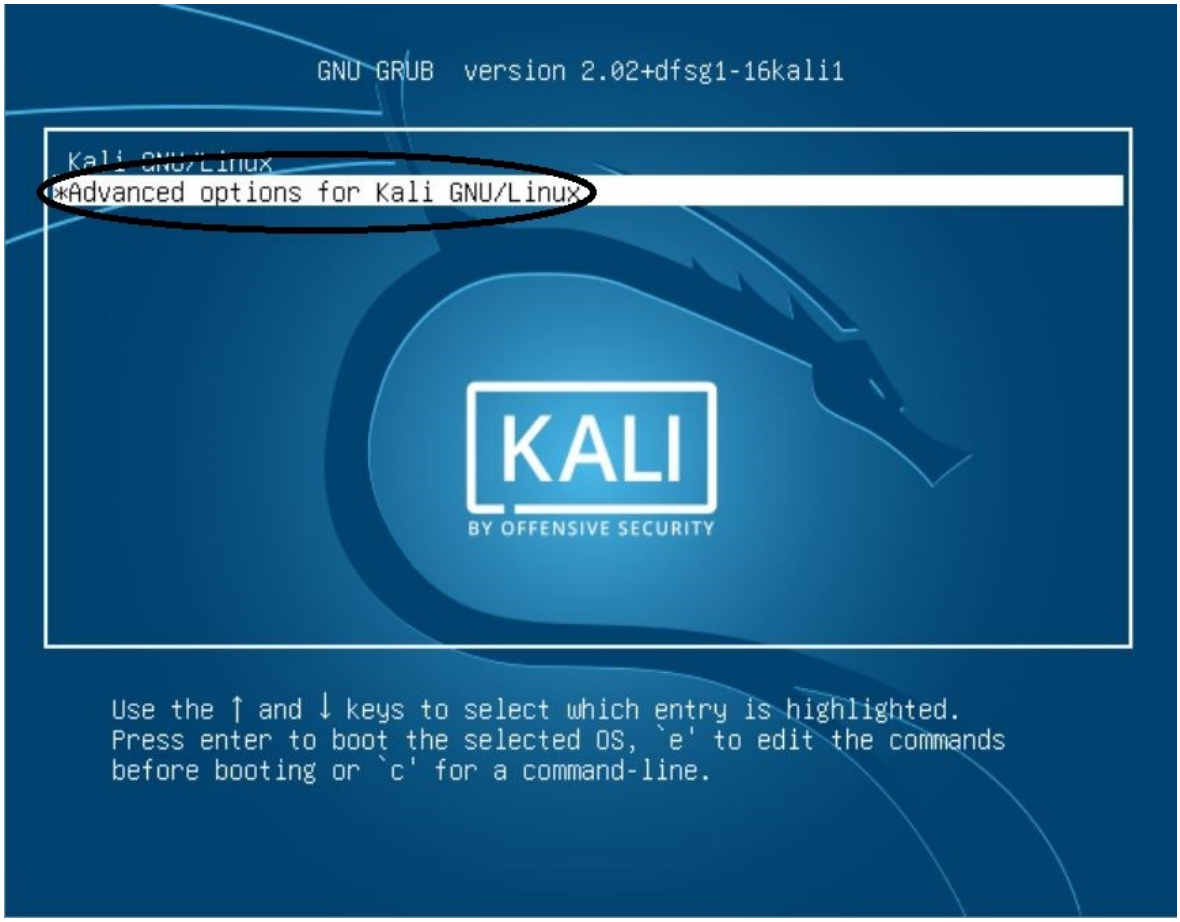
5.3 OS Kali Linux

Systém Kali Linux je určen pro různé bezpečnostní testování. Kvůli lepšímu zabezpečení tohoto systému bylo nutné ho analyzovat a přesvědčit se, zda je opravdu lépe zabezpečen. Následující útok ukázal, jak na tom OS Kali je.

U ysstému Kali byl použit obdobný způsob jako u Ubuntu. Opět bylo použito několik příkazů, díky kterým se bylo možné dostat až do bodu, kdy se mohlo změnit heslo.

