



VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ

FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION

ÚSTAV TELEKOMUNIKACÍ

DEPARTMENT OF TELECOMMUNICATIONS

ZABEZPEČENÍ SLUŽEB NA PLATFORMĚ MIKROTIK

SECURING SERVICES ON MIKROTIK PLATFORM

BAKALÁŘSKÁ PRÁCE

BACHELOR'S THESIS

AUTOR PRÁCE

AUTHOR

Vanesa Kociská

VEDOUCÍ PRÁCE

SUPERVISOR

Ing. Ondřej Krajsa, Ph.D.

BRNO 2023

Bakalářská práce

bakalářský studijní program **Informační bezpečnost**

Ústav telekomunikací

Studentka: Vanesa Kociská

ID: 231244

Ročník: 3

Akademický rok: 2022/23

NÁZEV TÉMATU:

Zabezpečení služeb na platformě Mikrotik

POKYNY PRO VYPRACOVÁNÍ:

Prostudujte možnosti zabezpečení jednotlivých služeb a funkcí systému RouterOS ve verzi 7.x. Provedte analýzu jednotlivých možností z hlediska bezpečnosti a navrhněte a realizujte tato doporučení na zařízení s RouterOS. Navrhněte a realizujte vhodné testování zabezpečení.

DOPORUČENÁ LITERATURA:

- [1] Hardening Network Devices. NSA [online]. [cit. 26. 11. 2022]. Dostupné z URL: <https://media.defense.gov/2020/Aug/18/2002479461/-1/-1/0/HARDENING_NETWORK_DEVICES.PDF>
- [2] Getting Started. mikrotik [online]. [cit. 25. 11. 2022]. Dostupné z URL: <<https://help.mikrotik.com/docs/display/ROS/Getting+started>>

Termín zadání: 6.2.2023

Termín odevzdání: 26.5.2023

Vedoucí práce: Ing. Ondřej Krajsa, Ph.D.

doc. Ing. Jan Hajný, Ph.D.
předseda rady studijního programu

UPOZORNĚNÍ:

Autor bakalářské práce nesmí při vytváření bakalářské práce porušit autorská práva třetích osob, zejména nesmí zasahovat nedovoleným způsobem do cizích autorských práv osobnostních a musí si být plně vědom následků porušení ustanovení § 11 a následujících autorského zákona č. 121/2000 Sb., včetně možných trestněprávních důsledků vyplývajících z ustanovení části druhé, hlavy VI. díl 4 Trestního zákoníku č.40/2009 Sb.

ABSTRAKT

Bakalárska práca ma za cieľ informovať čitateľa o správnom zabezpečení sieťových zariadení. Zameriava sa na zabezpečenie smerovačov s RouterOS kde sú porovnané funkcie starej a novej verzie operačného systému. Na základe odporúčaní v teoretickej časti práce je navrhnutý podrobný postup konfigurácie. Následné je vykonané testovanie zariadenia pomocou simulácie najbežnejších sieťových útokov na zabezpečený smerovač. Súčasťou praktickej časti je aj jednoduchý konfiguračný skript pre RouterOS pomocou ktorého sa dá nakonfigurovať nové zariadenie a bash skript na otestovanie funkčnosti navrhnutých zabezpečení.

KĽÚČOVÉ SLOVÁ

Mikrotik, RouterOS, smerovač, bezpečnosť

ABSTRACT

This bachelor's thesis goal is to familiarize the reader with the correct methods of securing network devices. It focuses on securing routers with RouterOS, where the functionalities of the old and new version of the operating system are compared. Based on the recommendations the theoretical part, a detailed configuration process is suggested. Subsequently, testing of the devices is performed with the most common network attacks on a secured router. The practical part also includes a simple configuration script for RouterOS, with which a new device can be configured and a bash script to test the functionality of the suggested security measures.

KEYWORDS

Mikrotik, RouterOS, router, security

KOCISKÁ, Vanesa. *Zabezpečení služeb na platformě Mikrotik*. Brno: Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, Ústav telekomunikací, 2023, 87 s. Bakalářská práce. Vedúci práce: Ing. Ondřej Krajsa, Ph.D

Vyhlásenie autora o pôvodnosti diela

Meno a priezvisko autora: Vanesa Kociská
VUT ID autora: 231244
Typ práce: Bakalárska práca
Akademický rok: 2022/23
Téma záverečnej práce: Zabezpečení služeb na platformě Mikrotik

Vyhlasujem, že svoju záverečnú prácu som vypracovala samostatne pod vedením vedúcej/cého záverečnej práce, s využitím odbornej literatúry a ďalších informačných zdrojov, ktoré sú všetky citované v práci a uvedené v zozname literatúry na konci práce.

Ako autorka uvedenej záverečnej práce ďalej vyhlasujem, že v súvislosti s vytvorením tejto záverečnej práce som neporušila autorské práva tretích osôb, najmä som nezasiahla nedovoleným spôsobom do cudzích autorských práv osobnostných a/alebo majetkových a som si plne vedomá následkov porušenia ustanovenia § 11 a nasledujúcich autorského zákona Českej republiky č. 121/2000 Sb., o práve autorskom, o právach súvisiacich s právom autorským a o zmene niektorých zákonov (autorský zákon), v znení neskorších predpisov, vrátane možných trestnoprávných dôsledkov vyplývajúcich z ustanovenia časti druhej, hlavy VI. diel 4 Trestného zákonníka Českej republiky č. 40/2009 Sb.

Brno

.....

podpis autorky*

*Autor podpisuje iba v tlačenej verzii.

POĎAKOVANIE

Rada by som poďakovala vedúcemu bakalárskej práce pánovi Ing. Ondrejovi Krajsovi, Ph.D. za odborné vedenie, konzultácie, trpezlivosť a podnetné návrhy k práci.

Obsah

Úvod	21
Cíle práce	23
1 Známe odporúčania CISA a NSA	25
1.1 Všeobecné odporúčania	25
1.2 Zabezpečenie sieťových zariadení	26
1.2.1 Správa účtov, autentizácia a autorizácia	26
1.2.2 Služby	27
1.2.3 Rozhrania a porty prepínačov	29
1.2.4 Aktualizácia hardwaru a softwaru	30
1.2.5 Monitorovanie a logovanie	31
2 Odporúčania NÚKIB a smernica NIS2	33
2.1 Odporúčania NÚKIB	33
2.1.1 Infraštruktúra	33
2.1.2 Zariadenia	34
2.1.3 Správa účtov	35
2.2 Smernica NIS2	35
2.2.1 Povinnosti	36
3 RouterOS	37
3.1 RouterOS 7	37
3.2 Kernel 3.3.5+ vs. Kernel 5.6	37
3.2.1 Bezpečnosť Linux Kernelu 3.3.5	37
3.2.2 Bezpečnosť Linux Kernelu 5.6	38
3.3 Zraniteľnosti RouterOS 7 vs RouterOS 6	38
3.3.1 RouterOS 6	38
3.3.2 RouterOS 7	39
3.4 Pridané služby RouterOS 7	40
3.4.1 WifiWave 2	40
3.4.2 WireGuard	41
3.4.3 Let's Encrypt certifikáty	41
3.5 Analýza bezpečnosti RouterOS služieb	41
3.5.1 Konfiguračný prístup	42
3.5.2 Bezdrôtové siete	43
3.5.3 Firewall	43

4	Návrh zabezpečenia služieb RouterOS	45
4.1	Príprava topológie a prostredia	45
4.1.1	Príprava EVE-NG	46
4.2	Aktualizácia systému	48
4.3	Prístup do zariadenia	49
4.3.1	Vytvorenie užívateľa	49
4.3.2	Mac Server	50
4.3.3	Bezpečný prístup	51
4.4	Vypnúť nepoužívané rozhrania	51
4.5	Vypnúť nepoužívané služby	51
4.5.1	Ostatné služby	52
4.6	Záloha konfigurácie	54
4.7	Firewall	55
4.7.1	Povolenie už nadviazaných spojení	55
4.7.2	Bogon adresy	56
4.7.3	Filtrovanie pomocou geolokácie	57
4.7.4	UDP flood	57
4.7.5	SYN flood	57
4.7.6	Port scan	58
4.7.7	SSH a Winbox Brute force	58
4.7.8	NAT maškaráda	59
4.8	Konfiguračný skript	59
4.8.1	Obsah skriptu	59
5	Testovanie zabezpečenia	63
5.1	Port scan	63
5.1.1	Zabezpečenie pred port scan útokom	63
5.2	UDP flood	64
5.2.1	Zabezpečenie pred UDP flood	64
5.3	SYN flood	65
5.3.1	Zabezpečenie pred SYN flood	66
5.4	SSH brute force	67
5.4.1	Príprava Metasploit Frameworku na útok	68
5.4.2	Zabezpečenie pred SSH brute-force	69
5.5	CDP flood	71
5.5.1	Zabezpečenie proti CDP flood útoku	72
5.6	Testovací skript	73
5.6.1	Spustenie logovania na syslog	73
5.6.2	Prispôbenie resource skriptu pre Metasploit	74

5.6.3	Vytvorenie a spustenie testovacieho skriptu	74
5.7	Testovanie pomocou Routersploitu	75
	Závěr	77
	Literatúra	79
	Zoznam symbolov a skratiek	83
	A Obsah elektronické přílohy	87

Zoznam obrázkov

3.1	Známe zranitelnosti RouterOS od roku 2009	39
4.1	Návrh testovacej siete	45
4.2	Nainštalovaný virtuálny EVE-NG server	46
4.3	Vytvorenie nového labu	47
4.4	Zapojenie siete v EVE-NG	48
4.5	Vytvorenie nového užívateľa	49
4.6	Prihlásenie pomocou SSH s novým užívateľom	50
4.7	Vypnutie MAC služieb	50
4.8	Vypnutie nepotrebných služieb a zmena portov SSH a winbox	52
4.9	Vypnutie discovery protokolov na všetkých rozhraniach	52
4.10	Vypnutie Bandwidth serveru	53
4.11	Vypnutie dns cache	53
4.12	Zapnutie RP filtra a TCP SYN cookies	54
4.13	Vytvorenie zálohy vo Winboxe	55
5.1	Port scan pomocou nástroja nmap	63
5.2	Port scan zablokovaný firewallom	64
5.3	UDP flood na nezabezpečený smerovač	65
5.4	Zablokované UDP packety	65
5.5	SYN flood útok pomocou hping3	66
5.6	SYN flood útok zablokovaný firewallom	66
5.7	Útočník pridaný do blacklistu	67
5.8	Náhodné zdrojové IP adresy	67
5.9	Parametre SSH brute force útoku	68
5.10	Úspešný ssh útok	69
5.11	SSH brute force blokový firewallom	70
5.12	Prihlasovanie pomocou ssh kľúča	71
5.13	CDP flood Yersinia	72
5.14	CDP flood RouterOS	72
5.16	Routersploit	76
5.17	Výsledky testovania	76

Zoznam výpisov

4.1	Ukážka premenných	60
5.1	Metasploit resource skript	74
5.2	Testovací skript	74

Úvod

V dnešnom svete, keď je všetko pripojené na internet treba myslieť aj na bezpečnosť. Či už užívateľov, alebo samotnej siete a jej zariadení aby sa predišlo nežiadúcim útokom. Technológiami sa vyvíjajú aj samotné znalosti a nástroje útočníkov a administrátori siete by nemali zaostávať a udržiavať zariadenia aktuálne a správne zabezpečené aby týmto útokom predišli. V posledných rokoch narastá počet kybernetických útokov po celom svete. Jednou z najviac postihnutých oblastí podľa analýzy IBM[2] celosvetovo je práve zdravotníctvo, kedy môže prísť až ku strate životov. Útok na nemocnicu v Benešove z roku 2019 alebo útok na fakultní nemocnicu v Brne z roku 2020 je príkladom toho, že ani Česká republika nie je výnimkou[1].

Preto sa táto práca venuje zabezpečeniu služieb na platforme MikroTik. Prvá a druhá kapitola obsahuje analýzu odporúčaní, ktoré by sa mali dodržiavať pre základnú bezpečnosť. Vychádza sa hlavne z odporúčaní od spoločností CISA, NSA a NÚKIB. Sú tu stručne vymenované oblasti na ktoré sa zamerať a vysvetlené akých spôsobom postupovať pri návrhu siete a neskôr aj konkrétnejšie napísané, ktoré známe služby a protokoly sa odporúča vypnúť.

Tretia kapitola sa zameriava na porovnanie starších verzií RouterOS a najnovšej verzie RouterOS 7, ktorá so sebou priniesla veľa noviniek. Porovnané sú zraniteľnosti oboch verzií kernelov. Spomenuté sú hlavné služby a protokoly, ktoré súvisia s bezpečnosťou. Ďalej sa táto kapitola zameriava už na služby a protokoly, ktoré sú v tomto operačnom systéme často využívané alebo dôležité. Sú popísané ich bezpečnostne silné stránky alebo naopak zraniteľnosti.

V štvrtej kapitole sa už prakticky ukazuje akým spôsobom tieto služby zabezpečiť. Podrobne sú ukázané postupy pomocou Winboxu a terminálu. Sú ukázané postupy zabezpečenia konfiguračného prístupu, tvorba nových užívateľov, vypnutie služieb ako telnet, ftp alebo MAC Server a tvorba vlastného Firewallu. Táto kapitola taktiež obsahuje základný konfiguračný skript, pomocou ktorého si užívateľ dokáže nastaviť bezpečný smerovač.

V piatej a poslednej kapitole sa všetky tieto nastavenia testujú pomocou simulovaných útokov. Takýmto spôsobom sa porovnáva chovanie nezabezpečeného a zabezpečeného smerovača. Súčasťou je aj Linuxový skript pomocou ktorého si užívateľ dokáže tento proces testovania do určitej miery zautomatizovať a zjednodušiť.

V závere sú spísané dosiahnuté výsledky a poznatky získané vypracovaním tejto práce.

Ciele práce

Cielom tejto bakalárskej práce je preštudovať si možnosti zabezpečenia jednotlivých služieb a funkcií systému RouterOS vo verzií 7.x a porovnať ju so staršou verziou 6.x. Vytvoriť analýzu jednotlivých možností z hľadiska bezpečnosti a navrhnúť a realizovať tieto odporúčania na zariadenia s RouterOS. Po samotnej realizácii následne toto zabezpečenie aj otestovať a vytvoriť jednoduchý skript na automatickú konfiguráciu nového zariadenia a druhý na otestovanie zariadenia.

1 Známe odporúčania CISA a NSA

CISA je Agentúra pre kybernetickú bezpečnosť a bezpečnosť infraštruktúry v Spojených štátoch. Poskytujú aktuálne informácie z oblasti kyberbezpečnosti a vydávajú bezpečnostné odporúčania [3]. NSA je národná bezpečnostná agentúra, ktorá spadá pod ministerstvo obrany spojených štátov[4]. Obidve tieto organizácie vydali aj doporučenia na zabezpečenie sieťových zariadení, ktorými je dobré sa riadiť.

1.1 Všeobecné odporúčania

Je viac úrovní v ktorých sa dá zabezpečiť sieťová infraštruktúra. Už pri návrhu siete je potrebné myslieť na správnu segmentáciu aby sa znížili možnosti útočníkov. Pod správnu segmentáciou sa rozumie rozdelenie siete na menšie časti v ktorých budú zoskupené podobné zariadenia, aby sa obmedzilo prístupu k citlivým informáciám. Takýmto spôsobom sa napríklad oddelí časť siete pre zamestnancov alebo administrátorov či vnútorná sieť od vonkajšej a zabezpečí sa izolácia kritických zariadení. Medzi kritické zariadenia patria napríklad aj tlačiarne, pretože sú pre útočníkov ľahšie zneužitelné ako ochránené serveri alebo klientské počítače. Po fyzickom rozdelení je dôležité pre bezpečnosť aj oddeliť siete virtuálne, pomocou VLANiek. To zabezpečí virtuálnu segmentáciu a zároveň ušetrí použité hardwarové prostriedky.

Pri firmách, ktoré majú viacero pobočiek a potrebujú medzi sebou zdieľať prostriedky sa odporúča nastaviť site-to-site VPN. Ak zamestnanci potrebujú pracovať z domu a potrebujú prístup k prostriedkom, ktoré sa nachádzajú na firemnej sieti, použije sa klientská VPN. V oboch prípadoch sa vytvorí zabezpečený šifrovaný tunel cez internet. Takýmto spôsobom nebudú citlivé informácie prístupné pre neautorizovaných ľudí.

Brány VPN sú často náchylné na útoky hrubou silou, sieťové skenovanie a zero-day zraniteľnostiam. Sú prístupné z vonkajšej siete a preto je dôležité ich adekvátne zabezpečiť. NSA odporúča obmedziť prístup VPN brány na UDP port 500 a 4500 a ESP. Pri použití IPsec VPN tunela sa vyjednávajú parametre každej fázy, ktoré sa použijú pri vytvorení samotného tunela. Ak sa pri ktorejkoľvek fáze použijú slabé kryptografické prostriedky, bezpečnosť celého spojenia je ohrozená. Každá IKE politika obsahuje minimálne tri komponenty

- Diffie-Hellman algoritmus
- Šifrovací algoritmus
- Hashovací algoritmus

Minimálne odporúčania Výboru pre národné bezpečnostné systémy 15 pre tieto komponenty sú:

- Šifrovací algoritmus AES-256

- Hashovací algoritmus SHA-384
- Diffie-Hellman skupina 16 s modulárnym 4064 bitovým exponentom
- Diffie-Hellman skupina 20 s 384-bitovou skupinou eliptických kriviek

Nebezpečnými zadnými vrátkami do vnútornej siete pre útočníkov, môže byť aj nefiltrovaná peer-to-peer komunikácia. Preto sa odporúča filtrovať nepotrebné pakety pomocou firewall pravidiel a access listov. Prístup k zariadeniam a prostriedkom v sieti, ktoré bežne nie sú dostupné majú hlavne administrátori. Administrátorské oprávnenia by malo mať čo najmenej ľudí a mali by byť čo najviac chránené, pretože sú pre bezpečnosť kľúčové. Útočníci bežne útočia na slabý proces overovania, preto sa odporúča používať viac-faktorové overovanie užívateľov, autentifikačné servery a nastavovať silné heslá. Na správu siete používať oddelené zabezpečené kanály mimo ostatnej prevádzky. Kupovať a sťahovať software len z overených zdrojov. Pravidelne ho aktualizovať, pretože zastaraný software je náchylný na zneužitie zverejnených zraniteľností. Robiť si zálohy, ktoré ukladať na offline nosiče aby v prípade napadnutia útočníkom boli tieto informácie uložené aj inde a bola možnosť obnovy. Monitorovať prevádzku aby v prípade potreby bolo možné dohľadať čo sa stalo. Pravidelne školiť a trénovať zamestnancov o bezpečnostných hrozbách aby sa predišlo úniku informácií z vnútra organizácie [5].

1.2 Zabezpečenie sieťových zariadení

Jednou z veľmi dôležitých súčastí bezpečnosti infraštruktúry je bezpečné nastavenie samotných zariadení.

1.2.1 Správa účtov, autentizácia a autorizácia

Najbezpečnejší spôsob správy účtov je pomocou centralizovaných AAA serverov, pretože prihlasovacie údaje nie sú uložené priamo v zariadeniach. Prítomnosť týchto serverov v sieti taktiež zlepšuje konzistentnosť riadenia prístupu, obmedzuje údržbu konfigurácie a znižuje náklady na správu. NSA odporúča používať aspoň dva takéto servery, aby bola zabezpečená dostupnosť v prípade výpadku jedného z nich.

Ak centralizovaná autentizácia pomocou serverov zlyhá, je dôležité aby mali administrátori prístup na zariadenie aj pomocou lokálnych účtov. Tieto účty by mali spĺňať určité požiadavky. Väčšina zariadení má základný administrátorský účet, ktorý je verejne známy. Ako prvý krok, ešte pred vložením zariadenia do siete by malo byť vytvorenie nového účtu s unikátnym menom a silným heslom. Niektoré základné účty dokonca nemajú heslo vôbec, preto ho treba nastaviť. Následne základný účet vymazať, ak sa nedá tak ho premenovať, vypnúť alebo mu zmeniť oprávnenia. V organizáciách sa často menia zamestnanci, preto je dôležité také účty, ktoré patrili

ludom čo už pre organizáciu nepracujú pravidelne odstraňovať. Heslá sa ukladajú v zariadeniach v lokálnych databázach ako čitateľný nešifrovaný text, šifrovaný alebo v podobe hashu. Niektoré hashovacie a šifrovacie funkcie sa považujú za nebezpečné, preto by sa mali využívať tie najbezpečnejšie dostupné ako napríklad SHA-256 a lepšie pre hash funkcie a AES pre šifrovanie. Hlavné je nikdy heslá neukladať ako čitateľný text.

