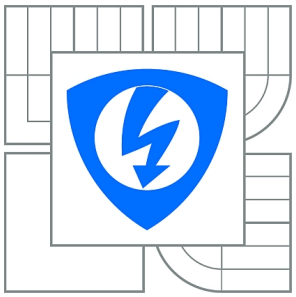
VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

BRNO UNIVERSITY OF TECHNOLOGY



FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ
ÚSTAV TELEKOMUNIKACÍ

FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION
DEPARTMENT OF TELECOMMUNICATIONS

BEZPEČNOSTNÍ RIZIKA SOUČASNÝCH SMĚROVAČŮ

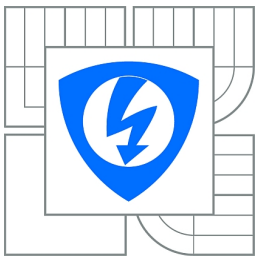
SAFETY RISKS OF CURRENT ROUTERS

BAKALÁŘSKÁ PRÁCE
BACHELOR'S THESIS

AUTOR PRÁCE — PETER BUBELÍNY
AUTHOR

VEDOUCÍ PRÁCE — Ing. PETR VYCHODIL
SUPERVISOR

BRNO 2010



VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

Fakulta elektrotechniky a komunikačních technologií

Ústav telekomunikací

Bakalářská práce

bakalářský studijní obor
Teleinformatika

Student:	Peter Bubelíny	***ID:***	106382
Ročník:	3	***Akademický rok:***	2009/2010

NÁZEV TÉMATU:

Bezpečnostní rizika současných směrovačů

POKYNY PRO VYPRACOVÁNÍ:

Prostudujte a vhodně zdokumentujte problematiku zabezpečení směrovačů. Diskutujte známá řešení a proveďte jejich zhodnocení. Na základě těchto poznatků proveďte vybrané útoky na směrovače a výsledky vhodně prezentujte.

DOPORUČENÁ LITERATURA:

[1] SCHUDEL, G., SMITH, D. Router Security Strategies Securing IP Network Trafic Planes, 2007
[2] THOMAS, M. Zabezpečení počítačových sítí. 2005

Termín zadání:	29.1.2010	***Termín odevzdání:***	2.6.2010

Vedoucí práce: Ing. Petr Vychodil

prof. Ing. Kamil Vrba, CSc.
Předseda oborové rady

ABSTRAKT

Bakalárska práca si kladie za cieľ preštudovať a zdokumentovať problematiku zabezpečenia smerovačov. Podáva charakteristickú informáciu o smerovači, jeho funkciách, typoch a umiestneniach v počítačovej sieti. Keďže je smerovač neoddeliteľnou súčasťou siete, sú ďalej opísané najčastejšie typy útokov a zároveň všeobecne dostupné bezpečnostné techniky. Práca ďalej ponúka pohľad na smerovač v úlohe bezpečnostného zariadenia a to v roli hrdla siete, súčasti hlbšej bezpečnostnej infraštruktúry alebo prístupového bodu v bezdrôtových sieťach. Sú opísané vybrané techniky zabezpečenia, voči niektorým už spomenutým útokom a zároveň sú ponúknuté možnosti zvýšenia bezpečnosti samotného smerovača. Ďalej sú demonštrované útoky typu DoS a „hrubou silou“ na smerovač v ethernetovej sieti a útoky založené na metóde odpočúvania paketov na smerovač v bezdrôtovej sieti. Na záver sú názorne prezentované dosiahnuté výsledky.

KĽÚČOVÉ SLOVÁ

smerovač, bezpečnosť smerovača, sieťová bezpečnosť, sieťový útok, filtrovanie obsahu, riadenie prístupu , ICMP, smerovanie, firewall, odoprenie služieb, DoS, hrubá sila, Medusa, Aircrack-ng, wep, wpa2, MAC adresa

ABSTRACT

The thesis aims to study and document the problem router security. It present the characteristic information about a router, functions, types and locations in a computer network. Because router is integrated part of network, next are described the most commonly types of attacks and generally available security technologies. The thesis also offers insight into thevrouter as a safety device in the role of the throat network, part of the deeper security infrastructure or access point in wireless networks. Next are described the selected security technologies against some of already mentioned attacks and also are offered opportunities to improve safety router. The next are demonstrated DoS and brute-force attacks on router in ethernet network and attacks based on sniffing packets on router in wireless network. Finally, the results are presented.

KEYWORDS

router, router security, network security, network attack, content filtering, access control, ICMP, routing, firewall, denial of service, DoS, brute-force, Medusa, Aircrack-ng, wep, wpa2, MAC address

BUBELÍNY P. *Bezpečnostní rizika současných směrovačů.* Brno: Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, 2010. 89 s. Vedoucí bakalářské práce Ing. Petr Vychodil.

PROHLÁŠENÍ

Prohlašuji, že svou bakalářskou práci na téma „Bezpečnostní rizika současných směrovačů“ jsem vypracoval samostatně pod vedením vedoucího bakalářské práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou všechny citovány v práci a uvedeny v seznamu literatury na konci práce.

Jako autor uvedené bakalářské práce dále prohlašuji, že v souvislosti s vytvořením této bakalářské práce jsem neporušil autorská práva třetích osob, zejména jsem nezasáhl nedovoleným způsobem do cizích autorských práv osobnostních a jsem si plně vědom následků porušení ustanovení § 11 a následujících autorského zákona č. 121/2000 Sb., včetně možných trestněprávních důsledků vyplývajících z ustanovení § 152 trestního zákona č. 140/1961 Sb.

V Brně dne ....

(podpis autora)

POĎAKOVANIE

Ďakujem vedúcemu práce Ing. Petrovi Vychodilovi za užitočnú metodickú pomoc a cenné rady pri spravcovávaní bakalárskej práce, spoločnosti KyberTech s.r.o. za zapožičanie smerovača RB433 a taktiež svojej priateľke, ktorá mi bola podporou pri písaní práce.

V Brně dňa ....

(podpis autora)

OBSAH

ZOZNAM OBRÁZKOV

ZOZNAM TABULIEK

ÚVOD

Dnešná moderná doba nám prináša nesmierne veľký a rýchly pokrok technológií. Človek je súčasťou „informačnej spoločnosti“, v ktorej je samozrejmosťou každodenné používanie výpočtovej techniky. Výpočtová technika nám uľahčuje život a my sa stávame čoraz viac pohodlnejšími, ba dokonca sa až príliš na ňu spoliehame. Musíme si však uvedomiť, že mnohokrát so sebou prináša aj isté riziká v podobe cielených útokov, ktorých účelom je napríklad získanie informácií s veľkou hodnotou.

Používanie počítača je rutinnou záležitosťou, ba až nutnosťou dnešnej doby. Pripojenie do Internetu je dnes k dispozícii takmer všade, a preto neustále rastie potreba bezpečnosti nielen Internetu, ale aj lokálnych, firemných či domácich sietí. Bezpečnosť je veľmi nutným prvkom, ale nie každý si uvedomuje jej možnosti, dôležitosť a s ňou spojené riziká. Bezpečnosť sietí závisí od viacerých faktorov a taktiež použitých prvkov. Jedným z týchto prvkov je smerovač. Keďže je smerovač určený k prepájaniu dvoch alebo viacerých sietí, jeho úlohou je pôsobiť ako brána medzi sieťami. Tým, že je pomerne často centrálnym bodom zabezpečenia, zároveň sa stáva aj prístupovým bodom do zabezpečovacieho obvodu našej siete.

Cieľom tejto bakalárskej práce je preštudovať a vhodne zdokumentovať problematiku zabezpečenia smerovačov a následne predviesť vybrané útoky na smerovače a výsledky vhodne prezentovať. Keďže je smerovač aktívnym prvkom počítačovej siete, je nevhodné analyzovať problematiku bezpečnosti smerovača ako samotného zariadenia, ale ako zariadenia v rámci zapojenia v nejakej sieti.

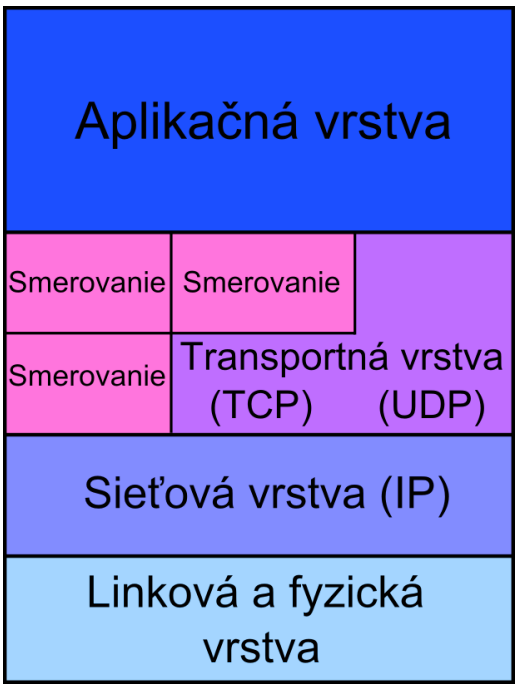
Práca je rozdelená do piatich kapitol. Prvá kapitola sa zaoberá charakteristikou a funkciou smerovača, jeho základnými princípmi, jednotlivými typmi smerovačov a ich umiestnením. Druhá kapitola je venovaná útokom na sieť ako takú, pretože smerovač je jej súčasťou. Sú tu objasnené vybrané typy útokov a ich cieľ. Tretia kapitola v krátkosti popisuje niektoré bezpečnostné mechanizmy sietí, ktoré nám poskytujú ochranu pred nežiadúcimi útokmi. Štvrtá kapitola vysvetľuje funkciu smerovača v úlohe bezpečnostného zariadenia, a to ako jediného alebo ako súčasti hlbšej bezpečnostnej ochrany. Ďalej je vysvetlená funkcia smerovača ako súčasti bezdrôtovej siete, taktiež spôsoby, ktorými môžeme smerovač zodolniť a lepšie ochrániť pred napadnutím. Piata kapitola predstavuje praktickú časť tejto bakalárskej práce. Sú tu demonštrované vybrané útoky na smerovače v ethernetovej sieti, ale i v bezdrôtovej sieti a k záveru tejto kapitoly je podané názorné zhodnotenie.

1 SMEROVAČ

Smerovač (anglicky router) patrí medzi najinteligentnejšie aktívne prvky počítačovej siete. Je to viacportové zariadenie, ktoré pracuje na úrovni sieťovej vrstvy modelu ISO/OSI. Podľa nárokov kladených na výkon, smerovačom môže byť obyčajný počítač s viacerými sieťovými rozhraniami, ale aj špecializované zariadenie s hardwarovou podporou smerovacích funkcií.

1.1 Charakteristika a funkcia smerovača

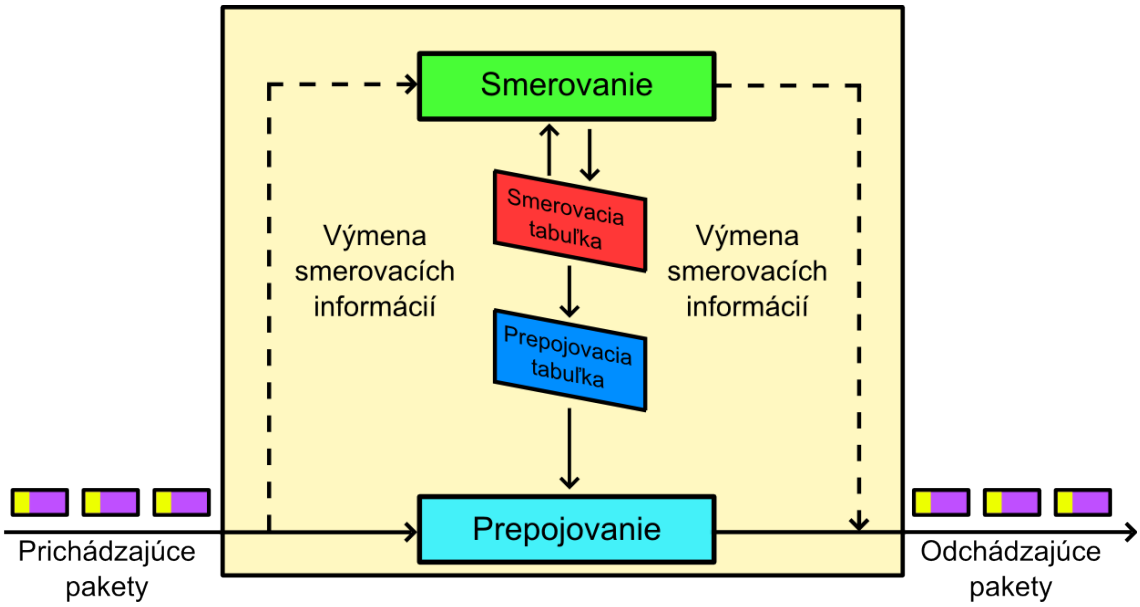
Prvoradou a hlavnou úlohou smerovača je zhromažďovať informácie o pripojených sieťach a následne vyberať najvýhodnejšiu cestu, ktorou sa sprostredkuje prenos dát medzi dvoma, alebo viacerými počítačovými sieťami. Tento proces sa nazýva smerovanie (anglicky routing) a z hľadiska referenčného modelu ISO/OSI je to jedna z najdôležitejších funkcií sieťovej vrstvy. Skutočné smerovacie protokoly však nie sú vždy implementované do sieťovej vrstvy. Možné umiestnenie smerovacích funkcií v referenčnom modely TCP/IP je ilustrované na obrázku 1.1 . [17]



Obr. 1.1: Možné umiestnenie smerovacích funkcií v referenčnom modeli TCP/IP.

Smerovač ďalej analyzuje každý IP datagram, ktorý dostane na jednom zo svojich sieťových rozhraní a rozhoduje, do ktorého iného sieťového rozhrania má IP datagram poslať. Tento proces sa už nazýva prepojovanie (anglicky forwarding).

Smerovač dokáže poslať IP datagram aj do toho istého rozhrania, z ktorého IP datagram prišiel. Takáto možnosť nastáva obvykle vtedy, keď smerovače navzájom komunikujú a vymieňajú si informácie o stave siete, smerovaní a o zmene topológie prostredníctvom služobného protokolu ICMP.



Obr. 1.2: Funkcia smerovača.

Aby smerovač získal potrebné informácie k správnemu rozhodnutiu, kam má prijatý IP datagram odoslať, musí v dostatočnej miere poznať topológiu siete. Smerovač tieto znalosti môže získať formou statickej konfigurácie, ktorú vytvorí napríklad správca siete. Vtedy hovoríme o statickom smerovaní. Smerovač taktiež môže informácie o topológii siete získať výmenou informácií s ďalšími smerovačmi v sieti, v tomto prípade potom pôjde o dynamické smerovanie. Dynamické smerovanie dokáže automaticky detekovať zmeny v topológii, akými napríklad sú: pripojenie nových sietí, odpojenie sietí, výpadok linky a iné. Všetky tieto informácie sú rozosielané ostatným smerovačom, aby mohli urobiť príslušné aktualizácie a uložiť si ich do smerovacej tabuľky.

Smerovacia tabuľka je vytváraná smerovacím algoritmom, založená na informáciách získaných od susedných smerovačov, slúži k mapovaniu IP prefixu na jednom zo susedných uzlov a je optimalizovaná pre rýchly prepočet v prípade zmien v topológii. Smerovač ešte obsahuje prepojovaciu tabuľku, ktorá je na rozdiel od smerovacej tabuľky vytváraná samotným smerovačom. Táto tabuľka mapuje IP prefixy na konkrétnom rozhraní smerovača, je optimalizovaná pre rýchle vyhľadávanie a môže obsahovať ďalšie prídavné informácie, napríklad MAC adresu daného rozhrania. Na základe tejto tabuľky smerovač vykonáva prepojovanie IP datagramu

zo vstupného rozhrania na príslušné výstupné rozhranie. Pre správnu komunikáciu medzi smerovačmi slúžia smerovacie protokoly. Poznáme dva typy smerovacích protokolov. Prvým z nich sú protokoly typu „distance-vector“, ktoré vyberajú najkratšiu cestu k cieľovej sieti, cestu s najmenším počtom preskokov (anglicky hop). Jedným z predstaviteľov tohto typu je napríklad protokol RIP. Druhým typom sú protokoly typu „link-state“, ktoré priraďujú každej linke váhový koeficient, nazývaný metrika. Na linke môže byť priradených aj viacero metrík. Správy šíriace informácie o metrikách liniek sa nazývajú LSA, a najlepšia je tá cesta, ktorá má najmenší celkový súčet metrík. Jedným z typov takého protokolu je protokol OSPF. [19]

Ďalšou dôležitou funkciou smerovača je implementácia zaistenia kvality služieb (anglicky Quality of Service, QoS). Služba QoS zabezpečuje dodržanie vopred stanovených pravidiel pri prenose dát. Na linkovej vrstve sa QoS rieši pre technológiu ATM a na sieťovej vrstve i pre klasické IP siete. Pri implementácii na úrovni IP existuje však niekoľko metód. Najznámejšie sú Integrované služby (anglicky Integrated Service, IntServ) a Diferencované služby (Differentiated services, DiffServ).

Pretože obvykle je smerovač bránou do siete, zohráva významnú úlohu v zabezpečení siete. Práve z tohto dôvodu bol smerovač navrhnutý s mnohými vstavanými bezpečnostnými prvkami, ako sú paketový filter, integrovaný firewall či podpora virtuálnych súkromných sietí (anglicky Virtual Private Networks, VPN).

1.2 Typy smerovačov a ich umiestnenie

1.2.1 Chrbtový smerovač

Chrbtový smerovač (anglicky core router) je súčasť chrbtovej siete poskytovateľa dátového pripojenia. Jeho úlohou je prepájať tisíce sietí s veľkým počtom užívateľov. Nároky na jeho výkon sú veľmi vysoké, pričom dôraz sa kladie na vysokú rýchlosť, priepustnosť a spoľahlivosť, z čoho vyplýva, že je cenovo náročný. Takýto typ smerovača realizuje také kritické operácie, akými sú prehľadávanie rozsiahlych smerovacích a prepojovacích tabuliek.

1.2.2 Hraničný smerovač

Hraničný smerovač (anglicky edge/access router) umožňuje pripojenie zákazníkov k poskytovateľovi dátového pripojenia. Nároky na jeho výkon sú v porovnaní s chrbtovým smerovačom oveľa menšie, pretože slúžia na agregáciu prevádzky z rôznych prístupových technológií, ako napríklad: DSL, Ethernet a iné. Okrem iného je charakteristický veľkým počtom portov a veľkou intenzitou prevádzky. Podporuje väčšie množstvo protokolov pre vzdialený prístup, napríklad: PPTP, PPPoE, IPSec atď.

Takýto typ smerovača je vždy posledným prvkom siete pred vstupom do internetu. [19]

1.2.3 Okrajový smerovač

Okrajový smerovač (anglicky igress/egress router) leží obvykle na okraji DiffServ domény, v časti siete, ktorá nepoužíva značkovanie paketov. Je to menšia počítačová sieť, spomedzi viacerých sietí, ktoré tvoria jednu rozsiahlu sieť. Má samostatnú správu a je organizačne inak usporiadaná, a preto v nej dochádza k odlišnému spracovaniu paketov z dôvodu zaistenia QoS na určitej úrovni. Okrajový smerovač je podľa svojho umiestnenia buď vstupný (anglicky ingress), alebo výstupný (anglicky egress) smerovač. Jeho nároky na výkon sú skoro rovnaké ako pri hraničnom smerovači, pričom okrajový smerovač má za úlohu klasifikovať tok dát a posielať pakety ďalej do DiffServ domény, to znamená, že má označovať pakety značkou, ktorá určuje ako sa má s paketom zaobchádzať, podľa požadovanej úrovne QoS. [6]

1.2.4 Podnikový smerovač

Podnikový smerovač (enterprise router) slúži na prepojenie koncových staníc, serverov a iných prvkov siete, taktiež na hierarchické usporiadanie podsietí. Jeho základnými požiadavkami sú veľký počet portov, bežne pre prenos 10/100/1Gb Ethernet, podpora zaistenia kvality služieb, efektívna podpora skupinového a viacsmerového prenosu a tiež podpora zabezpečovacích mechanizmov akými sú: filtrovanie sieťového prenosu, integrovaný firewall a technológia VLAN. [19]

2 TYPY NAJČASTEJŠÍCH ÚTOKOV NA SIEŤ

Nové útoky pribúdajú obrovskou rýchlosťou, a to doslova denne. Tisícky sietí sú vystavované rizikám napadnutia a cieľom útoku môže byť čokoľvek. Preto je veľmi dôležité vedieť o najčastejších typoch útokov a spôsobov zneužitia.

2.1 Odoprenie služieb

Útok odoprenie služieb (anglicky Denial of Service, DoS) je útok, pri ktorom sa útočník snaží falošnými požiadavkami odoprieť bežné služby všetkým, i právoplatným užívateľom daného systému. Možností, ako zrealizovať tento útok je veľké množstvo, jedným z nich je napríklad zaplavenie (anglicky floods) obete množstvom falošných požiadaviek o pripojenie. Ak má útočník vyššiu sieťovú kapacitu než hostiteľ, útok záplavou je o to efektívnejší a silnejší.

2.2 Distribuované odoprenie služieb

Distribuované odoprenie služieb (anglicky Distributed Denial of Service, DDoS) je typ útoku, ktorý útočí na vyhliadnutú obeť z väčšieho množstva rôznych napadnutých, nič netušiacich systémov. Úspešnosť tohto útoku sa zvyšuje tým, ak na cieľ posiela falošné požiadavky niekoľko útočiacich strojov s nezávislým hardvérom a nezávislým prenosovým pásmom. V praxi sa počet takýchto strojov pohybuje rádovo v stovkách až tisíckach. Tieto útočiace stroje sú spravidla pripojené do jedného BotNetu a tým pádom je útok distribuovaný a decentralizovaný, ale centrálne ovládaný a silne koordinovaný.