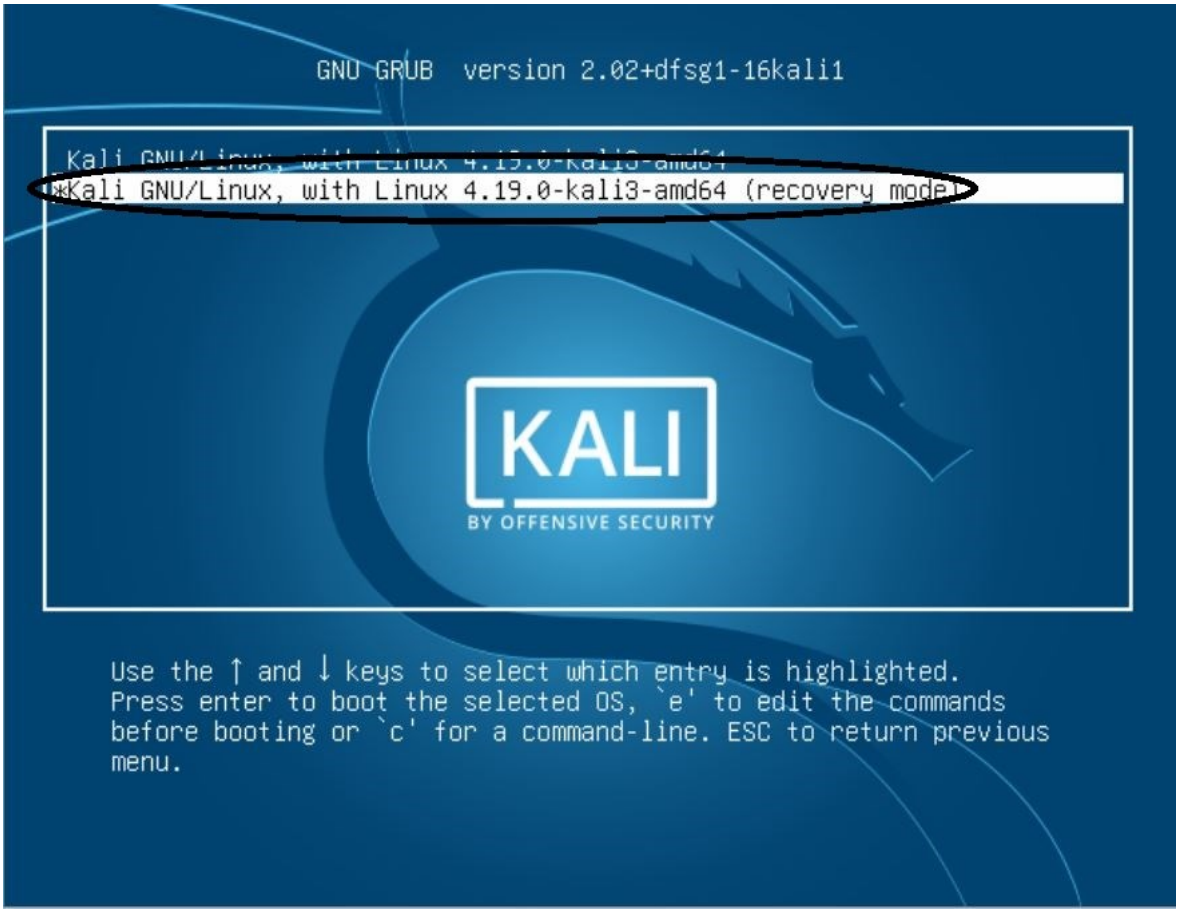
5.3.1 Změna root hesla

Analýza probíhala podobně jako u OS Ubuntu, jelikož je to také Linux. Mnoho věcí je podobných, ale Kali je distribuce přímo určená pro bezpečnostní testování a penetrační útoky. Stejně jako u Ubuntu jsme se po zapnutí za pomoci „Shift“ dostali do GNU GRUB menu, kde bylo cílem dostat se do „recovery mode“. První krok byl výběr „pokročilé možnosti“, což je vyznačeno na obrázku 28.



Obrázek 28 – GNU GRUB u OS Kali Linux [Zdroj: vlastní]

Druhý krok je již zmíněný „recovery mode“, ale u systému Kali by se po potvrzení možnosti zobrazil požadavek pro zadání „root“ hesla (dá se říci, že je to administrátorské heslo). Proto se jen možnost označila a stiskem písmene „e“ jsme se přesunuli k dalšímu kroku.