Zariadenia, ktoré používajú slabé heslá, sú náchylné na uhádnutie tohto hesla. Útočníci často využívajú verejne dostupné nástroje, ktoré sú pomocou slovníkov alebo hrubou silou schopné prelomiť tieto heslá a tým získať prístup do zariadenia a ohroziť bezpečnosť. Preto je dôležité nastaviť silné a unikátne heslá. Pod silných heslom sa predstavuje:

- aspoň 12 znakov dlhé
- rôzne od užívateľského mena
- rôzne od predchádzajúceho hesla
- nepoužívať prázdne, základné alebo verejne známe heslá
- používať rôzne znaky ako čísla, špeciálne znaky, veľké, malé písmená
- nepoužívať jedno heslo na viacerých miestach

Pravidelné zmeny hesla užívateľov odradzovalo a viedlo ku voľbe slabších hesiel. Preto toto odporúčanie, nie je také dôležité ak sa dodrží to, že sa použije silné heslo. Ak však príde ku odhaleniu hesla je potrebné ho okamžite zmeniť [7]. Ďalším spôsobom ako predchádzať útokom hrubou silou je obmedziť počet pokusov na prihlásenie. NSA odporúča nastaviť maximálny počet neúspešných pokusov na 3 a následne nastaviť časový limit na ďalšie prihlásenia.

1.2.2 Služby

Všetky sieťové zariadenia sú vybavené službami, ktoré sú od výroby povolené. Útočník však vypnuté služby využiť nevie, preto sa odporúča všetky nepoužívané zakázať [6].

Vzdialená správa

Služby vzdialeného prístupu sa využívajú na vzdialenú správu zariadení administrátormi. NSA odporúča používať len zašifrované služby ako SSH a zakázať tie, ktoré prenášajú komunikáciu ako otvorený text (Telnet, HTTP, SNMP v1 a v2c...).

Služby, ktoré prenášajú komunikáciu ako otvorený text boli vytvorené ešte pred rozšírením šifrovania. V dnešnej dobe by sa však nemali používať, pretože to môže viesť k odchyteniu tejto komunikácie a odhaleniu prihlasovacích alebo konfiguračných údajov.

Služby, ktoré používajú šifrovanie, potrebujú dostatočne silné algoritmy a kľúče aby ich spojenie nebolo možné prelomiť. To však môže spomaliť čas pripojenia.

- 3072 bitov pre asymetrické kľúče
- 384 bitov pre kľúče eliptických kriviek
- 256 bitov pre symetrické kľúče

Tiež je dôležité aby sa používali najnovšie verzie protokolov s primerane povolenými nastaveniami.

- SSHv2 na vzdialený prístup
- HTTP server s použitím TLS 1.2 a vyššie
- SNMPv3

TLS verzie 1.0 a 1.1 už nie sú podporované a nedokážu nadviazať bezpečné spojenie, keďže používali kombináciu MD5/SHA-1, ktoré sú považované za prelomené. TLS 1.2 používa len jeden hash a to SHA-256. Už je však dostupná aj lepšia verzia a to TLS 1.3, ktorá so sebou priniesla ešte lepšiu bezpečnosť. Nepodporuje nebezpečnú RC4 šifru, prenos kľúčov pomocou RSA, MD5 algoritmus, 3DES alebo CBC šifry [18].

Ak je potrebné používať SNMP, odporúča sa používať verzia 3, pretože podporuje šifrovanie komunikácie a autentifikáciu. Používa sa užívateľské meno, heslo a kľúč.

NSA odporúča obmedziť počet zariadení, ktoré sú oprávnené pripojiť sa k týmto službám vzdialeného prístupu len pre administrátorov pomocou ACL. Ak zariadenie nepodporuje ACL, je dobré ho umiestniť do špeciálnej VLAN, ktorá slúži na správu. V prípade, ak je obmedzený počet pripojení v jednom čase, odporúča sa nastaviť limit 5 minút a menej pre nečinné pripojenia, čo spôsobí automatické ukončenie spojenia po uplynutí časového limitu nečinnosti. Takýmto spôsobom sa predíde blokovaniu spojení. Ak by sa útočníkovi podarilo získať prístup pomocou administrátorského konta do zariadenia, vedel by toto pripojenie využiť na postup v sieti. Preto sa odporúča vypnúť odchádzajúce spojenia zo sieťových zariadení [7].

Protokoly FTP a TFTP sa používajú na vzdialený prenos dát medzi zariadeniami. Nepodporujú šifrovanie ani autentifikáciu preto sa tieto služby vypínajú, aby nedošlo k odchyteniu citlivých informácií. Ak je potrebné prenášať dáta vzdialene, odporúča sa použiť bezpečnejšiu verziu tohto protokolu a to SFTP, keďže dáta sa posielajú zašifrované cez SSH.

Discovery protokoly

CDP, LLDP, MNDP sú protokoly, ktoré automaticky posielajú informácie o topológii siete. Sú užitočné na získanie informácií o sieti ale sú aj nebezpečné, keďže si takýmto spôsobom útočník vie zistiť modely zariadení, verzie operačných systémov, MAC a IP adresy. NSA odporúča tieto protokoly vypnúť. Ak sú potrebné pre fungovanie

napríklad VoIP telefónov, povolia sa len na týchto rozhraniach alebo point-to-point spojeniach [7].

IP protokoly

Jeden z protokolov, ktorý nie je často využívaný ale existuje je **IP source routing**. Ten umožňuje užívateľovi poslať paket dopredu určenou cestou po sieti. Takýmto spôsobom dokáže útočník presmerovať pakety tak, aby obišli sieťové obmedzenia až k nemu. Táto služba je spojená so smerovaním ale dá sa využiť aj na prepínačoch, preto sa odporúča vypnúť na všetkých sieťových zariadeniach [7]. **IP Unreachables** sú ICMP správy, ktoré sa dajú využiť na zmapovanie siete. **IP Mask Reply** správy posielajú informácie o maske danej siete, preto sa obidve odporúčajú na rozhraniach vypnúť [6].

Protokoly určené na testovanie a monitorovanie

Existuje viacero protokolov, ktoré sa v systéme používa na monitorovanie a testovanie siete. Niektoré z nich majú svoje zraniteľnosti alebo nie sú využívané často, preto sa odporúčajú vypnúť. Medzi ne patria napríklad **Chargen Protocol**. Ďalší zo skupiny testovacích protokolov je **Daytime protocol**, ktorý odpovedá datagramom s aktuálnym časom [6].

1.2.3 Rozhrania a porty prepínačov

Porty rozhraní fyzicky spájajú sieťové zariadenia. Útočník musí získať fyzický prístup aby sa mohol pripojiť do siete. Správne nastavené porty môžu zabrániť útočníkovi v jeho úmysloch o narušenie fungovania siete alebo vynášania informácií.

Podobne ako je to pri nepoužívaných službách, tak aj nepoužívané porty na zariadeniach sa odporúča vypnúť.

Port security

Na portoch, ktoré sa aktívne využívajú sa odporúča nastaviť port security, kde sa nastaví maximálny počet pripojených MAC adries na jednu alebo dve (VoIP) pre každý port. Ak sa tento počet presiahne, port sa vypne. V prvom rade je však potrebné prepnúť port na statický, pretože na dynamickom sa port security nastaviť nedá. Toto opatrenie však nie je náhrada za NAC [7].

Dynamický trunk

Trunk je spojenie, na ktorom si zariadenia vymieňajú rámce s informáciami o VLAN-kách. Rozhranie sa dokáže automaticky nastaviť na trunk alebo access. Nie je to

však bezpečné preto sa odporúča po pridaní zariadenia do siete nastaviť všetky porty ručne na trunk alebo access [7].

Predvolená VLAN

Väčšina prepínačov používa VLAN 1 ako predvolenú, vrátane portov pre správu, ktoré si posielajú dôležité informácie po tejto VLAN. Keďže je to verejne známe z bezpečnostného hľadiska je preto dôležité aby sa táto VLAN vypla a všetka prevádzka správy siete sa presunula na iné VLAN. VLAN 1 sa odporúča vypnúť na všetkých trunk a access portoch aby sa predišlo posielaniu nepotrebných dát [7].

Proxy ARP

Technika pri ktorej proxy server odpovedá na ARP požiadavky v sieti. Je to však bezpečné len medzi dôveryhodnými LAN segmentami. Inak to predstavuje zraniteľnosť, ktorú útočník môže využiť. Preto sa proxy ARP odporúča vypnúť na všetkých rozhraniach v prípade ak sa zariadenie nepoužíva ako LAN bridge alebo na umožnenie prichádzajúceho NAT na viaceré cieľové IP adresy [7].

Monitorovanie portov

Monitorovanie je dôležité pre neskoršie riešenie problémov v sieti. Prevádzka z monitorovaného portu sa prekopíruje na iný port, na ktorom sa potom monitoruje. Nie je však dôležité monitorovať všetky porty. Preto sa odporúča vypnúť monitorovanie na všetkých nepoužívaných portoch a povoliť ho len na portoch kde je to nevyhnutné. Útočník toto monitorovanie môže využiť tak, že sa pripojí na cieľový port a odtiaľ môže odpočúvať celú prevádzku [7].

1.2.4 Aktualizácia hardwaru a softwaru

Zastaraný hardware alebo software predstavuje bezpečnostné riziko, keďže môže obsahovať známe zraniteľnosti. Toto riziko sa dá zmierniť pravidelnou aktualizáciou. Väčšina zariadení však nepodporuje automatickú aktualizáciu, preto je potrebné aktualizácie robiť ručne. Pred a počas používania by sa mala kontrolovať aj integrita samotného softwaru. Útočník môže zaviesť škodlivý kód do zariadenia úpravou súborov operačného systému, zavadzača alebo firmwaru. Pomocou takto upraveného softwaru môže útočník docieľiť únik citlivých dát alebo DoS útok. Integrita súborov operačného systému sa docieľi porovnaním kryptografického hashu so známym hashom od výrobcu pred a po nainštalovaní aby nedošlo k žiadnym zmenám. Na výpočet sa využíva hashovacia funkcia SHA-512 alebo MD5 pri starších zariadeniach. Jednoduchšie je však vykonať zmenu konfigurácie samotného zariadenia. Preto sa

odporúča vytvárať pravidelné zálohy a každú zmenu konfigurácie odôvodniť a zdokumentovať. Postupom času výrobca prestane podporovať konkrétne modely zariadení a v prípade poruchy ich nie je možné opraviť a aktualizovať software. Takéto zariadenia sa odporúča vymeniť za novšie modely.

Dodržiavaním týchto odporúčaní sa zníži riziko ohrozenia a zabezpečí sa bezpečnejšia a lepšie chránená sieť.

1.2.5 Monitorovanie a logovanie

Na sledovanie siete sa využíva logovanie a monitorovanie zariadení. Pomáha to na bližšie určenie príčiny výpadku, alebo bezpečnostného incidentu. Administrátori majú takýmto spôsobom možnosť sledovať a zistiť, čo sa v systéme stalo. Na to aby boli logovacie správy dostupné, je potrebné ich na zariadení zapnúť. NSA odporúča používať syslog logovanie. Nastaviť vnútornú vyrovnávaciu pamäť na minimálne 16 megabytov a zaviesť pravidelnú kontrolu a overovanie týchto správ.

Bezpečnejšia cesta ukladania logov je posielanie ich na centralizované logovacie servery. Tam sú chránené v prípade kompromitácie zariadenia, reštarte alebo zaplnenia vyrovnávajúcej pamäte. Na dosiahnutie redundancie a dostupnosti týchto správ sa odporúča používať aspoň dva logovacie servery. Aby však bol bezpečný aj prenos správ, je potrebné aby boli šifrované.

Na to aby boli logy časovo synchronizované je dobré aby všetky zariadenia vrátane logovacieho servera používali minimálne dva NTP servery, ktoré slúžia na získanie aktuálneho času. Takto sa zabezpečí, že zariadenia budú mať nastavený rovnaký čas, čo zjednoduší hľadanie logov z minulosti.

2 Odporúčania NÚKIB a smernica NIS2

2.1 Odporúčania NÚKIB

Každá krajina má svoj úrad, ktorý sa stará o kybernetickú bezpečnosť. V Českej republike je to NÚKIB[8]. Na ich stránkach sa nachádzajú odporúčania[9] pre administrátorov, ktoré pomáhajú zabezpečiť bezpečnejšiu sieť a zariadenia.

2.1.1 Infraštruktúra

Jednou z prvých vecí na ktoré je potrebné dávať pozor je práve segmentácia a segregácia siete, tak ako bolo podrobnejšie popísané v prvej kapitole 1.1. Vytvorí sa tak časť siete s rôznou úrovňou bezpečnosti.

Na detekciu a prevenciu prienikov používať systémy IDS a IPS. Tie pomocou signatúr a heuristiky pomôžu identifikovať a predchádzať škodlivým udalostiam. Systémy IPS a IDS sa odporúčajú nasadzovať pred firewall z pohľadu vnútornej siete. Keďže IPS a IDS vykonávajú hĺbkovú kontrolu paketov, majú za následok zníženie výkonnosti siete. Takto nebudú vystavené veľkému množstvu dát, ktoré prichádza z internetu, pretože sa vyfiltrujú pomocou firewallu a k IPS/IDS sa dostane len relevantná komunikácia.

Pre prípadne forenzné skúmanie sa odporúča uchovávať sieťovú komunikáciu z a do kritických zariadení minimálne 12 mesiacov. V prípade kritickej informačnej infraštruktúry a informačných systémov základnej služby sa podľa zákona o kybernetickej bezpečnosti a nadväzujúcich vyhlášok predlžuje táto doba na 18 mesiacov. Ak ide o sieť strategického významu je na mieste zvážiť aj automatické uchovávanie plného záznamu dátovej komunikácie. Pod kritickou informačnou infraštruktúrou sa rozumie všetko čo spĺňa kritéria uvedené v tomto dokumente[10].

Zabezpečiť centralizované a časovo synchronizované monitorovanie a logovanie, ktoré sa ukladá tiež po dobu minimálne 18 mesiacov.

Pri emailovej komunikácii odporúčajú kontrolovať jednotlivé emaily pomocou mechanizmov SPF (Sender Policy Framework) a DKIM (DomainKeys Identified Mail), ktoré obe slúžia na overovanie dôveryhodnosti emailu na základe domény. DMARC (Domain-based Message Authentication, Reporting and Conformance) je doplnok k vyššie uvedeným technológiám, ktorý umožňuje nastaviť požadované chovanie emailového serveru, keď obdrží podozrivý email. Jedna z nich je aj posielanie reportov [11]. Ak existujú v sieti emailové servery, je dobré zabezpečiť ich spojenie pomocou TLS. Týmto spôsobom sa zabezpečí šifrovanie správ a ich dôveryhodnosť. V ideálnom prípade je dobré použiť DANE (DNS-based Authentication of Name Entities), protokol, ktorý dovoľuje TLS certifikáty viazať na doménové mená pomocou DNSSEC.

V prípade volby mena emailovej domény je lepšie ak sa zvolí jednoduchý názov. To pomôže k lepšej identifikácii podvrhnutej vo phishingových emailoch.

Pomocou firewallu filtrovať len žiaducu komunikáciu z vonkajšej siete pomocou firewall pravidiel a povoliť na ňom len potrebné služby. To pomôže bezpečnosti a plynulosti komunikácie.

Proti DDoS útokom, ktoré ohrozujú správne fungovanie siete sa odporúčajú nasaďiť anti-DDoS technológie, pri ktorých sa ochránia celé IP rozsahy.

Môže sa stať, že príde k nečakanej situácii, ktorá spôsobí výpadok systému alebo siete. Na takéto situácie je dobré mať vypracovaný takzvaný disaster recovery plan. Dokument, ktorý obsahuje presný postup ako postupovať v krízových situáciách a tým minimalizovať následky. Príklad takejto situácie je napríklad výpadok prúdu, prírodná katastrofa, kybernetický útok, pád dôležitej aplikácie alebo porucha v dátovom centre [12]. Je dôležité mať pripravené zálohy a kontakty na ostatných administrátorov, nadriadených pracovníkov a bezpečnostné CERT/CSIRT tými [13].

2.1.2 Zariadenia

Severy, stanice, smerovače alebo prepínače majú operačné systémy a software, ktorý je potrebné pravidelne aktualizovať. Zastaralé môžu byť aj verzie firmwaru zariadení. Neodporúča sa používať produkty, ktoré sú end of life. Čo sa znamená, že sú nepodporované a nevychádzajú na nich nové aktualizácie.

Hardening by sa mal vykonávať nie len na samotných zariadeniach ale aj na užívateľských a serverových aplikáciách. Povoľovať len funkcie, ktoré sú pre prácu zamestnanca dôležité. Zakázať by sa mali makrá v MSOffice alebo flash vo webovom prehliadači.

Na ochranu pred zero-day zraniteľnosťami sa odporúčajú používať preventívne mechanizmy ako napríklad DEP (Data Execution Prevention), ktorý sa nachádza v operačnom systéme Windows ako ochrana pred spúšťaním kódu v určitých častiach pamäte, čo by malo za následok poškodenie systému.

Systémy IDP a IPS sa dajú aktivovať aj na koncových stanicach, čím sa môže detegovať anomálne chovanie ako zmena chránených registrových kľúčov, načítanie neznámych ovládačov alebo injekcia kódu do procesov.

S emailami ľudia posielajú aj rôzne prílohy v ktorých sa môže skrývať aj malware. Preto sa odporúča zablokovať všetky nepotrebné typy príloh ako je napríklad spustiteľný kód.

Na koncových stanicach a serveroch sa odporúča používať antivírusový program, šifrovať disky a používať zabezpečený trusted platform modul, na generovanie a ukladanie hesiel a kryptografických kľúčov. Nastaviť heslo pre UEFI/BIOS a vy-nucovať secure boot. Taktiež obmedziť prístup k server message blocku a netbiosu.

Pre správu zariadení na diaľku sa na prihlasovanie odporúčajú používať bezpečnostné kľúče a nie heslá. A na pripájanie užívateľov mimo sieť organizácie používať zabezpečený tunel VPN [13].

2.1.3 Správa účtov

Správne nastavenie užívateľských alebo administrátorských účtov je pre bezpečnosť dôležité. Preto by v organizácii mala byť zavedená jednotná bezpečnostná politika, kde je zavedená centrálna správa užívateľských účtov a oprávnení. Užívateľom, pri ktorých to nie je potrebné, zakázať inštaláciu softwaru, úpravy registrov a iné rozšírené oprávnenia.

Pri práci s citlivými informáciami sa odporúča používať viac faktorové overovanie.

Pre každého administrátora v sieti je potrebné vytvoriť vlastný účet so silným heslom a nepoužívať jeden zdieľaný. Na lokálnych účtoch staníc by mali byť nastavené unikátne heslá, na čo môže poslúžiť aj Local Administrator Password Solution na Windows.

Pri sieťových prvkoch by sa nemali používať základné prednastavené účty a heslá, keďže sú verejne známe a predstavujú riziko zásahu do bezpečnosti [13].

2.2 Smernica NIS2

Európska únia v roku 2016 schválila smernicu NIS, ktorá sa zaoberá bezpečnosťou sietí a informačných systémov. Členské štáty si následne mali túto smernicu transponovať do svojich právnych poriadkov. V roku 2020 však vydali druhú verziu tejto smernice a to NIS2, ktorá nahrádza pôvodnú smernicu.

V novej smernici sa rozširuje pôsobnosť na väčší okruh odvetví a subjektov, ktoré budú touto smernicou regulované. Po novom sa má vzťahovať aj na stredné a malé podniky v určitých odvetviach.

NIS (Network and Information Systems Directive) sa vzťahovala na takzvaných prevádzkovateľov základných služieb medzi ktorých patrili podniky, ktoré sa starali o dopravu, energetiku, zdravotníctvo a pod. Druhá skupina bola takzvaná poskytovatelia digitálnych služieb. Medzi ne patrili služby cloud computingu alebo internetové vyhľadávače. V smernici NIS2 sa tieto povinne subjekty po novom delia na základné a dôležité.