2.3 Záplava paketov ICMP

Tento útok patrí do skupiny DoS útokov a znamená, že pakety ICMP alebo ping preťažia cieľový systém takým množstvom požiadaviek na opakovanie (anglicky echo), že systém vyčerpá svoje prostriedky na odpovede a nebude môcť spracovávať normálnu prevádzku. Správ ICMP existuje niekoľko typov, pričom každá správa má svoj osobitý význam [28]:

- ICMP Echo Reply. Odpoveď na opakovanie, kód 0. Ide o odpoveď ping.
- ICMP Host Unreachable. Hostiteľ je nedosiahnuteľný, kód 3. Chybová správa od hostiteľa alebo smerovača, že odoslaný paket nedorazil do cieľa.

- ICMP Source Quench. Spomalenie zdroja, kód 4. Indikácia zahltenia určitého miesta v internete.
- ICMP Redirect: Presmerovanie, kód 5. Správa so žiadosťou o presmerovanie prevádzky.
- ICMP Echo Request. Žiadosť o opakovanie, kód 8. Pakety s požiadavkou ping.
- ICMP Time Exceeded for a Datagram. Prekročenie času pre prenos datagramu, kód 11. Chybová správa, že paket nedorazil do cieľa z dôvodu prekročenia určitého časového limitu.
- ICMP Parameter Problem on Datagram. Problém v parametri datagramu, kód 12. Táto správa je obvykle indikátorom útoku.
- Veľký paket ICMP. Paket ICMP o veľkosti 1024 bajtov môže pri niektorých zariadeniach znamenať problémy, pretože nie je považovaný za normálny.

2.4 Smurf útok

Smurf útok patrí medzi typy DoS útokov, nazýva sa „smurfing“ a je odvodený od prvého programu s názvom Smurf, ktorý tento útok vykonával. Pri tomto útoku útočník vyšle veľkú sériu za sebou idúcich ICMP správ typu Echo Request na broadcast adresu siete. Ak potom všetky počítače v sieti pošlú odozvu na výzvu na zasiahnutú adresu, útočník v rozsiahlej sieti pomocou jedného požiadavku vyvolá pomerne značne veľkú vlnu paketov s odozvou. Výsledok takéhoto náporu paketov môže spôsobiť pád linky. [22]

2.5 Útok so záplavou paketov UDP

Útok so záplavou paketov UDP je podobný útoku záplave ICMP. Jeho úlohou je taktiež, výrazne spomaliť spracovanie platných spojení na cieľovom systéme. V tomto útoku sa dajú zneužiť služby postavené na UDP protokole. Jednou z nich je služba DNS, ktorá je obsluhovaná na porte 53. Ďalšími službami sú chargen na porte 19 a echo na porte 7, slúžiace k testovaniu spojenia či priepustnosti. Tieto služby odpovedajú prichádzajúcim paketom zaslaním paketu obsahujúci bezvýznamné dáta. Toto môže útočník využiť k vytvoreniu smyčky, medzi dvoma systémami, ktoré si medzi sebou budú vymieňať bezvýznamné UDP pakety. [13]

2.6 Útok so záplavou paketov SYN

Podobne ako v predchádzajúcej podkapitole existujú záplavy postavené aj na protokole TCP. Jediným rozdielom oproti UDP záplave je možnosť nastavenia rozličných príznakov TCP paketom. V rámci tohto útoku sa sieť taktiež zahltí, a to paketami SYN, ktoré primárne znamenajú zahájenie požiadavky o spojenie zo strany klienta. V skutočnosti je to obyčajný TCP paket s príznakom SYN, očakávajúci odpoveď SYN/ACK. Klient opätovne potvrdí ACK, a v tom okamihu na strane serveru dochádza k ukladaniu polootvorených spojení do rady. Tu spojenie čaká na potvrdzovací paket ACK, a keďže rada nie je neobmedzená, problémom je veľké množstvo polootvorených spojení. Ak sa útočníkovi podarí odosielať ACK pakety tak rýchlo, že radu zaplní, server prestane prijímať žiadosti o spojenia na všetkých portoch. Výsledkom takéhoto obsadenia nielen sieťového rozhrania, ale i procesoru a pamäte vzniká odoprenie služieb - DoS. Útok tohto typu využíva nedokonalosti a nedostatky v špecifikácii protokolu TCP/IP. [13]

2.7 Smrteľný ping

Špecifikácia protokolu TCP/IP určuje pre prenos IP datagramu presnú veľkosť paketu. Mnohé implementácie protokolu ping, umožňujú užívateľovi podľa potreby zadať inú, väčšiu veľkosť paketu. Výrazne neprimerane veľký paket ICMP môže v systéme vyvolať množstvo nežiaducich účinkov, akými napríklad sú: odoprenie služieb, havárie či reštart systému a iné. V prílohe možno vidieť porovnanie veľkosti odozvy lokálneho smerovača s adresou 192.168.1.1 klientovi na žiadosť ping. Ak je smerovač zaťažený veľkými paketami ICMP typu ping, napríklad programom NetTester (príloha A.1), zaťaženie smerovača v domácej LAN sieti je badateľné na hodnote *time*, ktorá je v priemere 303 ms (príloha A.2). Bez zaťaženia smerovača je hodnota *time* menšia ako 0 (príloha A.3).

2.8 Prehľadávanie portov

Tento útok znamená vysielanie paketov s rôznymi číslami portov. Jeho cieľom je nájsť dostupnú službu k následnému zneužitiu. V prílohe A.4 môžeme vidieť prehľadanie portov na adrese 147.229.2.90 (www.vutbr.cz) pomocou programu Zenmap. Port s bežiacou službou je možné i odhadnúť, a to jedine v takom prípade, že sú dodržané určité konvencie. Nie je určené, či napríklad http server musí byť spustený na štandardnom porte 80. Jediné pravidlo, ktoré platí bez výnimky je, že na jednom porte môže bežať iba jedna služba.

2.9 Prehľadávanie so žiadosťou ping

Účelom tohto útoku je získať IP adresu potenciálnej obete, a to sledovaním odpovede, na zaslané požiadavky opakovaním echo ICMP na rôzne cieľové adresy, podobne ako pri prehľadávaní portov.

2.10 Zdrojové smerovanie

Mechanizmus zdrojového smerovania je variantom hlavičky paketu IP, v ktorej samotný zdroj definuje spôsob smerovania paketov. Smerovacie informácie v hlavičkách IP datagramu môžu napríklad obsahovať inú zdrojovú IP adresu, ako samotný zdroj v hlavičke, čo spôsobuje, že pakety budú poslané iným smerom. Smerovanie paketov ICMP je možné ovládať niekoľkými ďalšími spôsobmi [28]:

- Záznam cesty. Útočník odosiela pakety s voľbou IP 7, záznam cesty (anglicky Record Route). Zaznamenanú cestu tvorí postupnosť internetových adries. Jej analýzou môže pozorovateľ zistiť informácie o schéme adresovania a topológie vnútornej siete.
- Voľné zdrojové smerovanie. Útočník odosiela pakety s voľbou IP 3, voľné zdrojové smerovanie (anglicky Loose source routing). To znamená, že zdroj paketu môže určiť smerovanie, podľa ktorého sa bude paket odosielať do cieľa cez jednotlivé brány. Každá z brán a hostiteľov môže ale odoslať paket na ďalšiu adresu v požadovanej ceste cez ľubovoľný počet medziľahlých brán.
- Striktné zdrojové smerovanie. Útočník odosiela pakety s voľbou IP 9, striktné zdrojové smerovanie (anglicky Strict source routing). V tomto prípade zdroj určí paketu presné smerovanie do cieľa. Každá z brán a hostiteľov musí ale odoslať datagram na ďalšiu adresu v požadovanej ceste priamo a iba cez priamo prepojenú sieť.

2.11 Falšovanie IP adries

Pri útoku falšovaním IP adries (anglicky IP spoofing), sa útočník pokúša obísť bezpečnostné kontroly firewallu tým, že napodobňuje, predstiera IP adresu, alebo iné ID platného klienta. Toto je dôležité predovšetkým pri zneužití vzťahu dôvery medzi počítačmi, ktorá je v sieti často definovaná.

2.12 Falšovanie ARP

Podobne ako pri útoku falšovaním IP adries, je pri falšovaní ARP (anglicky ARP spoofing) hlavným cieľom predstierať ARP odpovede. ARP mechanizmus slúži na získanie ethernetovej MAC adresy počítača z jeho IP adresy. Princíp útoku teda spočíva v zasielaní podvrhnutej ARP odpovede so svojou MAC adresou, pričom si cieľ falošnú adresu zaznamená a na ňu posiela pakety. [24]

2.13 Falšovanie DNS

Falšovanie DNS (anglicky DNS spoofing), je útok na službu DNS. Cieľom je, aby útok zmenil DNS záznam tak, aby odkazoval na falošnú adresu, inú ako bola pôvodne správne nastavená. Tým môže útočník svoju obeť bez jej vedomia presmerovať na svoje stránky za dôvodom napríklad odcudzenia rôznych údajov.

2.14 Falošný DHCP server

V dnešnej dobe väčšina klientov, používa pre svoje sieťové nastavenie údaje, ktoré získa automaticky z DHCP serveru. Keďže DHCP protokol nie je nijako zabezpečený, ponúka sa nám ďalšia príležitosť zneužitia. Klient sa nezaujíma, od ktorého DHCP serveru dostane pridelenú IP adresu, a preto, ak mu útočník pridelí správnu IP a sprevádzkuje komunikáciu medzi ním a skutočným DHCP serverom, môže odchytávať celú komunikáciu. Stačí, aby mal klient nastavenú ako predvolenú bránu práve falošný DHCP server. Ak stanica posiela dáta smerom von k serveru, všetky dáta idú cez útočníka. Skutočný DHCP server je možné dokonca i zaplaviť, požiadavkami prichádzajúcimi z mnohých staníc. [9]

2.15 Pozemný útok

Kombináciou útokov so záplavou paketov SYN a falšovaním IP adries vzniká pozemný útok (anglicky land attack). Jeho úlohou je zasielať do cieľovej siete sfalšované pakety SYN, pričom ich zdrojovú a cieľovú IP adresu tvorí skutočná IP adresa obete. Cieľový systém na pakety reaguje odoslaním paketu SYN/ACK sebe samému. Takto vzniká prázdne spojenie, ktoré je otvorené až do vypršania časového limitu. Záplava prázdnymi spojeniami dokáže systém úplne zahltiť. [28]

2.16 Slzička

Slzička (anglicky tear drop) zneužíva mechanizmus rekonštrukcie fragmentovaných paketov IP. Keďže jedným z údajov hlavičky IP datagramu je relatívna adresa (anglicky offset), musí sa súčet relatívnej adresy a veľkosti jedného fragmentovaného paketu rovnať so súčtom a veľkosťou nasledujúceho fragmentovaného paketu, inak sa oba pakety prekrývajú a server môže pri pokuse o ich rekonštrukciu havarovať.

2.17 WinNuke

Je to aplikácia, ktorej jediná úloha je priviesť k havárii akýkoľvek počítač s operačným systémom Windows do verzie 95, pripojený do Internetu. Program WinNuke odosiela do cieľového počítača s nadviazaným spojením dáta mimo rozsah, obvykle na port NetBIOS s číslom 139 a vyvolá prekrytie fragmentov NetBIOS, čo spôsobuje haváriu počítača. [28]

2.18 Odpočúvanie paketov

Technika odpočúvania paketov (anglicky sniffing) predstavuje pasívnu metódu útoku, ale o to nebezpečnejšiu. Ak sa útočníkovi podarí dostať do lokálnej siete (anglicky Local Area Network, LAN) nástroj pre odpočúvanie, alebo sa v horšom prípade zmocní akéhokoľvek stroja v LAN dochádza k veľmi vážnemu narušeniu bezpečnosti siete, pretože útočník vidí väčšinu paketov v sieti. Je to spôsobené tým, že dáta sú po LAN posielané v paketoch a každý obsahuje MAC adresu stroja, pre ktorý je určený. Adresa je síce jedinečná, ale neznamená to, že sa nedá zmeniť. Dôležité je, že v sieti je paket viditeľný pre všetky zariadenia, ale príjme ho len stroj s požadovanou adresou, ostatné ho ignorujú. Keď paket vstúpi do sieťovej karty (NIC), na jeho cieľovú adresu sa aplikuje hardvérový filter. Ten rozhodne, či paket bude ignorovaný, alebo prijatý. Väčšina ethernetových NIC však umožňuje tento hardvérový filter vypnúť a dostať NIC do promiskuitného režimu, čo spôsobí, že systém zachytáva všetky pakety a následne ich odovzdáva užívateľským programom, ktoré celú sieťovú komunikáciu môžu ukladať do súboru. V ňom útočník môže nájsť veľmi zaujímavé, zneužiteľné informácie akými napríklad sú: údaje z hlavičiek paketov, užívateľské mená či heslá. [13]

3 BEZPEČNOSTNÉ PROSTRIEDKY A MECHANIZMY SIETÍ

Bezpečnosť siete sa skladá z rôznych prostriedkov, ktoré závisia vždy na tom, akým potenciálnym útokom a hrozbám je sieť vystavená. Aby sme znížili riziko vniknutia útočníka do siete, mali by sme použiť všetky dostupné prostriedky a mechanizmy, ktoré sú nám k dispozícii.

3.1 Firewall

Firewall je špeciálnym bezpečnostným zariadením, ktoré je umiestnené na hranu internetového pripojenia. Jeho hlavnou úlohou je neustále dohliadať na bezpečnosť všetkých prvkov vnútornej siete. Toto zariadenie pracuje na sieťovej vrstve a kontroluje všetku sieťovú prevádzku, ktorá vstupuje do niektorého z jeho rozhraní. V dnešnej dobe je už napríklad softvérový firewall vo väčšej miere súčasťou operačných systémov. Firewall implementuje rôzne filtračné mechanizmy, o ktorých sa zmienim v nasledujúcich kapitolách.

3.2 Filtrovanie paketov

Tento spôsob zabezpečenia je jeden z najstarších a najrozšírenejších spôsobov riadenia prístupu k sieťam. Podľa určitých identifikačných údajov v hlavičke paketu rozhodneme, či daný paket môže vstúpiť, prípadne vystúpiť zo siete. Metóda konfigurácie a riadenia paketových filtrov sa označuje ako prístupový zoznam (anglicky access control lists, ACL). Technológia filtrovania paketov je dnes súčasťou mnohých operačných systémov, softvérových i hardvérových firewallov, a taktiež patrí medzi bezpečnostné funkcie väčšiny smerovačov.

3.3 Stavová inšpekcia paketov

Stavová inšpekcia paketov (anglicky Stateful Packet Inspection, SPI) je pokročilejšia metóda filtrácie paketov. Táto technológia je väčšinou implementovaná vo firewalle a je orientovaná na spojenie, pretože spojenie sa skladá z prenosu množstva paketov. Mechanizmus stavovej inšpekcie sa spustí hneď s prvým paketom, ktorý zahajuje komunikáciu v spojení. Inšpekcia spojenia vytvorí záznam a ďalšie pakety sa prepustia len vtedy, ak patria k povolenému existujúcemu spojeniu, inak sa spojenie preruší.[28]

3.4 Preklad sieťových adries

Mechanizmus prekladu sieťových adries (anglicky Network Address Translation, NAT) je zavedený a spustený na vhodnom zariadení, akým je firewall, smerovač a počítač, ktorý je umiestnený medzi vnútornú sieť s privátnymi IP adresami a vonkajším Internetom obsahujúci verejné IP adresy. Toto zariadenie potom pomocou tohto mechanizmu robí preklady adries z privátnych na verejné. Technológia NAT je pomerne dosť rozšírená, pretože rieši problém s nedostatkom verejných adries IPv4 a taktiež poskytuje zvýšenie bezpečnosti siete.

3.5 Ochrana pomocou proxy

Služba proxy je v počítačovej sieti sprostredkovaná pomocou proxy servera alebo proxy firewallu. Proxy server je prvok, ktorý voči svojim klientom vystupuje ako server a voči cieľovému serveru vystupuje ako klient. Jeho úlohou je sprostredkovať komunikáciu medzi klientom a cieľovým serverom. Tento server je niekedy označovaný ako aplikačná brána, pretože funguje ako brána a zaisťuje spojenie so vzdialenou službou. Spolu s proxy firewallmi zabezpečujú na aplikačnej úrovni jeden z najbezpečnejších typov dátového spojenia, pretože dokážu v komunikácii, ktorá cez ne prebieha skúmať úplne všetky vrstvy modelu TCP/IP. Proxy firewally môžeme rozdeliť do nasledujúcich typov. Prvým z nich je štandardný proxy firewall, ktorý pracuje v aplikačnej vrstve TCP/IP a z funkčného hľadiska kontroluje prijaté pakety podľa definovanej množiny pravidiel. Druhým typom je dynamický proxy firewall, ktorý sa vyvinul z predchádzajúceho typu, ale je rozšírený o funkciu filtrovania paketov, čím môže vykonávať úplnú inšpekciu paketov. [22]

3.6 Virtuálne súkromné siete

Technológia VPN nám poskytuje pripojenie, pomocou šifrovacích mechanizmov, nad existujúcou verejnou sieťou. VPN môžeme vytvárať cez časť zdieľanej LAN, WAN alebo Internet. Poznáme tri základné typy VPN sietí:

- VPN pre vzdialený prístup, ktorá umožňuje bezpečné pripojenie cez Internet medzi sieťou LAN, centrálnym pracoviskom, a užívateľom, napríklad pracovníkom v teréne.
- VPN pre spojenie pracovísk. Ide o rozšírenie siete LAN napríklad vo firme do ďalších budov či pracovísk pomocou špecializovaného vybavenia. Tento typ VPN je stále aktívne pripojený a je označovaný ako intranetový VPN „LAN-to-LAN“.

- Extranetové VPN. Sú rozšírením intranetových VPN a umožňujú priamu a rýchlejšiu komunikáciu napríklad medzi firmou, dodávateľom a ďalším parnetrom.

Každý vzdialený užívateľ pripojený cez VPN, môže bezpečne komunikovať so súkromnou sieťou LAN cez Internet, pomocou štandardu pre šifrovanie VPN, ktorým je protokol IPSec. V referenčnom modeli ISO/OSI protokol IPSec tvorí sieťovú vrstvu a zaisťuje autentizáciu IP datagramov medzi zariadeniami akými napríklad sú smerovač a firewall, v ktorom je VPN implementované. [28]

3.7 Technológia AAA

Ak chceme cez počítačovú sieť pristupovať k určitým službám, vždy budeme potrebovať tri veci:

- Autentizácia - overenie totožnosti (anglicky authentication). Hlavnou úlohou autentizácie je overenie pravosti užívateľa, pretože neoprávnený prístup k sieti je nežiaduci a zvyčajne ju zaisťuje zdieľaná tajná informácia. Pomocou autentizácie sieťový administrátor vie, kto sa prihlásil k sieťovému zariadeniu alebo do Internetu.

- Autorizácia - stanovenie oprávnenia (anglicky authorization). Po úspešnom dokončení autentizácie prichádza na rad mechanizmus autorizácie. Pri autentizovanom užívateľovi musíme rozhodnúť, či je oprávnený k prevedeniu požadovaných informácií. Sieťový administrátor môže pomocou autorizácie kontrolovať úroveň prístupu, ktorú má užívateľ po prihlásení, a to obvykle pomocou ACL.

- Zúčtovanie - zber informácií (anglicky accounting). Zúčtovanie, alebo inak povedané zber informácií, nastáva po úspešnom dokončení procesu autentizácie a autorizácie. Sieťový administrátor pomocou nich zhromaždí informácie o prihlásených užívateľoch k sieťovému zariadeniu a ich činnosti. Tieto informácie môžu neskôr poslúžiť ako právoplatný dôkaz odpočúvania, falšovania alebo iných nežiaducich procesov.

Tieto tri časti sa spoločne označujú skratkou AAA, ktorá vyplýva z vyššie uvedených anglických výrazov, a často sa aj vyslovuje ako „triple A“. Medzi AAA protokoly patria napríklad RADIUS či TACACS. [28]

3.8 Detekcia sieťového narušenia

Systém detekcie narušenia (anglicky Intrusion Detection System, IDS) má za úlohu sledovať a identifikovať útoky, bezpečnostné prieniky a každé narušenie siete. IDS systémov existuje dosť veľké množstvo, ale každý tento systém pomocou senzorov analyzuje všetky prenosy, zachytáva pokusy o zneužitie všetkých známych zraniteľností a snaží sa nájsť rôzne signatúry, ktoré môžu indikovať nežiaducu činnosť. Signatúra je vzor, ktorým je označený každý útok v súbore známych útokov [7]. Ak je signatúra útoku nájdená v tomto súbore, vygeneruje sa výstraha, poprípade sa táto udalosť inak zaznamená. Väčšina systémov IDS sa spolieha na túto takzvanú detekciu signatúr (anglicky signature detection). Na rozdiel od paketového filtra či firewallu, IDS systém nezasahuje do prenosu a nerozhoduje či povolí alebo nepovolí prevádzku, ale iba analyzuje všetok prenos. Samozrejme existujú aj také IDS systémy, ktoré môžu reagovať na podozrivý prenos aktívnym spôsobom, akým je prerušenie dátového spojenia. [22]

3.9 Honey pot

Sú to programy, ktoré simulujú bežiace sieťové služby. Slúžia ako návnada pre útočníka, ktorý chce zneužiť zraniteľnosť bežiacich služieb. Sieťová prevádzka je sledovaná, všetky procesy systému sú logované a poskytujú informácie o útočníkovej aktivite. Ďalšie využitie je ako ochrana dôležitých serverov, kedy je útočník z portu obete presmerovaný do pasce honey potu. Po detekcii útoku nasledujú adekvátne protiopatrenia. Keďže služby bežiace na takomto systéme nie sú skutočne využívané užívateľmi, každé spojenie je podozrivé. [10]

3.10 Infraštruktúra verejného kľúča

Infraštruktúra verejného kľúča (anglicky Public Key Infrastructure, PKI) je technológia, ktorá vytvára základ systému, ktorý podporuje rôzne bezpečnostné služby, napríklad integritu a dôveryhodnosť dát. PKI zaisťuje autentizáciu, overenie totožnosti a platnosti oboch strán komunikácie, prostredníctvom pokročilých digitálnych certifikátov a certifikačných autorít.