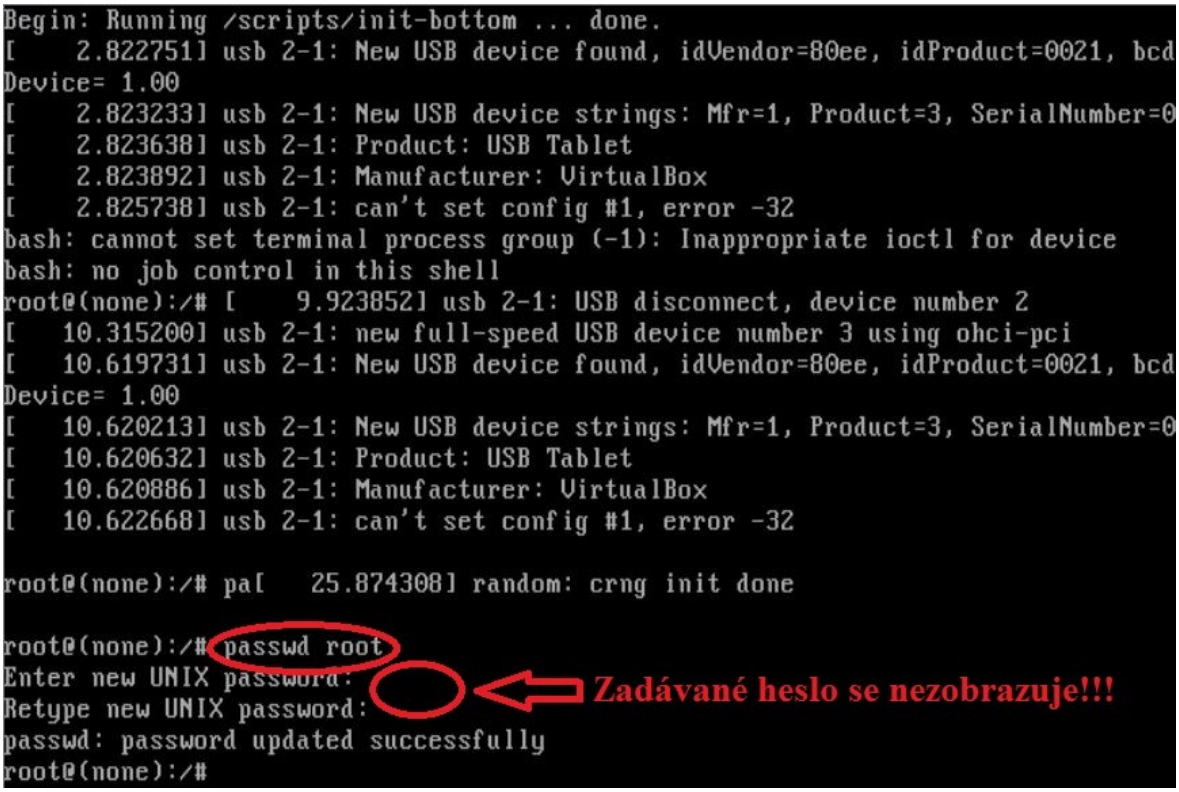


Obrázek 29 – Výběr možnosti tzv. „záchranného módu“ [Zdroj: vlastní]

V tomto kroku bylo třeba přepsat některé příkazy, díky kterým je možnost změnit root heslo. Na obrázku jsou označené dopsané příkazy. Místo „ro“ se napsalo „rw“ a na konec řádku se po mezeře dopsalo „init=/bin/bash“. Vše se potvrdilo stiskem „F10“.

Obrázek 30 – Přepisování příkazů pro změnu root hesla [Zdroj: vlastní]

Jako poslední krok stačilo po načtení obrazovky napsat „passwd root“, zadat nové heslo a ještě jednou ho napsat a potvrdit. Nakonec restartovat počítač a zadat nové heslo pro zpřístupnění systému. Nakonec i přes lepší zabezpečení, byla změna hesla za pomoci návodu velmi jednoduchá.



Obrázek 31 – Závěrečný krok se změnou hesla [Zdroj: vlastní]