Medzi základné patria prevádzkovatelia základných služieb a po novom aj z digitálnych služieb napríklad siete pre doručovanie obsahu, služby dátových centier, služby elektronických komunikácií.

Medzi dôležité potom patria odvetvia ako poštové služby, výroba a distribúcia potravín, výroba počítačov a zdravotníckych prostriedkov alebo dopravných prostriedkov.

Samozrejme je tu oveľa viac odvetví a preto sa odporúča si tieto subjekty podrobne prečítať a zistiť či sa medzi nimi nenachádzate.

Veľmi dôležitá pri týchto odvetviach je aj veľkosť podnikov, podľa ktorej sa určuje či regulácia bude platiť. Keďže smernica sa vzťahuje na stredné a veľké podniky, ktoré určuje Komisia 2003/361/ES[14] podľa svojich kritérií. Za stredný podnik považujú podnik, ktorý ma viac ako 50 a menej ako 250 zamestnancov a ročný obrat do rozsahu 50 000 000 eur.

2.2.1 Povinnosti

Medzi povinnosti týchto subjektov patrí napríklad to, že si podnik musí vypracovať analýzu rizík a postup ako sa týmto rizikám vyvarovať. Zamerať sa na prevenciu a riešenie bezpečnostných incidentov. Zaznamenávať straty dát alebo útoky na sieť a následné ich nahlásiť príslušným národným orgánom. Mať zálohy v prípade výpadkov a byť schopný rýchlo obnoviť prevádzku. Zabezpečiť údržbu sietí a informačných systémov, robiť pravidelné aktualizácie a zverejňovať informácie o ich zraniteľnostiach. Mať v sieti firewall a iné zabezpečenia, mať zabezpečené koncové zariadenia, aktualizovaný software a silné heslá. Používať šifrovanie a robiť pravidelné testovania a auditu aby otestovali zavedené opatrenia. Vzdelávať svojich zamestnancov a kybernetickej bezpečnosti a bezpečnej práci s firemnými prostriedkami. Zabezpečiť si spoľahlivých dodávateľov IT služieb. Robiť si dokumentácie o aktívach a IT vybavení. Toto všetko by malo byť v spolupráci s národnými orgánmi aby sa predišlo kybernetickým útokom a aby subjekty boli dostatočne chránené. Je však potrebné myslieť na to, že presné povinnosti sa môžu líšiť podľa konkrétneho štátu.

Ak tieto pravidlá nedodržia hrozí im pokuta vo výške minimálne 10 000 000 eur[15, 16].

3 RouterOS

RouterOS je operačný systém od spoločnosti MikroTik, založený na jadre Linuxu. Beží primárne na MikroTik zariadeniach, avšak je možnosť ho aj virtualizovať [19].

3.1 RouterOS 7

V roku 2021 bola vydaná RouterOS verzia 7, ktorá so sebou priniesla viacero zmien a vylepšení. Hlavnou zmenou oproti RouterOS verzií 6 bol update Kernelu na verziu 5.6, ktorý umožnil pridanie nových funkcií a podporu nového hardwaru. Sľubovaných bolo mnoho zmien, ktoré mali napomôcť odľahčiť starší hardware a vylepšiť výkon. Prerobilo sa smerovanie, čo spôsobilo zlepšenie výkonu. Vytvoril sa nový User Manager a pridal sa ZeroTier support, ktorý otvoril nové možnosti virtualizácie a správy siete [20].

3.2 Kernel 3.3.5+ vs. Kernel 5.6

Najväčším rozdielom medzi RouterOS 6 a RouterOS 7 je zmena vo verzií kernelu. Kernel 3.3.5 vznikol v roku 2012 a kernel 5.6 až v roku 2020. Z bezpečnostného hľadiska to bol dobrý krok, keďže verzia 3.3.5 mala mnoho bezpečnostných hrozieb.

3.2.1 Bezpečnosť Linux Kernelu 3.3.5

Keďže táto verzia kernelu je na trhu už približne 10 rokov, za ten čas užívatelia objavili mnoho bezpečnostných chýb. Medzi najzávažnejšie patria tie, ktoré útočníkom dovoľujú spôsobiť DoS útok, čo spôsobí výpadok služby. DoS útoky sú najbežnejšie útoky na sieťové zariadenia. Ďalšie typy útokov sú zvýšenie privilégií a pretečenie buffera. Medzi najzávažnejšie zraniteľnosti kernelu 3.3.5 patria :

CVE-2013-6282 - tu boli zraniteľné funkcie API na platformách v6k a v7 ARM, ktoré neoverovali určité adresy, čo umožnilo útočníkom čítať alebo modifikovať pamäť jadra prostredníctvom aplikácie [21].

CVE-2013-4587 - chyba indexu poľa vo funkcii v podsystéme KVM umožňuje lokálnym používateľom získať oprávnenia pomocou veľkej hodnoty id [22].

CVE-2013-4563 - zraniteľnosť, ktorá spôsobila vzdialeným používateľom možnosť DoS útoku prostredníctvom veľkého balenia IPv6 UDP. Pri zapnutom UDP Fragmentation Offload sa nevykoná správne porovnanie veľkosti pred vložením do hlavičky fragmentu [23].

CVE-2012-3400 - zraniteľnosť, v ktorej dochádza ku odmietnutiu služby alebo k iným nešpecifikovaným dopadom kvôli preplneniu zásobníka haldy vo funkcii `udf_load_logicavol` pri vytvorení súborového systému UDF [24].

CVE-2013-7027 - zraniteľnosť, ktorá môže spôsobiť odmietnutie služby, prostredníctvom vytvorenej hlavičky. Funkcia `ieee80211_radiotap_iterator_init` nekontroluje, či rámec obsahuje údaje mimo hlavičky [25].

3.2.2 Bezpečnosť Linux Kernelu 5.6

Verzia 5.6 má len dve známe slabosti a to konkrétne CVE-2020-14381 a CVE-2022-1419.

CVE-2022-1419 môže spôsobiť race condition v ovládači virtuálneho GPU vgem, ktorý môže viesť k use-after-free. Lokálny používateľ s povoleným prístupom k zariadeniu GPU to môže zneužiť na spôsobenie odmietnutia služby (pád alebo poškodenie pamäte), prípadne na zvýšenie oprávnení [26]. Toto sa však netýka sieťových zariadení.

CVE-2020-14381 je chyba, ktorá umožňuje lokálnemu užívateľovi poškodiť systémovú pamäť, alebo zvýšiť svoje oprávnenia pri vytváraní futexu na súborovom systéme [27]. Tiež však neovplyvňuje bezpečnosť smerovačov.

Do dnešného dňa sa neobjavili žiadne bezpečnostné hrozby spojené s verziou kernelu 5.6, ktoré by spôsobili ohrozenie zariadenia bežiacie na verzií RouterOS 7.

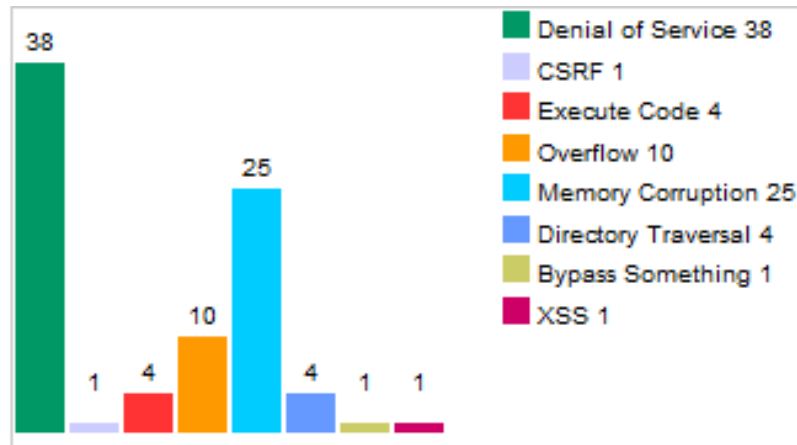
3.3 Zraniteľnosti RouterOS 7 vs RouterOS 6

Za posledných 13 rokov sa objavilo mnoho zraniteľností samotného operačného systému, ktoré útočníci mohli využiť a užívatelia sa proti nim museli zabezpečiť rôznymi spôsobmi. Ako sa už v tejto práci spomínalo medzi najčastejšie útoky na sieťové zariadenia a v tomto prípade aj na MikroTik a RouterOS sú Denial of Service, teda odmietnutie služby a poškodenie pamäte. Ďalšie zraniteľnosti sú spomenuté v nasledujúcom grafe(3.1).

3.3.1 RouterOS 6

Asi jedna z najznámejších zraniteľností v RouterOS 6.41.2 bola **CVE-2018-7445 - SMB memory corruption**. Bola objavená v roku 2018 a jedná sa o SMB pretečenie buffera pri spracovávaní požiadaviek na reláciu NetBIOS. Zraniteľnosť je možné zneužiť vzdialene a môže ju vykonať neoverený útočník. Keďže je však SMB služba zo základu v RouterOS vypnutá, pravdepodobnosť zneužitia je oveľa menšia [28].

Obr. 3.1: Známe zraniteľnosti RouterOS od roku 2009



Pred verziami 6.42.7 a 6.40.9 bol RouterOS zraniteľný na pretečenie zásobníka cez rozhranie na aktualizáciu licencie. Vzdialený overený útočník dokáže vďaka tejto zraniteľnosti spustiť ľubovoľný kód v systéme. Táto zraniteľnosť je známa pod označením CVE-2018-1156 [29].

Vo verzii 6.38.5 je RouterOS zraniteľný na záplavový útok, od neovereného útočníka, ktorý na diaľku dokáže vyčerpať všetky prostriedky CPU.

Takýchto podobných útokov je veľké množstvo, preto je potrebné si sledovať najnovšie zraniteľnosti a pravidelne aktualizovať systém.

3.3.2 RouterOS 7

RouterOS 7 je relatívne nový operačný systém, preto tých známych zraniteľností nie je až také množstvo. Napriek tomu však nie je bez chyby.

25.8.2022 bola publikovaná zraniteľnosť RouterOS 7.4 s označením CVE-2022-34960. Pomocou tejto zraniteľnosti dokáže útočník vytvoriť body, smerujúce na symbolické odkazy v systéme a tým dokáže umiestniť ľubovoľný súbor na ľubovoľné miesto v systéme [30].

Až do verzie RouterOS 7.0 Beta 5 bol tento operačný systém zraniteľný na zrušenie SMB servera prostredníctvom upravených paketov, kvôli chybe s indexáciou poľa systému [31].

Sú aj zraniteľnosti, ktoré pretrvávajú dlhšiu dobu a jednou z nich je aj zraniteľnosť s označením CVE-2018-5951. Jedná sa o chybu systému, kedy sa po odoslaní paketu veľkosti 1 bajt na ipv6 adresu s protokolom IP 97, reštartuje RouterOS [32].

3.4 Pridané služby RouterOS 7

Ako už bolo spomínané, RouterOS 7 priniesol so sebou veľa zmien. Medzi zmeny, ktoré ovplyvnili bezpečnosť patria nasledovné.

3.4.1 WifiWave 2

WifiWave2, prídavný programový balíček, pridáva novú funkcionality bezdrôtových sietí a podporu štandardov 802.11ac a 802.11ax. Na zariadeniach, ktoré podporujú 802.11ax štandard je tento balíček nainštalovaný automaticky. Pri RouterOS 7 môže byť tento balíček pridaný po stiahnutí a nainštalovaní. Rozhrania wifiwave2 sa konfigurujú v záložke Wireless v nástroji WinBox alebo WebFig. Pri konfigurovaní pomocou CLI sa menia príkazy oproti klasickému bezdrôtovému rozhraniu. Príchodom wifiwave 2 sa pridali nové možnosti autentifikácie a to WPA3 šifrovanie [33].

Podpora WPA3

V roku 2018 sa predstavil novší šifrovací algoritmus WPA3, ktorý je dostupný pre najnovšie bezpečnostné štandardy 802.11ac a 802.11ax. Oproti WPA2 prichádza WPA3 s ďalšími bezpečnostnými vylepšeniami. Chráni pred slabými heslami, ktoré sa dajú pomerne ľahko prelomiť hádaním. WPA2 fungovala na 4-way handshake, ktorý je náchylný na takzvané KRACK útoky. WPA3 už túto zraniteľnosť nemá, pretože používa Dragonfly výmenu kľúčov, ktorá je odolná voči offline dešifrovaniu a slovníkovým útokom [34].

OWE

Oportunistické bezdrôtové šifrovanie je nová funkcia WPA3, ktorá nahrádza overovanie 802.11, ktoré sa bežne používa v bezdrôtových prístupových bodoch. Hlavnou myšlienkou je použitie Diffie-Hellman mechanizmu výmeny kľúčov medzi zariadením a prístupovým bodom. Toto zabezpečuje, že aj pri odpočúvaní komunikácie nie je možné dešifrovať kľúč, pretože kľúč sa mení každou komunikáciou. Veľkou výhodou je, že OWE šifruje komunikáciu aj otvoreným sieťam bez hesla [34].

802.11w

Súčasťou balíčka wifiwave2 je aj 802.11w protokol, ktorý sa aplikuje na robustné riadiace rámce pri bezdrôtovej komunikácii. Konkrétne rámce asociácie, disasociácie, autentifikácie a de-autentifikácie, ktoré sa používajú na nadviazanie alebo zrušenie spojenia. Tieto rámce nemôžu byť šifrované narozdiel od dát, preto sú náchylné na

odposluch a následne na podvrh ak nie sú chránené iným spôsobom. Ochrana klienta sa realizuje tak, že prístupový bod pridá do rámcov ochranu na tieto rámce čím sa zabráni ich podvrhnutiu. Ochrana infraštruktúry sa pridáva pridaním ochranných mechanizmov, ktoré zabránia podvrhutej žiadosti o asociáciu odpojiť už pripojeného klienta [35].

3.4.2 WireGuard

Príchodom nového kernelu prišla aj podpora WireGuard VPN. Pôvodne navrhnutá pre Linux, dnes multiplatformová a široko nasaditeľná. Je známa používaním modernej kryptografie a jednoduchou konfiguráciou. Keďže WireGuard je obmedzený len na malé množstvo šifrovacích algoritmov, z ktorých všetky sú bezpečné, užívateľ nemá možnosť si zvoliť nezabezpečenú možnosť ako v prípade IPsecu, ktorý má veľa možností medzi ktorými sa nachádzajú aj staršie metódy overovania ako je PSK. Aj napriek tomu, že sa tieto možnosti nepovažujú v súčasnej dobe za bezpečné, IPsec užívateľ má možnosť si takúto metódu vybrať a ohroziť tak bezpečnosť VPN. Z tohto dôvodu sa WireGuard považuje za bezpečnejšiu možnosť ako IPsec. Konfigurácia je jednoduchá ako na strane servera tak na strane klienta. Treba si však dávať pozor na to, že po definovaní sietí, ktoré budú súčasťou VPN tunelu treba tento tunel povoliť aj pomocou firewall pravidiel. Tam je zo základu zakázaný [36]. RouterOS podporuje viacero typov VPN tunelov, ktoré sa dajú použiť. Jedným z nich je PPTP, ktorý používa šifru RC4 a malé kľúče. Je starý a nespoľahlivý, ľahko blokovateľný firewallom. Preto sa odporúča používať IPsec, alebo práve WireGuard.

3.4.3 Let's Encrypt certifikáty

Od verzie RouterOS 7 je k dispozícii certifikačná autorita, pomocou ktorej sa dá vygenerovať certifikát pre www-ssl službu, na podporu HTTPS. Potrebne sú na to verejná IP adresa a doménové meno. Generuje sa cez terminál a takýto certifikát má platnosť 90 dní. Po 90 dňoch sa dá vygenerovať nový. Vec na ktorú si treba dávať pozor je to, že si treba skontrolovať platnosť doménového mena a dostupnosť portu 80 z WAN rozhrania [37].

3.5 Analýza bezpečnosti RouterOS služieb

RouterOS tak ako aj iné operačné systémy od iných výrobcov obsahujú podobné služby. Niektoré sa využívajú viac ako ostatné a niektoré sú špecifické pre daný operačný systém. V tejto podkapitole sa nachádzajú služby a protokoly, ktoré sa v

RouterOS používajú najčastejšie a treba ich správne zabezpečiť alebo sa starať o bezpečnosť zariadenia.

3.5.1 Konfiguračný prístup

Winbox

Medzi najčastejšie metódy prístupu do zariadenia sa využíva práve Winbox. Jednoduchý multiplatformový program, ktorý používa rýchle grafické rozhranie. Na pripojenie k zariadeniu je potrebné zadať IP adresu, alebo MAC adresu zariadenia, meno a heslo. Dá sa využiť aj takzvaný “neighbor discovery”, ktorý vypíše aktuálne dostupných susedov v sieti, z ktorých sa dá vybrať. Winbox podporuje aj IPv6 adresy, musia byť však napísané v hranatých zátvorkách.

Z bezpečnostného hľadiska je na Winboxe zaujímavé to, že nie sú možné takzvané “Man in the middle” útoky, keďže potvrdzovanie znalosti hesla prebieha na oboch stranách spojenia. Celé spojenie je šifrované pomocou AES 128-CBC-SHA algoritmu a na výmenu kľúčov sa používa ECSR. [38].

SSH - Secure Shell

Prístup ktorý sa odporúča využívať v produkčných sieťach hlavne kvôli bezpečnosti spojenia sa nazýva SSH. Je určený na vzdialený prístup alebo prenos dát. Vznikol ako náhrada za telnet, ktorý je považovaný za nebezpečný pretože sa komunikácia posiela nešifrovaná. Komunikácia pomocou SSH je šifrovaná a zabezpečuje autentifikáciu oboch účastníkov komunikácie. Funguje na princípe klient-server.

RouterOS má vstavaný SSH server, ktorý počúva na porte 22. Dá sa však aj vypnúť alebo zmeniť číslo portu, čo sa aj z bezpečnostného hľadiska odporúča. Taktiež je dobré zapnúť strong crypto, čo zabezpečí lepšie šifrovanie a silnejšie kľúče.

Špecifikácie strong-crypto oproti základnému SSH:

- Uprednostňuje 256 a 192 bitové šifrovanie namiesto 128.
- Preferuje funkciu sha256 pred sha1
- Nepoužíva md5 šifru
- Používa 2048 bitové prvočísla pre Diffie Hellman výmenu kľúčov namiesto 1024 bitových.

MAC Server

V tejto sekcii sa nastavujú MAC Telnet, MAC WinBox Server a MAC Ping Server. Všetky tieto nástroje umožňujú komunikáciu pomocou MAC adresy zariadenia a sú v

RouterOS povolené na všetkých portoch. Z bezpečnostného hľadiska sa doporučuje tieto nástroje vypnúť, alebo obmedziť len na určité porty. Dôvod, prečo sa tieto služby vypínajú a považujú za nebezpečné je ten, že sa MAC adresa jednoducho podvrhne útočníkom.

3.5.2 Bezdrôtové siete

RouterOS ponúka veľké množstvo možností nastavení bezdrôtových sietí a podporuje množstvo prídavných modulov pre bezdrôtovú komunikáciu. V RouterOS 7 je možnosť nainštalovať balíček WifiWave2, ktorý obsahuje lepší šifrovací algoritmus na zabezpečenie bezdrôtového spojenia a to WPA3, ktorý je popísaný v časti 3.4.1.

Blacklist - Whitelist

Ďalšiu možnosť zabezpečenia prístupového bodu sa dá dosiahnuť pomocou volieb "Default Authenticate" alebo "Default Forward". Default Forward slúži k zákazu komunikácie medzi klientmi pripojenými na prístupový bod v rovnakom radiu.

Ak je Default Authenticate možnosť povolená, pre prístupový bod to znamená, že sa môžu pripojiť všetky zariadenia, okrem tých, ktoré sú v access liste zakázané. Ak je Default Authenticate vypnutá, prístupový bod si kontroluje Access List a potom rozhodne, či pripojenie povolí alebo nie.