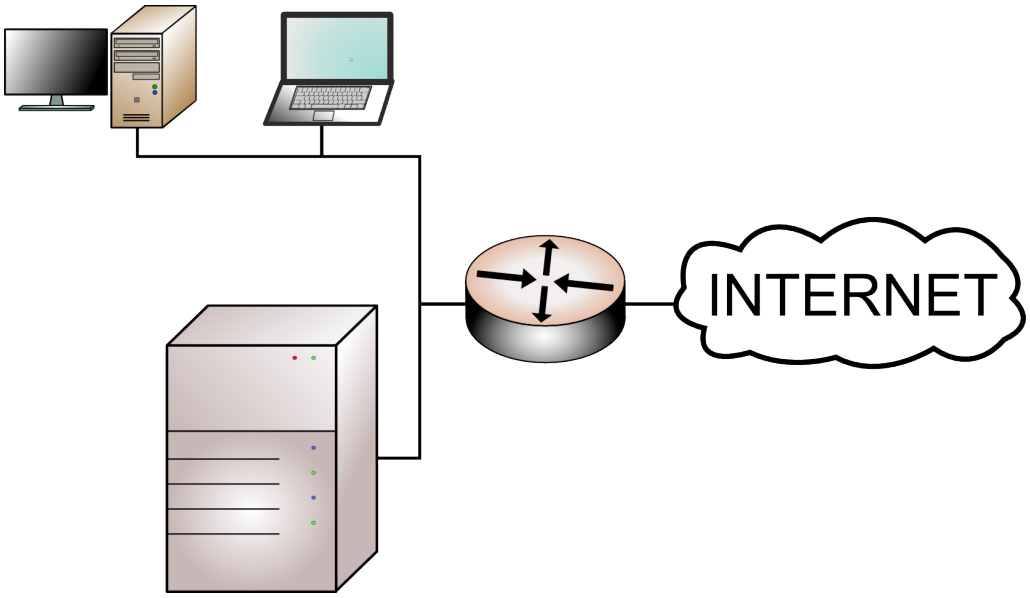
4 SMEROVAČ AKO BEZPEČNOSTNÉ ZARIADENIE

V prvej kapitole sme sa oboznámili s hlavnou funkciou smerovača, s ktorou sa spája jeho ďalšia dôležitá funkcia a tou je zabezpečenie počítačovej siete. Závisí však na tom, kde je smerovač umiestnený, a z tohto dôvodu smerovač môžeme využiť ako jediné bezpečnostné zariadenie, alebo ako súčasť oveľa väčšej a hlbšej bezpečnostnej štruktúry. Pri akomkoľvek umiestnení smerovača bude ale vždy platiť to, že ak smerovač správne zabezpečíme, zvýšime tým bezpečnosť a odolnosť celej siete a tým pádom môžeme:

- zabrániť smerovaču v neúmyselnom úniku informácií o sieti k útočníkovi
- zabrániť padnutiu smerovača a tým pádom aj celej siete pri útoku
- nedovoliť zneužitie smerovača v roli základne pri vedení útoku v rámci lokálnej siete, či útoku vedeného z vonka
- znížiť zaťaženie siete a zastaviť všetky nežiaduce pakety a s nimi spojené útoky

4.1 Hranový smerovač ako hrdlo siete

Ak smerovač slúži ako jediné bezpečnostné zariadenie, hovoríme o smerovači, ktorý plní funkciu hrdla siete. Každý takýto smerovač (obr 4.1), je prvým obranným prvkom celej počítačovej siete, cez ktorý prechádza každá komunikácia do Internetu a späť. Význam hranového smerovača v úlohe hrdla siete je veľký a jeho cieľom je zabraňovať v prístupe ku konkrétnym sieťovým zariadeniam a aplikáciám. Je taktiež posledným nami riadeným aktívnym prvkom, a preto je veľmi dôležité, aby bol v dnešnej modernej dobe dobre zabezpečený a správne nastavený.



Obr. 4.1: Hranový smerovač ako hrdlo siete.

4.1.1 Prístupové zoznamy ACL

Každý smerovač má v sebe implementovanú funkciu filtrovania sieťovej prevádzky podľa vopred definovaných pravidiel. Ako sme už raz spomenuli v kapitole 3.2 ide o prístupové zoznamy ACL, najrozšírenejšie paketové filtry od firmy Cisco. Je to jedna z hlavných zabezpečovacích technológií smerovača, ktorej úlohou je prečítať obsah IP datagramu podľa hlavičky rozhodnúť či má IP datagram poslať ďalej, a ak áno, tak kam.

Podľa typu filtrovania rozlišujeme dva základné typy prístupových zoznamov, sú to štandardné, rozšírené a reflexné prístupové zoznamy. Štandardné a reflexné prístupové zoznamy slúžia k filtrácii na základe zdrojovej adresy, zatiaľ, čo rozšírené prístupové zoznamy pakety vyhodnocujú nielen podľa zdrojovej adresy, ale aj cieľovej adresy, a pre podrobnejšiu kontrolu voliteľne aj podľa protokolu a čísla portu.

Podľa syntaktického zápisu rozlišujeme číslované prístupové zoznamy v tvare *access-list číslo kritériá*. V tomto prípade v časti *číslo* je číslo z intervalu, ktorý určuje daný typ prístupového zoznamu. Štandardné prístupové zoznamy sú označované číslami 1 - 99 a 1300 - 1999, rozšírené 100 - 199 a 2000 - 2699. Ostatné číselné intervaly sú vyhradené napríklad pre alternatívne protokoly a iné. V časti *kritériá* definujeme vlastné pravidlá pre filtráciu, ktoré chceme, aby sa uplatnili. Ďalej podľa syntaktického zápisu máme pomenované zoznamy v tvare *ip access-list typ názov*, pričom *typ* označuje slovo *standard* alebo *extended* a iné. Časť *názov* označuje nami určený názov zoznamu, má informatívny charakter. Ak máme vytvorený pomenovaný prístupový zoznam, až v ňom definujeme pravidlá filtru, a to spôsobom

permit/deny kritériá . [22]

Každý takto vytvorený prístupový zoznam sa vyhodnocuje zhora nadol. Znamená to, že ak testovaný paket nesúhlasí s výrazom na prvom riadku, pokračuje testovanie na ďalšom riadku a ak testovaný paket prejde až na koniec bude naň uplatnené implicitné pravidlo *deny all*, ktoré sa neuvádza v zozname a má za úlohu automaticky testovaný paket zahodiť. Správne poradie definovaných pravidiel je veľmi zložitou úlohou. Ak naozaj chceme, aby prístupový záznam ACL bol skutočne dobrý, je nevhodné, aby sme v ňom pravidlá náhodne menili, ale mali by sme si vždy vopred premyslieť a stanoviť, čo je potrebné a dôležité a vytvoriť ich od úplných základov. Nesprávne zostavený prístupový zoznam môže mať nepríjemné dopady na prevádzku či výkon celej siete. Ukážky rozšíreného prístupového zoznamu môžeme vidieť na obr. 4.2 podľa publikácie [28].

```
access-list 132 permit tcp 67.34.15.1 0.0.0.255 any eq 22
access-list 132 permit udp 67.34.15.1 0.0.0.255 any eq domain
access-list 132 permit icmp 67.34.15.1 0.0.0.255 any echo
access-list 132 permit icmp 67.34.15.1 0.0.0.255 any echo-reply
access-list 132 permit tcp 67.34.15.1 0.0.0.255 any eq ftp
access-list 132 permit tcp 67.34.15.1 0.0.0.255 any eq http
access-list 132 permit tcp 67.34.15.1 0.0.0.255 any gt 1023 established
access-list 132 permit udp 67.34.15.1 0.0.0.255 any gt 1023

access-list 133 permit tcp any any eq 22
access-list 133 permit udp any any gt 1023
access-list 133 permit icmp any any gt 1023
access-list 133 permit icmp any any echo-replay
access-list 133 permit icmp any any unreachable
access-list 133 permit icmp any any administratively-prohibited
access-list 133 permit icmp any any time-exceeded
access-list 133 permit icmp any any packet-too-big
access-list 133 permit tcp any 67.34.15.80 eq ftp
access-list 133 permit tcp any 67.34.15.81 eq smtp
access-list 133 permit tcp any 67.34.15.81 eq domain
access-list 133 permit udp 67.34.15.81 eq domain
```

Obr. 4.2: Rozšírený prístupový zoznam ACL číslo 132 a 133.

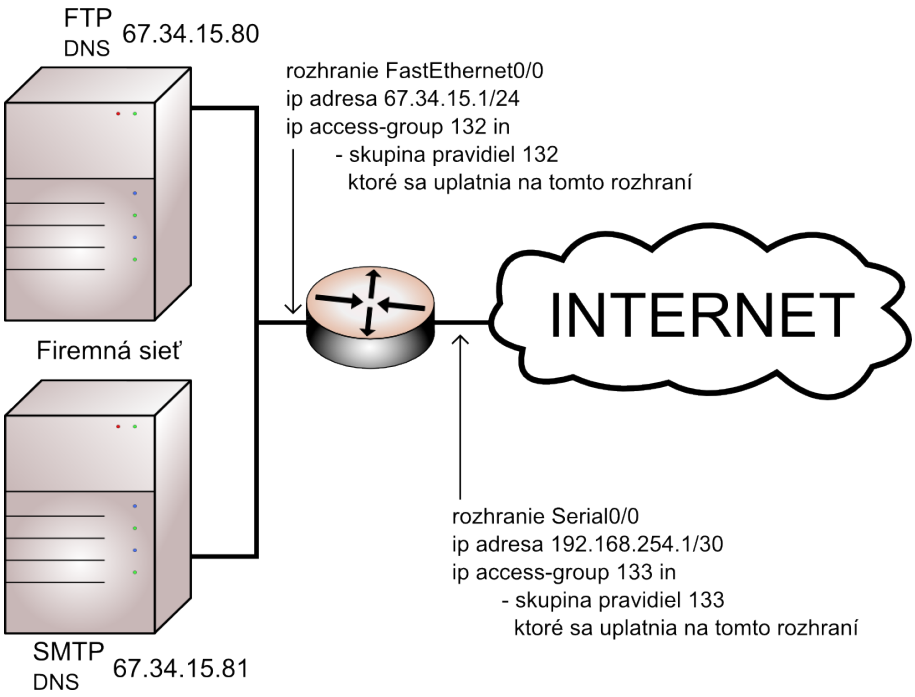
Ak na smerovač, ktorý plní funkciu hrdla firemnej siete aplikujeme prístupové zoznamy ACL (obr 4.3) podľa obrázku 4.2, povolíme len nasledujúci typ prevádzky a ostatná prevádzka bude zakázaná:

- doručenie prichádzajúcej e-mailovej pošty na server SMTP s IP adresou 67.34.15.81

- prenosy súborov na server FTP s IP adresou 67.34.15.80
- služba DNS presmerovaná na server DNS s IP adresou 67.34.15.81 (prenos zóny protokolom UDP a požiadavky na vyhľadanie názvu cez TCP)
- prevádzka v protokoloch TCP a UDP nad port 1023, ktorý umožňuje činnosť odchádzajúceho spojenia zo súkromnej siete
- povolenie istých, vybraných typov paketov ICMP

ale užívatelia v smere do Internetu budú mať povolené iba tieto odchádzajúce spojenia:

- SSH na porte 22
- DNS na porte 53
- FTP na porte 20 a 21
- HTTP na porte 80



Obr. 4.3: Smerovač v roli hrdla siete s aplikovanými ACL záznamami.

Tento spôsob ochrany má určite svoje uplatnenie, ale na druhej strane nám neposkytuje úplne riešenie v otázke bezpečnosti. Obyčajný hranový smerovač, ktorý

nemá implementované vyspelejšie techniky zabezpečenia nedokáže kontrolovať vyššie vrstvy modelu ISO/OSI, to je 5 - 7 vrstva [28], neuspokojivo rieši problémy s bezpečnosťou protokolov a aplikácií.

Nedostatkom prístupových zoznamov je napríkad to, že ACL niekedy nezistí podvrhnutie komunikačného spojenia, a to sa dá zneužiť napríklad fragmentáciou, pod ktorú spadajú spomenuté útoky z kapitoly 2 slzička a smrteľný ping či sfalšovanie paketov. Tento typ útoku sa útočníkovi naskytá tým, že samotný prístupový zoznam ACL pre komunikáciu povoľuje určité služby, a tie môžu poslúžiť ako otvor do siete. Ako môžeme vidieť na vyššie uvedom príklade s povolením prevádzky v sieťových protokoloch TCP a UDP nad port 1023 a s povolením istých, vybraných typov paketov ICMP sa útočníkovi naskytá príležitosť sfalšovania paketov UDP, TCP či ICMP. Jednou z ďalších možností útoku cez prístupové zoznamy je zdrojové smerovanie, ktorý ale môžeme vyriešiť vypnutím tejto funkcie alebo správnym blokovaním paketov pri vstupe do našej vnútornej siete.

Dôležitú úlohu v rozšírených prístupových zoznamoch zohráva kľúčové slovo *established*. Teoreticky slúži na blokovanie akejkoľvek komunikácie okrem návratovej prevádzky. V praxi to znamená, že slovo *established* sleduje príznaky v prijatých paketoch. Stačí ak smerovač príjme podvrhnutý paket, s príznakom ACK a prístupový zoznam na smerovači ho prepustí ďalej. Toto sa dá zneužiť pri útoku nazývanom pozemný útok, spomenutom v 2 kapitole.

4.1.2 Technológia NAT

V minulosti bola táto technológia rozvíjaná kvôli nedostatku verejných adries IPv4 a ako sme už raz spomenuli, s jej funkciou prišla aj ďalšia možnosť ako zvýšiť bezpečnosť a ochranu siete. Hlavnou úlohou tejto technológie, ako je už uvedené v kapitole 3.4 je preklad IP adries z privátnych na verejné tak, že vonkajšia - verejná adresa je priradená zariadeniu, so svojou vnútornou - súkromnou adresou. Z tejto funkcionality nám vyplýva napríklad nižšie riziko mapovania topológie siete, zistenia počtu spustených staníc a systémov, či ďalej zaútočenia na sieť pomocou útokov DoS alebo prehľadávaním portov. NAT má niekoľko podôb a môže pracovať v troch základných režimoch [28]:

- Statický NAT, ktorý definuje jedinečné zobrazenie privátnych IP adries na verejné, jedna k jednej.
- Dynamický NAT, ktorý zaisťuje mapovanie privátnych IP adries na verejnú IP adresu, vybranú zo skupiny registrovaných adries. I pri tomto preklade NAT je medzi adresami jednoznačné zobrazenie, jedna k jednej.

- Preťažený NAT, ktorý je špeciálnym typom dynamického NAT. Má za úlohu prevádzať väčšiu skupinu privátnych IP adries na jednu verejnú IP adresu, pričom ich rozlišuje pomocou rôznych portov TCP a z tohto dôvodu patrí medzi najčastejšie používané. Keďže tento mechanizmus rozlišuje porty, hovoríme o preklade portov (anglicky Port Address Translation, PAT) alebo o jednoadresovom NAT.

Ak zoberieme príklad uvedený od skupiny autorov v knihe [22] môžeme usúdiť, že technológia PAT je bezpečnejšia, a to z dôvodu sledovania portov pre každé spojenie.

I keď preklad sieťových adries prináša ďalšiu funkciu zabezpečenia, taktiež má svoje obmedzenia. Jedným z problémov je nedostatočné filtrovanie odchádzajúcej komunikácie, čím vzniká možnosť napadnutia cez aktuálny sieťový preklad. Tento problém sa dá jednoducho odstrániť pridaním hĺbkovej inšpekcie paketov. Ďalším z problémov tvorí kontrola stavu spojenia v protokole UDP, pretože tento protokol je nespojovaný. Keďže sa spojenie vôbec nevytvára, NAT nedokáže rozhodnúť, či je paket súčasťou prebiehajúcej komunikácie, alebo tvorí samostatný prenos dát a prvok s funkciou NAT vtedy môže jedine predpokladať dĺžku UDP komunikácie. S kombináciou firewallu je možné určovať dobu nečinnosti pre takýto prípad spojenia. Ako je vyššie spomenuté PAT mechanizmus je bezpečnejší, ale aj tu môže dôjsť k zneužitiu a to práve pomocou portov, ktoré sú hlavnou časťou tohto mechanizmu. Ak útočník pozná našu IP adresu, s veľkou pravdepodobnosťou dokáže odhaliť nami používané porty. Tým pádom útočník môže spoznať kombináciu adresa/port a správne vytvorenou komunikáciou môže tento mechanizmus obísť, ale len za podmienky, že klient v sieti stále sleduje port, na ktorý bol kontaktovaný pri vytvorení prekladu adresy. Ak by sme chceli funkciu NAT na našom používanom zariadení rozšíriť o autentizačnú či šifrovaciu technológiu, narazíme na problém, pretože sa v mnohých prípadoch stáva, že NAT s nimi nedokáže spolupracovať. Je to spôsobené tým, že NAT pakety pozmeňuje a práve spomínané systémy zabezpečujú integritu a neporušenosť dát pri prenose.

4.1.3 Firewall Future Set

Bezpečnostná technológia SPI je často implementovaná vo firewalloch, ako je už spomenuté v kapitole 3.3 . Ak chceme aby smerovač, ktorý plní funkciu hrdla siete mohol využívať funkciu SPI je nutné použiť Firewall Future Set (FFS), ktorý je dostupný na smerovačoch spoločnosti Cisco. Práve jadrom funkcií FFS je kontextovo-závislé riadenie prístupu (anglicky Context-Based Access Control, CBAC). Tento mechanizmus je určený pre stavovú inšpekciu paketov a rozširuje možnosti filtrovania paketov v smerovači až do 7 vrstvy referenčného modelu ISO/OSI. [28]

Možností využitia funkcií CBAC je viacero. Prvou a hlavnou úlohou je dynamické filtrovanie. Toto filtrovanie je založené na vytvorení stavového záznamu, keďže pri protokoloch TCP, UDP a ICMP prebieha filtrovanie spätnej cesty. Tým pádom, CBAC otvára porty dynamicky iba po dobu trvania komunikácie na základe pravidiel ACL a zároveň na aplikačnej vrstve overuje či spojenie skutočne patrí uvedenému zdroju. Funkcie pre filtrovanie taktiež tvoria:

- Štandardné a rozšírené prístupové zoznamy ACL
- Dynamické prístupové zoznamy so zámkom a kľúčom. Prideľujú dočasnú priepustnosť cez firewall identifikovanému užívateľovi.
- Autentizácia a autorizácia. Je to kontrola užívateľského prístupu podľa IP adresy a rozhrania.

Nasledujúcou funkciou je kontrola UDP a ICMP, ktoré sú nespojované a ich kontrola je preto dosť náročná. CBAC tieto spojenia sleduje pomocou dynamického filtrovania a pomocou časovača, ktorý približne určuje dĺžku i stav komunikácie. Ako už bolo spomenuté v predchádzajúcej kapitole, toto riešenie je veľmi vhodným doplnkom technológie NAT.

Ďalšou funkciou, ktorú implementuje požitie CBAC je monitorovanie poradových čísel či v prichádzajúcej, ale aj odchádzajúcej komunikácii, podľa ktorých protokol TCP sleduje stav spojenia. Toto riešenie je vhodné na ochranu pred útokom, akým je napríklad únos relácie, pri ktorom sa útočník zmocní pomocou podvrhnutých paketov práve prebiehajúceho spojenia medzi dvoma klientmi.

Riadenie prístupu CBAC taktiež sleduje otvorené i uzavreté relácie TCP. Takto priebežne sleduje a kontroluje koľko relácií je otvorených, koľko prenosov prebehlo za určitý čas a porovnáva ich so stanovenou prahovou hodnotou. Týmto spôsobom sa môžeme brániť voči útokom typu DoS, napríklad záplavou paketov SYN. [27]

CBAC okrem kontrolou TCP, UDP a ICMP dokáže taktiež kontrolovať narušenia pravidiel v rôznych aplikačných protokoloch. Len čo sa objaví takéto narušenie, komunikácia sa hneď zablokuje. Aplikačná inšpekcia paketov je pre všetky nižšie uvedené protokoly z knihy [28], v ktorých boli objavené zraniteľné miesta:

- CU-SeeMe (port 7648). Dvojstranná videokonferencia.
- FTP (port 21). Prenos súborov medzi klientom a serverom.
- H.323 (port 1720). Paketovo orientovaný multimediálny komunikačný protokol, pre hlasové prenosy VoIP, ktorý pomocou inšpekcie riadiacich správ Q931 a H.245 otvára ďalšie kanály UDP pre prenos obrazových a zvukových dát, patria sem tiež protokol SIP (port 5060)

- Inšpekcia ICMP. Množina firewallových funkcií FFS robí inšpekciu paketov a dôveruje iba tým správam, ktoré pochádzajú z vnútornej siete.
- MGCP (port 2427). Hlasové prenosy VoIP.
- MSRPC (port 135). Protokol vzdialeného volania, ktorý zabezpečuje komunikáciu medzi procesmi na vzdialených systémoch.
- Net show (port 1755). Je to platforma prúdových médií od Microsoftu.
- R-EXEC (port 512). Protokol pre vzdialenú realizáciu príkazu na Berkeley Unix.
- R-SHELL (port 514). Protokol pre vzdialený príkazový interpret (anglicky shell) na Berkeley Unix.
- RTSP (port 544). Multimédiá a hlasové prenosy VoIP.
- SMTP (port 25). Poštový protokol, ktorý kontroluje neplatné príkazy SMTP a nahrádza nutnosť externého preposielania pošty v demilitarizovaných zónach.
- SQLnet (port 1521). Vrstva middleware pre komunikáciu klientov s databázami a vzájomnú komunikáciu databáz v architektúre klient/server.
- Stream Works (port 1558). Platforma pre prúdové médiá, ktorých vlastníkom je Real Networks.
- SUNrpc (port 111). Protokol vzdialeného volania procedúr firmy Sun Microsystems.
- Real Audio (port 7070). Platforma pre prúdové médiá od firmy Real Networks.
- Telnet (port 23). Protokol klasického virtuálneho terminálu.
- TFTP (port 69). Jednoduchý prenos súborov.
- VDOlive (port 7000). Protokol prúdových médií

Technológia CBAC dokáže zaznamenávať užitočné a dôležité informácie do systémového protokolu, akými bez pochýb sú začiatok a ukončenie komunikácie, zdrojový i cieľový klient a port, či celkový počet prenesených dát. CBAC umožňuje zaznamenávať a kontrolovať aplikácie v reálnom čase, čo je veľkou výhodou.