6 OPATŘENÍ PROTI ÚTOKU

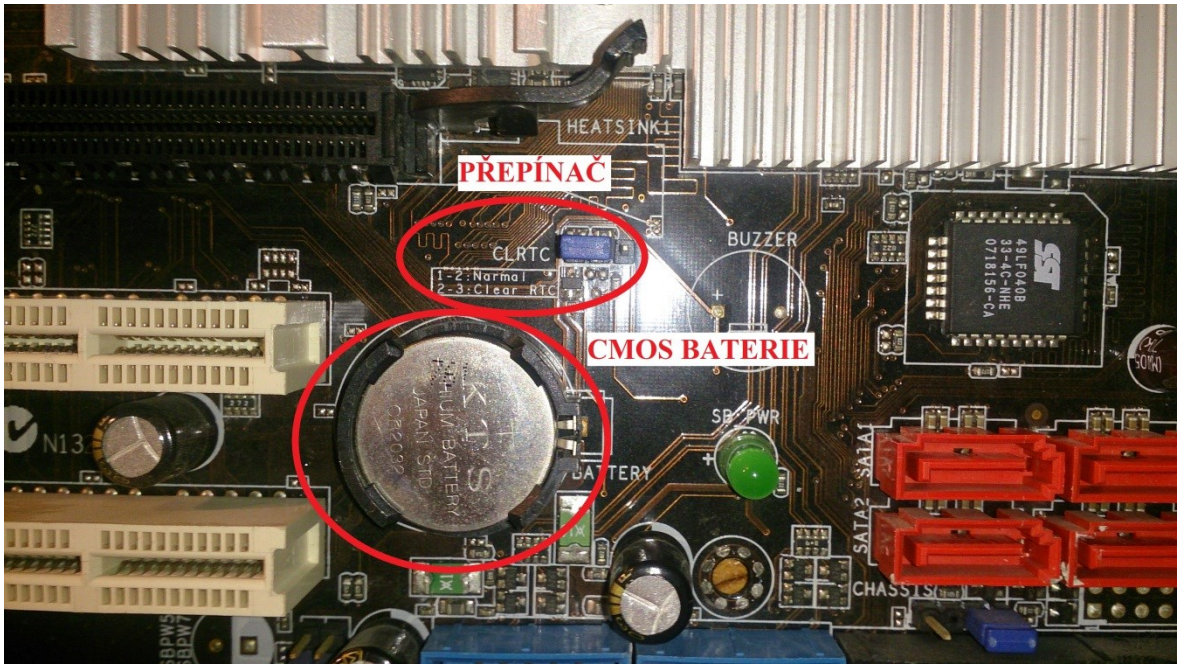
Po analýzách útoků na různé OS lze říci, že pro lepší ochranu dat, je třeba udělat více než jen nastavit heslo do systému. Zabezpečit data v počítači lze hned několika způsoby, které jsou v následujících podkapitolách dále rozvedeny.

6.1 Vytvoření hesla v BIOSu

Asi nejjednodušší opatření proti napadení počítače výše zmíněnými programy je vytvoření hesla v BIOSu. V každém BIOSu se dá nastavit heslo. Může se nastavit heslo přímo do BIOSu, které se spouští, jen když se do něj chce uživatel přihlásit. Pak se dá nastavit i heslo, které je požadováno při každém zapnutí počítače. Jakmile BIOS provede všechny operace, zobrazí se požadavek hesla. Toto je opatření pro obyčejné uživatele, kteří nejsou moc zběhlí v ovládání počítače, ale je jednoduché. [47]

I toto opatření má svou slabinu. První možností napadení počítače je použití „Master password“. Funguje pouze u notebooků. Po opětovném zadávání špatného heslo se zablokuje systém a na obrazovce se ukáže kód. Ten se na webových stránkách (bios-pw.org/) zadá do určeného pole a poté se vygeneruje kód k odemknutí systému, které se zadává po restartu počítače v BIOSu. Další možnost je u stolních počítačů, kde je to složitější. Na základní desce se vytáhne CMOS baterie a poté vrátí zpět. To je první způsob a druhý je resetování přepínače (jumper). Po krátkém přepojení do polohy „clear RTC“ se odstraní heslo a po restartu počítače naní vyžadováno. [47,48]

Opatřením proti vytažení baterie nebo resetu přepínače je ochrana hardwaru. Počítačovou skříň můžeme ochránit v místnosti nebo prostoru opatřené a uzamčené zámkem, zabezpečením objektu, kde se nachází.



Obrázek 32 – Ukázka přepínače a CMOS baterie na základní desce [Zdroj: vlastní]

6.2 Šifrování dat v počítači

Jedná se o velmi efektivní opatření, kde se šifrují data a pro dešifrování je třeba zadat heslo. Je to proces přeměny dat za pomoci kryptografie do formy, kterou nelze dešifrovat bez příslušného klíče. Šifrování se používá nejčastěji na přenosná paměťová úložiště jako USB a externí HDD, lze použít i na HDD v počítači. Pro účel šifrování je k dispozici několik programů. [12]

BitLocker je asi nejznámější program pro šifrování dat. Je podporován v různých verzích systémů Windows Vista, 7, 8, 8.1 a 10. Šifruje celý diskový oddíl nebo v případě USB Flash Disku celé úložiště. Při šifrování jen nějaké části je to komplikovanější. [49]

Další je **VeraCrypt**, který vychází z již nepoužívaného TrueCrypt. Opravil jeho nedostatky a zesílil algoritmy při generování šifrovacích klíčů. Pracuje s „šifrovanými kontejnery“, které jsou virtuálními disky, do kterých ukládají data. Zvládá šifrovat celý USB Flash Disk i diskový oddíl. Jeho nevýhodou je nutnost mít další USB Flash Disk s přenosnou verzí programu. [49]