Access List

Používa sa na definovanie pravidiel podľa ktorých prístupový bod povolí alebo zamietne pripojenie. Pravidlá sú spracovávané postupne zhora nadol. Použije sa prvé zhodujúce sa pravidlo a ďalej sa nepokračuje. Ak sa nenájde žiadne zhodujúce sa pravidlo, použije sa predvolená hodnota, ktorá je nastavená na bezdrôtovom rozhraní. Ak je default authenticate možnosť vypnutá a prístupový bod si kontroluje každý pokus o pripojenie v access liste, je potrebné aby tu boli definované všetky povolené MAC adresy a všetky zakázané. Ak sa MAC adresa zariadenia nezhoduje so žiadnym pravidlom jej prístup je zamietnutý[33].

3.5.3 Firewall

Firewall je dôležitou súčasťou zabezpečenia RouterOS a samotnej siete. Slúži na filtrovanie sieťovej komunikácie na základe zadaných pravidiel. Využíva stavovú kontrolu paketov. RouterOS beží na jadre Linuxu, preto využíva iptables.

Domáce MikroTik smerovače už majú v sebe prednastavené základné firewall pravidlá, ktoré sa odporúča nechať zapnuté a na pokročilejšie filtrovanie si pridať svoje vlastné.

V základnom nastavení má firewall len pár statických pravidiel, ktoré väčšine užívateľom stačí, nechráni ich však v prípade keď je smerovač viditeľný cez verejnú IP adresu smerom z internetu. Tým sa dá predchádzať skenovaniu od port skenerov alebo DoS útokom [39].

Pri vytváraní pravidiel, je potrebné myslieť na to, aké hardwarové prostriedky máme k dispozícii. Môže sa totiž stať, že si vytvoríme také množstvo pravidiel, že to nás smerovač nemusí ustáť.

Zadávať pravidlá sa pomocou príkazového riadku. Nevýhoda tohto prístupu je však v tom, že keď je potrebné zmeniť poradie pravidiel, treba pravidlá vymazať a pridať v správnom poradí. Konfigurácia pomocou Winboxu je preto jednoduchšia a pohodlnejšia.

Pravidlá sa skladajú z dvoch častí a to matcher a action. Matcher sú parametre podľa ktorých sa vyberie paket a action je akcia ktorá sa vykoná a určuje čo sa s paketom stane. Jednoduchšie pravidlá by sa mali písať prvé a postupne prejsť k zložitejším.

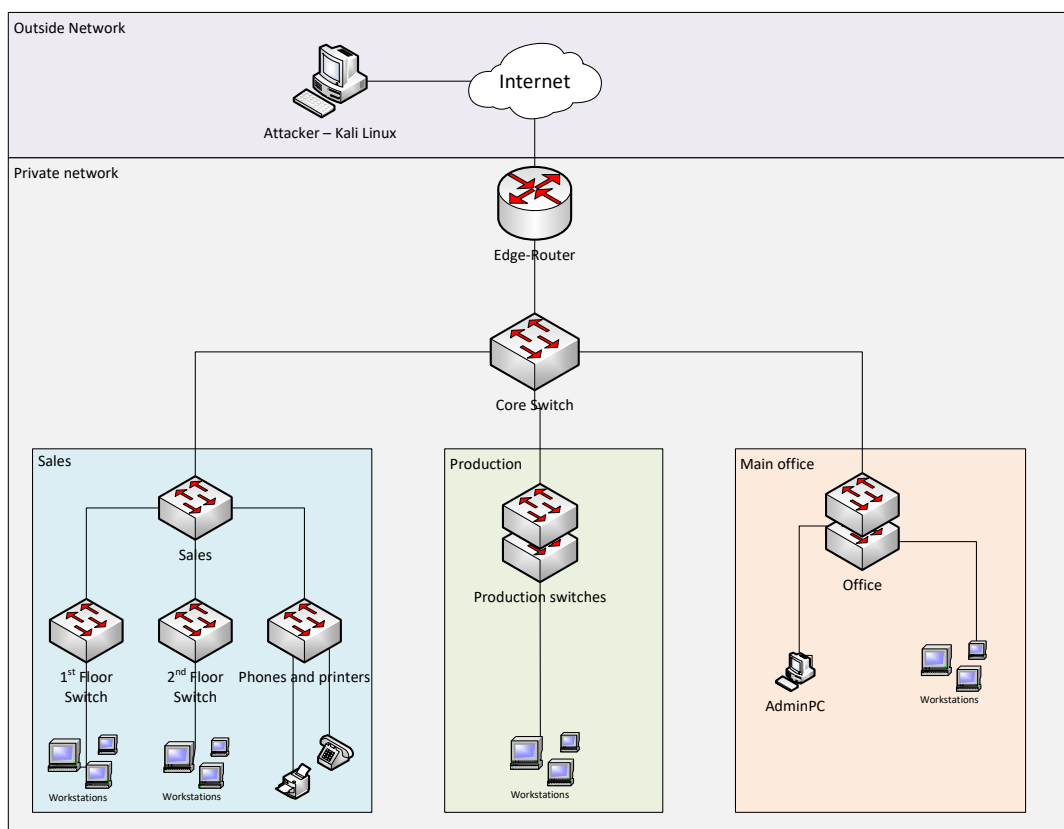
4 Návrh zabezpečenia služieb RouterOS

Po analýze bezpečnostných odporúčaní a rizík RouterOS nasleduje implementácia konkrétneho riešenia. Každý si musí zväžiť, čo potrebuje chrániť a akým spôsobom to chce dosiahnuť. Cieľom tejto časti práce je navrhnuť zabezpečenie firemnej siete pred neautorizovaným prístupom do zariadení a pred DoS útokmi na sieťové zariadenia, ktoré by mohli spôsobiť vyradenie prevádzky.

4.1 Príprava topológie a prostredia

Pre demonštráciu sa vytvorila jednoduchá topológia firemnej siete v ktorej sa nachádza zariadenie na ktorom beží RouterOS 7.8. Toto zariadenie sa bude zabezpečovať a následne testovať. Edge Router slúži ako hraničný smerovač a spája vnútornú sieť s internetom (4.1).

Obr. 4.1: Návrh testovacej siete

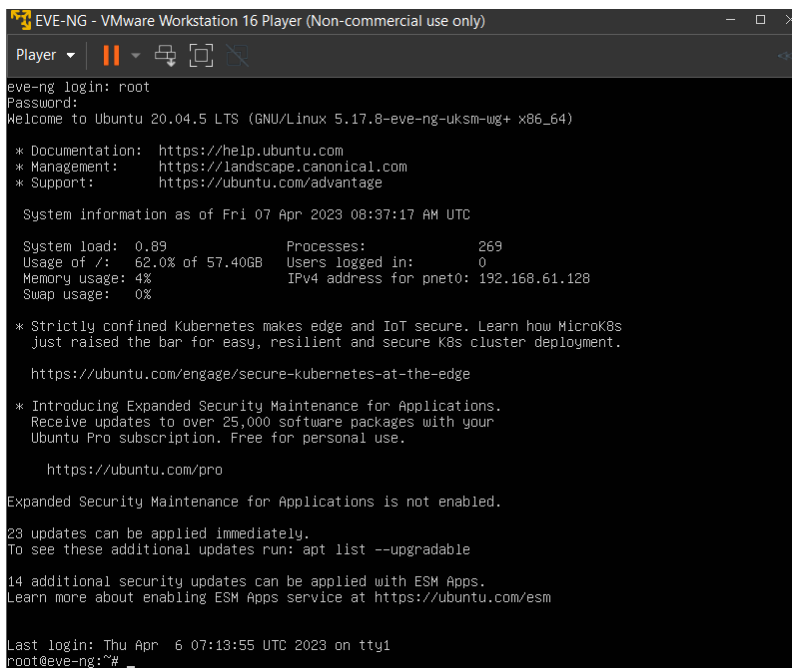


Na simuláciu sa využíva virtuálne prostredie EVE-NG Community, vďaka ktorému sa dá vytvoriť simulovaná sieť virtuálnych a fyzických zariadení.

4.1.1 Príprava EVE-NG

EVE-NG server beží ako virtuálny stroj v programe VMWare Workstation. Iso je dostupné na oficiálnych stránkach EVE-NG, odkiaľ sa dá stiahnuť a nainštalovať. V tejto práci sa používa community verzia, ktorá je voľne dostupná a pre potreby tejto práce dostačujúca. Podrobný návod inštalácie je dostupný v dokumentácií.

Obr. 4.2: Nainštalovaný virtuálny EVE-NG server



```
EVE-NG - VMware Workstation 16 Player (Non-commercial use only)
Player
eve-ng login: root
Password:
Welcome to Ubuntu 20.04.5 LTS (GNU/Linux 5.17.8-eve-ng-uksm-wg+ x86_64)

* Documentation:  https://help.ubuntu.com
* Management:    https://landscape.canonical.com
* Support:       https://ubuntu.com/advantage

System information as of Fri 07 Apr 2023 08:37:17 AM UTC

System load:  0.89          Processes:      269
Usage of /:   62.0% of 57.40GB  Users logged in:  0
Memory usage: 4%           IPv4 address for pnet0: 192.168.61.128
Swap usage:   0%

* Strictly confined Kubernetes makes edge and IoT secure. Learn how MicroK8s
  just raised the bar for easy, resilient and secure K8s cluster deployment.

  https://ubuntu.com/engage/secure-kubernetes-at-the-edge

* Introducing Expanded Security Maintenance for Applications.
  Receive updates to over 25,000 software packages with your
  Ubuntu Pro subscription. Free for personal use.

  https://ubuntu.com/pro

Expanded Security Maintenance for Applications is not enabled.

23 updates can be applied immediately.
To see these additional updates run: apt list --upgradable

14 additional security updates can be applied with ESM Apps.
Learn more about enabling ESM Apps service at https://ubuntu.com/esm

Last login: Thu Apr  6 07:13:55 UTC 2023 on tty1
root@eve-ng:~#
```

Po prihlásení a obdržaní IP adresy sa môže prejsť na prihlásenie cez webové rozhranie. Do prehliadača sa zadá IP adresa servera v tomto prípade `http://192.168.61.128`. Zobrazí sa základné prihlasovacie okno, do ktorého sa zadajú užívateľské meno a heslo (admin/eve). Po prihlásení sa objaví file manager, kde sú vypísané všetky vytvorené laby. Keďže na začiatku je tento file manager prázdny, je potrebné si vytvoriť prvý lab. Pomocou možnosti add new lab sa vytvorí nový lab, kde je potrebné zadať názov a ostatné voliteľné informácie ako meno autora, popis alebo úlohy.

Po vytvorení sa môžu začať pridávať zariadenia, ktoré sa nazývajú "nodes". Tieto nody predstavujú virtuálne zariadenia do ktorých treba nahráť reálne operačné systémy zariadení. EVE-NG podporuje veľké množstvo obrazov sieťových zariadení ale aj počítačov.

Vloženie RouterOS

Pre virtuálne prostredie sa používa Mikrotik Cloud Router z oficiálnej Mikrotik web stránky. Následne sa pomocou SSH pripojí na EVE-NG server a vytvorí sa

Obr. 4.3: Vytvorenie nového labu

The screenshot shows the 'Add New Lab' form in the EVE-NG File Manager. The form has the following fields and values:

- Name***: Mikrotik (with a note: Use only [A-Za-z0-9_]chars)
- Version***: 1 (with a note: Must be interger ([0-9]chars))
- Author**: Vanesa Kociska
- Config Script Timeout**: 300 (with a note: Seconds)
- Description**: Ente
- Tasks**: Ente

* - Required Fields

priečinok.

```
mkdir /opt/unetlab/addons/qemu/mikrotik-7.8/
```

Pomocou programu SCP sa nahrá stiahnutý obraz operačného systému do zvoleného priečinka a následne sa obraz prekonvertuje na správny formát, aby ho eveng bol schopný prečítať.

```
cd /opt/unetlab/addons/qemu/mikrotik-7.8/  
mv chr-6.40.4.img hda.qcow2
```

Posledným krokom je opraviť povolenia pomocou príkazu

```
/opt/unetlab/wrappers/unl_wrapper -a fixpermissions
```

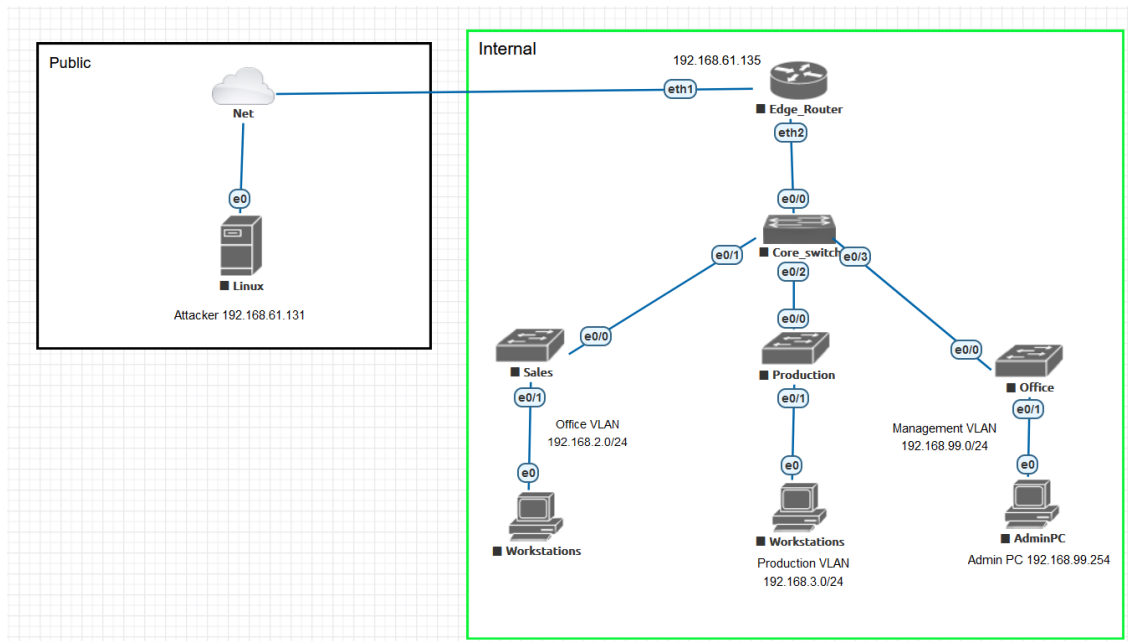
Pre rôzne operačné systémy sú dostupné podrobné návody dostupné aj v sekcií Documentation -> How to create images na stránkach EVE-NG. V tejto práci sa používajú obrazy systémov RouterOS, Cisco IOL switch, Kali Linux a Windows 7.

Po nahraní všetkých zariadení sa vytvorí požadovaná topológia (4.4). Okrem zariadení sa dajú pridávať aj rôzne tvary, texty, obrázky a prepojenia.

Popis topológie

Topológia je rozdelená na dve časti. Vonkajšiu, ktorá reprezentuje nezabezpečenú sieť internet a vnútornú, ktorá predstavuje zabezpečenú sieť firmy. Tento návrh

Obr. 4.4: Zapojenie siete v EVE-NG



predstavuje jednoduchú možnosť rozdelenia siete na 3 časti. Oddelenia sú segmentované fyzicky a zároveň aj virtuálne pomocou VLAN sietí. Nachádza sa tu aj sieť výhradne pre správu a to konkrétne Management, do ktorej majú prístup len administrátori siete. Takýmto spôsobom môžu spravovať zariadenia bezpečne mimo ostatnej prevádzky.

Sieť pozostáva z Windows 7 počítačov, ktoré reprezentujú klientov v sieti. V pravej časti sa nachádza Admin PC, pomocou ktorého sa pristupuje na hlavný smerovač. Smerovač a klienti sú prepojený pomocou Cisco prepínačov, na ktorých je len jednoduchá konfigurácie VLAN sietí. Hlavnou časťou tejto siete je Edge Router, na ktorom je nahraný RouterOS 7.8. Tento smerovač oddeľuje sieť od internetu a sú na ňom nastavené bezpečnostné opatrenia. Edge Router je prepojený s cloudom, ktorý predstavuje internet a za týmto cloudom sa nachádza klient, ktorý predstavuje útočníka. Pomocou tohto počítača sa budú simulovať útoky na smerovač, pomocou ktorých sa otestuje zabezpečenie vnútornej siete.

Virtuálne prostredie je pripravené a môže sa prejsť na samotné nastavenia smerovača.

4.2 Aktualizácia systému

Jedným z prvých krokov pri zabezpečovaní RouterOS je, udržiavať systém aktualizovaný. Každá verzia má svoje slabosti, ktoré vývojári časom opravujú. Vo Winboxe

alebo Webfigu je možnosť zapnúť možnosť check for updates. Vtedy bude smerovač kontrolovať, či je na serveri k dispozícii nová verzia operačného systému. Samotnú aktualizáciu je potrebné spustiť manuálne. Aktualizovať by sa malo len na stabilné verzie a prečítať si denník zmien, ktoré nová verzia systému prináša, aby sa nám nestalo, že nám aktualizáciou prestala fungovať funkcia, ktorú používame.

4.3 Prístup do zariadenia

4.3.1 Vytvorenie užívateľa

V základe je v RouterOS len jeden užívateľ a to administrátor bez hesla s plnými právami. Toto je potrebné zmeniť. Najlepší spôsob je pridať nový užívateľský účet. To sa dosiahne pomocou :

- *System -> Users*
- Pomocou tlačítka + sa vytvorí nový užívateľ
- Vyplní sa meno na iné ako admin
- Zvolí sa *permission group = full*, aby mal užívateľ plné práva
- Novému užívateľovi je potrebné nastaviť silné heslo, preto je dobré použiť generátor na heslá, kde sa vygeneruje minimálne 12 znakové heslo.
- Na ešte bezpečnejší prístup do zariadenia sa povolí prístup len z konkrétnej IP adresy. Do políčka *Allowed address* sa zapíše konkrétna adresa alebo adresný priestor v tomto prípade to je adresa administrátorského počítača.
- Užívateľ sa vytvorí *Apply* a *OK*(4.5) [40].

Obr. 4.5: Vytvorenie nového užívateľa

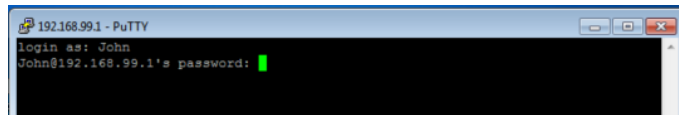
The screenshot shows the 'User <John>' configuration window in RouterOS. The 'Name' field is set to 'John', 'Group' is 'full', 'Allowed Address' is '192.168.99.254', and 'Last Logged In' is 'Apr/11/2023 11:06:42'. A 'Change Password' dialog box is open, prompting for a 'New Password' and 'Confirm Password', both shown as asterisks. The main window has buttons for 'OK', 'Cancel', 'Apply', 'Disable', 'Comment', 'Copy', 'Remove', 'Password...', and 'Expire Password'. At the bottom, there are checkboxes for 'enabled' and 'expired'.

Alebo pomocou terminálu kde sa zadá príkaz :

```
/user add name=John password=7FbbKwHNt4Cj group=full  
/user set 0 allowed-address=192.168.99.254  
/user remove admin
```

Následne sa odstráni základný účet admin. Ak je vo firme viacero administrátorov, dá sa vytvoriť viacero účtov s rôznymi právami poprípade skupina užívateľov.

Obr. 4.6: Prihlásenie pomocou SSH s novým užívateľom



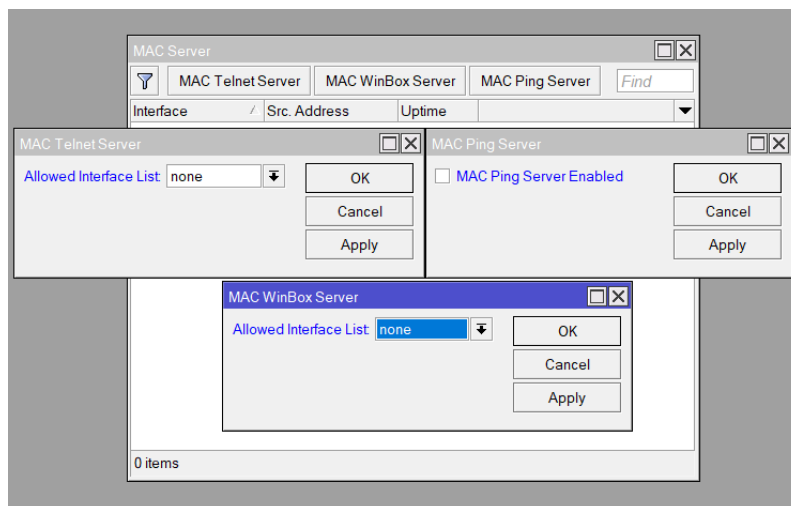
Na obrázku (4.6) je vidieť prihlásenie pomocou novo vytvoreného užívateľa.