Pomocou CBAC môžeme ďalej napríklad nastaviť úroveň ochrany proti java appletom, ktoré môžu obsahovať škodlivý kód. Podľa nastavenia smerovač potom dokáže filtrovať alebo úplne zakázať prístup k java appletom.

Smerovač, zabezpečuje v prvom rade funkciu smerovania paketov a spolu s množinou funkcií FFS i funkciu firewallu. Takýto smerovač s firewallovými funkciami, musíme naučiť správnej dôvere, teda ho musíme nakonfigurovať ručne, pretože FFS nefunguje ako pravý firewall. Firewallové funkcie FFS nám ponúkajú ďalšiu inšpekciu paketov, a to obsahovú. CBAC pomocou detekčného systému IDS, ktorý je taktiež zabudovaný vo fukciách FFS, robí obsahovú inšpekciu paketov. V celom tomto procese platí vždy ale jedno pravidlo, že filtrovanie musí prebehnúť až po inšpekcii paketov.

Mechanizmus FFS nám tiež ponúka ďalšie rozšírenie a zvýšenie bezpečnosti, a to v podobe systému IDS, ktorý je priblížený vo veľmi malej stručnosti v kapitole 3.8 . Systém IDS implementovaný v FFS, nesie pomerne značné obmedzenie tým, že je súčasťou Cisco IOS a signatúry pomocou ktorých môže IDS odhaliť pokus o útok sú napevno zasadené do systému IOS. V porovnaní so špecializovanými detekčnými zariadeniami IDS, do ktorých sú nové signatúry zavádzané ľahšie, musíme signatúry udržovať, čo v najaktuálnejšom stave a to jedine náhradou systému IOS novšou verziou. Systém IDS delí všetky útoky do štyroch nasledujúcich skupín uvedených v publikácii [28]:

- Informatívny atomický prejav. Detekcia pokusu o prístup k portu na klientovi, typický predstaviteľ je útok prehľadávanie portov.
- Informatívny zložený prejav. Detekcia postupnosti určitých operácií, rozdelených po náhodnom časovom intervale medzi niekoľkých klientov.
- Atomický prejav útoku. Detekcia pokusu útočníka o prístup ku klientovi.
- Zložený prejav útoku. Detekcia zložitých útočných aktivít, rozdelených po náhodnom časovom intervale medzi viacerých klientov.

Množina funkcií FFS nám v dnešnej dobe ponúka pomerne silné mechanizmy pre zabezpečenie siete a opäť vidíme, že smerovač môžeme využiť i k ďalším úlohám okrem smerovania. Samozrejme i CBAC, čo je hlavá funkcia FSS, má svoje chyby a nedostatky, o ktorých by sme mali vedieť.

Výkonnosť každého smerovača je závislá od jeho konfigurácie či veľkosti sieťovej prevádzky. Ak ale vypneme alebo zapneme pár funkcií výkonnosť smerovača moc neovplyvníme, na rozdiel od podrobnejšej inšpekcie paketov, pri ktorej dochádza k predĺženiu doby času kontroly, či času na prejdenie prístupových zoznamov, pričom tento čas môže potenciálny útočník využiť vo svoj prospech. Ako už bolo raz spomenuté CBAC napomáha k obrane pred útokom s odoprením služieb, ale zároveň si musíme uvedomiť, že ak je veľké množstvo polootvorených za sebou idúcich, v krátkom časovom intervale, spojení môže to znamenať začiatok útoku typu DoS.

Ďalej sa inšpekcia CBAC nezaoberá paketami, ktoré nesú zdrojovú či cieľovú adresu nejakého rozhrania smerovača. Tým pádom, terminálová relácia telnet, či prevádzka v protokoloch TARCS a RADIUS, slúžiace pri mechanizme AAA, nepodliehajú žiadnej inšpekcii. Inšpekcii taktiež nepodliehajú pakety v sieti VPN, okrem smerovača, ktorý je koncovým bodom šifrovanej linky. [28]

4.2 Smerovač ako súčasť hlbšej bezpečnostnej štruktúry

Úloha smerovača ako časti hĺbkovej ochrany sa mení podľa špecifikácií pripojenia či umiestnenia. Výkon smerovača by sme ale mali vždy využiť tak, aby bol čo najefektívnejší a ak je súčasťou väčšej bezpečnostnej štruktúry, na ochranu siete použijeme aj iné ďalšie samostatné riešenia, poprípade kombináciu riešení, akým je napríklad hardvérový firewall, proxy server či iné bezpečnostné mechanizmy.

4.2.1 Sieťový prieskum na aplikačnej úrovni

Jedným zo spôsobov ako využiť smerovač v systéme hĺbkovej ochrany je pomocou funkcie, implementovanej v Cisco smerovačoch, sieťového prieskumu na aplikačnej úrovni (anglicky Network Based Application Recognition, NBAR).

Prvoradou úlohou funkcie NBAR je vymedzenie určitého množstva kapacity spoja pre prenos dát, pretože multimediálne aplikácie, ktoré vyžadujú vysokú kvalitu služieb QoS zaberajú veľké množstvo kapacity linky určenú pre prenos dát. Musíme si uvedomiť, že pod bezpečnosť spadá taktiež ochrana požiadaviek služieb a dostupnosti linky, pretože práve útoky typu DoS využívajú nedostatočnú kapacitu linky, či zlé využitie kapacity spoja. Pomocou tejto funkcie teda môžeme správne riadiť vyťaženosť linky a aktivity, ktoré zaberajú väčšiu časť množstva kanálu a nie sú pre nás také podstatné.

NBAR dokáže rozoznať prenos založený na rôznych protokoloch a získavať tak rôzne informácie. Niektoré protokoly, ktoré môže NBAR identifikovať:

- DNS
- EIGRP
- FTP
- HTTP / HTTPS
- ICMP

- IPSec
- IRC
- NetBIOS
- POP3
- RIP
- SFTP
- SSH
- StreamWorks
- SUNrpc
- VDOlive

Týchto protokolov je samozrejme ešte oveľa viac. NBAR taktiež dokáže nachádzať informácie o statických a dynamických portoch. Hneď ako identifikuje aktuálny prenos môže naň uplatniť nastavenia, ktoré riadia prideľovanie šírky použitého pásma. Takýmto mechanizmom dokážeme riadiť QoS a ochranu šírky spoja. [27]

4.2.2 VPN

Mechanizmus VPN, ako už bolo raz v tejto práci spomenuté, patrí medzi viaceré možnosti zabezpečenia sietí. Ako táto technológia presne funguje so všetkými jej funkciami, možnosťami či režimami, sa môžeme dočítať v rôznej inej odbornej literatúre, a preto len v krátkosti nahliadneme do tejto problematiky a na to, akú úlohu v mechanizme VPN zohráva smerovač.

Hneď na úvod by sme mali vedieť, že siete VPN sú realizované nielen smerovačmi, ale aj rôznymi inými zariadeniami, akými napríklad sú firewally, či koncentrátory sietí VPN, ktoré sú špeciálne určené pre túto technológiu. Ak používame smerovač ako súčasť tejto technológie hovoríme o smerovači s podporou VPN. Pri implementácii siete VPN to pre smerovač, ktorý v základe nepodporuje túto funkciu, znamená isté rozšírenie, ktorým napríklad môže byť pridanie špecializovaného hardvéru pre VPN a v smerovačoch Cisco napríklad zmena systému, ktorá taktiež prináša špeciálne funkcie pri zachovaní základných funkcií smerovania, bezpečnosti či kvality služieb QoS.

Ako už bolo spomenuté v kapitole 3.6 technológia VPN nám poskytuje pripojenie, pomocou šifrovacích mechanizmov, nad existujúcou verejnou sieťou. VPN môžeme vytvárať cez časť zdieľanej LAN, WAN alebo Internet a to cez takzvané tunely

pomocou procesu tunelovania. Podstatou tohto procesu je to, že funkčný systém zoberie paket a zapuzdruje ho do iného paketu, ktorý potom prenesie po sieti. Táto sieť musí poznať iba protokol prvotného paketu, pretože pomocou neho vstupuje do siete a vystupuje zo siete. V celom tomto procese zohrávajú tieto tri protokoly [28]:

- Prenášaný protokol, obvykle IP. Pôvodný protokol, ktorý sa má zašifrovať pre prenos v sieti VPN.
- Zapuzdrovací protokol, zvyčajne v dnešnej dobe štandard IPSec, ale taktiež aj PPTP, L2TP, L2F, GRE. Tento protokol zapuzdruje, obaľuje pôvodné prenášané dáta. Na to, aby tunel pracoval správne musia obe rozhrania tunelu podporovať daný zapuzdrovací protokol.
- Nosný protokol, ktorý prenáša výsledné zapuzdrené informácie po verejnej sieti. Výsledný paket je rozšírený o hlavičku nosného protokolu, je ním taktiež zvyčajne IP protokol.

Zapuzdrovací protokol je azda najdôležitejšou súčasťou prenosu, pretože chráni všetky prenášané dáta v nechránených sieťach. Štandardný protokol IPSec, ktorý patrí medzi mnohé zapúzdrovacie protokoly je pomerne dosť známy a rozšírený. Poskytuje nám mechanizmus autentizačných a šifrovacích služieb a v sieťach zabezpečuje nasledovné funkcie [28]:

- Dôveryhodnosť dát. To znamená, že dáta sú pred prenosom šifrované a tým pádom sú sčasti chránené pred potenciálnym útočníkom.
- Integrita. Prijímacie rozhranie kontroluje neporušenosť či zmenu prenášaných dát.
- Autentizácia pôvodu. Pri každom prenose je autentizovaný zdroj odoslaných dát. Tento mechanizmus je závislý na integrite dát.
- Ochrana proti opakovaniu. Príjemca dokáže detekovať opakované dáta a zamietnúť ich.

Protokol IPSec môže šifrovať dáta medzi dvojicami rôznych zariadení, a to:

- smerovač - smerovač
- firewall - smerovač
- firewall - firewall

- klient - smerovač
- klient - firewall
- klient - koncentrátor VPN

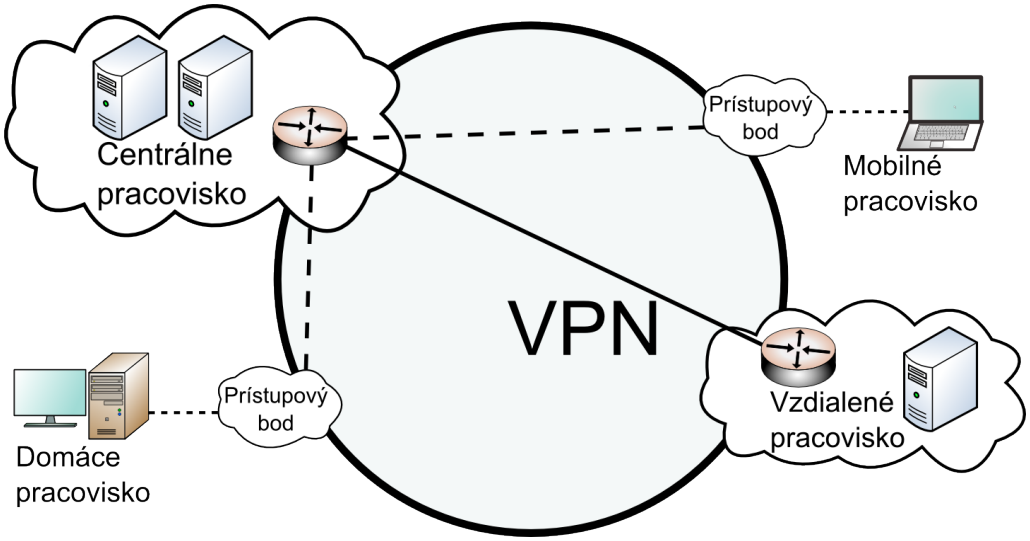
a tak ďalej, ale samozrejme tieto zariadenia musia takýto mechanizmus podporovať. Podrobnejší princíp funkčnosti režimov a činnosti protokolu IPSec a aj iných šifrovacích protokolov používaných vo VPN sieťach je možné dočítať sa v iných odborných publikáciách.

Keďže technológia VPN nám poskytuje širšiu a hlbšiu bezpečnostnú štruktúru, ktorá je zložená z viacerých bezpečnostných prvkov, poskytujúce efektívne riešenie zabezpečenia informácií, isto patrí medzi jedno z lepších možností riešenia otázky bezpečnosti sietí. VPN prichádza taktiež s mnohými výhodami, akými napríklad bezpochyby sú:

- Vzdialený prístup k sieťovým prostriedkom z akéhokoľvek miesta.
- Zjednodušenie topológie siete, tým že strategicky rozmiestnime zariadenia VPN.
- Nižšie nároky pripájania do centrály pre vzdialené pracoviská. Efektívnejšie a lepšie riešenie než klasické WAN siete.
- Mobilita pre užívateľov či zamestnancov pri práci na diaľku.
- Zabezpečenie externého prístupu k internetu a interného prístupu k intranetu cez zabezpečené pripojenie.

Mechanizmus VPN so sebou prináša aj svoje negatívne vlastnosti. Jednou z nich je napríklad zaťaženie prenosovej brány alebo zariadenia slúžiaceho k vytváraniu tunelu VPN. Je to spôsobené tým, že všetky činnosti spojené so šifrovaním sú veľmi zložitými matematickými výpočtami. Tie zaťažujú celkovú kapacitu VPN spojenia a mnohokrát sa pre zlepšenie výkonu musí použiť špeciálny adaptér, zariadenie s hardvérovou akceleráciou, označované „offload card“ ktoré je pomerne dosť drahé [22]. Opäť tu platí čím viac nárokov, tým nižší výkon, ale taktiež to závisí na tom, ako a na čo chceme VPN spojenie použiť. Ďalšou z negatív, ktoré mechanizmus VPN prináša je spojené so zapuzdrovaním dát. Prenášané dáta vždy nesú ďalšie informácie, ktoré sú k nim pridané a tým pádom sa zväčšuje aj ich veľkosť. Samotný problém sa netýka veľkosti zastielaného paketu, ale toho, že takto zväčšený paket bude pravdepodobne potrebovať fragmentáciu pri prechode prenosovými bránami či smerovačmi. Táto fragmentácia potom môže negatívne ovplyvniť výkon celej siete.

Z pohľadu funkcie smerovača v sieťach VPN môžeme povedať, že patrí medzi viaceré prvky, ktoré slúžia na zostavenie VPN siete, tvoria celkovú štruktúru zabezpečenia a ďalšou funkciou smerovača je spájanie rôznych vzdialených pracovísk (obr. 4.4). Mechanizmus VPN je pomerne dosť pružný systém a ponúka nám rôzne varianty použitých zariadení. Záleží na výbere daného hardvéru a jeho nastavenia, poprípade kombinácie zariadení voči našim požiadavkám na funkcionalitu siete. Z bezpečnostného hľadiska v celom systéme taktiež zohrávajú veľmi dôležitú úlohu autentizačné a šifrovacie protokoly.



Obr. 4.4: Ilustrácia technológie VPN.

4.3 Smerovač ako prvok bezdrôtovej siete a jeho bezpečnosť

Bezdrôtové siete sú v súčasnej dobe pomerne dosť rozšírené a obľúbené u väčšiny ľudí. Stretávame sa s nimi na pracovisku, v školách, kaviarňach ale aj na verejných priestranstvách a iných miestach, teda skoro na každom kroku. Ponúkajú veľké množstvo výhod, medzi ktoré nepochybne patrí ich mobilita, rýchle a flexibilné spustenie, cena a náklady na prevádzku, ale napríklad aj ich rýchlosť a mnohé iné. V moderných bezdrôtových sieťach si určite nájde miesto aj smerovač, ktorý častokrát patrí medzi hlavné prvky bezdrôtových sietí a tvorí ich prístupové body. Práve na smerovači potom záleží aké bude zabezpečenie, voči útokom mierené na akúkoľvek bezdrôtovú sieť.

4.3.1 Štandardy a činnosť bezdrôtových sietí

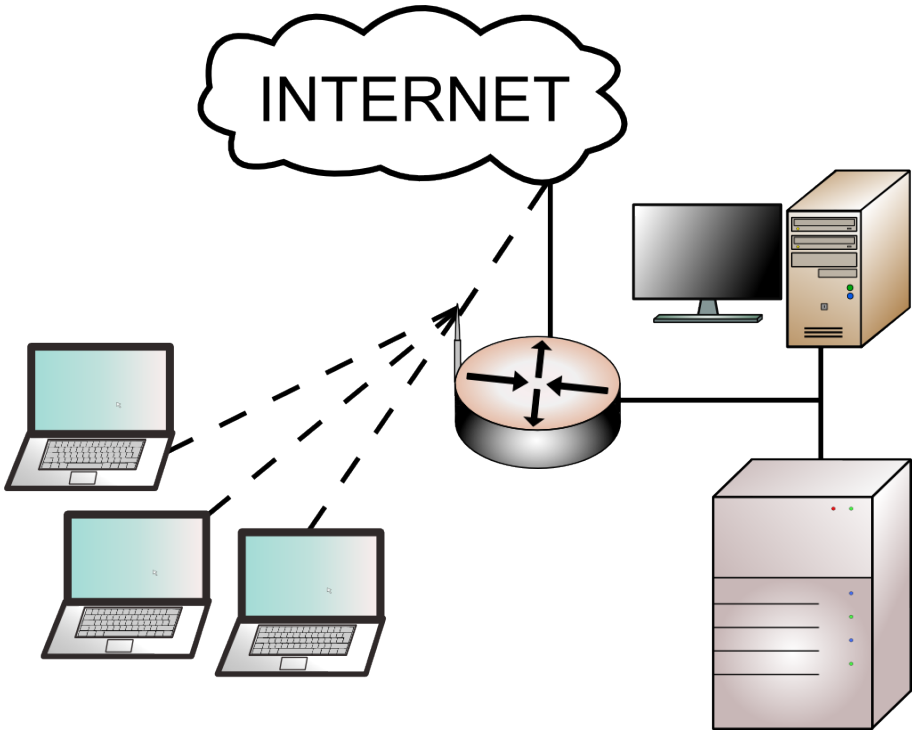
Bezdrôtové siete (anglicky Wireless LAN, WLAN), všeobecne známe pod skratkou Wi-Fi, v dnešnej dobe ponúkajú viacero štandardov. Okrem označenia sa tieto štandardy od seba líšia (tab. 4.1) frekvenčným pásmom, v ktorom prenášajú signál či šírkou pásma, ktorá určuje rýchlosť prenosu dát, ale aj inými ďalšími parametrami. Väčšina bezdrôtových sietí pracuje so štandardom označeným IEEE 802.11b.

Tabuľka 4.1: Porovnanie štandardov WiFi [30]

Štandard	Vydanie	Pásmo [GHz]	Max. teoretická priepustnosť [Mbit/s]	Max. reálna priepustnosť [Mbit/s]	Dosah v zastavanej ploche [m]	Dosah v nezastavanej ploche [m]
802.11	1997	2,4	2	0,9	20	100
802.11a	1999	5	54	23	35	120
802.11b	1999	2,4	11	4,3	38	140
802.11g	2003	2,4	54	19	38	140
802.11n	2009	2,4 a 5	300 - 600	74 - 144	70	250

Pri činnosti bezdrôtových sietí si musíme uvedomiť to, že spojenie medzi dvomi či viacerými klientmi je realizované pomocou obyčajných rádiových frekvencií a teda obecne je to rádiová technológia, pomocou ktorej prebieha komunikácia bez akéhokoľvek fyzické spojenia a to nad štandardnými sieťovými protokolmi, napríklad IP protokolom.

Siete WLAN môžu pracovať v náhodnom režime, označovanom ad hoc, pre ktorý je charakteristická komunikácia klientov bez bezdrôtového prístupového bodu (anglicky Wireless Access Point, WAP). Ďalej poznáme siete WLAN s infraštruktúrou, kde klienti komunikujú s prístupovým bodom, v našom prípade je to smerovač, ktorý je zväčša fyzicky pripojený k pevnej sieti (obr. 4.5)



Obr. 4.5: Infraštruktúra siete WLAN, kde smerovač plní funkciu prístupového bodu.

4.3.2 Možnosti zneužitia v bezdrôtových sieťach

Pretože bezdrôtové siete prenášajú dáta vzduchom, môžeme povedať, že celá sieť je otvorená nielen ľuďom, pre ktorých je určená, ale aj nežiaducim používateľom, teda útočníkom.