Alternativou VeraCrypt je **Rohos Mini Drive**. Je zaměřen na přenášení šifrovaných dat. Pracuje na stejném principu. Přenosná aplikace má opatření proti keyloggeru ve formě virtuální klávesnice. Zdarma je šifrování dat do velikosti 8 GB. [49]

Poslední zmíněná je aplikace **AxCrypt**. Tato aplikace je určena oproti výše zmíněným pro šifrování souborů. Samotná aplikace zabírá jen 1 MB a je zcela zdarma. Lze ji použít na šifrování příloh k e-mailům, které po stažení příjemcem budou dešifrovány. Lze s ní vytvářet archivy, které se „zabalí“ do souboru s koncovkou „EXE“ a pro spuštění se musí zadat heslo. Aplikace nemusí být na počítači nainstalovaná, což je její výhoda. [49]

Je potřeba myslet na to, že pro dešifrování musíme mít tento program. Je to aktuální u USB Flash Disků, které se přenáší z počítače do počítače.

6.3 Ukládání dat na cloudová úložiště

Mnoho lidí si ukládá data na cloudová úložiště. Člověk by mohl říct, že se jedná se o jednoduchou ochranu proti jakémukoliv napadení dat. V počítači nemusí být uložena žádná důležitá data a uživatel nemusí mít strach z odcizení, poškození či změně dat. Samozřejmě i cloudová úložiště mohou být napadena a data v nich uložená mohou být ohrožena. Nestává se to často, ale možnost tady je. I přesto je to možné opatření proti útokům na osobní počítače.

Co je to cloudové úložiště? Je to služba, která nabízí možnost uložení dat, jak soukromým osobám, tak firmám. Data jsou uložena na úložištích spravovaných poskytovateli služby. Přístup k uloženým datům je možný odkudkoliv. Majitel dat tudíž nemusí nosit žádná úložná zařízení. [50]

Jeden z nejznámějších je **OneDrive**, který je provozován firmou Microsoft a je součástí OS Windows 10 a 8. Do 5 GB je služba bezplatná, ale pokud někdo chce více úložného místa pro data, tak se od toho odvíjí cena. Například za 50 GB místa se platí 50 Kč měsíčně.

Google zase v rámci Gmail poskytuje **Google Disk**, kde mají uživatelé zdarma 15 GB. Cena se odvíjí od velikosti úložiště (cca. 45 Kč za 100 GB za měsíc).

Službu také nabízí Apple a nese název **iCloud**. Stejně jako OneDrive nabízí zdarma 5 GB za příplatek 25 Kč měsíčně je k dispozici 50 GB.

Jedním z posledních významných provozovatelů cloudového úložiště je **Dropbox**. Služby jsou dostupné nejen pro PC, ale i pro mobilní telefony. Nabízí snadný a bezpečný přístup k datům odkudkoliv. S Dropboxem spolupracuje mnoho významných organizací jako Adidas, Hewlett Packard, National Geographic a další. Zdarma nabízí 2 GB. [52]

Je daleko více poskytovatelů cloudového úložiště, kteří se tím živý a bezplatně nabízejí pouze místo od 2 do 10 GB. Při zvýšení úložného místa se vždy zvedne i cena za službu. Záleží jen na požadavku zákazníka. [51]

ZÁVĚR

Cílem v teoretické části bylo zpracovat rešerši současného stavu vztahující se k dané problematice s důrazem na monografie a analytické materiály. Po nastudování materiálů, které souvisely s problematikou práce, byly vymezeny základní pojmy a názvosloví, které jsou důležité pro celou práci. Další cíl, který měl seznámit se současnými útoky na osobní počítače, byl pojat formou vysvětlení principu fungování těch nejznámějších útoků na osobní počítače. Útoky byly rozděleny podle způsobu provedení na fyzické, vzdálené a kombinované, kdy byly popsány a uvedeny nástroje k provedení těchto útoků.

Praktická část měla dva cíle. Realizace útoků na tři vybrané operační systémy. Nejdříve, ale proběhla instalace virtuálního počítače pro následnou realizaci útoků. Virtuální počítač nebyl původně zamýšlen použít, ale protože bylo třeba analyzovat útoky na více operačních systémů, tak byl nejlepší volbou. Další výhoda byla lepší kvalita pořízených snímků. Následná instalace operačního systému Windows 10, Ubuntu a Kali Linux a realizace vybraných útoků. Tento cíl byl splněn a u každého operačního systému byl proveden minimálně jeden útok, který byl detailně popsán i s obrázky. Na závěr navržená opatření pro ukládání dat, lepší zabezpečení šifrováním nebo nastavení dalšího hesla, tentokrát v BIOSu sice nemusí být stoprocentní, ale jedná se o další ochranu dat uživatele PC.