4.3.2 Mac Server

RouterOS má možnosť ľahkého prístupu na zariadenie pomocou MAC adresy. V produkčných sieťach sa to neodporúča používať preto sa to vyplo pomocou :(4.7).

- *Tools -> MAC server*
- *MAC Telnet Server -> Allowed interface list -> none*
- *MAC Winbox Server -> Allowed interface list -> none*
- *MAC Ping Server -> Odkliknúť možnosť MAC Ping Server Enabled*

Obr. 4.7: Vypnutie MAC služieb



```
/tool mac-server set allowed-interface-list=none
```

```
/tool mac-server mac-winbox set allowed-interface-list=none
/tool mac-server ping set enabled=no
```

Úplne vypnutie nie je v niektorých situáciach žiaduce, pretože pri problémoch s pripojením na IP, môže prísť vhod pripojenie cez MAC adresu. Táto alternatíva sa zabezpečí tým, že sa MAC Winbox Server povolí len pre VLAN, ktorá je určená pre administráciu alebo konkrétne rozhranie.

4.3.3 Bezpečný prístup

Všetky zariadenia v produkcii musia používať zabezpečený prístup cez SSH, zabezpečený Winbox alebo Webfig cez HTTPS. Vo Winboxe sa zaklikne možnosť *Secure Mode*. V novších verziách RouterOS už je táto možnosť zapnutá automaticky, preto nie je táto možnosť na výber.

Bezpečnejšie SSH, ktoré sa aj odporúča používať sa nastavuje pomocou príkazu:

```
/ip ssh set strong-crypto=yes
```

Toto nastavenie zabezpečilo, že sa zamietnu ssh spojenia s klientmi, ktorých šifrovacie algoritmy sa považujú za slabé.

4.4 Vypnúť nepoužívané rozhrania

Dobrym zvykom je vypnúť všetky nepoužívané fyzické rozhrania ak sa útočník dostane fyzicky ku zariadeniu, aby nemal priamy prístup do siete. To sa robí použitím príkazu:

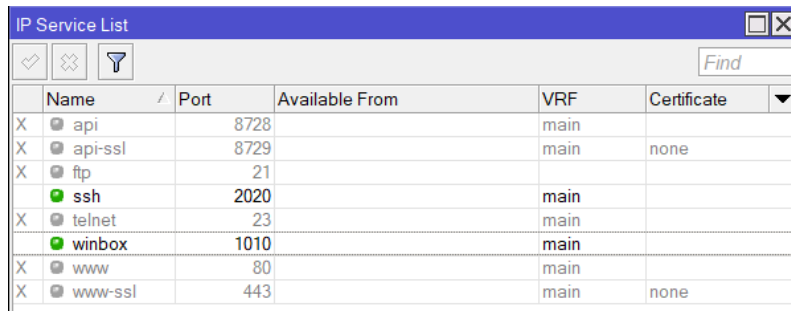
```
/interface ethernet disable ether3
```

4.5 Vypnúť nepoužívané služby

Všetky služby na prístup do zariadenia nie je potrebné ani bezpečné mať zapnuté. Zapnuté sa nechajú len SSH a Winbox. Na zvýšenie bezpečnosti sa týmto službám zmenia porty(4.8). Zmena portov má však aj svoju nevýhodu a to tú, že sa môže stať, že sa na nové čísla zabudne.

- *Výpis všetkých služieb sa nachádza v IP -> Services.*
- *Vypnutie vybranej služby sa robí kliknutím na službu pravým tlačítkom myši a vybraním možnosti Disable.*

Obr. 4.8: Vypnutie nepotrebných služieb a zmena portov SSH a winbox



	Name	Port	Available From	VRF	Certificate
X	api	8728		main	
X	api-ssl	8729		main	none
X	ftp	21			
	ssh	2020		main	
X	telnet	23		main	
	winbox	1010		main	
X	www	80		main	
X	www-ssl	443		main	none

```
/ip service disable www-ssl,telnet,ftp,www,api,api-ssl  
/ip service set ssh port=2020  
/ip service set winbox port=1010
```

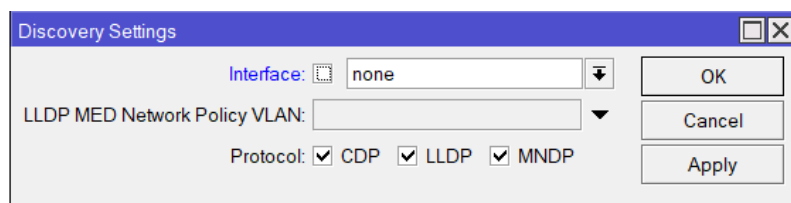
4.5.1 Ostatné služby

Neighbor Discovery

Využíva sa na výpis pripojených zariadení k smerovaču. Táto služba predstavuje risk, pretože ak útočník získa prístup na zariadenie, na ktorom je táto služba povolená tak si vie zistiť informácie o susedoch. V RouterOS sú k dispozícii CDP, LLDP, MNDP. Všetkým sa dá nastaviť či budú zapnuté na všetkých rozhraniach, na niektorých alebo na žiadnych(4.9).

- *IP -> Neighbors*
- *Interface -> vybrať možnosť none*
- *Apply a potom OK*

Obr. 4.9: Vypnutie discovery protokolov na všetkých rozhraniach



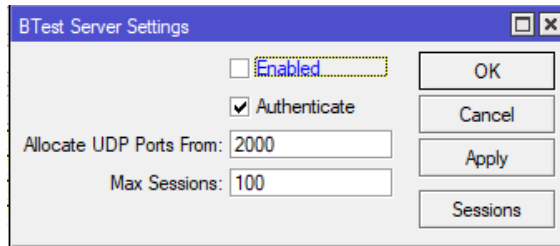
```
/ip neighbor discovery-settings set discover-interface-list=none
```

Bandwidth server

Využíva sa na meranie šírky pásma medzi dvoma Mikrotik smerovačmi. Táto služba sa odporúča vypnúť v produkčných sieťach. Ak je potrebná, zapne sa len na potrebný

čas a potom sa znova vypne administrátorom(4.10).

Obr. 4.10: Vypnutie Bandwidth serveru

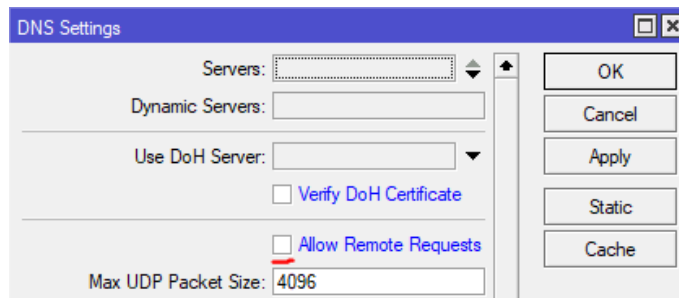


```
/tool bandwidth-server set enabled=no
```

DNS cache

V RouterOS je možnosť vypnúť vyrovnávajúcu pamäť cache, ktorá skraca čas pri riešení DNS požiadavkov. Ak však máme v sieti smerovač, ktorý toto už robí alebo túto službu nepotrebujeme, je dobré DNS cache vypnúť(4.11).

Obr. 4.11: Vypnutie dns cache

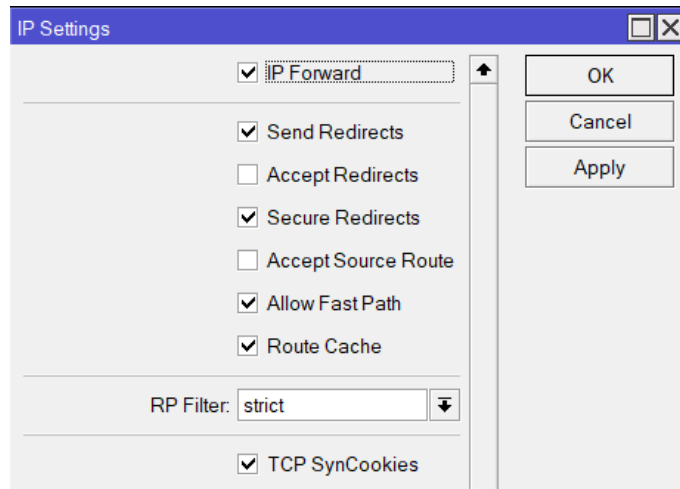


```
/ip dns set allow-remote-requests=no
```

RP filtering a TCP Syn cookies

Na odporúčanie RFC3704 sa zapína ochrana pred podvrhnutím IP adres pomocou RP filtra, ktorý sa nastaví na strict v nastaveniach IP settings. Taktiež na ochranu pred SYN floodom sa zapnú TCP Syn Cookies 4.12.

Obr. 4.12: Zapnutie RP filtra a TCP SYN cookies



Synchronizácia času pomocou NTP

Ako bolo spomínané, je dôležité monitorovať prevádzku a ukladať si logy zo zariadení. Kvôli tejto skutočnosti potrebujeme, aby zariadenia boli časovo synchronizované, keďže nám to pomôže pri ľahšej identifikácii problémov. Na to sa odporúča zapnúť NTP synchronizáciu. Či už smerovač nastaviť ako klient alebo server. Ak je v sieti vlastný NTP server, tak stačí ostatné smerovače nastaviť ako klientov a zapísať tam adresu servera.

4.6 Záloha konfigurácie

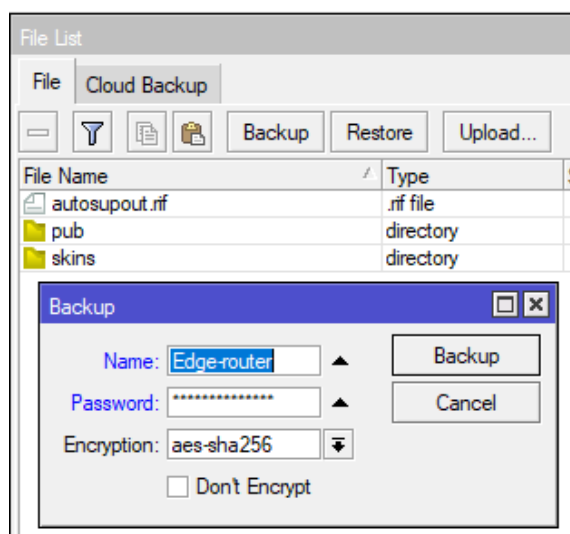
Nastavenia by sa mali pravidelne zálohovať, aby v prípade poškodenia systému alebo nežiadúcej zmeny bolo možné smerovač obnoviť do posledného funkčného stavu. Rovnako by sa každá zmena mala dokumentovať aby administrátori siete mali prehľad. Pomocou Winboxu sa konfigurácia zálohuje nasledovne 4.13 :

- *Tools -> Files*
- *V záložke File sa klikne sa tlačítko backup*
- *Otvorí sa nové okno, kde sa vyplní názov súboru, zadá sa heslo a typ šifrovania*

Po tom, ako sa záloha vytvorí, stačí aby sa myškou súbor chytil a pretiahol do PC. Tým si zabezpečíme aj externú zálohu. Treba si pamätať, že ak sa nezadá žiadne heslo, súbor bude automaticky bez šifrovania. Taktiež je dôležité si vybrať možnosť šifrovania pomocou aes-sha256, pretože šifra RC4 nie je dostatočne bezpečná.

Pomocou terminálu si zálohy vieme spraviť nasledovne :

Obr. 4.13: Vytvorenie zálohy vo Winboxe



```
/system backup save name=Edge-router password=strongpassword
```

Následne sa dá pomocou príkazu */system backup load name=Edge-router* nahrat uložená konfigurácia.

Exportovať konfiguráciu sa dá aj pomocou príkazu */export file=Edge_router*. Takto sa vyexportuje skript, ktorý sa dá aj otvoriť pomocou textového editora a upraviť si ho. Následne sa dá znova naimportovať pomocou príkazu *import file=Edge_router.rsc*.

4.7 Firewall

RouterOS má v sebe zabudovaný firewall, ktorý má v základe len pár pravidiel. Tieto však na pokročilejšie útoky nie je dostačujúci, preto sa vytvoria nasledujúce pravidlá.

4.7.1 Povolenie už nadviazaných spojení

Na to aby sa znížilo zaťaženie procesora, sa vytvorí pravidlo, ktoré zabezpečí selektívne posielanie paketov na filtrovanie. To znamená, že firewallom ďalej prejdú len pakety, ktoré sú v stave new. Všetky, ktoré sú v stave established a related budú povolené a invalid budú zahodené. Toto sa dosiahne pomocou pravidiel:

```
add action=accept chain=input comment="Established, Related" connection-  
state=established,related  
add action=accept chain=forward comment="Established, Related"
```

```
connection-state=established,related
add action=drop chain=input comment="Drop invalid"
connection-state=invalid log=yes log-prefix= drop invalid
add action=drop chain=forward comment="Drop invalid"
connection-state=invalid log=yes log-prefix= drop invalid
```

Firewall v RouterOS filtruje pakety na základe chain hodnoty. To znamená že pravidlo, ktoré má nastavené chain input, bude filtrovať pakety, ktoré vstupujú na dané rozhranie smerovača. Forward chain filtruje pakety, ktoré prechádzajú cez smerovač.

4.7.2 Bogon adresy

Bogon adresy, sú adresy, ktoré by sa nemali nachádzať vo verejnom priestore na internete. To znamená že takéto IP adresy nie sú oficiálne priradené v žiadnom z rozsahov od IANA. Takéto ip adresy by sa nemali dostávať na smerovač z vonkajšej siete, pretože môžu predstavovať podvrhnutú adresu útočníka. Pre tento dôvod sa vytvorí zoznam takýchto bogon adries [41].

```
/ip firewall address-list
add list="BOGONS" address=0.0.0.0/8
add list="BOGONS" address=100.64.0.0/10
add list="BOGONS" address=127.0.0.0/8
add list="BOGONS" address=169.254.0.0/16
add list="BOGONS" address=172.16.0.0/12
add list="BOGONS" address=192.0.0.0/24
add list="BOGONS" address=192.0.2.0/24
add list="BOGONS" address=192.168.0.0/16
add list="BOGONS" address=198.18.0.0/15
add list="BOGONS" address=198.51.100.0/24
add list="BOGONS" address=203.0.113.0/24
add list="BOGONS" address=224.0.0.0/3
```

Následne sa tento zoznam adries zablokuje nasledujúcim pravidlom pre forward chain. Druhé pravidlo sa vytvorí pre input.

```
/ip firewall filter add action=drop chain=forward comment="Block Bogon Add-
resses" in-interface=ether1 log=yes log-prefix="drop bogon address" src-address-
list=BOGONS
```


4.7.3 Filtrovanie pomocou geolokácie

Filtrovanie prevádzky z určitých krajín sa dá dosiahnuť pomocou geo-ip filtrovania. Každá krajina má pridelený určitý rozsah ip adries na základe čoho sa dá zistiť z akej krajiny daná ip adresa pochádza. Tieto zoznamy sú verejne dostupné, preto sa dá vo firewalle filtrovať z ktorých krajín sa zakáže alebo povolí komunikácia. Každá krajina má množstvo IP adries a ak by sa filtrovali všetky, mohlo by to výrazne zahltiť prostriedky smerovača. Z tohto dôvodu sa vyfiltrujú len krajiny, z ktorých chodia útoky najčastejšie. V tomto prípade to bude Rusko a Čína. Na vygenerovanie zoznamu týchto adries sa použije nasledovný nástroj[42]. Druhým prístupom môže byť naopak povoliť len bezpečné krajiny. Vygenerovaný zoznam sa stiahne ako skript, ktorý stačí nahráť do smerovača a pustiť príkazom

```
import file="nazovsuboru.rsc"
```

Následne sa už len vytvorí filter, ktorý bude kontrolovať prítomnosť týchto ip adries na vstupe WAN rozhrania.

```
/ip firewall filter add action=drop chain=input comment="Geo-ip locations addresses" in-interface=ether1 log=yes log-prefix="drop geo location" src-address-list=CountryIPBlocks
```

4.7.4 UDP flood

Na ochranu pred UDP záplavovým útokom sa vytvorí nasledujúce pravidlo, ktoré zakáže DNS komunikáciu zvonka. Použije sa raw pravidlo, ktoré má výhodu toho, že sa filtruje ešte pred sledovaním spojení, čo odľahčí záťaž na CPU. Ďalším parametrom pravidla je cieľový port, kde sa určil port 53, ktorý patrí službe DNS, ktorá pracuje s UDP. Ako chain sa použije prerouting, ktorý filtruje všetky pakety, ktoré vstúpia do smerovača.

```
/ip firewall raw add action=drop chain=prerouting comment="UDP flood prevention" dst-port=53 in-interface-list=WAN log=yes log-prefix="udp flood" protocol=udp  
add action=accept chain=prerouting dst-port=53 in-interface=!ether1 limit=100,5:packet protocol=udp
```

4.7.5 SYN flood

Tieto pravidlá obmedzia počet nových spojení, ktoré majú príznak SYN a tým sa pomôže predísť SYN flood útokom. Toto sa zabezpečí pomocou tcp-flags, kde sa vyberie možnosť syn.

```

add action=jump chain=input comment="SYN Flood protect"
connection-state=new jump-target=SYN-Protect protocol=tcp tcp-flags=syn
add action=jump chain=forward comment="SYN Flood protect"
connection-state=new jump-target=SYN-Protect protocol=tcp tcp-flags=syn
add action=add-src-to-address-list address-list="SYN attacker"
address-list-timeout=none-dynamic chain=SYN-Protect
add action=accept chain=SYN-Protect connection-state=new limit=400,5:packet
protocol=tcp tcp-flags=syn add action=drop chain=SYN-Protect connection-
state=new log=yes log-prefix="drop SYN flood" protocol=tcp tcp-flags=syn

```

4.7.6 Port scan

V prípade ak sa chce zabrániť skenovaniu portov, použijeme nasledujúce pravidlá, ktoré zahodia všetky pakety, ktoré odpovedajú nasledujúcim parametrom. Privilegované porty majú hodnotu 1 a neprivilegované 3 a počet sekúnd medzi paketmi s rôznymi číslami portov sú 3 sekundy. Ak súčet prekročí číslo 21 môže to indikovať port scan a nasledujúce pakety sa zahodia.

```

add action=add-src-to-address-list address-list=PortScanners chain=input com-
ment="Port scanners" in-interface=ether1 log=yes log-prefix="port scan"
protocol=tcp psd=21,3s,3,1
add action=drop chain=input log=yes log-prefix="drop port scan" src-address-
list=PortScanners

```

4.7.7 SSH a Winbox Brute force

Pre obe služby sa obmedzí počet neúspešných prihlásení. V prípade, ak sa klient pokúsi pripojiť k serveru pomocou TCP portu 2020 a všetky parametre šifrovania, verzií a hesla sedia, vytvorí sa SSH spojenie. V opačnom prípade sa tento pokus vyhodnotí ako neúspešný a firewall zdrojovú adresu pridá do zoznamu neúspešných pokusov [43]. Po troch neúspešných pokusoch sa klient pridá na blacklist a ďalšie spojenia sú zablokované. Tento výsledok sa dosiahne nasledujúcimi pravidlami.

```

/ip firewall filter add action=drop chain=input comment="block SSH brute
force" dst-port=2020 log=yes log-prefix="block ssh brute force" protocol=tcp
src-address-list=ssh_blacklist
add action=add-src-to-address-list address-list=ssh_blacklist
address-list-timeout=1d chain=input connection-state=new dst-port=2020 pro-
tocol=tcp src-address-list=ssh_stage3
add action=add-src-to-address-list address-list=ssh_stage3

```

```
address-list-timeout=1m chain=input connection-state=new dst-port=2020 protocol=tcp src-address-list=ssh_stage2
add action=add-src-to-address-list address-list=ssh_stage2
address-list-timeout=1m chain=input connection-state=new dst-port=2020 protocol=tcp src-address-list=ssh_stage1
add action=add-src-to-address-list address-list=ssh_stage1
address-list-timeout=1m chain=input connection-state=new dst-port=2020 protocol=tcp
```

Pre winbox sa spraví to isté len sa použije zmenený port 1010 a pridá jedno pravidlo na koniec, ktoré povolí ostatnú winbox komunikáciu.

```
add action=accept chain=input dst-port=1010 protocol=tcp
```

4.7.8 NAT maškaráda

NAT maškaráda sa nastaví ako spôsob prekladu adres, keď je verejná IP adresa dynamická.

```
/ip firewall nat add action=masquerade chain=srcnat out-interface=ether1
```

V prípade, ak je IP adresa statická a nebude sa meniť, môže sa použiť klasický source NAT, kedy sa IP adresa na WAN porte zmení na jednu špecificky zvolenú adresu.