Jednou z možností ako využiť to, že komunikácia prebieha formou vysielania rádiových vĺn je pomocou útoku odpočúvania paketov, ktorý je spomenutý v kapitole 2.18 . Stačí, aby útočník bol v dosahu WLAN siete a pomocou nástroja na odpočúvanie nemá problém v nechránenej komunikácii sledovať sieťovú premávku nielen v pevnom alebo aj bezdrôtovom pripojení.

Ďalšou hrozbou pre WLAN siete môže byť i útočník, ktorému sa nepodarilo získať priamy prístup do siete, prostredníctvom útoku typu DoS. Útočník totižto môže sieť napríklad zaplavovať statickým šumom, vďaka ktorému začne dochádzať ku kolíziám bezdrôtového signálu a tiež k vzniku chýb kontrolného súčtu CRC, ktorý slúži k detekcii chýb behom prenosu dát. V konečnom dôsledku sa môže celá bezdrôtová sieť výrazne spomaliť, ba dokonca stať nefunkčnou.

Nesprávne nakonfigurovanie prístupového bodu, ktorým vo WLAN sieťach je niekedy aj smerovač, môže pre útočníka znamenať ďalšiu šancu na útok a pre nás iba ďalší problém. Veľké množstvo prístupových bodov je z továrenskej konfigurácie

nastavená pre otvorené vysielanie SSID, čo je identifikátor každej WLAN siete, všetkým oprávneným užívateľom. Zneužitie plynie z nesprávneho použitia SSID v úlohe hesla pre overenie oprávnenosti užívateľa a keďže SSID sa vysiela nesmerovo, môže sa potenciálny útočník zmocniť SSID a tým pádom sa môže ďalej vydávať za právoplatného užívateľa. [28]

4.3.3 Zabezpečenie bezdrôtových sietí pomocou smerovača

Ak používame v bezdrôtovej sieti smerovač s podporov WLAN, slúži nám ako prístupový bod. Je dôležité, aby tento prístupový bod, ktorý tvorí cestu do a z bezdrôtovej siete bol čo najlepšie zabezpečený voči napadnutiu siete.

Za prvú úroveň zabezpečenia môžeme považovať vysielanie SSID v *bacon frame*. Vďaka tejto funkcii dokáže väčšina detekčných nástrojov nájsť bezdrôtovú sieť bez toho aby poznala SSID siete. Je dobré ak továrenské SSID, ktoré napríklad býva WLAN či Wireless a iné, zmeníme na text čo s najmenšou pravdepodobnosťou uhádnutia. Toto riešenie nie je až tak efektívne akoby sme si priali, a preto v tomto prípade bude lepšou voľbou ak vypneme nesmerové vysielanie SSID, a tým pádom bude WLAN sieť pre bezdrôtových klientov dostupná až po manuálnom zadaní SSID.

Pre ochranu siete ale i našich dát je ďalšou možnosťou nakonfigurovanie funkcie pre zabezpečenie bezdrôtového prenosu pomocou šifrovacích a autentizačných mechanizmov. V súčasnosti poznáme viacero typov šifrovacích protokolov, ktoré sú dôkladne popísané v inej odbornej literatúre. V súčasnosti medzi základné šifrovacie algoritmy patrí WEP, WPA a WPA2 šifrovanie. WEP šifrovanie patrí k základnému zabezpečeniu a preto v dnešnej dobe nie je problém pomocou špecializovaných programov odchytiť špecifické pakety a následnou analýzou zneužiť jeho nedostatky. Vyššiu úroveň zabezpečenia nám ponúkajú algoritmy WPA a WPA2, pričom novšie WPA2 šifrovanie je náročnejšie na výkon a preto ho nemôžeme používať na starších zariadeniach, ktoré toto šifrovanie nepodporujú. Takže ak máme v sieti zariadenia pracujúce len s WPA šifrou a smerovač ako prístupový bod podporujúci aj WPA2 šifru, bezpečnosť nemôže byť zabezpečená na najvyššej úrovni prostredníctvom silnejšieho WPA2 šifrovania. Medzi autentizačné mechanizmy, ktoré je ešte možné použiť pre zvýšenie bezpečnosti, patrí napríklad autentizácia EAP-PSK, LEAP od firmy Cisco, EAP-TLS od spoločnosti Microsoft alebo EAP-TTLS od firmy Funk Software, pričom tieto mechanizmy často krát spolupracujú ešte s protokolom RADIUS alebo s funkciou PKI. [8]

Ak v bezdrôtovej sieti používame smerovač, ktorého funkčná výbava je dosť široká nesmie tam chýbať podpora riadenia prístupu na základe filtrovania MAC adries (príloha A.5). Potom môžeme v prístupovom bode definovať povolenia prístupu

len pre vybrané, oprávnené zariadenia. Toto riešenie ale nie je tak úplne bezpečné ako sa na prvý pohľad zdá, pretože fyzické MAC adresy sú pri odpočúvaní stále viditeľné. Je to spôsobené tým, že šifrovanie neprebieha vo fyzickej vrstve ISO/OSI modelu. Tým pádom, útočník môže zistiť aká MAC adresa má prístup do siete a následne sa za ňu nepravdivo vydávať. Ďalšie negatívum ktoré prináša táto technológia je udržiavanie databázy MAC adries WLAN zariadení rozsiahlej podnikovej siete, pretože oproti spravovaniu dvadsiatich alebo tridsiatich zariadení je správa stoviek a viac zariadení dosť obtiažna. [28]

4.4 Zvýšenie bezpečnosti smerovača

Veľmi dôležitým faktorom pri bezpečnosti smerovača zohráva jeho samotné nastavenie či zabezpečenie, ktoré vyplýva z jeho umiestnenia v sieti. Smerovač ktorý je súčasťou väčšej bezpečnostnej štruktúry nie je osamotený a jednotlivé prvky, napríklad firewall a iné mechanizmy si dokážu navzájom vypomôcť. Ale ak smerovač používame ako jediné hranové zariadenie a má ochraňovať našu celú sieť je potrebné aby aj samotný smerovač bol chránený všetkými možnými prostriedkami. Z tohto dôvodu je zvýšenie odolnosti veľmi dôležitým bodom v sieťovej bezpečnosti a preto by sme naň nemali zabúdať.

4.4.1 Zabezpečenie konfigurácie

Jednou z viacerých a veľmi dôležitých častí je zabránenie nepovolenej a nežiaducej konfigurácie smerovača. Existuje viacero spôsobov cez ktoré sa dá vykonať vzdialená konfigurácia smerovača.

Veľmi známym spôsobom je služba Telnet prebiehajúca na porte 23. Problémom tejto služby je to, že informácie, ktoré zahŕňajú napríklad prihlasovacie meno a heslo k sieťovému zariadeniu putujú sieťou nezabezpečené, teda čisto v textovej podobe. Ak sa podarí útočníkovi tieto informácie zachytiť môže získať prístup ku konfigurácii. Asi najlepším riešením tohto problému je použitie šifrovaného protokolu.

Pomerne dosť rozšíreným protokolom, ktorý poskytuje šifrovanie je SSH protokol bežiaci na porte 22. Tento protokol už prenášané informácie šifruje. V dnešnej dobe sa používa SSH verzie 2 a podľa porovnania [2] zistíme, že SSH verzia 2 nám poskytuje oveľa vyššiu úroveň bezpečnosti.

Ďalším známym spôsobom na spravovanie sieťových zariadení, teda aj smerovača slúži protokol SNMP. Tento protokol nám uľahčuje správu v sieťach pomerne veľkých a dosť rozptýlených. Negatívom tohto spôsobu riadenia je jeho povolenie z Internetu do našej siete. Týmto spôsobom sa poskytne útočníkovi možnosť ovládať a riadiť naše zariadenia a sieť. V dnešnej dobe existuje už tretia verzia SNMP, ktorá

podporuje šifrovanie a kryptografickú autentizáciu, a preto je viac než vhodné sa vyhnúť používaniu starších verzií, podľa organizácie IETF zastaralých a neplatných. Asi najlepším spôsobom ako chrániť bezpečnosť smerovača je vypnutie všetkých SNMP prenosov na typických portoch 161 a 162.

Veľmi dôležitou úlohou pri zabezpečení smerovača zohráva taktiež bezpečnosť hesiel a ich autentizácie. Poznáme dva typu autentizácie a to vzdialenú a lokálnu. Pri vzdialenej autentizácii používame externé zariadenia, zvyčajne servery s podporou AAA protokolov RADIUS, TACACS či DIAMETER, ktoré overujú prihlasovacie mená a heslá na vzdialené zariadenie. Ak používame lokálnu autentizáciu, informácie o administrátorskom mene a hesle sú dostupné na smerovači. Nech pri prístupe na smerovač požijeme spomenutý protokol Telnet alebo zabezpečený protokol SSH, v každom prípade bude medzi nami a potenciálnym útočníkom iba prihlasovacie meno a heslo. Teda autentifikácia na smerovači nám nemusí zabezpečovať takú dôležitú bezpečnosť akú požadujeme. Z tejto situácie nám plynie to, že ak presunieme tieto dôverné informácie mimo smerovač zvýšime bezpečnosť nášho zariadenia. Pri takomto riešení môže nastať problém vtedy, ak náhodou vypadne spojenie s autentizačným zariadením, alebo sa autentizačný zdroj stane nefunkčným. Vtedy by nebola možnosť inej autentizácie a nedokázali by sme sa prihlásiť na smerovač. [22]

4.4.2 Zakázanie nepotrebných služieb

Ďalšou z možností, ako dosiahnuť zvýšenie bezpečnosti na smerovači je zakázanie všetkých služieb. I keď pre nás niektoré zakázané služby nemusia predstavovať žiadne riziko, môžeme týmto riešením len prispieť k zvýšeniu bezpečnosti zariadenia.

Spoločnosť Cisco vyvinula pre svoje smerovače proprietárny protokol CDP, určený pre zisťovanie vzájomných detailných informácií o konfigurácii. Kvôli tým informáciám o konfigurácii sa protokol CDP stáva dôležitým bodom nášho bezpečnostného záujmu. Ak tento protokol nutne nepotrebujeme, je na mieste ho zakázať.

Ďalší z protokolov, ktorý opäť ak nebudeme potrebovať vypneme je protokol NTP. Tento protokol slúži pre synchronizáciu časových prostriedkov v sieti. Taktiež je vhodný pri porovnávaní záznamových súborov, takzvaných logov, alebo poslúži pri autentizácii aktualizácií zariadenia a dá pozor, aby aktualizačné informácie boli vždy podpísané hashom MD5 a tým pádom neboli prijímané od nedôveryhodného zdroja. Ak sa ale rozhodneme NTP protokol používať, nesmieme zabudnúť na zapnutie autentizačného mechanizmu.

4.4.3 Blokovanie protokolu ICMP

Tento protokol je z hľadiska funkčnosti celého Internetu veľmi dôležitý. Slúži ku generovaniu a prenosu chybových a riadiacich správ na IP vrstve. Vďaka týmto správam môže Internet správne fungovať [22]. Žiaľ v dnešnej dobe väčšina moderných útokov prechádza práve týmto protokolom.

Jednou z viacerých možností ako zneužiť správy ICMP je správa s kódom 3, Host Unreachable. Smerovač túto správu rozosiela v tom prípade, ak je hostiteľská stanica vypnutá alebo neexistuje. Ak útočník začne tieto správy porovnávať s ostatnými odozvami rozsahu IP adries, môže sa dopracovať k platným adresám. Pomocou týchto funkčných adries a trasovania, je útočník schopný približne zmapovať našu sieť. Najlepšou voľbou ako zabrániť tomuto zneužitiu je zakázanie tohto typu správy.

Pre zvýšenie bezpečnosti smerovača je taktiež vhodné zakázať prenosy broadcast adresy po sieti, a to na všetkých rozhraniach smerovača. Touto voľbou môžeme zamedziť útokom typu Smurf, ktorý dokáže generovať stovky odpovedí na jednu žiadosť. Nielenže sa týmto spôsobom chránime pred útokmi používajúce ICMP protokol, ale je to taktiež dobrá obrana pred broadcast útokmi používajúce IP, TCP a UDP protokoly.

Ďalšou možnosťou ako obmedziť správy ICMP je vypnutie presmerovania. Toto použitie v spolupráci s prístupovými zoznamami zabráni nežiaducim spojeniam a prenosom a ďalej nám prinesie vylúčenie možnosti manipulácie s cestou spätných prenosov.

5 PRAKTICKÉ PREVEDENIE VYBRANÝCH ÚTOKOV

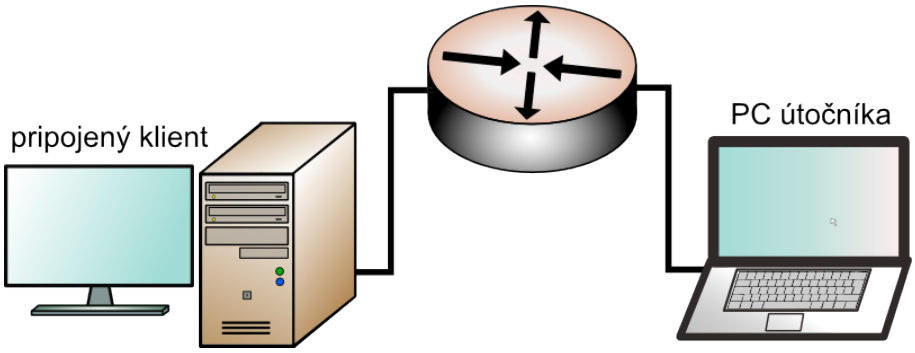
Pre praktické prevedenie útokov na smerovače, bolo vybratých niekoľko typov útokov. Prvým z nich je útok typu DoS, opísaný v kapitole 2, a to z dôvodu, že v dnešnej dobe sú takéto útoky pomerne rozšírené a ak sú ešte k tomu distribuované, majú obrovskú silu. O tom, že ich sila je skutočne veľká svedčia útoky z pred pár rokov, kedy konkrétne v roku 2008 sila DDoS útoku dosiahla až 40 Gb/s, pričom za posledné 4 roky boli zaznamenané dovtedy najväčšie útoky so silou 24 Gb/s a 17 Gb/s, pričom práve druhý spomentý útok bol namierený na Slovensko. [11][20]

Ako ďalší bol realizovaný útok typu „brute-force“, teda hrubou silou. Takto označované útoky nie sú ani tak namierené na počítačovú sieť, ale ich primárnym cieľom je sieťové zariadenie. Hlavnou črtou tohto útoku je hádanie hesiel opakovaným prihlasovaním pod určitým účtom. Tento útok nepatrí medzi sofistikované typy útokov, ale v kombinácii kvalitného slovníka hesiel s nie príliš vhodne zvoleným heslom a žiadnym zabezpečením na zariadení, môže byť pomerne veľmi účinný a nebezpečný. Nebezpečný z takého dôvodu, že ak sa útočníkovi podarí zmocniť napríklad hranového smerovača, alebo iného smerovača s dôležitou funkciou v sieti, dostane príležitosť nielen meniť konfiguráciu zariadenia pre svoju záškodnícku činnosť, ale prakticky aj celý chod siete.

Posledný útok, ktorému bola venovaná pozornosť, pri útokoch na smerovač v úlohe prístupového bezdrôtového zariadenia, je založný na metóde odpočúvania paketov. Tento útok, ako je spomenuté v kapitole 2 patrí medzi pasívne typy, ale svojou činnosťou o to nebezpečnejšie. Ak si útočník prepne svoju sieťovú kartu do promiskuitného módu môže sa bez nášho vedomia zmocniť rôznych zneužiteľných informácií či údajov, ktoré následne dokáže veľmi efektívne využiť pri útoku na našu sieť.

5.1 Použité hárdverové vybavenie

Vybrané útoky sú demoštrované na štyroch rôznych smerovačoch, ktoré sú opísané nižšie. Na realizáciu útokov slúžil notebook s operačným systémom Linux, distribúcia Kubuntu 9.10 s jadrom 2.6.31-20, ďalšie použité počítače tvorili pripojených klienov zväčša s operačným systémom Windows. Topológia v akej boli jednotlivé smerovače zapojené je uvedená na obrázku 5.1, pričom v jednom prípade bola v sieti zapojená i IP kamera.



Obr. 5.1: Topológia zapojenia smerovača v sieti.

5.1.1 Smerovač Cisco 2821 CE

Smerovač Cisco 2821 CE patrí medzi prístupové, hraničné smerovače. Jeho výrobcom Cisco je zaradený do série 2800, ktorá je určená pre stredne veľké firmy s ďalšími menšími pobočkami. Tento smerovač disponuje operačným systémom Cisco IOS verzie 12.4, presnejšie 12.4(24)T1, má 256 MB pamäte DDR DRAM s rozšíriteľnosťou až do 1 GB, ďalej obsahuje pamäť Flash s kapacitou 64 MB s rošíriteľnosťou až do 256 MB. Smerovač taktiež obsahuje 4-portový ethernet prepínač, 2 Gigabit-ethernetové porty, 1 sériový port a 2 USB porty. Jeho vybavenie zďaleka nekončí na, tu vymenovaných súčastiach, ale obsahuje ešte ďalšie porty či sloty. Pre úplnú špecifikáciu funkcií, vlastností a taktiež vlastností operačného systému Cisco IOS, ktorý je veľmi rozsiahly a obsahuje kvantum funkcií je potrebné navštíviť stránky výrobcu. [4][5]

5.1.2 Smerovač MikroTik RouterBOARD 433

RouterBOARD (RB) 433, ktorý je vyvíjaný spoločnosťou MikroTik. Smerovač disponuje s procesorom Atheros 300 MHz, s pamäťou 64 MB RAM, s 3 ethernetovými portami, s 3 miniPCI slotmi, s 1 štandardným sériovým portom RS232C a s operačným systémom MikroTik RouterOS v3 s licenciou Level4. Smerovač RB433 svojím výkonom môže slúžiť ako centrálny, chrbtový prvok v stredne veľkej počítačovej sieti a preto jeho operačný systém RouterOS disponuje robusnou ponukou širokej škály funkcií, nástrojov a nastavení, ktorý mi sú napríklad hlbšie nastavenie smerovania a QoS, firewall s pokročilým filtrovaním, podpora protokolu RADIUS a VPN, správa certifikátov, ale taktiež i nástroje na sledovanie systému a správu siete. Po hárdverovom rozšírení môže smerovač slúžiť taktiež ako výkonnvý bezdrôtový prístupový bod. [26]

5.1.3 Smerovač DrayTek Vigor 2700VG

Smerovač DrayTek Vigor 2700VG je domáci smerovač určený k pripojeniu do Internetu. Síce patrí do kategórie domácich, svojou širokou podporov a taktiež vysokou úrovňou funkcií, si nájde miesto aj v menšej firme. Tento smerovač disponuje 4 ethernetovými portami, 2 portami určenými pre VoIP a samozrejme nechýba ani podpora bezdrôtového pripojenia. Konfigurácia tohto smerovača sa prevádza pomocou webového rozhrania, kde nájdeme napríklad tieto funkcie: podpora funkcie VLAN a NAT, pokročilejší firewall napríklad s podporov obrany voči DoS útokom, podpora QoS a VPN, podpora VoIP a ďalšie nástroje na správu a diagnostiku. Z pohľadu na bezpečnosť bezdrôtového pripojenia smerovač ponúka okrem skrytia SSID aj filtrovanie na základe MAC adresy a taktiež šifrovanie WEP a WPA2.

5.1.4 Smerovač D-Link DSL-2641R

D-Link DSL-2641R, ide taktiež o ADSL smerovač určený pre domáce pripojenie k Internetu. Tento model je distribuovaný spoločnosťou T-Com a je to okresaná verzia originálneho modelu DSL-2640B. Okresaná preto, lebo v užívateľskom móde je odopretých viacero nastavení, podľa mňa pomerne dosť dôležitých, ktorý mi napríklad sú nastavenia vstupných filtrov, nastavenie vzdialenej správy či rôzne sieťové nástroje. Dostať sa k administrátorskému módu nie je až tak náročné. Vyžaduje si to zmenu rozsahu IP adries v ktorom je tento mód prípustný. Nám ale práve toto okresanie funkcií vyhovuje pretože máme smerovač, ktorý nám poskytuje iba určitú úroveň funkcií. Smevač DLS-2641R poskytuje pripojenie pre 4 počítače pomocou ethernetového pripojenia a taktiež bezdrôtové pripojenie pre viacerých klientov. V užívateľskom móde podporuje napríklad len nastavenie QoS, nastavenie DNS, jednoduchý firewall a v zabezpečení bezdrôtového pripojenia ponúka skrytie SSID a šifrovanie na úrovni protokolu WEP a WPA2. [12]

5.2 Použité softérové vybavenie

Softvérové vybavenie tvorilo viacero nástrojov. Pre DoS útok bol využitý voľne siahnuteľný exploit napísaný v jazyku C, ktorý na nami zadanú adresu posielal potvrzdujúce ACK pakety z náhodných IP adries. Výsledkom takéhoto zahltenia je buď čiastočné zaťaženie alebo úplné vyradenie linky či zariadenia.

Na útok typu „brute-force“ bol použitý open-source nástroj Medusa vydaný pod licencou GPLv2. Tento šikovný nástroj podporuje rôzne sieťové protokoly či služby a veľké množstvo parametrov slúžiace k presnému nastaveniu.

Útok pomocou odopčúvania paketov bol realizovaný pomocov súboru nástrojov programu Aircrack-ng, ktorý slúži na audit bezdrôtových sietí. Tento program je voľne šíriteľný, vydaný pod licenciou GPLv2. S programom Medusa a Aircrack-ng bol taktiež použitý slovník hesiel, ktorý sa nachádzal v balíku nástrojov programu Aircrack-ng.