SEZNAM POUŽITÉ LITERATURY

[1]TECHOPEDIA. *Information and Communications Technology (ICT)*. Technopedia [online]. Techopedia, ©2019 [cit. 2019-05-06]. Dostupné z: https://www.techopedia.com/definition/24152/information-and-communications-technology-ict

[2] BEZPALEC, Pavel. Management ICT systémů. *Publi.cz: Co je ICT - systém* [online]. [cit. 2019-05-06]. Dostupné z: https://publi.cz/books/242/01.html

[3]MINISTERSTVO VNITRA ČR. *Terminologický slovník pojmů z oblasti krizového řízení, ochrany obyvatelstva, environmentální bezpečnosti a plánování obrany státu* [online]. [cit. 2019-05-06]. Dostupné z: https://www.mvcr.cz/soubor/terminologicky-slovnik-mv-verze-ke-stazeni.aspx

[4] *Úmluva o kyberkriminalitě*. [online]. [cit. 2019-05-06]. Dostupné z: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016804931c0

[5] KOLOUCH, Jan. *CyberCrime*. Praha: CZ.NIC, z.s.p.o., 2016. CZ.NIC. ISBN 978-80-88168-15-7.

[6] ŠULC, Vladimír a Marek ČANDÍK. *Vybrané aspekty bezpečnosti informačních systémů* [online]. , 21 [cit. 2019-05-06]. Dostupné z: http://www.teorieib.cz/pbi/files/344-SuCa.pdf

[7] *Heavy Duty Computer Enclosures* [online]. Dalen Limited, c2019 [cit. 2019-05-06]. Dostupné z: https://www.top-tec.co.uk/IT-Security-Enclosures/PC-Security/Heavy-Duty-Computer-Enclosures/

[8] LOLOVÁ, Veronika. *Zabezpečení hardwaru a softwaru* [online]. 2017 [cit. 2019-05-06]. Dostupné z: https://medium.com/edtech-kisk/zabezpe%C4%8Den%C3%AD-hardwaru-a-softwaru-2470684e9f19

[9] ACSA. *Informační bezpečnost* [online]. Akademické centrum studentských aktivit, ©2019 [cit. 2019-05-06]. Dostupné z: https://www.acsa.cz/verejnost/sluzby/podle-temat/informacni-bezpecnost/

[10] SOCA. *Tři pilíře počítačové bezpečnosti* [online]. SOCA, 2015 [cit. 2019-05-06]. Dostupné z: https://www.soca.cz/blog/article/tri-pilire-pocitacove-bezpecnosti-45?page=3

[11] ČESKO. Zákon č. 181/2014 Sb. In: *Zákony pro lidi.cz* [online]. © AION CS 2010-2019 [cit. 2019-05-06]. Dostupné z: https://www.zakonyprolidi.cz/cs/2014-181

[12] JIRÁSEK, Petr, Luděk NOVÁK a Josef POŽÁR. *Výkladový slovník kybernetické bezpečnosti: Cyber security glossary*. Třetí aktualizované vydání. Praha: Policejní akademie ČR v Praze, 2015. ISBN 978-80-7251-436-6.

[13] KOVÁŘ, Petr. Slovníček odborných termínů. *Historiepocitacu.cz* [online]. 2019 [cit. 2019-05-06]. Dostupné z: https://www.historiepocitacu.cz/slovnicek-odbornych-terminu.html

[14] PROCHÁZKA, David. *Nebojte se počítače - pro Windows 7 a Office 2010*. Praha: Grada, 2011. Snadno a rychle (Grada). ISBN 978-80-247-3717-1.

[15] HLAVENKA, Jiří. *Výkladový slovník výpočetní techniky a komunikací: 5500 pojmů z oblasti výpočetní techniky : přes 7000 křížových vazeb : výklad anglických a českých odborných pojmů*. 3. vyd. Praha: Computer Press, 1997. ISBN 80-722-6023-5.