4.8 Konfiguračný skript

Jedným z cieľov tejto práce bolo vytvoriť konfiguračný skript, pomocou ktorého sa automaticky nakonfigurujú základne nastavenia, ktoré sa dajú upravovať užívateľom.

Je napísaný pomocou Mikrotik skriptovacieho jazyka, ktorý je súčasťou RouterOS. Je založený na RouterOS CLI príkazoch a využíva sa na automatizáciu udalostí. Tieto skripty sa dajú ukladať do System-> Scripts alebo ich užívateľ vie písať priamo do príkazového riadku.

V tomto prípade si pred pripravený konfiguračný skript stačí nahráť do záložky Files v RouterOS a spustiť pomocou príkazu *import file=PreConfigure.txt*.

Pred spustením si však treba skript upraviť podľa svojich preferencií a siete. Čo všetko sa skriptom nakonfiguruje?

4.8.1 Obsah skriptu

Na prvých riadkoch sú popísané požiadavky, ktoré je potrebné splniť pred spustením. Tie obsahujú postup nahratia skriptu a pomocných súborov do RouterOS a

následne príkaz na spustenie.

V hlavičke skriptu sa nachádzajú lokálne premenné, ktoré sa používajú pri konfigurácií. Nasleduje časť, kde sa priradujú hodnoty lokálnym premenným podľa užívateľských preferencií. Všetky majú prednastavené hodnoty, ktoré sa dajú zmeniť podľa potreby.

Výpis 4.1: Ukážka premenných

```
#Nastavovanie premenných

#Nastavte si nového užívateľa a (admin sa vymaže)
:set name John;
:set pass longpassword;

#časová zóna
#:set timezone "Europe/Bratislava";

#Vyberte si WAN-interface
:set wan "ether1"

#Vyberte si či chcete na wan povoliť dhcp, statickú
#adresu alebo PPPoE
:set configureDHCPonWan true; #false
:set staticonwan false; #true
:set configurePPPOE false; #true
```

Po nastavení všetkých premenných sa v skripte nachádza konfiguračná časť, v ktorej sa nachádzajú CLI príkazy ktoré postupne nastavia smerovač na požadovaný stav. Celý skript sa nachádza v prílohách.

Podrobný obsah základných funkcií:

- Vytvorenie nového užívateľa a vymazanie základného účtu admin
- Vytvorenie zoznamu WAN a priradenie WAN interfacu
- Pridelenie IP adresy na WAN interface
- V prípade potreby vytvorenie PPPoE
- Vytvorenie VLAN sietí alebo bridge LAN
- Vytvorenie DHCP serverov pre VLAN alebo bridge LAN

Obsah bezpečnostných opatrení:

- Vypnutie nepotrebných mikrotik služieb (telnet, ftp, www, api, api-ssl)

- Zmena čísiel portov služieb SSH a Winbox
- Nastavenie SSH strong-crypto
- Nastavenie NTP servera
- Vypnutie MAC služieb (MAC telnet, ping, winbox)
- Vypnutie bandwidth servera
- Vypnutie Mikrotik caching, socks proxy
- Vypnutie UPNP služby
- Vypnutie DDNS a ip cloud
- Vypnutie neighbor discovery protokolov
- Zapnutie syn-cookies a rp-filter strict
- Nastavenie Firewallu a NAT

5 Testovanie zabezpečenia

Testovanie zabezpečenia sa vykonáva pomocou simulácie útokov na smerovač. Na to, aby výsledky boli viditeľné, je potrebné v prvom rade zaútočiť na nezabezpečené alebo veľmi slabo zabezpečené zariadenie a následne na zabezpečené. Takýmto spôsobom sa porovnajú výsledky a zistí sa, či sú vybrané opatrenia dostačujúce.

5.1 Port scan

Jeden z prvých krokov pre útočníka pred tým ako zaútočí na sieť alebo konkrétne zariadenie je prieskum prostredia. To zahŕňa aj skenovanie otvorených portov na zariadení. Skenovanie portov sa dá vykonať viacerými nástrojmi, avšak jeden z najpopulárnejších je nmap.

Obr. 5.1: Port scan pomocou nástroja nmap

```
root@kali:~# nmap 192.168.61.135
Starting Nmap 7.80 ( https://nmap.org ) at 2023-05-02 07:12 EDT
Nmap scan report for 192.168.61.135
Host is up (0.00094s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE
1010/tcp  open  surf
2020/tcp  open  xinupageserver
MAC Address: 50:00:00:03:00:00 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 8.99 seconds
```

5.1.1 Zabezpečenie pred port scan útokom

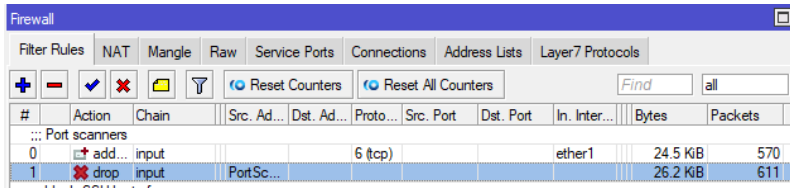
Takýmto skenom prostredia sa dá predísť implementáciou firewall pravidla. Ten pozostáva z dvoch riadkov a to konkrétne:

```
/ip firewall filter add chain=input protocol=tcp psd=21,3s,3,1 action=add-src-
to-address-list address-list="PortScanners"address-list-timeout=2w
in.interface=ether1 comment="Port scanners"disabled=no
```

Toto pravidlo zabezpečí to, že sa odfiltrujú IP adresy, ktoré vykonávajú port scan a pridajú sa do zoznamu adries PortScanners. Následne pridaním ďalšieho pravidla sa tieto ip adresy zablokujú a nebudú schopné pokračovať v útoku.

```
add chain=input src-address-list="PortScanners"action=drop disabled=no
```

Obr. 5.2: Port scan zablokovaný firewallom



The screenshot shows the Firewall configuration interface. The 'Filter Rules' tab is active. A table lists the rules, with rule 1 highlighted. Rule 1 has the action 'drop' and is applied to the 'input' chain. The protocol is 'tcp' and the destination port is '53'. The statistics show 26.2 KiB of data and 611 packets dropped.

#	Action	Chain	Src. Ad...	Dst. Ad...	Proto...	Src. Port	Dst. Port	In. Inter...	Bytes	Packets
0	add...	input			6 (tcp)			ether1	24.5 KiB	570
1	drop	input		PortSc...					26.2 KiB	611

5.2 UDP flood

UDP flood patrí medzi najčastejšie útoky z rodiny Denial of service, čo v preklade znamená odmietnutie služby. Funguje na princípe posielania veľkého množstva UDP paketov na určitý port, čím vyčerpá prostriedky servera alebo zariadenia, na ktoré je tento útok cielený. UDP flood pracuje s protokolom UDP, ktorý je narozdiel od TCP rýchlejší, keďže nevyžaduje na vytvorenie spojenie žiadny handshake [?].

Tento útok sa simuluje pomocou nástroju `hping3`, ktorý je dostupný na operačnom systéme Kali Linux. V pripravenej topológii je tento počítač označený ako attacker. Zapne sa počítač, prihlási sa pomocou `root/toor`. Na zapnutie útoku sa do terminálu zadá nasledujúci príkaz v ktorom sa špecifikuje typ útoku, protokol, číslo portu a ip adresa na ktorú je útok smerovaný. V tomto prípade to je WAN interface smerovača.

```
hping3 -flood -udp -p 53 192.168.61.135
```

Zároveň sa na smerovači otvoria Tools -> Profile, kde vidieť aktuálne zaťaženie smerovača. V prvom kroku sa vypne firewall pravidlo, ktoré smerovač ochraňuje a spustí sa útok 5.3.

5.2.1 Zabezpečenie pred UDP flood

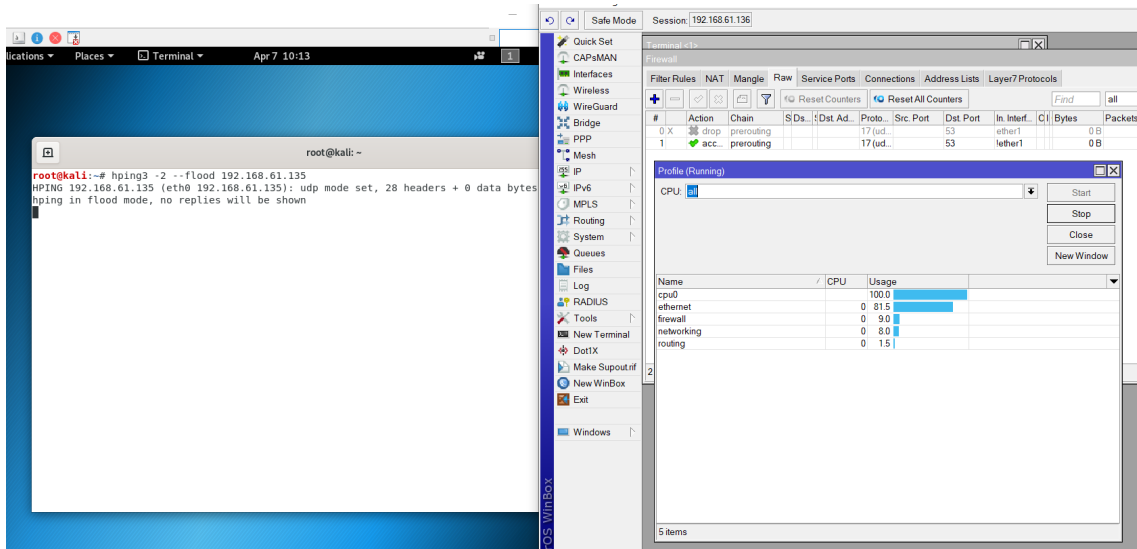
V prvom kroku ako sa proti takýmto typom útokov chrániť je vypnutie možnosti Allow remote requests v časti DNS.

A následne pomocou raw firewall pravidla.

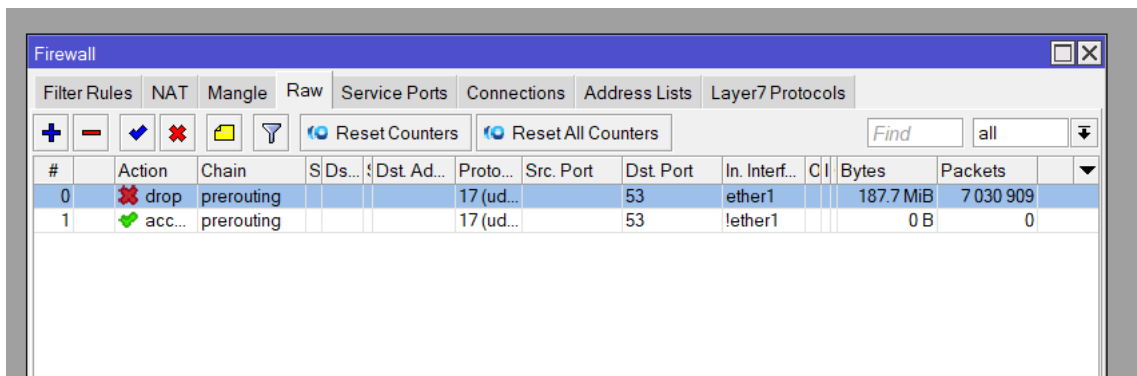
```
/ip firewall raw add action=drop chain=prerouting dst-port=53  
in-interface=ether1 protocol=udp
```

Po aplikácii nasledovného pravidla a spustenia útoku je vidieť v štatistikách firewallu zablokované pakety 5.4.

Obr. 5.3: UDP flood na nezabezpečený smerovač



Obr. 5.4: Zablokované UDP packety



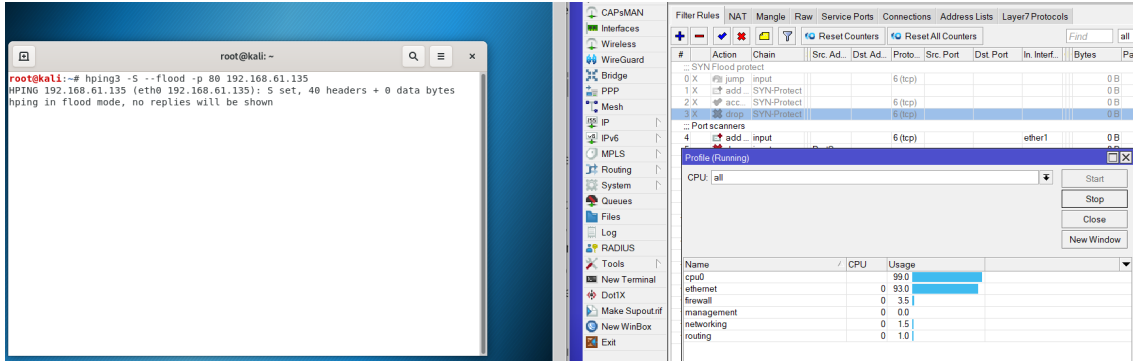
5.3 SYN flood

SYN flood ako aj UDP flood je záplavový útok z rodiny Denial of Service. Funguje na princípe posielania veľkého množstva paketov, ktoré obsahujú príznaky SYN. Na ne však ďalej už neodpovedá, čím vznikne veľké množstvo nedokončených spojení. Takýmto spôsobom útočník vyčerpá prostriedky zariadenia na ktoré je útok cielený [44].

Tento útok sa bude taktiež simulovať pomocou nástroju hping3, ktorý je dostupný na virtuálnom počítači attacker. Útok sa spustí pomocou nasledovného príkazu:

```
hping3 -S --flood -p 80 192.168.61.135
```

Obr. 5.5: SYN flood útok pomocou hping3



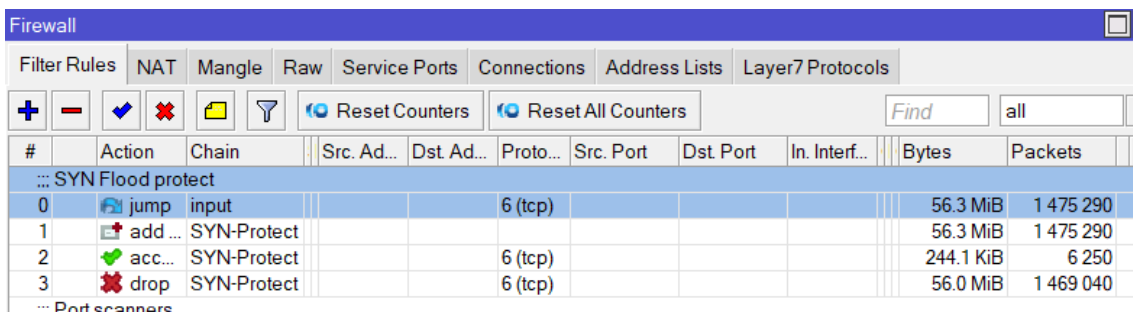
5.3.1 Zabezpečenie pred SYN flood

RouterOS má vstavanú funkciu syncookies, ktorá funguje ako ochrana proti SYN flood útokom. Funguje na princípe pridania malého kryptografického hashu do odpovede SYN-ACK. Ak následne kernel neuvidí tento hash v pakete, bude považovať spojenie za podvrhnuté a zahodí ho. Táto funkcia sa zapne pomocou:

```
/ip/settings/set tcp-syncookies=yes
```

Ďalšia ochrana sa zabezpečí nasledujúcimi firewall pravidlami, ktoré pridajú ip adresu útočníka do blacklistu a následne všetku jeho komunikáciu zablokujú.

Obr. 5.6: SYN flood útok zablokovaný firewallom



V prípade, ak by bol útok vykonávaný z viacerých zariadení, blacklist by vyzeral nasledovne 5.8.

Obr. 5.7: Útočník pridaný do blacklistu

Name	Address	Timeout	Creation Time
SYN attacker	192.168.61.131		Apr/13/2023 10:58:...

Obr. 5.8: Náhodné zdrojové IP adresy

Name	Address	Timeout	Creation Time
SYN attacker	167.148.186.63		Apr/13/2023 11:02...
SYN attacker	114.28.12.14		Apr/13/2023 11:02...
SYN attacker	244.9.69.160		Apr/13/2023 11:02...
SYN attacker	69.224.188.86		Apr/13/2023 11:02...
SYN attacker	84.167.0.58		Apr/13/2023 11:02...
SYN attacker	190.237.84.207		Apr/13/2023 11:02...
SYN attacker	28.32.177.233		Apr/13/2023 11:02...
SYN attacker	240.168.207.231		Apr/13/2023 11:02...
SYN attacker	58.31.152.19		Apr/13/2023 11:02...
SYN attacker	158.78.18.208		Apr/13/2023 11:02...
SYN attacker	190.111.71.253		Apr/13/2023 11:02...
SYN attacker	244.28.136.177		Apr/13/2023 11:02...
SYN attacker	47.111.177.170		Apr/13/2023 11:02...
SYN attacker	18.52.227.49		Apr/13/2023 11:02...
SYN attacker	243.135.136.204		Apr/13/2023 11:02...
SYN attacker	129.79.58.63		Apr/13/2023 11:02...
SYN attacker	122.3.135.208		Apr/13/2023 11:02...
SYN attacker	126.207.116.127		Apr/13/2023 11:02...
SYN attacker	144.38.40.190		Apr/13/2023 11:02...
SYN attacker	170.203.218.168		Apr/13/2023 11:02...
SYN attacker	158.228.15.241		Apr/13/2023 11:02...
SYN attacker	180.253.161.180		Apr/13/2023 11:02...
SYN attacker	63.26.86.217		Apr/13/2023 11:02...
SYN attacker	95.94.194.8		Apr/13/2023 11:02...
SYN attacker	190.230.144.237		Apr/13/2023 11:02...
SYN attacker	190.75.203.252		Apr/13/2023 11:02...
SYN attacker	246.48.240.203		Apr/13/2023 11:02...
SYN attacker	134.127.6.178		Apr/13/2023 11:02...
SYN attacker	252.222.5.134		Apr/13/2023 11:02...
SYN attacker	91.218.196.69		Apr/13/2023 11:02...

31509 items out of 249904

5.4 SSH brute force

Útok hrubou silou je spôsob, ako sa pomocou skúšania rôznych kombinácií mena a hesla prihlásiť do zariadenia. Je to jednoduchý ale časovo náročný spôsob získania prístupu na zariadenie. Existujú nástroje, ktoré pomocou rôznych slovníkov postupne zadávajú kombinácie známych hesiel za vás.

Jeden z týchto nástrojov sa nazýva Metasploit Framework. Je to populárny open source nástroj, ktorý sa používa na penetračné testovanie. Tento Framework sa využije aj na SSH brute force attack.

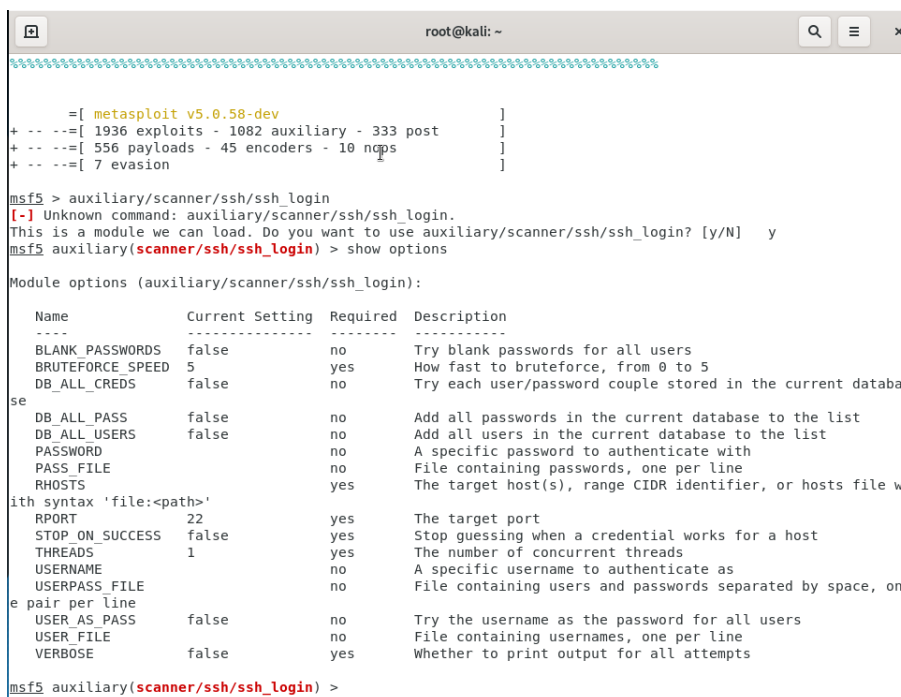
V základe je na RouterOS jeden užívateľ a to admin, ktorému sa nastaví pri prvom prihlásení heslo. Zvolilo sa jednoduché heslo napríklad "password1".