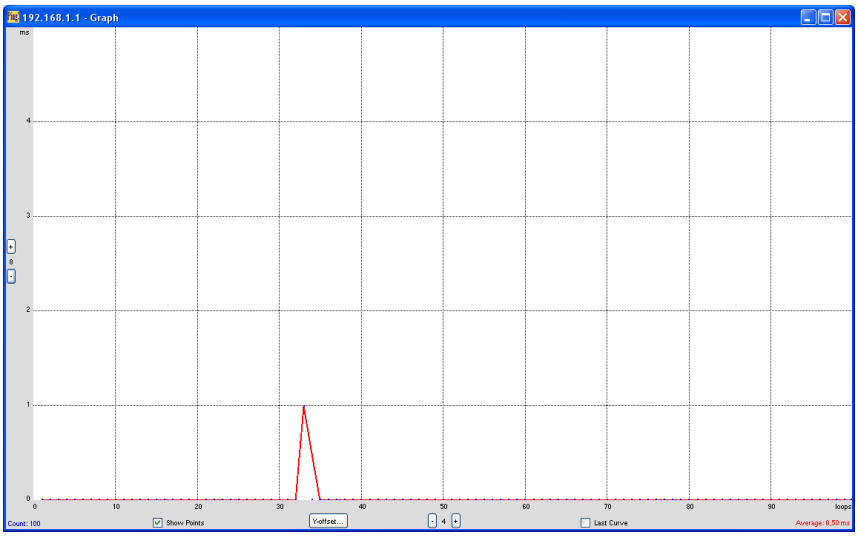
Ďalšie softérové vybavenie tvorili programi, ktoré sme využili pri sieťových analýzach. Ide o program Wireshark vydaný pod licenciou GPLv2 a program WinPing, ktorý je iba voľne šíriteľný.

5.3 Útoky na smerovač D-Link DSL-2641R

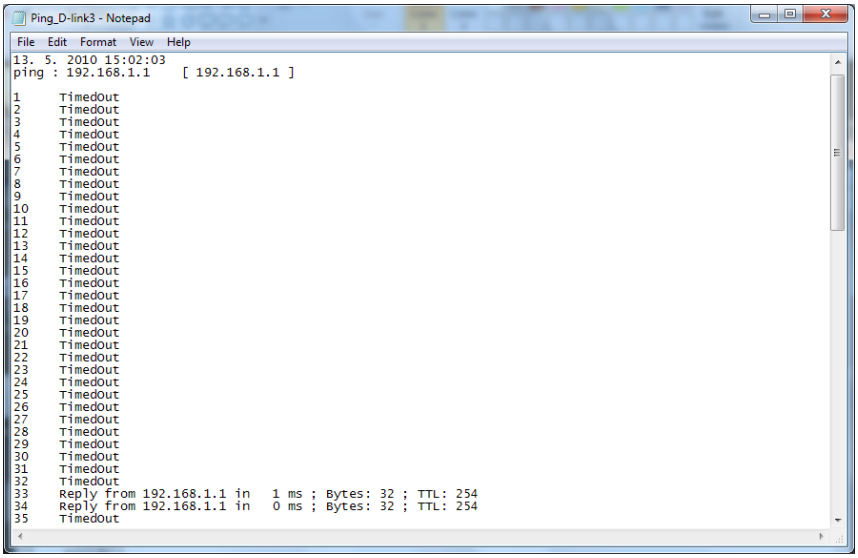
Smerovaču D-Link DSL-2641R patrí z pomedzi ostaných smerovačov, uvedených v kapitole 5.1, posledné miesto, a to nielen svojim hádverovým výkonom ale aj svojou funkcionalitou. Z tohto dôvodu bol tento smerovač ako prvý vystavený dvom útokom, a to typu DoS a typu „brute-force“.

Pri prvom útoku bol použitý exploit napísaný v jazyku C s názvom stream. Daný exploit sa spúšťal v nasledovnom tvare: *./stream IP adresa cieľa port veľkosť paketov* (príloha B.1), ak bol druhý parameter *0* , tak útok smeroval na náhodný port a ak bol tiež tretí parameter *0* , tak veľkosť paketov ostala nezmenená. Ako už bolo spomenuté v predchádzajúcej kapitole tento exploit mal za úlohu na nami zadanú adresu posielať potvrzdujúce ACK pakety z náhodných IP adries. Zaťaženie smerovača bolo vyhodnocované pomocou programu WinPing, ktorý bežal na počítači predstavujúceho pripojeného klienta, ktorý odozvu smerovača na príkaz *ping* vyniesol do grafu. Treba podotknúť, že bolo treba rozlíšiť dve okolonosti, a to také, že ak bola odozva okamžitá teda 0 ms, tak sa v grafe na osi X zobrazila hodnota nula a ak odozva smerovača nebola žiadna,teda *TimedOut* , tak graf opäť zobrazil na osi X nulu. Pre rozlíšenie týchto dvoch okoloností slúži export nameraných dát do textového súboru.

Pri nulovom zaťažení smerovača DSL-2641R bola odozva okamžitá. Ako náhle bol spustený daný exploit zo stanice útočníka, smerovač prestal odpovedať a v rozsahu 100 pingov po sebe program WinPing zaznamenal odozvu len dva krát ako možno vidieť na obrázku 5.2 a 5.3. Tento jednoduchý exploit vyvolal na smerovači zaťaženie až také, že zariadenie bolo odrezané od Internetu a až po následnom reštartovaní bol smerovač opäť plne schopný prevádzky.



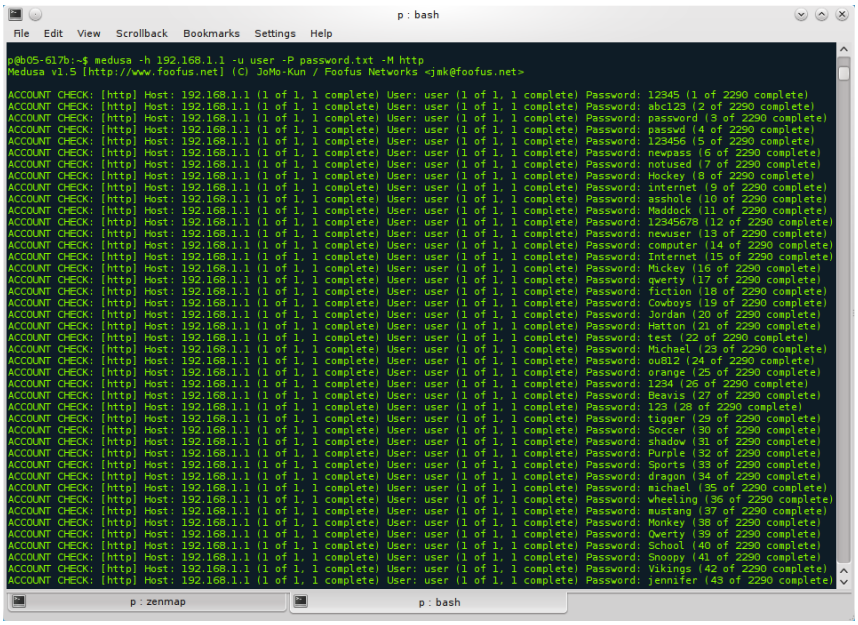
Obr. 5.2: Zaznamenaná odozva smerovača DSL-2641R pri záťaži.



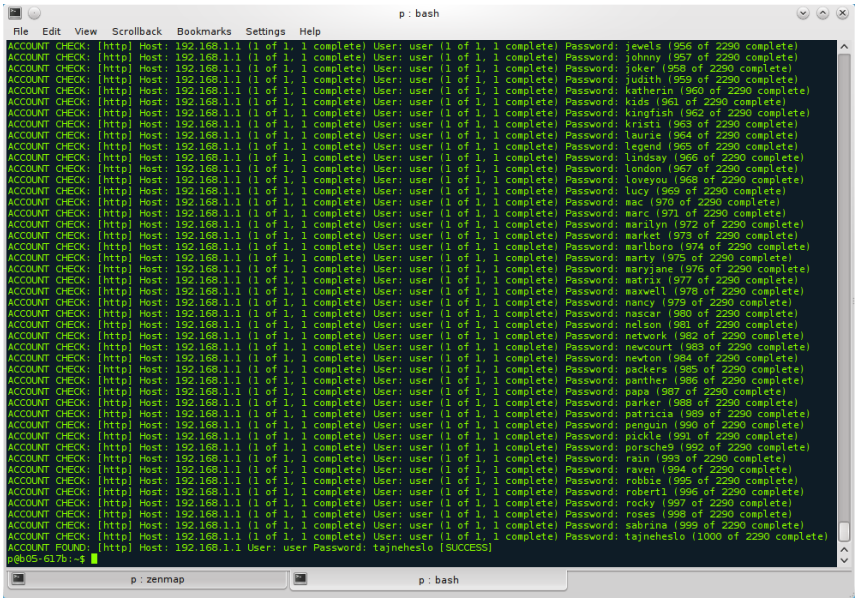
Obr. 5.3: Textový záznam odozvy smerovača DSL-2641R pri záťaži.

Pri druhom útoku na smerovač DSL-2641R bol využiťý nástroj Medusa. Tento program sa spúšťal nasledovne: *medusa -h adresa cieľu -u prihlasovacie meno -P použitý slovník -M modul* (obr. 5.4) a jeho úlohou bolo primitívne dosadzovanie hesiel zo slovníka k zvolenému prihlasovaciemu menu. Slovník, ktorý bol použitý, bol upravený tak, aby obsahoval heslo k danému smerovaču, a tak behom niekoľkých sekúnd bolo dané heslo úspešne uhádnuté (obr. 5.5). Tento smerovač neobsahuje žiadne funkcie pomocou ktorých by bolo možné ošetriť počet nesprávnych prihlásení za sebou v rade či v určitom časovom limite. Dokonca neobsahuje ani funkcie na to, aby sa

dali zmeniť porty na ktorých dané služby bežia. Táto funkcia by viedla len k oddialeniu možného útoku, pretože zmenu portov nemožno v žiadnom prípade považovať za ochranu a zabezpečenie. Obyčajným prehľadaním portov ľahko zistíme, kde beží aká služba a útok možno potom teda realizovať na inom porte.



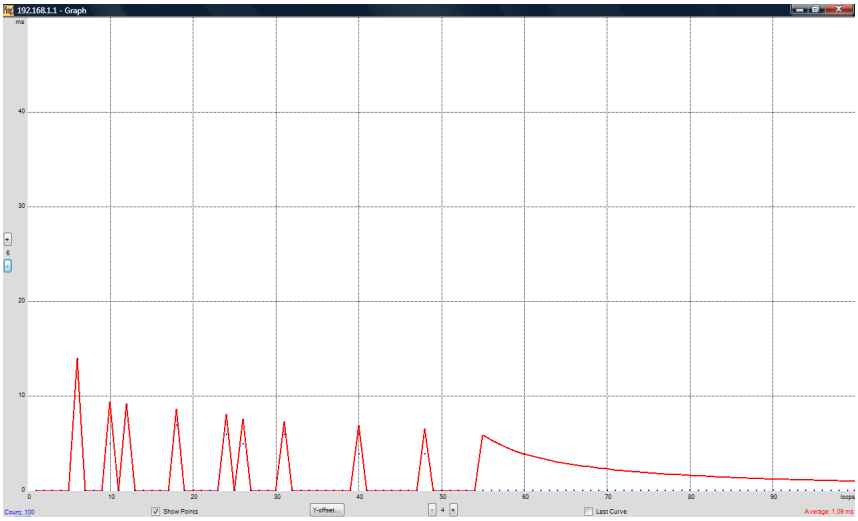
Obr. 5.4: Spustenie programu Medusa.



Obr. 5.5: Odhalenie hesla smerovača DSL-2641R.

5.4 Útoky na smerovač DrayTek Vigor 2700VG

Smrovač DrayTek Vigor 2700VG možno považovať za lepšie vybavený funkciami než smerovač D-Link DSL-2641R, o čom svedčí jeho oveľa pestrejšia ponuka funkcií. Ako v predchádzajúcom prípade aj na tento smerovač boli realizované dva útoky. Pri útoku typu DoS bol postup presne taký istý ako pri smerovači DSL-2641R, s rozdielom že útok bol prevedený na konkrétny port a to port 23 na ktorom beží služba Telnet. Ak bol smerovač nezaťažený, odozva bola opäť okamžitá. Ak bol smerovač vystavený útoku pomocou exploitu stream, tak zariadenie dokázalo odpovedať približne na polovicu požiadaviek príkazom *ping* a na ostatnú časť požiadaviek nereagoval (obr. 5.6).

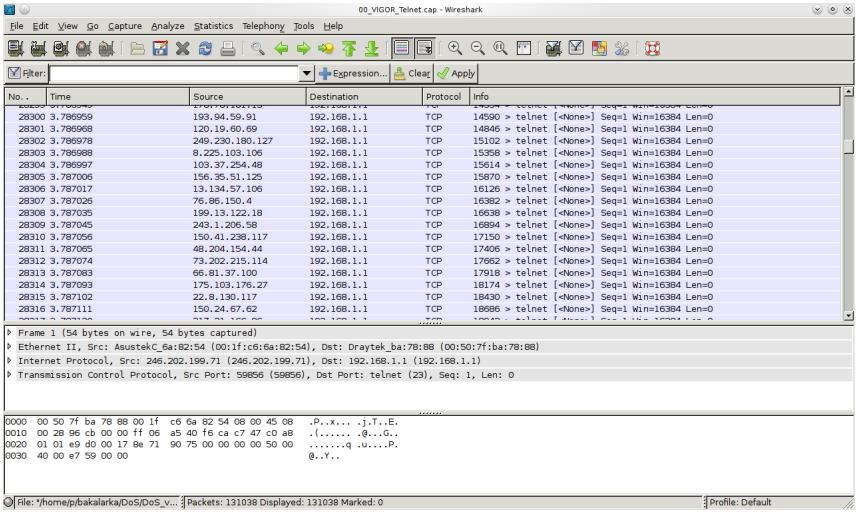


Obr. 5.6: Zaznamenaná odozva smerovača Vigor 2700VG pri záťaži.

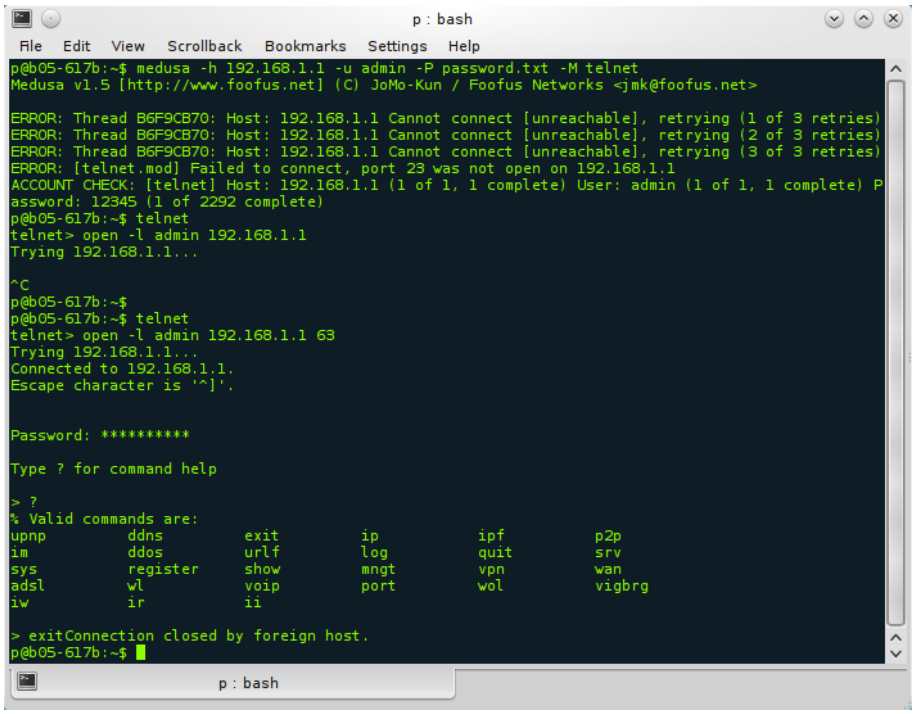
Pre ilustráciu je na obrázku 5.7 ukážka ako odosielané pakety vyzerali a v prílohe B.2 možno vidieť ukážku, ako smerovač nedokázal reagovať ak sa chcel pripojený klient prihlásiť pomocou služby Telnet a ako po ukončení útoku bola služba Telnet prístupná. Tento útok poznačil výkon smerovača natoľko, že nedokázal ponúknuť pripojenému klientovi pripojenie do Internetu, ale oproti smerovaču DSL-2641R bol v priebehu niekoľkých sekúnd po ukončení útoku plne k dispozícii.Smerovač Vigor 2700VG ponúka bezpečnostnú funkciu obrany proti DoS útokom, ale v tomto prípade nebola vôbec účinná a funkčná, pretože aj po zapnutí všetkých ponúkaných možností (príloha B.3), bol pri útoku smerovač vyťažený a neschopný prevádzky.

Pri ďalšom útoku typu „brute-force“ bol postup opäť podobný ako v kapitole 5.3, s rozdielom že útok prebiehal na službu Telnet. Uhádnutie hesla s upraveným slovníkom trvalo menej než pár sekúnd (príloha B.4). Smerovač Vigor 2700VG taktiež neobsahuje funkcie na zabezpečenie prihlasovania ako predchádzajúci smero-

vač, ale umožňuje zmenu portu. Ako už bolo spomenuté, zmenu portu nemožno považovať za zabezpečenie, ale pre ilustráciu na obrázku 5.8 vidieť, že útok na štandardný port Telnetu je neúspešný ale následné prihlásenie cez už zmenený port 63 je úspešné.



Obr. 5.7: Odosielané ACK pakety z náhodných IP adries.

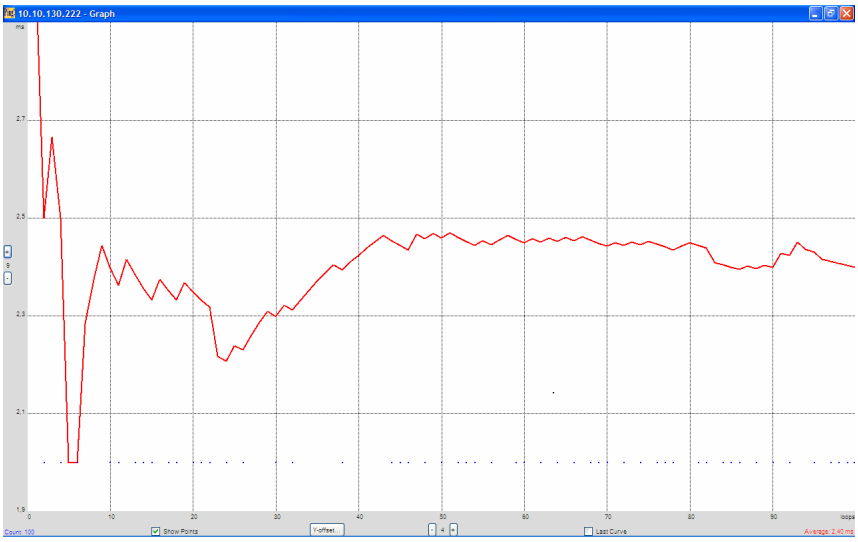


Obr. 5.8: Neúspešný útok typu „brute-force“.

5.5 Útoky na smerovač RouterBOARD 433

Smerovač RouterBOARD 433 je svojou funkcionalitou a taktiež hárverovým vybavením podstatne vyššie než sú dva predchádzajúce smerovače. Tak ako u ostatných dvoch smerovačoch aj tu bol postup oboch útokov pobobný.

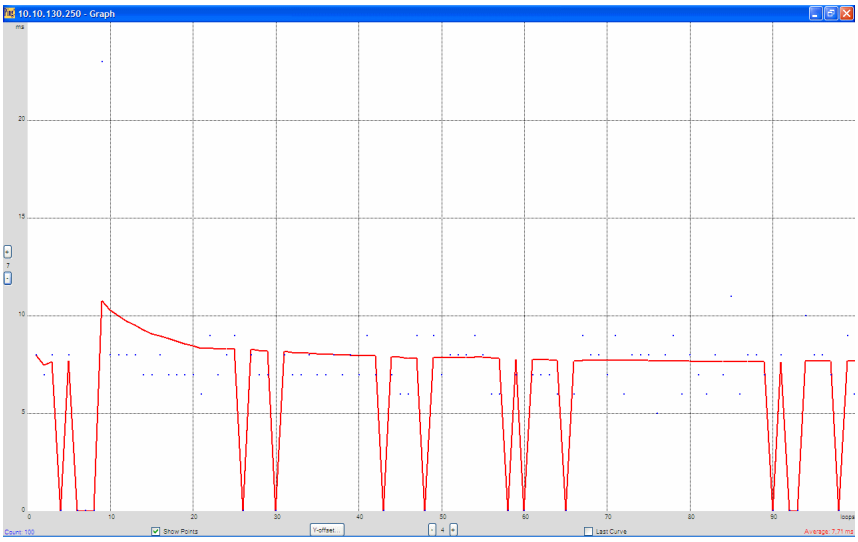
Pri útoku odoprenia služieb, DoS, bola na smerovač taktiež okrem jedného klienta pripojená i IP kamera. Počas normálnej prevádzky smerovač vykazoval 100% chod a maximálnu odozvnu a IP kamera mala odozvu na príkaz *ping* 0,1 ms. Útok opäť pomocou exploitu stream ale spôsobil trochu väčšie hodnoty odozvy smerovača čo sa prenieslo taktiež aj do grafu na obrázku 5.9. Pri odozve IP kamery to už bolo o dosť horšie, pretože kamera vykazovala odozvu s priemerom 7,71 ms a niekedy odozvu s úplným výpadkom (obr. 5.10), čo spôsobilo nefunkčnosť kamery. Po ukončení útoku smerovač a taktiež aj kamera boli okamžite k dispozícii.