[16] TECHOPEDIA. *Software* [online]. Techopedia, ©2019 [cit. 2019-05-06]. Dostupné z: https://www.techopedia.com/definition/4356/software

[17] FISHER, Tim. *BIOS (Basic Input Output System)* [online]. Lifewire, 2019 [cit. 2019-05-06]. Dostupné z: https://www.lifewire.com/bios-basic-input-output-system-2625820

[18] SVĚTHARDWARE Slovník. *Svethardware.cz* [online]. oXy Online, ©1998-2019 [cit. 2019-05-06]. Dostupné z: https://www.svethardware.cz/slovnik/b

[19] *Elitegroup 761GX-M754 - AMIBIOS (American Megatrends) in a Winbond W39V040APZ - Flash memory* [online]. Raimond Spekking, 2016 [cit. 2019-05-06]. Dostupné z: https://commons.wikimedia.org/wiki/Category:Basic_Input_Output_System#/media/File:Elitegroup_761GX-M754_-_AMIBIOS_(American_Megatrends)_in_a_Winbond_W39V040APZ-5491.jpg

[20] TECHTARGET. POST (Power-On Self-Test). *Whatis.techtarget.com* [online]. Tech-Target, 2005 [cit. 2019-05-06]. Dostupné z: https://whatis.techtarget.com/definition/POST-Power-On-Self-Test

[21] MINÁŘ, Pavel. Operační systém. *Jaknait.cz* [online]. ©2019 [cit. 2019-05-06]. Dostupné z: https://www.jaknait.cz/co-je/operacni-system/

[22] TECHOPEDIA. *Operating System (OS)* [online]. Techopedia, ©2019 [cit. 2019-05-06]. Dostupné z: https://www.techopedia.com/definition/3515/operating-system-os

[23] IT-SLOVNÍK. *Kernel* [online]. IT-Slovnik.cz team, ©2008-2018 [cit. 2019-05-06]. Dostupné z: https://it-slovnik.cz/pojem/kernel

[24] PCMAG. API. *PCmag.com* [online]. Ziff Davis, ©1996-2019 [cit. 2019-05-06]. Dostupné z: https://www.pcmag.com/encyclopedia/term/37856/api

[25] AGSEASONALS. *AGSeasonals* [online]. Ag Seasonals, c2019 [cit. 2019-05-06]. Dostupné z: http://www.agseasonals.com/images/workswith.png

[26] STATCOUNTER. *Desktop Operating System Market Share Worldwide - April 2019* [online]. StatCounter, 2019 [cit. 2019-05-06]. Dostupné z: http://gs.statcounter.com/os-market-share/desktop/worldwide

[27] UBUNTU ČESKÁ REPUBLIKA. *LiveCD* [online]. Ubuntu Česká republika, 2019 [cit. 2019-05-06]. Dostupné z: https://wiki.ubuntu.cz/livecd

[28] O'DONNELL, Andy. *Rainbow Tables: Your Password's Worst Nightmare* [online]. Lifewire, 2018 [cit. 2019-05-06]. Dostupné z: https://www.lifewire.com/rainbow-tables-your-passwords-worst-nightmare-2487288

[29] Hash. *Počet-znaků.cz* [online]. ©2010-2019 [cit. 2019-05-06]. Dostupné z: http://www.pocet-znaku.cz/hash

[30] NCKB. Sociální inženýrství. *Národní centrum kybernetické bezpečnosti* [online]. ©2019 [cit. 2019-05-06]. Dostupné z: https://www.govcert.cz/cs/informacni-servis/doporuceni/2486-socialni-inzenyrstvi/

[31] KOHOUT, Roman a Radek KARCHŇÁK. *Bezpečnost v online prostředí*. Karlovy Vary: Biblio Karlovy Vary, 2016. ISBN 978-80-260-9543-9.

[32] *Hacking* [online]. CZECH NEWS CENTER, ©2019 [cit. 2019-05-06]. Dostupné z: https://www.zive.cz/hacking/sc-381/default.aspx

[33] DURAČINSKÁ, Zuzana a Pavel BAŠTA. *DDoS – sofistikovaný útok nebo služba na objednávku?*. IT Systems [online]. 2015, , 3 [cit. 2019-05-06]. Dostupné z: https://www.nic.cz/files/nic/doc/IT_Security_DDoS_042015.pdf

[34] IPTECHNIK. *Co je botnet ?* [online]. IPTechnik.cz, 2017 [cit. 2019-05-06]. Dostupné z: https://iptechnik.cz/co-je-botnet/

[35] TEICHERT, Damian. *Jak funguje keylogger?* [online]. SpyShop, 2017 [cit. 2019-05-06]. Dostupné z: https://www.spyshop24.cz/blog_cz/jak-funguje-keylogger/

[36] AVAST. *Keylogger* [online]. AVAST Software, 2016 [cit. 2019-05-06]. Dostupné z: https://www.avast.com/cs-cz/c-keylogger

[37] AZURE. *Co je virtuální počítač?* [online]. Microsoft, ©2019 [cit. 2019-05-06]. Dostupné z: https://azure.microsoft.com/cs-cz/overview/what-is-a-virtual-machine/