5.4.1 Príprava Metasploit Frameworku na útok

Metasploit Framework býva pred-inštalovaný na operačnom systéme Kali linux. Zapne sa pomocou príkazu *msfconsole*. Po spustení sa pomocou príkazu *search ssh* dá vyhladať v databázi exploity, ktoré obsahujú slovo ssh. Na SSH brute force sa použije *auxiliary/scanner/ssh/ssh_login*.

Pred spustením je potrebné nastaviť parametre, ktoré bude používať. Tie sa vylisťujú pomocou príkazu *show options*

Obr. 5.9: Parametre SSH brute force útoku



```
root@kali: ~  
=====
```

```
msf5 > auxiliary/scanner/ssh/ssh_login  
[-] Unknown command: auxiliary/scanner/ssh/ssh_login.  
This is a module we can load. Do you want to use auxiliary/scanner/ssh/ssh_login? [y/N] y  
msf5 auxiliary(scanner/ssh/ssh_login) > show options  
Module options (auxiliary/scanner/ssh/ssh_login):
```

Name	Current Setting	Required	Description
BLANK_PASSWORDS	false	no	Try blank passwords for all users
BRUTEFORCE_SPEED	5	yes	How fast to bruteforce, from 0 to 5
DB_ALL_CREDS	false	no	Try each user/password couple stored in the current database
DB_ALL_PASS	false	no	Add all passwords in the current database to the list
DB_ALL_USERS	false	no	Add all users in the current database to the list
PASSWORD		no	A specific password to authenticate with
PASS_FILE		no	File containing passwords, one per line
RHOSTS		yes	The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
RPORT	22	yes	The target port
STOP_ON_SUCCESS	false	yes	Stop guessing when a credential works for a host
THREADS	1	yes	The number of concurrent threads
USERNAME		no	A specific username to authenticate as
USERPASS_FILE		no	File containing users and passwords separated by space, one pair per line
USER_AS_PASS	false	no	Try the username as the password for all users
USER_FILE		no	File containing usernames, one per line
VERBOSE	false	yes	Whether to print output for all attempts

```
msf5 auxiliary(scanner/ssh/ssh_login) >
```

Ešte pred nastavovaním parametrov je potrebné si vytvoriť alebo stiahnuť textové dokumenty, ktoré obsahujú mená a heslá, z ktorých bude nástroj vyberať. Jeden z najznámejších takýchto slovníkov sa volá rockyou, ktorý je dostupný na stiahnutie na internete. Ten sa použije aj v tomto prípade.

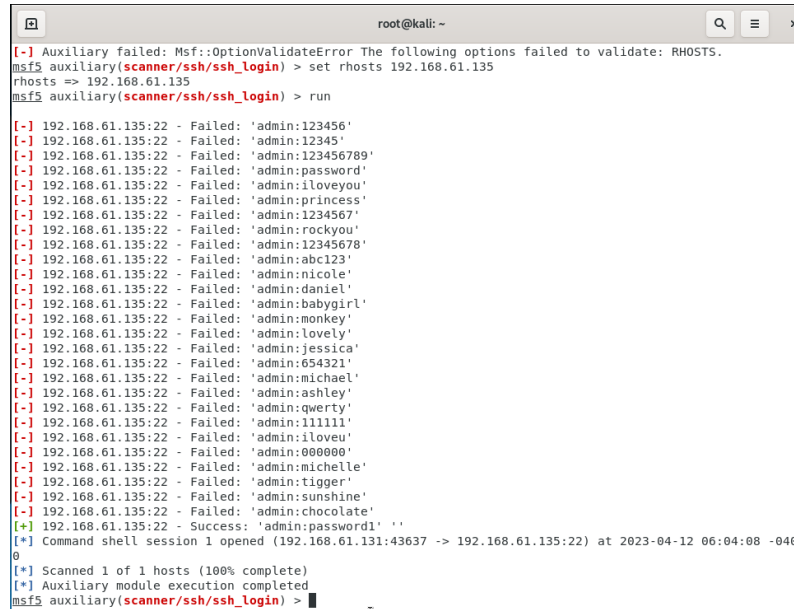
Nastavené parametre:

- set rhosts 192.168.61.135
- set username admin
- set verbose true
- set pass_file Downloads/rockyou.txt
- set stop_on_success true

Skúšať sa bude v tomto prípade len heslo, keďže sa predpokladá, že základný užívateľ admin nebol odstránený. V prípade zmeny mena sa nastaví slovník aj na

tento parameter. S takto nastavenými parametrami je možné spustiť útok pomocou príkazu *run*.

Obr. 5.10: Úspešný ssh útok



```
root@kali: ~
[-] Auxiliary failed: Msf::OptionValidateError The following options failed to validate: RHOSTS.
msf5 auxiliary(scanner/ssh/ssh_login) > set rhosts 192.168.61.135
rhosts => 192.168.61.135
msf5 auxiliary(scanner/ssh/ssh_login) > run
[-] 192.168.61.135:22 - Failed: 'admin:123456'
[-] 192.168.61.135:22 - Failed: 'admin:12345'
[-] 192.168.61.135:22 - Failed: 'admin:123456789'
[-] 192.168.61.135:22 - Failed: 'admin:password'
[-] 192.168.61.135:22 - Failed: 'admin:iloveyou'
[-] 192.168.61.135:22 - Failed: 'admin:princess'
[-] 192.168.61.135:22 - Failed: 'admin:1234567'
[-] 192.168.61.135:22 - Failed: 'admin:rockyou'
[-] 192.168.61.135:22 - Failed: 'admin:12345678'
[-] 192.168.61.135:22 - Failed: 'admin:abc123'
[-] 192.168.61.135:22 - Failed: 'admin:nicole'
[-] 192.168.61.135:22 - Failed: 'admin:daniel'
[-] 192.168.61.135:22 - Failed: 'admin:babygirl'
[-] 192.168.61.135:22 - Failed: 'admin:monkey'
[-] 192.168.61.135:22 - Failed: 'admin:lovely'
[-] 192.168.61.135:22 - Failed: 'admin:jessica'
[-] 192.168.61.135:22 - Failed: 'admin:654321'
[-] 192.168.61.135:22 - Failed: 'admin:michael'
[-] 192.168.61.135:22 - Failed: 'admin:ashley'
[-] 192.168.61.135:22 - Failed: 'admin:qwerty'
[-] 192.168.61.135:22 - Failed: 'admin:111111'
[-] 192.168.61.135:22 - Failed: 'admin:iloveu'
[-] 192.168.61.135:22 - Failed: 'admin:000000'
[-] 192.168.61.135:22 - Failed: 'admin:michelle'
[-] 192.168.61.135:22 - Failed: 'admin:tigger'
[-] 192.168.61.135:22 - Failed: 'admin:sunshine'
[-] 192.168.61.135:22 - Failed: 'admin:chocolate'
[*] 192.168.61.135:22 - Success: 'admin:password!'
[*] Command shell session 1 opened (192.168.61.131:43637 -> 192.168.61.135:22) at 2023-04-12 06:04:08 -0400
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf5 auxiliary(scanner/ssh/ssh_login) >
```

Dôvod prečo bol tento útok úspešný vo veľmi rýchlom čase je ten, že užívateľské meno nebolo zmenené a heslo bolo veľmi jednoduché.

5.4.2 Zabezpečenie pred SSH brute-force

Vytvorenie nového užívateľa

Jedným z prvých krokov ako sa proti takémuto útoku chrániť, je vytvorenie si iného užívateľa so silným heslom ako bolo ukázané v časti 4.3.1 a následne vymazať základného admina.

Zmena portu SSH služby

Ďalší spôsob, ako zťažiť útočníkovi tento útok, je zmeniť port služby zo známeho čísla 22 na iný nepoužívaný port, napríklad 2020 ako je ukázané v časti 4.5 . Pri tomto kroku je dôležité si zapamätať, že ak sa bude prihlasovať legitímny užívateľ, musí taktiež pri prihlasovaní špecifikovať zmenené číslo portu, inak bude prihlasovanie neúspešné.

Vytvorenie firewall pravidla

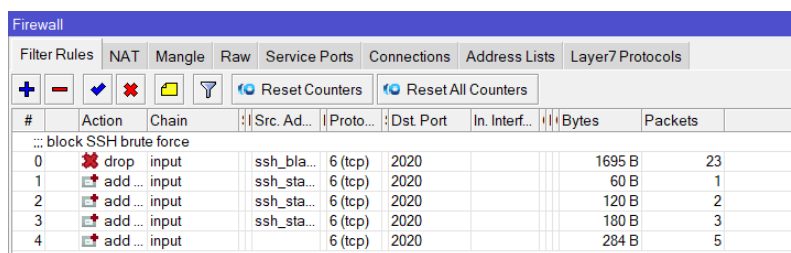
Ak by sa predsa len niekto pokúsil o tento útok a podarí sa mu obísť už nastavené zabezpečenie, je dobré mať nastavené firewall pravidlo, ktoré po troch neúspešných

pokusoch zablokuje danú IP adresu.

```
/ip firewall filter
add action=drop chain=input comment="block SSH brute force" dst-port=2020
protocol=tcp src-address-list=ssh_blacklist
add action=add-src-to-address-list address-list=ssh_blacklist
address-list-timeout=1w3d chain=input connection-state=new dst-port=2020
protocol=tcp src-address-list=ssh_stage3
add action=add-src-to-address-list address-list=ssh_stage3
address-list-timeout=1m chain=input connection-state=new dst-port=2020 pro-
tocol=tcp src-address-list=ssh_stage2
add action=add-src-to-address-list address-list=ssh_stage2
address-list-timeout=1m chain=input connection-state=new dst-port=2020 pro-
tocol=tcp src-address-list=ssh_stage1
add action=add-src-to-address-list address-list=ssh_stage1
address-list-timeout=1m chain=input connection-state=new dst-port=2020 pro-
tocol=tcp
```

Po každom neúspešnom pokuse sa zapíše do zoznamu adres a keď prekročí tri neúspešné pokusy, IP adresa sa zablokuje. Tento prípad je možné vidieť aj na nasledovnom obrázku 5.11 kedy sa tri krát zadalo zlé heslo.

Obr. 5.11: SSH brute force blokový firewallom



#	Action	Chain	Src. Ad...	Proto...	Dst Port	In. Interf...	Bytes	Packets
0	drop	input	ssh_bla...	6 (tcp)	2020		1695 B	23
1	add...	input	ssh_sta...	6 (tcp)	2020		60 B	1
2	add...	input	ssh_sta...	6 (tcp)	2020		120 B	2
3	add...	input	ssh_sta...	6 (tcp)	2020		180 B	3
4	add...	input		6 (tcp)	2020		284 B	5

Vytvorenie dvojice klíčův

Najbezpečnejší spôsob, ako sa prihlasovať na SSH je pomocou vygenerovanej dvojice klíčův. V takomto prípade majú obidve strany komunikácie uložený svoj klíč. Zariadenie na ktoré sa pripája má uložený verejný klíč a klient z ktorého sa užívateľ pripája má uložený súkromný klíč. Zariadenie následne overí klienta na základe jeho klíčův a povolí mu alebo zamietne prístup. Takto sa pri spojení nemusí zadávať žiadne heslo.

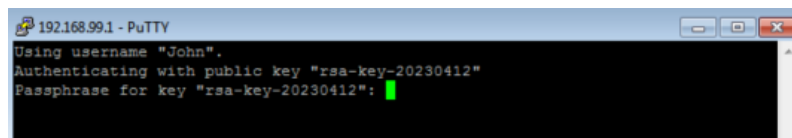
Klienti na unixových alebo windows 10 operačných systémoch si vedia vygenerovať dvojicu kľúčov pomocou príkazu *ssh-keygen*. V tomto prípade je administrátorský počítač windows 7, kde tento príkaz nie je podporovaný. Preto sa na vygenerovanie dvojice kľúčov použije program PuTTYgen. Súkromný kľúč sa uloží na disk a verejný kľúč sa skopíruje do vytvoreného textového dokumentu, ktorý sa následne vloží do RouterOS súborov. Tento súbor je pomenovaný *id_rsa.txt*. Po nakopírovaní sa musí ešte naimportovať pomocou príkazu:

```
/user/ssh-keys import public-key-file=id_rsa.txt user=John
```

Toto však nezakazuje iným klientom sa prihlasovať aj naďalej pomocou hesla. Preto je ešte potrebné zakázať prihlasovanie na SSH pomocou hesla. To sa urobí pomocou príkazu:

```
/ip ssh always-allow-password-login=no
```

Obr. 5.12: Prihlasovanie pomocou ssh kľúča



5.5 CDP flood

Tretí útok z rodiny DoS ktorý dokáže vyčerpať prostriedky smerovača je CDP flood. CDP je Cisco Discovery Protocol. Ako už z názvu vyplýva, je to proprietárny Cisco protokol, ktorý pracuje na druhej vrstve OSI modelu. Je však dostupný aj na RouterOS aj spolu s ďalšími protokolmi na vyhľadávanie susedov v sieti ako MNDP a LLDP. Každé zariadenie, ktoré má tento protokol zapnutý posiela každých 60 sekúnd multicastové rámce zo všetkých svojich portov. Zariadenia, ktoré tieto rámce dostanú si cieľovú MAC adresu uložia do svojej CDP tabuľky [?].

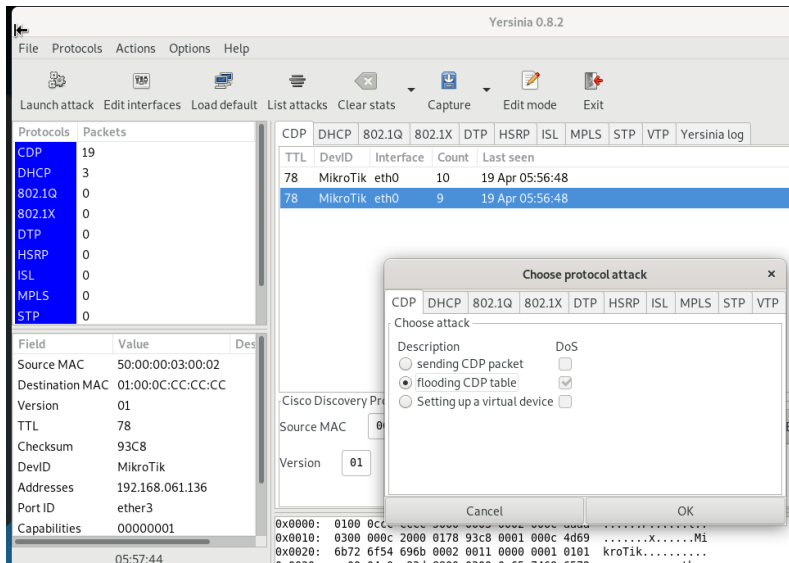
Tento útok sa simuluje pomocou nástroja Yersinia, ktorý je dostupný na operačnom systéme Kali Linux.

Grafická verzia tohto nástroja sa spustí pomocou príkazu *Yersinia -G*.

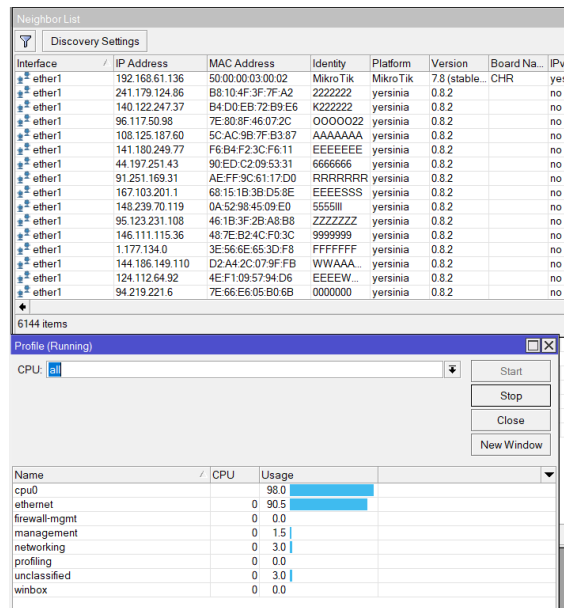
Keďže je na smerovači CDP protokol zapnutý, Yersinia vidí susedné porty na ktoré sa dá zaútočiť. Vyberie sa port s IP adresou 192.168.61.135 a spustí sa útok pomocou Launch attack a flooding CDP table 5.13.

Na smerovači sa dá pozorovať veľké množstvo záznamov susedov a taktiež veľké vyťaženie CPU 5.14.

Obr. 5.13: CDP flood Yersinia



Obr. 5.14: CDP flood RouterOS



5.5.1 Zabezpečenie proti CDP flood útoku

V tomto prípade je zabezpečenie veľmi jednoduché. Stačí aby sa CDP, LLDP a MNDP protokoly vypli, alebo obmedzili na určité porty. Ak však tieto protokoly nutne nie je potreba, odporúča sa ich vypnúť úplne poprípade zapínať, len v prípade potreby.

Vypnúť sa dajú vo Winboxe pod IP->Neighbors->Discovery Settings kde sa v záložke interface vyberie namiesto možnosti all možnosť none. Takýmto spôsobom

sa vypnú tieto protokoly na všetkých portoch. Popríklad pomocou príkazu:

```
/ip neighbor discovery-settings set discover-interface-list=none
```

5.6 Testovací skript

Dôvod takýchto manuálnych testov je ten, aby bolo jasne vidieť dôsledky vykonaného zabezpečenia. Vo väčšine prípadov však na takéto testovanie nie je priestor a čas, preto sa vytvoril skript v Bashi pre Linuxové distribúcie, ktorý tieto testy spraví automaticky.

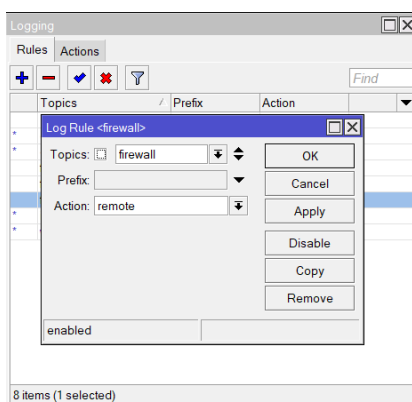
Skript slúži predovšetkým na to, aby otestoval firewall a prihlasovacie údaje na zariadenie. Na overenie funkčnosti zabezpečenia sa vytvárajú logy, z ktorých je viditeľné či nastavený firewall funguje správne. Keďže sa pri testovaní vytvorí množstvo logov z útokov na firewall, ktoré by zbytočne zaplňali disk smerovača, nastaví sa posielanie logov na vzdialený syslog server. Preto je na vykonanie takéhoto testovania v sieti nevyhnutný syslog server.

Prerekvizity na spustenie:

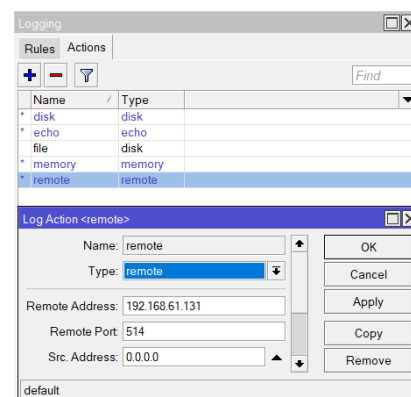
- stiahnutý slovník rockyou.txt na ssh brute force
- nainštalovaný nástroj hping3
- nainštalovaný nástroj Metasploit
- vytvorený resource skript pre automatizáciu Metasploit

5.6.1 Spustenie logovania na syslog

Keďže sa bude využívať posielanie logov na syslog server, je potrebné si toto logovanie zapnúť na smerovači v sekcii System -> Logging. Tu sa nastaví pravidlo, ktoré hovorí to, že všetky logy pochádzajúce z firewallu sa zalogujú na vzdialený server. V zápätí je potrebné si nastaviť aj IP adresu a cieľový port syslog servera 5.15b 5.15a.