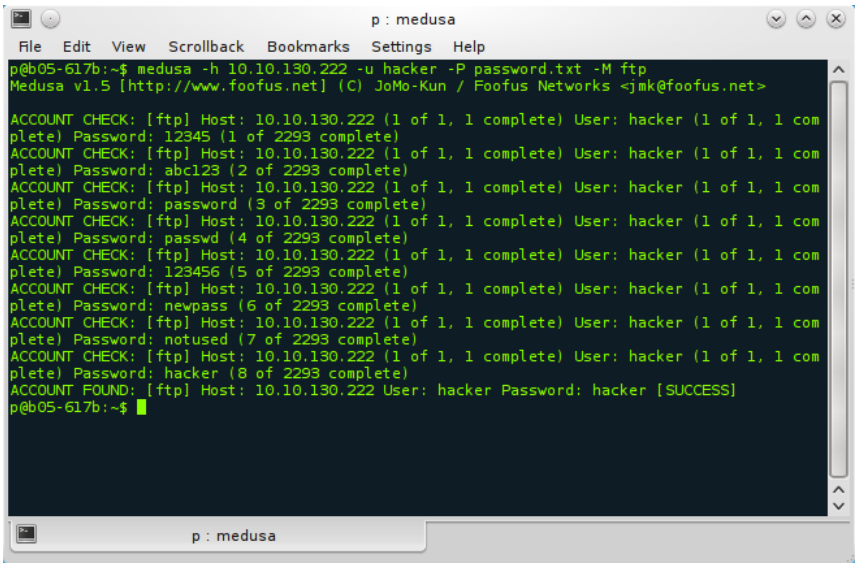
Obr. 5.9: Zaznamenaná odozva smerovača RB433 pri záťaži.

Pri druhom útoku bolo pomocou nástroja Medusa uhádnuté heslo k FTP prístupu do smerovača (obr 5.11). Opäť doba odhalenie hesla bola menej než pár sekúnd.

MikroTik RouterOS, ktorý beží na smerovačoch RouterBOARD, poskytuje voči takýmto útokom zabezpečenie v rámci nastavenia Firewallu. V skutočnosti ide o definíciu určitých pravidiel na vstupe a výstupe Firewallu. V systéme RouterOS sa dajú nastavenia realizovať nielen pomocou grafického ovládacieho panelu ale taktiež pomocou skriptov.



Obr. 5.10: Zaznamenaná odozva IP kamery pri záťaži smerovača.

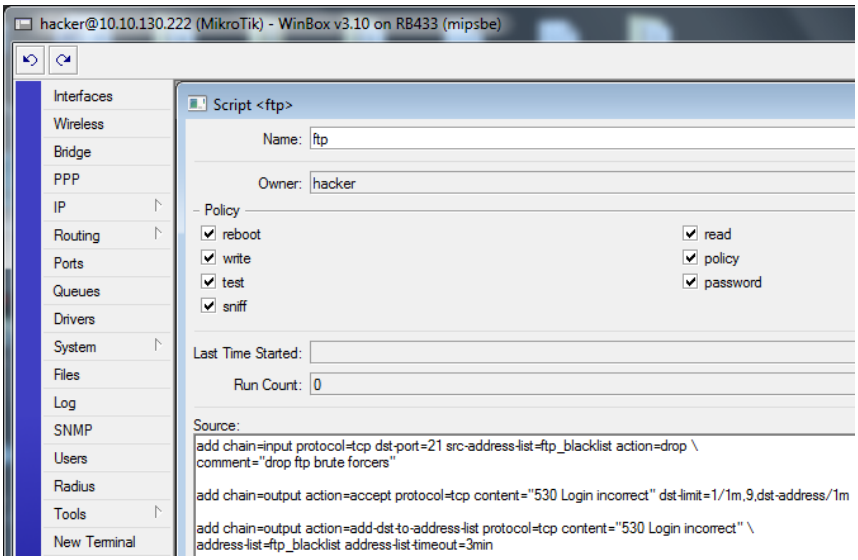


Obr. 5.11: „Brute-force“ útok programom nástrojom Medusa.

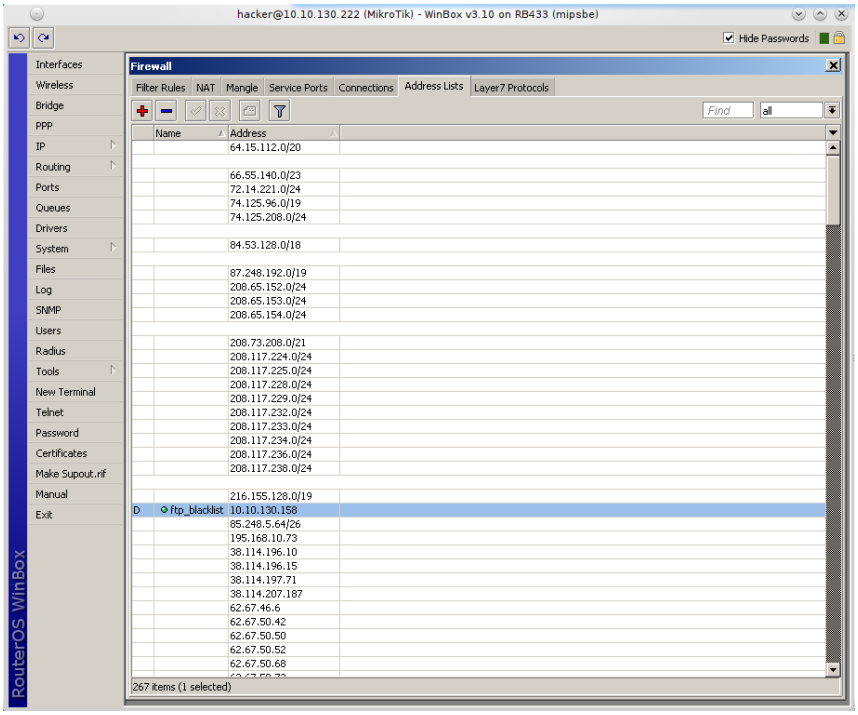
Na obrázku 5.12 možno vidieť skript ktorý zabezpečuje to, aby po desiatich nesprávnych prihláseniach v rámci jednej minúty na porte 21, čo je port pre FTP, sa IP adresa z ktorej chybné prihlásenie prišlo dostala do adresového zoznamu, nami nazvaného ftp_blacklist, ktorý nepripustí prihlásenie z danej IP adresy nasledujúce 3 minúty. V prílohe B.5 vidieť, že po desiatich neúspešných prihláseniach nám program Medusa ohlási chybu a na obrázku 5.13 možno vidieť, že IP adresa z ktorej neúspešné prihlásenia prišli je zaradená do zoznamu s názvom ftp_blacklist.

To že sa po dobu blokovania IP adresy nedá prihlásiť na smerovač dokazuje obrázok v prílohe B.6. Tento spôsob obrany nie je jediný voči tomuto útoku, pretože

existujú aj iné možnosti zamedzenia pokusov prístupu k zariadeniu. Nástrojom Medusa bolo taktiež skúšané odhaliť heslo cez SSH spojenie, ale ako je opäž uvedené v prílohe B.7, program Medusa hneď pri prvom pokuse ohlásil chybu. Počas celej práce nebolo zistené, z akého dôvodu nástroj Medusa ohlasuje chybu, či je spôsobená programom alebo nejakým skrytým nastavením v operačnom systéme RouterOS.



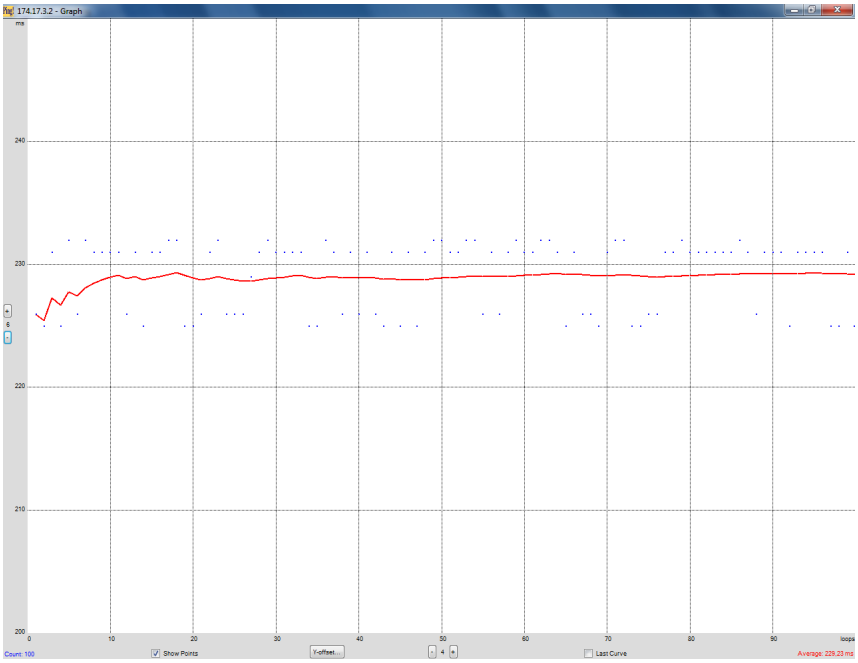
Obr. 5.12: Skript pre nastavenie Firewallu.



Obr. 5.13: Zaradenie nežiadúcej IP adresy do zoznamu ftp_blacklist.

5.6 Útoky na smerovač Cisco 2821 CE

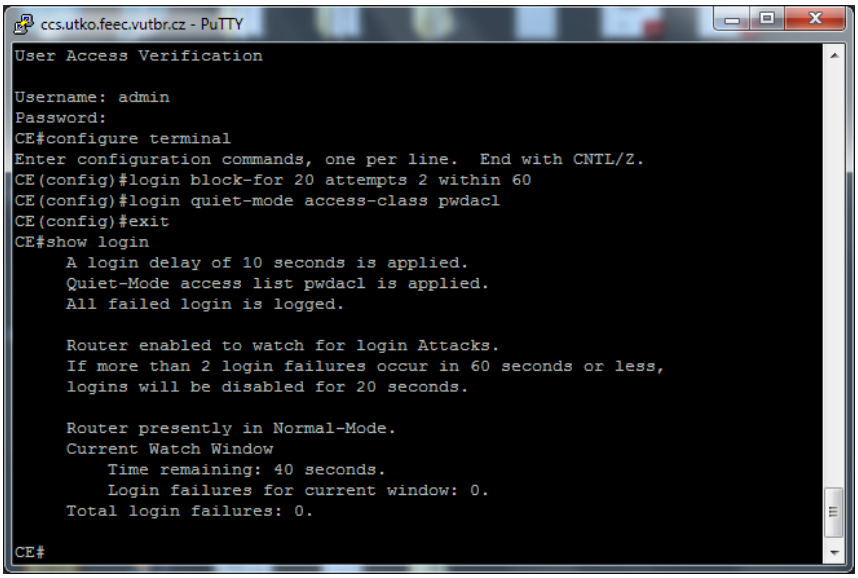
Smerovač Cisco 2821 CE je z pomedzi ostatných smerovačov spomínaných v predchádzajúcich kapitolách najvýkonnejší. Aj na tento smerovač bolo útočené ako v predchádzajúcich prípadoch z operačného systému Linux dvomi útokmi. Počas normálnej prevádazky smerovač vykazoval odozvnu v priemere 229,08 ms (priloha B.8), čo bolo pomerne veľa, pretože klientský počítač bol pripojený asi dva metre od smerovača. Prečo bola odozva takáto nebolo zistené. V prípade zaťaženia smervača Cisco 2821 CE exploitom stream, bola odozva približne taká istá, v priemere 229,23 ms (obr. 5.14). Predpoklad, že tento útok vôbec neovplyvní a nezaťaží chod smerovača sa iba potvrdil, pretože smerovač nevykazoval počas útoku nejaké zmeny oproti chodu za obvyklej prevádzaky.



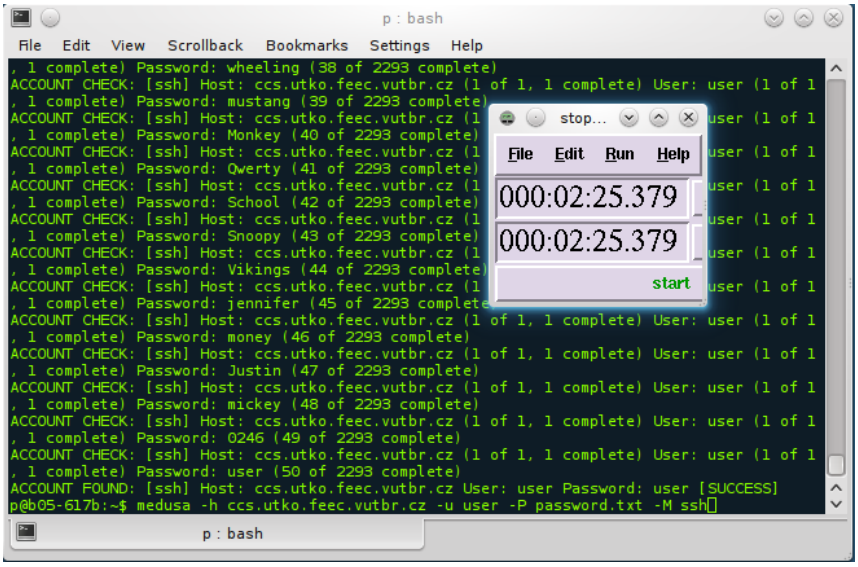
Obr. 5.14: Zaznamenaná odozva smerovača Cisco 2821 CE pri záťaži.

Pri nasledujúcom útoku typu hrubou silou bolo útočené na port 22, na ktorom beží SSH, cez ktorý sa da prípojiť do konfiguračného rozhrania smerovača. Výsledok bol opäť rovnaký ako vo všetkých predchádzajúcich prípadoch, heslo bolo odhalené. Operačný systém Cisco IOS 12.4, ktorý bol na smerovači, obsahuje nesmierne množstvo nastavení a funkcií. Samozrejnosťou je aj jeho možnosť konfigurovať prihlasovanie, ktorá patrí medzi základné prvky. Podľa príkladu uvedeného v Cisco IOS Login Enhancements [3] možno nastaviť, aby po dvoch nekorektných prihláseniach v rámci 1 minúty, sa nebolo možné prihlásiť nasledujúcich 20 sekúnd (obr. 5.15), ale prihlásenie bude možné iba z adries definovaných v ACL zozname.

Pre demonštráciu časovej dĺžky tohto typu útoku, bol zrealizovaný útok z Internetu na smerovač Cisco 1841. Prihlasovacie meno bolo nastavené ako *user* a heslo taktiež ako *user* . Heslo *user* bolo v slovníku umiestnené ako päťdesiate v poradí. Výsledný čas, ktorý bol potrebný na odhalenie hesla bol približne 2 minúty a 25 sekúnd. Otestovanie jedného hesla trvalo asi 2,9 sekundy, takže ak by sme heslo umiestnili ako dvetisíce v poradí, bolo by potrebných 5800 sekúnd, čo predstavuje 1 hodinu, 36 minút a 40 sekúnd na jeho odhalenie (obr. 5.16).



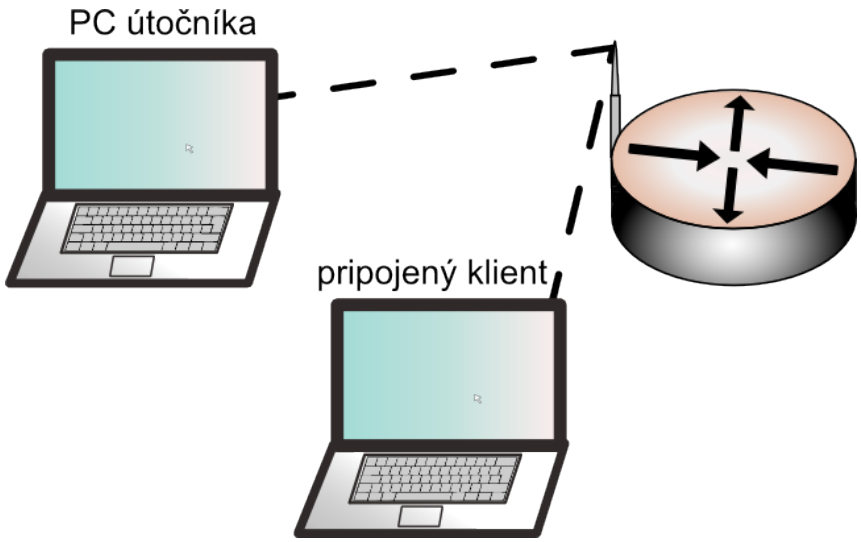
Obr. 5.15: Nastavenie konfigurácie prihlasovania k smerovaču Cisco.



Obr. 5.16: Čas potrebný na odhalenie správneho hesla, ktoré je päťdesiate v poradí.

5.7 Útoky na smerovač v bezdrôtovej sieti

Na útoky v bezrôtovej sieti sme si vybrali smerovač DrayTek Vigor 2700VG a smerovač D-Link DSL-2641R, pričom smerovač Vigor 2700VG sme využili pri troch demonštráciách útokov a smerovač DSL-2641R len pri jednej demoštrácii útoku. Tieto smerovače sme zvolili hlavne z dôvodu, že oba primárne podporujú bezdrôtové pripojenie a navyše sú určené pre domácnosti, kde v dnešnej dobe používanie mobilných zariadenia ktoré sú pripojené k Internetu úplne prirozdené. Oba smerovače slúžili ako bezdrôtové prístupové body v topológii znázornenej na obrázku 5.17. Na vykonanie všetkých útokov v bezdrôtovej sieti sme použili súbor nástrojov programu Aircrack-ng pod operačným systémom Linux.



Obr. 5.17: Topológia zapojenia smerovača v bezdrôtovej sieti.

5.7.1 Odhalenie skrytého SSID prístupového bodu

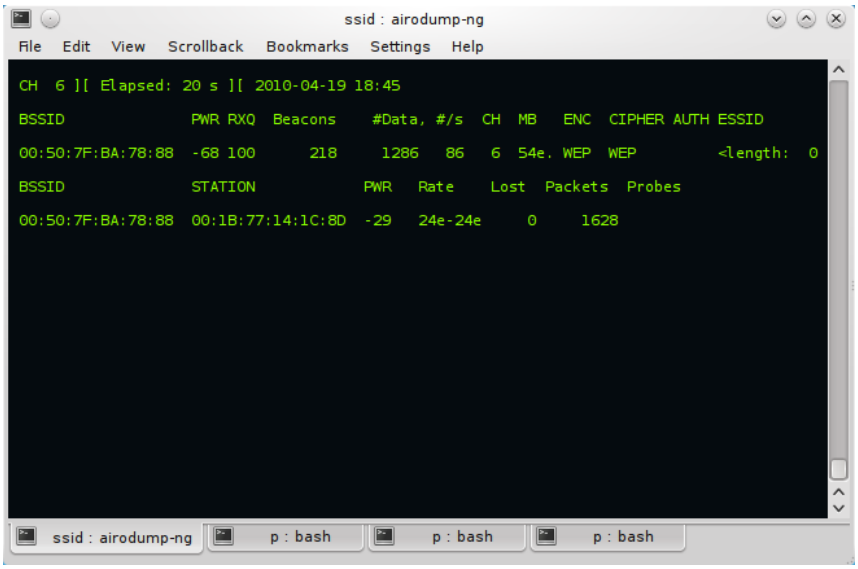
Ochrana prístupového bodu patrí medzi základné ochrany, a to z dôvodu, že bezdrôtový klient neuvidí skryté SSID bezdrôtovej siete. Táto problematika je viacej priblížená v kapitole 4.3.3. Skrytie SSID môžeme považovať za prvú obrannú líniu, pretože túto funkciu podporuje skoro každý smerovač. Pri tejto demonštrácii sme použili smerovač DrayTek Vigor 2700VG.

Preto, aby sme boli úspešný pri odhalení SSID nášho prístupového bodu musíme splniť nasledovné kritériá:

- WiFi karta musí podporovať promiskuitný mód
- s prístupovým bodom musí komunikovať aspoň jeden bezdrôtový klient

Ak sú tieto dve kritériá splnené môžeme postupovať nasledovne. Na začiatok našu WiFi kartu prepneme do promiskuitného módu. V našom prípade na to použijeme príkaz *airmon-ng start wlan0*, kde *wlan0* predstavuje naše Wi-Fi rozhranie. Týmto príkazom dosiahneme vytvorenie nového rozhrania nad našim fyzickým bezdrôtovým rozhraním s názvom *mon0* pričom na tomto rozhraní beží pre nás potrebný promiskuitný mód. V tomto okamžiku sa rozhranie *wlan0* dostáva do úzadia a praticky nijak neovplyvňuje naše načúvanie na rozhraní *mon0*.