[38] BOTT, Ed. *Introducing Windows 10 for IT Professionals, Preview Edition* [online]. Washington: Microsoft Press, 2015 [cit. 2019-05-06]. ISBN 978-0-7356-9696-9. Dostupné z: https://download.microsoft.com/download/D/2/B/D2B18586-8C4F-4F40-828D-99D96489152A/Microsoft_Press_eBook_Introducing_Windows_10_Preview_PDF.pdf

[39] MICROSOFT. *Microsoft Trademark & Brand Guidelines* [online]. Microsoft, ©2019 [cit. 2019-05-06]. Dostupné z: https://www.microsoft.com/en-us/legal/intellectualproperty/trademarks/usage/general.aspx

[40] UBUNTU. Ubuntu. *Ubuntu.cz* [online]. Canonical, 2019 [cit. 2019-05-06]. Dostupné z: https://www.ubuntu.cz/desktop/

[41] LINUX. *Výhody operačního systému Linux* [online]. CZLUG, ©2018 [cit. 2019-05-06]. Dostupné z: https://proc.linux.cz/proc/

[42] UBUNTU. *Downloads* [online]. Canonical, ©2018 [cit. 2019-05-06]. Dostupné z: https://design.ubuntu.com/downloads/

[43] HERTZOG, Raphaël, Jim O'GORMAN a Mati AHARONI. *Kali Linux Reve*aled [online]. Cornelius: Offsec Press, 2017 [cit. 2019-05-06]. ISBN 978-0-9976156-0-9. Dostupné z: https://kali.training/downloads/Kali-Linux-Revealed-1st-edition.pdf

[44] KALI. *About Kali Linux* [online]. Offensive Security, ©2019 [cit. 2019-05-06]. Dostupné z: https://www.kali.org/about-us/

[45] WIKIPEDIA. *Logo* [online]. Davod, 2016 [cit. 2019-05-06]. Dostupné z: https://cs.wikipedia.org/wiki/Kali_Linux#/media/File:Kali_Linux_2.0_wordmark.svg

[46] TRINITYHOME. *Trinity Rescue Kit 3.4: easier and better than ever before!* [online]. Trinityhome, 2019 [cit. 2019-05-06]. Dostupné z: http://trinityhome.org/

[47] HALCIN, Jakub. *Jak nastavit BIOS počítače* [online]. MAFRA, 2008 [cit. 2019-05-06]. Dostupné z: https://www.idnes.cz/hry/magazin/jak-nastavit-bios-pocitace.A070408_bios130408_bw

[48] *How to Reset a BIOS Password* [online]. wikiHow, c2019 [cit. 2019-05-06]. Dostupné z: https://www.wikihow.com/Reset-a-BIOS-Password

[49] JANŮ, Stanislav. *Nejlepší aplikace pro šifrované zabezpečení souborů, složek i flashky* [online]. CZECH NEWS CENTER, 2016 [cit. 2019-05-06]. Dostupné z: https://www.zive.cz/clanky/nejlepsi-aplikace-pro-sifrovane-zabezpeceni-souboru-slozek-i-flashky/sc-3-a-181473/default.aspx

[50] AZURE. *Co je cloudové úložiště?* [online]. Microsoft, ©2019 [cit. 2019-05-06]. Dostupné z: https://azure.microsoft.com/cs-cz/overview/what-is-cloud-storage/

[51] DTEST. *Jak vybrat cloudové úložiště* [online]. dTest, 2017 [cit. 2019-05-06]. Dostupné z: https://www.dtest.cz/clanek-6032/jak-vybrat-cloudove-uloziste

[52] *Dropbox* [online]. c2019 [cit. 2019-05-13]. Dostupné z: https://www.dropbox.com/

[53] NEZMAR, Luděk. Zákon o kybernetické bezpečnosti pro organizace – Implementace nových povinností do praxe. Grada, 2018. ISBN 978-80-271-0899-2.

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

AMI	American Megatrends Inc.
API	Application Programming Interface
BIOS	Basic Input-Output System
CD	Compact Disk
CMOS	Complementary Metal-Oxide-Semiconductor
DDoS	Distributed Denial of Service
DNS	Domain Name System
DoS	Denial of Service
DVD	Digital Video Disk
EXE	Executable
GB	Gigabyte
GNU	GNU's Not Unix!
GRUB	GRand Unified Bootloader
HDD	Hard Disk Drive
HW	Hardware
ICT	Informační a komunikační technologie
MB	Megabyte
OS	Operační systém
PC	Personal Computer
POST	Power-On Self-Test
RAM	Random-Access Memory
ROM	Read-Only Memory
TRK	Trinity Rescue Kit
USB	Universal Serial Bus
VDI	Virtual Desktop Infrastructure

VM Virtual Machine

SEZNAM OBRÁZKŮ