(a) Zapnutie logov na vzdialený server



(b) Nastavenie IP adresy syslogu

5.6.2 Prispôsobenie resource skriptu pre Metasploit

Ako už bolo ukázané SSH brute force pomocou nástroja Metasploit potrebuje prídavné nastavenie pred spustením a spôsob ako tento proces vieme automatizovať je pomocou takzvaného resource skriptu. Stačí ak sa vytvorí súbor s nasledujúcim textom, v ktorom si užívateľ len zmení IP adresu testovaného smerovača a názov súboru bude msf.rc.

Výpis 5.1: Metasploit resource skript

```
use auxiliary/scanner/ssh/ssh_login
set rhosts 192.168.61.135
set rport 2020
set verbose true
set username admin
set pass_file Downloads/rockyou.txt
set stop_on_success true
exploit
```

Následne sa ešte povolí spúšťanie súboru pomocou `chmod+x msf.rc`

5.6.3 Vytvorenie a spustenie testovacieho skriptu

- Vytvorí sa súbor `skript.sh`
- Skopíruje sa nasledujúci kód
- Povolí sa spúšťanie súboru pomocou `chmod+x skript.sh`
- Spustí sa pomocou `./skript.sh "Ip adresa smerovača"`

Výpis 5.2: Testovací skript

```
#!/bin/bash

echo "Ip adresa: $1"

#SYN Flood

hping3 -S --flood -p 80 $1 &
syn_pid=$!
sleep 5
kill $syn_pid
sleep 10
```

```
#UDP flood

hping3 --flood -udp -p 53 $1 &
udp_pid=$!
sleep 5
kill $udp_pid
sleep 10

#SSH brute force

msfconsole -r msf.rc &
sleep 10
```

Testovací skript pozostáva zo štyroch častí. V prvej časti si z konzole vypýta IP adresu testovaného smerovača. Táto IP adresa sa zoberie a spustí na ňu SYN flood útok. Uloží sa ID procesu do premennej `syn_pid` a po 5 sekundách sa tento proces ukončí. Takto sa vykoná aj UDP flood a v poslednej časti sa spustí Metasploit s už spomínaným resource skriptom. Keď prebehne SSH brute force všetko sa ukončí a užívateľ si môže pozrieť vytvorené logy na syslog serveri. Blokové útoky sú označené v logoch čo signalizuje, že firewall funguje správne.

5.7 Testovanie pomocou Routersploitu

Routersploit je voľne dostupný framework, ktorý obsahuje veľké množstvo exploitov na smerovače, IP kamery a na iné takzvané embedded zariadenia. Tento framework dokáže pomôcť otestovať zraniteľnosti zariadenia, nie však otestovať nastavený firewall.

Podrobný popis inštalácie tohto frameworku je popísaný na [github odkaze](#)[46]. Pre spustenie je potrebné sa prepnúť do adresára `routersploit`. V ňom spustiť samotný routersploit pomocou `python3 rsf.py` príkazu.

Pomocou príkazu `use scanners/autpwn` sa vyberie nástroj ktorý sa použije. Ako cieľ sa vyberie testovaný smerovač pomocou `set target 192.168.61.135` a spustí sa testovanie pomocou príkazu `run`.

Po otestovaní všetkých dostupných zraniteľností sa vypíšu výsledky. V názornom teste je možné vidieť, že po teste sa dá vyčítať či je smerovač zraniteľný na ktorúkoľvek zraniteľnosť a v prípade ak je, tak je vidieť aj na ktorú konkrétne. Zároveň tento test aj otestuje či sú zmenené základné prihlasovacie údaje.

Záver

Bezpečnosť sietí akejkoľvek veľkosti je veľmi dôležitý faktor, ktorému by sa každý sieťový administrátor mal venovať.

Táto bakalárska práca sa v teoretickej časti venovala analýze bezpečnostných odporúčaní na zabezpečenie sieťových zariadení od organizácií ako CISA, NSA a NÚKIB, ktoré pravidelne aktualizujú a vydávajú minimálne požiadavky, ktoré by sieť mala spĺňať. Keďže jedným z cieľov práce bolo preštudovanie a analýza možností zabezpečenia RouterOS verzie 7, tak sa teoretická časť práce venovala aj porovnávaniu starších verzií s novou. Najväčšou a najvýznamnejšou zmenou RouterOS 7 bola podpora vyššej verzie kernelu čo pomohlo zvýšiť výkon a bezpečnosť. Ďalej sa v práci popísali bezpečnostne silné a slabé stránky najpoužívanejších služieb a funkcií RouterOS.

Praktická časť pozostávala z vytvorenia virtuálneho prostredia, v ktorom sa následne nakonfigurovali služby podľa odporúčaní, ktoré boli popísané v teoretickom úvode. Keďže RouterOS nepodporuje virtualizáciu bezdrôtových sietí, táto možnosť bola v práci vynechaná. Bol navrhnutý postup, akým postupovať pri konfigurácii či už pomocou terminálu alebo Winboxu tak, aby sa splnili oficiálne odporúčania, a tak, aby bolo zariadenie chránené aj pred najznámejšími sieťovými útokmi ako sú SYN flood, UDP flood, CDP flood alebo SSH brute force. Po nastavení všetkých služieb a vytvorení firewallu sa smerovač otestoval pomocou simulácie útokov na vytvorenú virtuálnu sieť. Navyše boli vytvorené aj dva skripty. Jeden v skriptovacom jazyku od Mikrotiku, ktorý slúži na automatickú konfiguráciu nového zariadenia a druhý, napísaný v Bashi, ktorý slúži na automatické otestovanie funkčnosti nastavených firewall pravidiel a prihlasovacích údajov. Pri testovaní zabezpečenia sa porovnali výsledky zabezpečeného a nezabezpečeného smerovača, čím sa potvrdila funkčnosť navrhnutého zabezpečenia, ktoré zodpovedá aj odporúčaniam popísaným v teoretickej časti práce.

Literatúra

- [1] Útoky hackerů na nemocnice sílí. Umírají kvůli nim lidé. *seznam* [online]. [cit. 16.5.2022]. Dostupné z URL: <<https://www.seznamzpravy.cz/clanek/fakta-utoky-hackeru-na-nemocnice-sili-umiraji-kvuli-nim-lide-217153>>
- [2] Cost of a data breach 2022. *ibm* [online]. [cit. 16.5.2022]. Dostupné z URL: <<https://www.ibm.com/reports/data-breach>>
- [3] CYBERSECURITY. *cisa* [online]. [cit. 8.12.2022]. Dostupné z URL: <<https://www.cisa.gov/cybersecurity>>
- [4] National Security Agency/Central Security Service. *nsa* [online]. [cit. 8.12.2022]. Dostupné z URL: <<https://www.nsa.gov/>>
- [5] Security Tip (ST18-001). *cisa* [online]. [cit. 25.11.2022]. Dostupné z URL: <<https://www.cisa.gov/uscert/ncas/tips/ST18-001>>
- [6] Hardening Network Devices. *NSA* [online]. [cit. 26.11.2022]. Dostupné z URL: <https://media.defense.gov/2020/Aug/18/2002479461/-1/-1/0/HARDENING_NETWORK_DEVICES.PDF>
- [7] Network Infrastructure Security Guidance. *NSA* [online]. [cit. 26.11.2022]. Dostupné z URL: <https://kryptera.se/assets/uploads/CTR_NSA_NETWORK_INFRASTRUCTURE_SECURITY_GUIDANCE_20220301.pdf#%5B%7B%22num%22%3A101%2C%22gen%22%3A0%7D%2C%7B%22name%22%3A%22XYZ%22%7D%2C69%2C705%2C0%5D>
- [8] Národní úřad pro kybernetickou a informační bezpečnost. *NÚKIB* [online]. [cit. 20.1.2023]. Dostupné z URL: <<https://www.nukib.cz/cs/>>
- [9] Doporučení. *NÚKIB* [online]. [cit. 20.1.2023]. Dostupné z URL: <<https://www.nukib.cz/cs/infoservis/doporuceni/#1>>
- [10] Kritická informační infrastruktura. *govcert* [online]. [cit. 20.1.2023]. Dostupné z URL: <https://www.govcert.cz/download/kii-vis/Schema_KII.pdf>
- [11] DMARC - Domain-based Message Authentication, Reporting and Conformance. *slovaknet* [online]. [cit. 19.1.2023]. Dostupné z URL: <<https://napoveda.slovaknet.sk/inpage/dmarc/>>
- [12] disaster recovery plan (DRP). *techtarget* [online]. [cit. 18.1.2023]. Dostupné z URL: <<https://www.techtarget.com/searchdisasterrecovery/definition/disaster-recovery-plan>>

- [13] BEZPEČNOSTNÍ DOPORUČENÍ NÚKIB PRO ADMINISTRÁTORY 4.0. *NÚKIB* [online]. [cit. 20.1.2023]. Dostupné z URL: <<https://www.techtarget.com/searchdisasterrecovery/definition/disaster-recovery-plan>>
- [14] DEFINÍCIA MIKRO, MALÝCH A STREDNÝCH PODNIKOV, KTORÉ PRIJALA KOMISIA. *emas* [online]. [cit. 19.5.2023]. Dostupné z URL: <<https://www.emas.sk/wp-content/uploads/2019/06/odporucanieES361-2003.pdf>>
<https://www.emas.sk/wp-content/uploads/2019/06/odporucanieES361-2003.pdf>
- [15] Smernica NIS II – Čo čaká kybernetickú bezpečnosť na Slovensku?. *infoconsult* [online]. [cit. 19.5.2023]. Dostupné z URL: <<https://www.infoconsult.sk/n/smernica-nis-ii-co-caka-kyberneticku-bezpecnost-na-slovensku>>
- [16] Nové směrnice NIS 2: Kdo, jak a proč?. *computerworld* [online]. [cit. 19.5.2023]. Dostupné z URL: <<https://www.computerworld.cz/texty/nove-smernice-nis-2-kdo-jak-a-proc/>>
- [17] TLS 1.3 – Seznamte se s novým bezpečnostním standardem. *sslmarket* [online]. Posledná aktualizácia 31. Mája 2021 [cit. 24.11.2022]. Dostupné z URL: <<https://help.mikrotik.com/docs/display/ROS/Getting+started>>
- [18] TLS 1.3 – Seznamte se s novým bezpečnostním standardem. *sslmarket* [online]. Posledná aktualizácia 31. Mája 2021 [cit. 24.11.2022]. Dostupné z URL: <<https://help.mikrotik.com/docs/display/ROS/Getting+started>>
- [19] Getting Started. *mikrotik* [online]. [cit. 25.11.2022]. Dostupné z URL: <<https://help.mikrotik.com/docs/display/ROS/Getting+started>>
- [20] Are you ready for RouterOS v7 ?. *mikrotik* [online]. 2021, [cit. 25.11.2022]. Dostupné z URL: <https://www.i4wifi.cz/uploads/faq/1961_1_routeros-v7.pdf>.
- [21] Vulnerability Details : CVE-2013-6282. *CVE Details* [online]. [cit. 3.12.2022]. Dostupné z URL: <<https://www.cvedetails.com/cve/CVE-2013-6282/>>
- [22] Vulnerability Details : CVE-2013-4587. *CVE Details* [online]. [cit. 3.12.2022]. Dostupné z URL: <https://www.cvedetails.com/cve-details.php?t=1&cve_id=CVE-2013-4587>

- [23] Vulnerability Details : CVE-2013-4563. *CVE Details* [online]. [cit. 3.12.2022]. Dostupné z URL: <<https://www.cvedetails.com/cve/CVE-2013-4563/>>
- [24] Vulnerability Details : CVE-2012-3400. *CVE Details* [online]. [cit. 3.12.2022]. Dostupné z URL: <https://www.cvedetails.com/cve-details.php?t=1&cve_id=CVE-2012-3400>
- [25] Vulnerability Details : CVE-2013-7027. *CVE Details* [online]. [cit. 3.12.2022]. Dostupné z URL: <<https://www.cvedetails.com/cve/CVE-2013-7027/>>
- [26] Vulnerability Details : CVE-2022-1419. *CVE Details* [online]. [cit. 1.12.2022]. Dostupné z URL: <https://www.cvedetails.com/cve-details.php?t=1&cve_id=CVE-2022-1419>
- [27] Vulnerability Details : CVE-2020-14381. *CVE Details* [online]. [cit. 1.12.2022]. Dostupné z URL: <https://www.cvedetails.com/cve-details.php?t=1&cve_id=CVE-2020-14381+>
- [28] Finding and exploiting CVE-2018-7445 (unauthenticated RCE in MikroTik's RouterOS SMB). *medium* [online]. [cit. 3.12.2022]. Dostupné z URL: <<https://medium.com/@maxi./finding-and-exploiting-cve-2018-7445-f3103f163cc1>>
- [29] Vulnerability Details : CVE-2018-1156. *CVE Details* [online]. [cit. 3.12.2022]. Dostupné z URL: <<https://www.cvedetails.com/cve/CVE-2018-1156/>>
- [30] Mikrotik Routeros. *Stack.watch* [online]. [cit. 5.12.2022]. Dostupné z URL: <<https://stack.watch/product/mikrotik/routeros/>>
- [31] Vulnerability Details : CVE-2020-11881. *CVE Details* [online]. [cit. 5.12.2022]. Dostupné z URL: <<https://www.cvedetails.com/cve/CVE-2020-11881/>>
- [32] Vulnerability Details : CVE-2018-5951. *CVE Details* [online]. [cit. 5.12.2022]. Dostupné z URL: <https://www.cvedetails.com/cve-details.php?t=1&cve_id=CVE-2018-5951>
- [33] WifiWave2. *mikrotik* [online]. [cit. 25.11.2022]. Dostupné z URL: <<https://help.mikrotik.com/docs/display/ROS/WifiWave2>>
- [34] WPA2 vs WPA3. *Diffen* [online]. [cit. 25.11.2022]. Dostupné z URL: <https://www.diffen.com/difference/WPA2_vs_WPA3>
- [35] 802.11r, 802.11k, and 802.11w Deployment Guide, Cisco IOS-XE Release 3.3. *cisco* [online]. [cit. 25.11.2022]. Dostupné z URL: <<https://www>.

cisco.com/c/en/us/td/docs/wireless/controller/technotes/5700/software/release/ios_xe_33/11rkw_DeploymentGuide/b_802point11rkw_deployment_guide_cisco_ios_xe_release33/b_802point11rkw_deployment_guide_cisco_ios_xe_release33_chapter_0100.html>

- [36] WireGuard. *mikrotik* [online]. [cit. 25.11.2022]. Dostupné z URL: <<https://help.mikrotik.com/docs/display/ROS/WireGuard>>
- [37] Certificates. *mikrotik* [online]. [cit. 25.11.2022]. Dostupné z URL: <<https://help.mikrotik.com/docs/display/ROS/Certificates>>
- [38] Winbox. *mikrotik* [online]. [cit. 28.11.2022]. Dostupné z URL: <<https://help.mikrotik.com/docs/display/ROS/Winbox>>
- [39] Firewall na Mikrotiku. *Wifi Home* [online]. [cit. 6.12.2022]. Dostupné z URL: <<https://wifihome.cz/firewall-na-mikrotiku/>>
- [40] MikroTik User Management (RouterOS User). *System Zone* [online]. [cit. 28.11.2022]. Dostupné z URL: <<https://systemzone.net/mikrotik-user-management-routeros-user/>>
- [41] What is a bogon address?. *APnic* [online]. [cit. 7.5.2023]. Dostupné z URL: <<https://www.apnic.net/manage-ip/apnic-services/registration-services/resource-quality-assurance/what-is-a-bogon-address/>>
- [42] Firewall Tool. *mikrotikconfig* [online]. [cit. 7.5.2023]. Dostupné z URL: <<https://mikrotikconfig.com/firewall/>>
- [43] What Is SSH: Understanding Encryption, Ports and Connection. *hostinger* [online]. [cit. 17.5.2023]. Dostupné z URL: <https://www.hostinger.com/tutorials/ssh-tutorial-how-does-ssh-work?fbclid=IwAR2cYyW3vWmy2hgfxo2YsaMgy1qKWNWL0M2cw-6vW3zzkX7Q-n1MTiIHA7Q#Session_Encryption_Negotiation>
- [44] What is a SYN Flood Attack?. *f5* [online]. [cit. 7.5.2023]. Dostupné z URL: <<https://www.f5.com/glossary/syn-flood-attack>>
- [45] Cisco Discovery Protocol (CDP). *learningnetwork.cisco* [online]. [cit. 7.5.2023]. Dostupné z URL: <<https://learningnetwork.cisco.com/s/article/cisco-discovery-protocol-cdp-x>>
- [46] RouterSploit - Exploitation Framework for Embedded Devices. *github* [online]. [cit. 7.5.2023]. Dostupné z URL: <<https://github.com/threat9/routersploit>>

Zoznam symbolov a skratiek

AAA server Authentication, Authorization, and Accounting server

ACL Access List

API Application programming interface

ARP Address resolution protocol

BIOS Basic input/output system

CBC Cipher block chaining

CDP Cisco Discovery Protocol

CERT Computer Emergency Response Team

CISA Cybersecurity and Infrastructure Security Agency

CLI Command-line interface

CPU Central processing unit

DANE DNS-based Authentication of Named Entities

DDoS A distributed denial-of-service

DEP Data Execution Prevention

DHCP Dynamic Host Configuration Protocol

DKIM DomainKeys Identified Mail

DMARC Domain-based Message Authentication, Reporting and Conformance

DDNSEC The Domain Name System Security Extensions

DNS Domain Name System

DoS Denial of service

ECSR Elliptic curve based secure remote password

FTP File transfer protocol

GPU Graphics processing unit

HTTP Hypertext Transfer Protocol

HTTPS Hypertext Transfer Protocol Secure

IANA Internet Assigned Numbers Authority

ICMP Internet Control Message Protocol

IDS Intrusion Detection System

IKE Internet Key Exchange

IPS Intrusion prevention system

KRACK Key Reinstallation Attack

KVM Kernel-based Virtual Machine

LLDP Link Layer Discovery Protocol

MAC Media access control address

MD5 Message-digest algorithm

MNDP MikroTik Neighbor Discovery protocol

NAC Network access control

NAT Network address translation

NSA National Security Agency

NTP Network Time Protocol

NUKIB Národní úřad pro kybernetickou a informační bezpečnost

OWE Opportunistic Wireless Encryption

PPPoE Point-to-Point Protocol over Ethernet

PPTP Point-to-Point Tunneling Protocol

PSK Pre-Shared Key

RC4 Rivest Cipher 4

RSA Rivest–Shamir–Adleman

SFTP Secure File Transfer Protocol

SNMP Simple Network Management Protocol

SPF Sender Policy Framework

SSH Secure Socket Shell

SYN Synchronize

TCP Transmission Control Protocol

TFTP Trivial File Transfer Protocol

TLS Transport Layer Security

UDP User Datagram Protocol

UEFI Unified Extensible Firmware Interface

UPNP Universal Plug and Play

VLAN Virtual local area network

VoIP Voice over Internet Protocol

VPN Virtual Private Network

WAN Wide-area network

A Obsah elektronickej prílohy

Obsahom elektronickej prílohy je konfiguračný skript napísaný v skriptovacom jazyku od spoločnosti Mikrotik s názvom FirstConfig.txt. v zložke Prílohy.

Druhou prílohou je skript, ktorý vytvorí zoznam adres, ktoré budú použité v geolokačnom firewall pravidle pri konfigurácii firewallu a je potrebné ho mať stiahnutý spoločne s prvým konfiguračným skriptom. Názov tejto prílohy je geo.rsc a taktiež sa nachádza v zložke Prílohy.

```
/.....koreňový adresár priloženého archívu
├── Prílohy.....Prílohy
│   ├── FirstConfig.txt
│   └── geo.rsc
```