

Úkoly

1. Seznamte se zadáním a instalačním postupem u laboratorní úlohy č. 2
2. Nastavte a zprovozněte firewallový skript na OS Debian. Ověřte jeho nastavení.
3. Proveďte změnu výchozích hesel v konfiguračních souborech.
4. Proveďte změnu výchozích hesel ve webovém rozhraní FreePBX.

Nastavení a zprovoznění firewallového skriptu

Zabezpečení firewallu

Firewallový skript má na starost filtrování povolených IP adres a služeb, jenž jsou poskytovány serverem. Pravidla skriptu jsou definována pomocí **iptables** a má název **firewall.sh**. Soubor s pravidly je uložen ve složce `/etc/init.d` a spouští se ihned po startu operačního systému. **Celý zdrojový kód skriptu je vložen příloze této laboratorní úlohy.**

Skript je rozdělen na dvě části. Část **start_firewall ()** slouží k zavedení nastavených pravidel. Spuštěním této funkce se nastaví všechna pravidla a přístup k serveru mají pouze povolené IP adresy a také jsou povoleny dané služby (porty). Funkce **stop_firewall ()** má na starost smazání všech vložených pravidel a nastavení původních hodnot **iptables**. To znamená, že k serveru má přístup jakákoliv IP adresa a může využít kterýkoliv port.

Firewall má povoleny porty pro služby SSH (TCP 22), SIP (TCP 5060, UDP 5060), DNS (UDP 53), HTTP (TCP 80), RTSP (TCP 554, UDP 554), FTP (TCP 21), FTP-DATA (TCP 20), IXA2 (UDP 4569) a přenos hlasu (UDP 10000 - 20000). Pouze přes tyto porty lze provádět komunikaci s okolím. Pro úspěšnou komunikaci s ústřednou je nutné znát port dané služby, ale také se musí přistupovat z povolené IP adresy.

Jelikož se skript spouští automaticky po startu operačního systému, musí být skript **firewall.sh** umístěn ve složce `/etc/init.d` a také je nutné vytvořit symbolické odkazy na firewallový skript do složek, které reprezentují jednotlivé úrovně běhu systému. Jsou to složky `/etc/rc0.d`, `/etc/rc1.d`, `/etc/rc2.d`, `/etc/rc3.d`, `/etc/rc4.d`, `/etc/rc5.d`, `/etc/rc6.d`.

Skriptu se musí přiřadit práva pro spuštění. To se provede následovně:

```
# chmod +x /etc/init.d/firewall.sh
```

Vytvoření symbolických odkazů pro jednotlivé úrovně se provede příkazy:

```
# ln -s /etc/init.d/firewall.sh /etc/rc0.d/K98firewall.sh
# ln -s /etc/init.d/firewall.sh /etc/rc1.d/K98firewall.sh
# ln -s /etc/init.d/firewall.sh /etc/rc2.d/S98firewall.sh
# ln -s /etc/init.d/firewall.sh /etc/rc3.d/S98firewall.sh
# ln -s /etc/init.d/firewall.sh /etc/rc4.d/S98firewall.sh
# ln -s /etc/init.d/firewall.sh /etc/rc5.d/S98firewall.sh
# ln -s /etc/init.d/firewall.sh /etc/rc6.d/K98firewall.sh
```

Při vytvoření symbolických odkazů se vyskytují písmena S a K. Písmeno S označuje spuštění a K ukončení služby. Posledním krokem k automatickému spouštění skriptu je aktualizace seznamu služeb, která se vykoná následujícím příkazem:

```
# update-rc.d firewall.sh defaults
```

Laboratorní úloha č.2 – Zabezpečení ústředny

Ověření nastavených pravidel se provede příkazem:

```
# iptables -vnL
```

Ovládání firewallového skriptu je také možné manuální cestou. Skript je možné spustit, zastavit nebo restartovat. Spuštění nastaví všechna zadaná pravidla. Zastavení zajistí vymazání všech pravidel a nastavení původních hodnot. Restart ukončí a znovu spustí firewall.

Příkaz pro manuální spuštění:

```
# sh /etc/init.d/firewall.sh start
```

Příkaz pro manuální ukončení:

```
# sh /etc/init.d/firewall.sh stop
```

Příkaz pro manuální restart:

```
# sh /etc/init.d/firewall.sh restart
```

Změna výchozích hesel v konfiguračních souborech

Instalace Asterisku a FreePBX se provádí s výchozími hesly. Jedním ze základních bezpečnostních prvků je změna a volba dostatečně silného hesla. Hesla se mění v konfiguračních souborech pro uživatele *asteriskuser*, který je používán pro MySQL. Změna se provede pod uživatelem `it{root}` a zadáním následujících příkazů:

```
# NEWPASSWORD='heslo';
# sed -i "s/\(^AMPDBPASS=*\)\" (.*)\"/\1$NEWPASSWORD/"
/etc/ampportal.conf
# sed -i "s/\(^password = *\)\" (.*)\"/\1$NEWPASSWORD/"
/etc/asterisk/cdr_mysql.conf
# sed -i "s/\(^AMPDBPASS = *\)\" (.*)\"/\1$NEWPASSWORD/"
/etc/asterisk/extensions_additional.conf
# sed -i "s/\($amp_conf\[ 'AMPDBPASS' \]\t= '*\)\"
(.*)\"/\1$NEWPASSWORD';/" /etc/freepbx.conf
# echo "SET PASSWORD FOR 'asteriskuser'@'localhost' =
PASSWORD('$NEWPASSWORD');" | mysql -u root -p
```

Dalším krokem je změna výchozích hesel u Asterisk Manageru. Příkazy pro provedení změny jsou:

```
# NEWPASSWORD='heslo';
# sed -i "s/\(^secret = *\)\" (.*)\"/\1$NEWPASSWORD/"
/etc/asterisk/manager.conf
# sed -i "s/\(^AMPMGRPASS = *\)\" (.*)\"/\1$NEWPASSWORD/"
/etc/asterisk/extensions_additional.conf
# sed -i "s/\(^AMPMGRPASS=*\)\" (.*)\"/\1$NEWPASSWORD/"
/etc/ampportal.conf
# asterisk -r -x "module reload manager"
# echo "UPDATE freepbx_settings SET value='$NEWPASSWORD' WHERE
keyword='AMPMGRPASS';" | mysql -u root -p asterisk
```

Změna výchozích hesel ve webovém rozhraní FreePBX

Nyní jsou změněny všechna hesla, která se používala při instalaci. Na řadě je tedy změna hesel, která se týká samotného FreePBX. Změna hesla administrátora se mění v *Admin* → *Administrators*, kde se v pravé části vybere položka *admin*.

Ostatní hesla související s provozem FreePBX se mění v sekci *Settings* → *Advanced Settings*. Změna hesel je nutná u *FOP Password* a *User Portal Admin Password*.

Příloha – firewallový skript

```
#!/bin/sh

#####
# Firewall povoluje komunikaci jen s pocitaci, ktere maji povolenou IP.
# Komunikace je povolena pouze na povolene sluzby poskytovane serverem.
#####

# hlavicka potrebna pro spusteni pomoci /etc/init.d ve Squeeze
### BEGIN INIT INFO
# Provides:          firewall
# Required-Start:    $local_fs $network
# Required-Stop:     $local_fs $network
# Default-Start:     2 3 4 5
# Default-Stop:      0 1 6
# Short-Description: firewall
### END INIT INFO

# porty Asterisk UDP - hlas
HLAS="10000:20000"
IAX2="4569"

# definovani povolenych IP a sluzeb
POVOLENE_IP="10.0.0.0/8"
POVOLENE_IP_APT="10.0.0.0/8"
POVOLENE_SLUZBY_TCP="ssh sip http rtsp ftp ftp-data"
POVOLENE_SLUZBY_UDP="rtsp sip $HLAS $IAX2"

# spusteni a vlozeni pravidel
start_firewall () {
```

Laboratorní úloha č.2 – Zabezpečení ústředny

```
# definovani zakladnich pravidel (policy) pro tabulku filter
iptables -P INPUT DROP
iptables -P OUTPUT ACCEPT

# povoleni pravidla pro praci s DNS - nslookup
iptables -A INPUT -p udp --sport 53 -s 195.178.88.66 -j ACCEPT

# povoleni pravidla pro aktualizace - apt a freepbx (mirror)
for IP in $POVOLENE_IP_APT
do
    iptables -A INPUT -p tcp --sport 80 -s $IP -j ACCEPT
done

# definovani pravidel
# povoleni pro spojeni TCP
for SLUZBY in $POVOLENE_SLUZBY_TCP
do
    for IP in $POVOLENE_IP
    do
        iptables -A INPUT -p tcp --dport $SLUZBY -s $IP -j ACCEPT
    done
done

# povoleni pro spojeni UDP
for SLUZBY in $POVOLENE_SLUZBY_UDP
do
    for IP in $POVOLENE_IP
    do
        iptables -A INPUT -p udp --dport $SLUZBY -s $IP -j ACCEPT
    done
done

# povoleni pristupu z localhosta vsechno
iptables -A INPUT -j ACCEPT -i lo
```

Laboratorní úloha č.2 – Zabezpečení ústředny

```
# povoleni ICMP ze vsech stroju
iptables -A INPUT -p icmp -j ACCEPT

# co neni povoleno na TCP, dostane RST, na UDP ICMP Port Unreachable
iptables -A INPUT -i eth0 -p tcp -j REJECT --reject-with tcp-reset
iptables -A INPUT -i eth0 -p udp -j REJECT --reject-with icmp-port-
unreachable

}

# pri zastaveni smaze puvodni pravidla a vlozi zakladni pravidla, vse
povoleno
stop_firewall () {
    iptables -t filter -F
    iptables -t filter -P INPUT ACCEPT
    iptables -t filter -P OUTPUT ACCEPT
}

# rozhrani pri spousteni pres BASH
case "$1" in
    start)
        echo "Spoustim firewall a fail2ban!"
        start_firewall
        /etc/init.d/fail2ban start
        ;;

    stop)
        echo "Zastavuji firewall a fail2ban!!!"
        stop_firewall
        /etc/init.d/fail2ban stop
        ;;

    restart)
        echo "Restartuji firewall a fail2ban!!"
        stop_firewall
        start_firewall
        /etc/init.d/fail2ban restart
    ;;
esac
```

Laboratorní úloha č.2 – Zabezpečení ústředny

```
;;
```

```
*)
```

```
echo "Prikaz pro spusteni: firewall.sh start"
```

```
echo "Prikaz pro zastaveni: firewall.sh stop"
```

```
echo "Prikaz pro restart: firewall.sh restart"
```

```
;;
```

```
esac
```