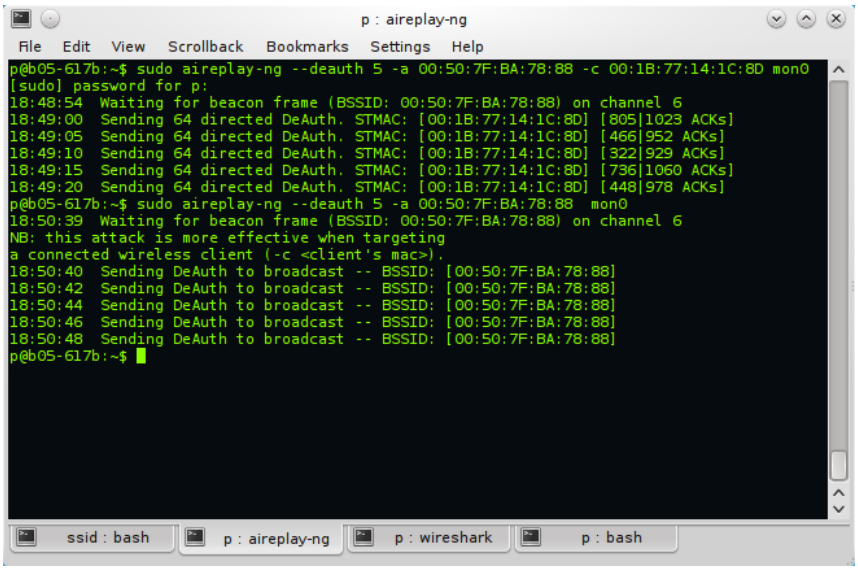
Po tomto kroku nasleduje odchytávanie komunikácie medzi pripojeným klientom a prístupovým bodom. Na spustenie odchytávania použijeme príkaz *airodump-ng -c 6 -w ssid mon0*, kde prvý parameter znamená kanál na ktorom budeme načúvať, druhý parameter znamená zápis odchytených paketov do súboru s názvom *ssid* a ako posledný výraz je naše vytvorené rozhranie. Ako môžeme vidieť na obrázku 5.18, po tomto príkaze uvidíme prístupový bod a komunikujúceho klienta s ich MAC adresami. Taktiež uvidíme, že prístupový bod používa šifrovanie WEP ale SSID viditeľné nebude.



Obr. 5.18: Odchytávanie komunikácie pomocou nástroja Airodump-ng.

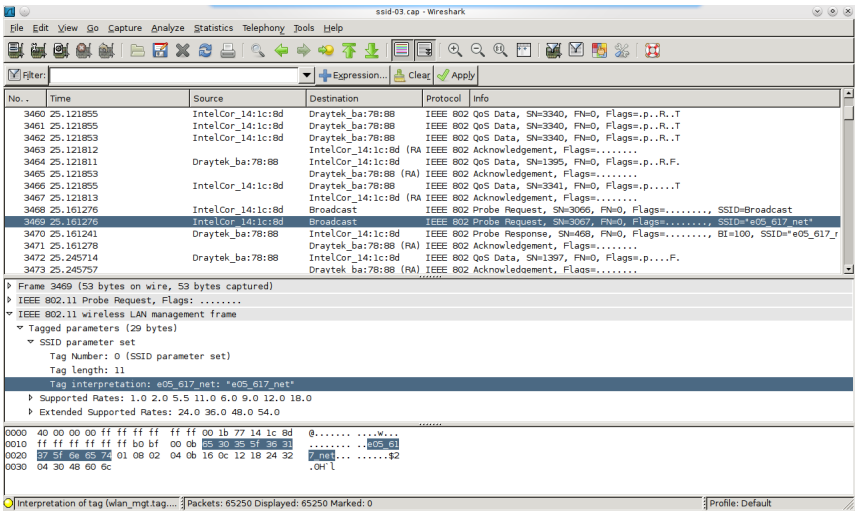
V tomto momente dochádza k jadru prevedenia tohto útoku, a to preto, lebo využijeme MAC adresu komunikujúceho klienta a nasimulujeme jeho odpojenie, čím sa nám podarí odchytiť pakety obsahujúce pre nás dôležité informácie. Na prevedenie tohto kľúčového momentu, využijeme nástroj príkaz *aireplay-ng*, ktorého hlavnou funkciou je tzv. *packet injection*, kedy je cielene vytváraná sieťová prevádzka, v našom prípade ide o falošnú deautentizáciu. Samotný príkaz vyzeral nasledovne: *aireplay-ng –deauth 5 -a 00:50:7F:BA:78:88 -c 00:1B:77:14:1C:8D mon0*, kde prvý parameter s číslom 5 znamená päť deautentizácií za sebou, parameter

druhý parameter nám udáva MAC adresu prístupového bodu a tretí MAC adresu klienta (obr. 5.19). Ak by sme tento príkaz použili bez druhého parametru, došlo by k tzv. Broadcast deautentizácii, ktorá nemusí byť efektívna, a to preto, lebo nie je presne definovaný klient (obr. 5.19).



Obr. 5.19: Falošná a Broadcastová deautentizácia pomocou nástroja Aireplay-ng.

Teraz nám už len stačí daný súbor do ktorého odchytávame komunikáciu otvoriť napríklad v sieťovom analyzátore Wireshark a nájsť SSID prístupového bodu (obr. 5.20).

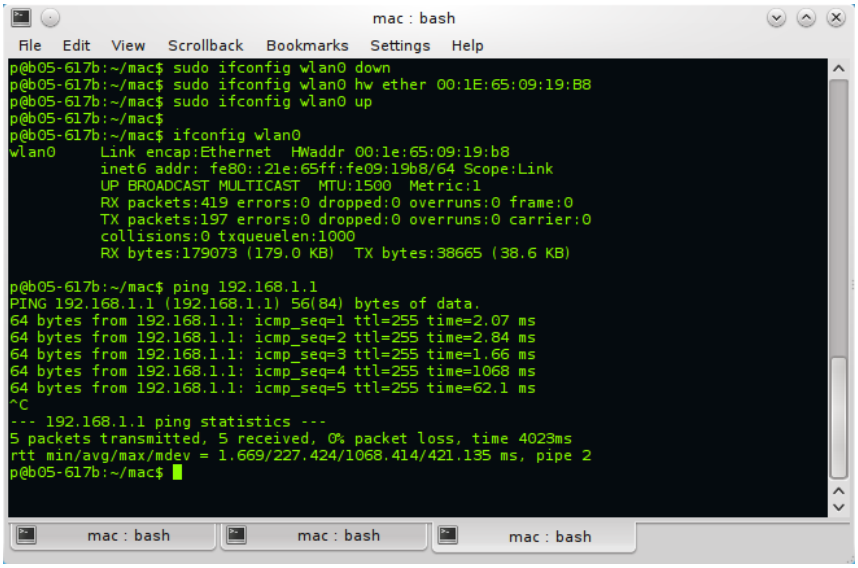


Obr. 5.20: Odhalenie skrytého SSID.

5.7.2 Obídenie filtrovania MAC adresy

Výhody i nevýhody filtrovania MAC adries sú bližie opísané už v kapitole 4.3.3 a oproti skrytiu SSID ho môžeme považovať za lepšiu obranu. Ak chcem prekonať filtrovanie MAC adriesy na bezdrôtovom smerovači, v našom prípade to je to opäť DrayTek Vigor 2700VG, musím postupovať približne ako v predchádzajúcom príklade.

Našu Wi-Fi kartu si opäť prepneme do promiskuitného módu, tento mód je opäť potrebnou podmienkou, a začneme s odchytávaním všetkej komunikácie. Ak poznáme MAC adresu prístupového bodu cez ktorého filtráciu sa chcem dostať, k príkazu *airodump-ng* z predchádzajúceho príkladu môžeme definovať paramter *-b* a za ním konkrétnu MAC adresu. Po zadaní tohto príkazu sa nám zobrazia všetci pripojený klienti a ich MAC adresy (príloha C.1). Stačí si už len vybrať danú MAC adresu, ktorá komunikuje s prístupovým bodom a sfalšovať ju, teda nastaviť ju na našom Wi-Fi adaptéry, ktorého MAC adresa nie je v zozname prípustných adries. Na obrázku 5.21, môžeme vidieť celý tento postup zmeny MAC adresy a následného úspešného pingnutia prístupového bodu.



Obr. 5.21: Zmena MAC adresy na bezdrôtovej sieťovej karte.

Treba ešte zdrôrazniť, že prístupový bod neumožní pripojenie dvoch klientov s rovnakou MAC adresov naraz a preto je prístupovým bodom preferovaný klient s vyššou kvalitou signálu. Ak ale nie je klient, ktorého MAC adresu zneužívame pripojený, môžeme sa pripojiť my a to bez akýchkoľvek problémov.

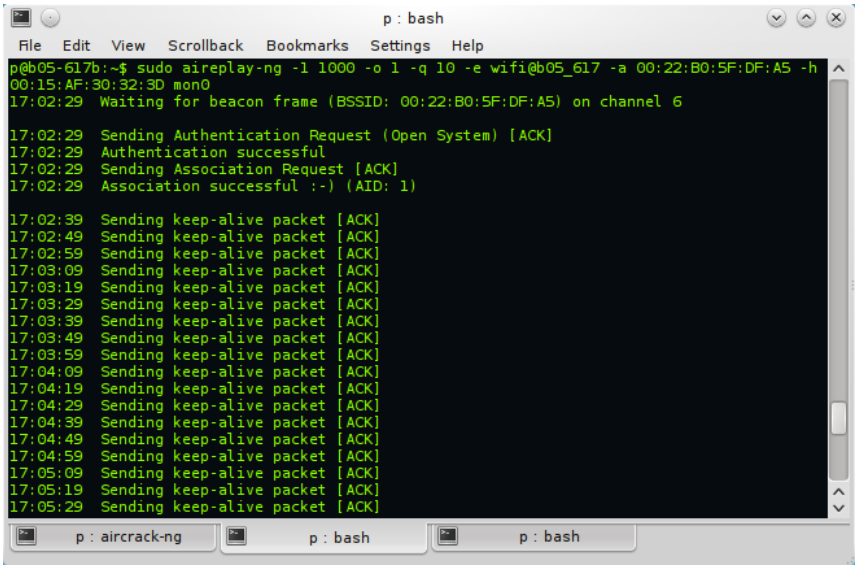
5.7.3 Prelomenie kľúča WEP

Pre zabezpečenie prenášaných dát pri bezdrôtovom pripojení slúži WEP kľúč, priblížený v kapitole 4.3.3. Je to štandard, ktorý je základnou súčasťou štandartu 802.11. Šifrovanie pomocou WEP ponúka teda každý smerovač, ktorý podporuje bezdrôtové pripojenie. Pri prelomení protokolu WEP bol použitý smerovač D-Link DSL-2641R s dĺžkou WEP kľúča 64-bitov, ktorý slúžil ako prístupový bod.

Aby bolo možné kľúč prelomiť bolo potrebné aby boli splnené nasledovné podmienky:

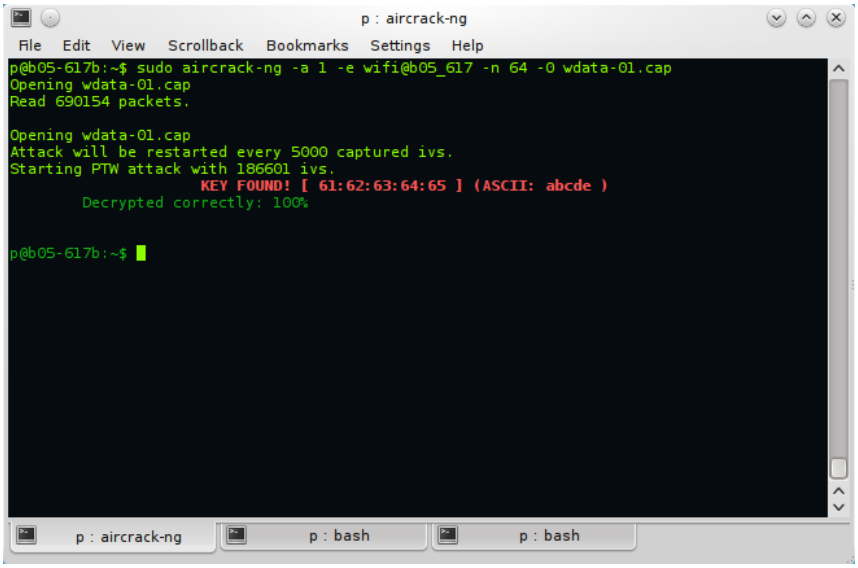
- WiFi karta musí podporovať promiskuitný mód
- s prístupovým bodom musí komunikovať aspoň jeden bezdrôtový klient
- podpora *packet injection* (príloha C.2) (táto podmienka nie je povinná, ale bez nej by bol útok časovo náročný)

Na začiatok bolo opäť potrebné zopakovať úkony z predchádzajúcich kapitol, a to prepnutie Wi-Fi karty do promiskuitívneho módu a spustenie odchytávania komunikácie, kde bol definovaný kanál na ktorom prebiehala komunikácia, MAC adresa prístupového bodu a súbor do ktorého boli ukladané odchytené rámce (príloha C.3). Na to, aby prístupový bod prijímal pakety z našej Wi-Fi karty bolo potrehné asociovať našu MAC adresu s prístupovým bodom a to nástrojom *aireplay-ng*, pomocou ktorého sme sa pokúšali o autentizáciu každých 10 sekúnd, ako je uvedená na obrázku 5.22.



Obr. 5.22: Prebiehajúca autentizácia medzi klientom a prístupovým bodom.

Aby bol útok prevedený rýchlejšie, na komunikujúcom klientovi bežalo sťahovanie z Internetu a taktiež boli pomocou nástroja *aireplay-ng* generované falošné ARP pakety (príloha C.4), na ktoré prístupový bod odpovedal všetkým pripojeným klientom novovygenerovanými inicializačnými vektormi. Vďaka tomuto bolo možné v kratšom čase zachytiť potrebné množstvo inicializačných vektorov. Po odchytení potrebného množstva inicializačných vektorov, stačilo spustiť nástroj *aireplay-ng*, ktorý sa postaral o prelomenie WEP kľúča, v tomto prípade išlo o kľúč abcde. Ako vidno na obrázku 5.23, jednotlivé parametre boli nasledovné: *-a 1* definuje že ide o prelomenie WEP kľúča, parameter *-e* určuje SSID prístupového bodu, parameter *-n 64* bližšie definuje že WEP kľúč je 64-bitový a posledná časť určuje z akého súboru odchytených dát bude WEP kľúč odhalený. Na základe tejto demonštrácie možno tvrdiť, že zabezpečenie pomocou WEP, ktoré je poskytované smerovačmi pri bezdrôtovom pripojení, je určite nedostatočné.

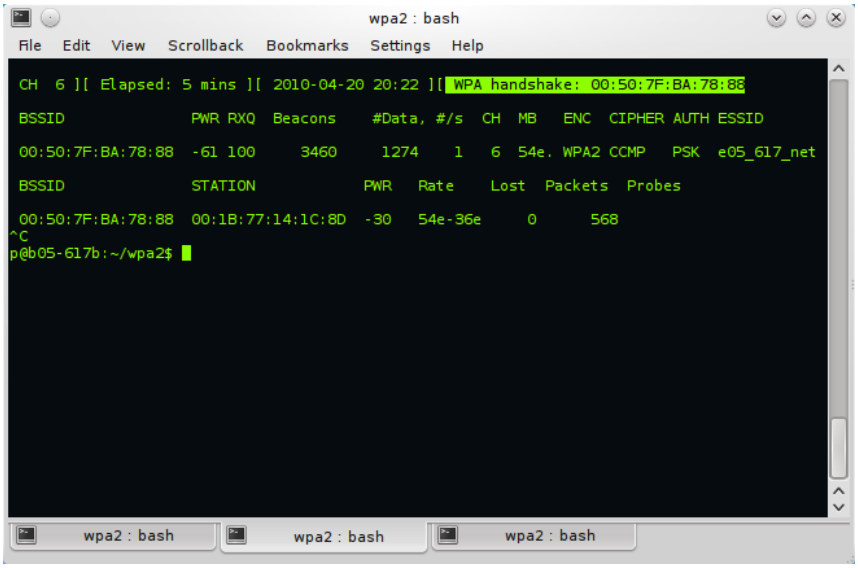


Obr. 5.23: Odhalenie WEP kľúča nástrojom Aircrack-ng.

5.7.4 Prelomenie WPA2 kľúča

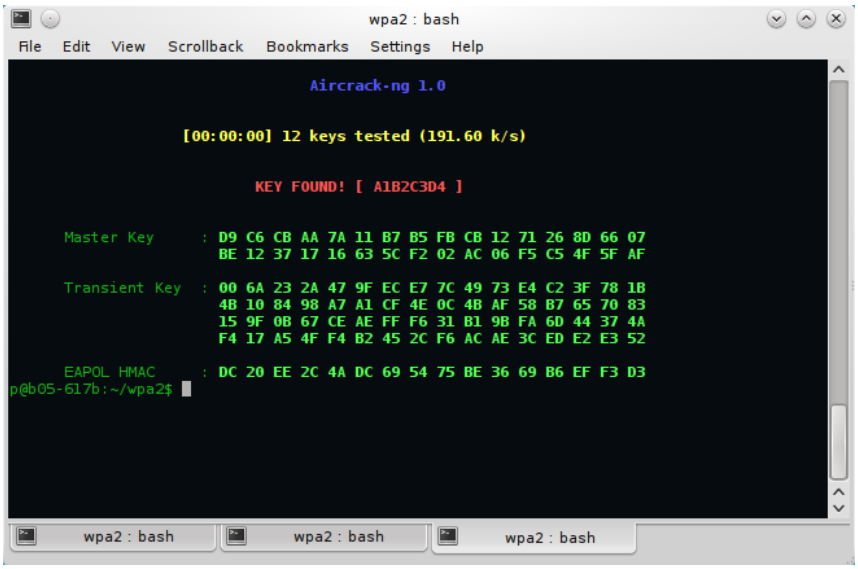
Zabezpečenie pomocou WPA2 kľúča bolo vytvorené pre lepšie zabezpečenie pri bezdrôtovom pripojení. Toto zabezpečenie poskytuje na rozdiel od WEP klúča aj autentizačný mechanizmus, a práve ten je možné zneužiť. Útok na WPA2 klúč bol zameraný na zdieľanú autentizáciu, ktorá je zabezpečovaná zdieľaným kľúčom. Cieľom je odchytiť autentizačný proces medzi prístupovým bodom a klientom, nazývaný štvrocestný handshake (4-way handshake). Pri tomto útoku bol použitý smerovač DrayTek Vigor 2700VG.

Postup pri prelamovaní WPA2 kľúča bol približne rovnaký ako pri prelamovaní kľúča WEP. Na začiatku bolo potrebné prepnúť Wi-Fi kartu do monitorovacieho módu a spustiť odchytávanie paketov do nami zvoleného súboru. Na to aby sme odchytili tie správne pakety, bolo možné buď generovať falošnú deautentizáciu, alebo stačilo aby sa aspoň jeden klient pripojil k smerovaču. Keďže pri prelamovaní boli vytvorené simulované podmienky, bolo prevedené pripojenie klienta k smerovaču. V tomto prípade ako vidno na obrázku 5.24, bol odchytený potrebný štvrocestný handshake. V sieťovom analyzátore Wireshark možno toto odchytenie taktiež pozorovať v prílohe C.5.



Obr. 5.24: Odchytenie potrebného štvrocestného handshaku.

Na prelomenie WPA2 kľúča bolo potrebné už len spustiť program *aircrack-ng* v nasledovnom tvare: *aircrack-ng -a 2 -e e05_617_net -w password.lst wpa2-01.cap* , kde prvý parameter označoval prelomenie WPA2, druhý vymedzoval SSID prístupového bodu, tretí parameteter zadával pomenovanie súboru heslami a posledný parameter bol súbor s odchyteným handshakom. Kľúč bol zistený okamžite (obr. 5.25), z dôvodu, že nástroj *aircrack-ng* nemusel testovať veľa hesiel, pretože heslo A1B2C3D4 bolo umiestnené medzi začiatočné heslá.



Obr. 5.25: Odhalenie WPA2 kľúča pomocou nástroja Aircrack-ng.

5.8 Zhodnotenie

V praktickej časti tejto bakalárskej práce boli prevedené vybrané útoky na jednotlivé smerovače zapojené v ethernetovej sieti a v bezdrôtovej sieti. Z každého útoku je na priloženom optickom médiu po jednej video ukážke. Na spustenie video ukážok je možné použiť priložený VLC media player [29]. Ako je uvedené v kapitole 5.1 boli použité dva súčastné smerovače určené pre stredne veľké firmy s rozsiahlejšou sieťovou infraštruktúrou a dva súčastné ADSL smerovače určené pre domáce pripojenie k Internetu, pričom práve tieto dva smerovče boli tiež použité pri útokoch v bezdrôtovej sieti.

V tabuľke 5.1, je zreteľne viditeľné, aké rozdiely boli medzi jednotlivými smerovačmi počas útokov. Najlepšie sa s útokom typu DoS vyrovnal smerovač Cisco 2821 CE a najhoršie smerovač D-Link DSL-2641R. Je to pochopiteľné z dôvodu, že úloha týchto smerovačov v sieti je vzájomne diametrálne odlišná a preto sa porovnávať nedajú. Porovnávať možno ale zariadenia, ktorých úloha v sieti je rovnaká, teda ADSL smerovače D-Link DSL-2641R a DrayTek Vigor 2700VG, a smerovače RouterBOARD 433 a Cisco 2821 CE.

Tabuľka 5.1: Vzájomné porovnanie použitých smerovačov.

Smerovač	DoS útok	brute-force útok
D-Link DSL-2641R	- nefunkčnosť zariadenia - po skončení útoku nutnosť reštartovať smerovač	- bez akejkoľvek možnosti zabezpečenia
DrayTek Vigor 2700VG	- nefunkčnosť zariadenia - implementovaná obrana proti DoS útokom nefunkčná - po skončení útoku opäť plne funkčný	- bez akejkoľvek možnosti zabezpečenia - možnosť zmeniť porty služieb (nie je účinné)
RouterBOARD 433	- minimálne zaťaženie	- možnosť nastavenia Firewallu pri určitom počte nekorektných prihlásení v pribehu určitého časového intervalu
Cisco 2821 CE	- žiadne zaťaženie	- primárna implementácia konfigurácie zabezpečenia prihlasovania

V porovnaní ADSL smerovačov jednoznačne ako lepší vyšiel smerovač Vigor 2700VG. Tento smerovač bol kráto po útoku, v priebehu pár sekúnd plne funkčný, ale smerovač DSL-2641R nebol schopný prevádzky a vyžadoval manuálny reštart. Útoku typu „brute-force“ neodolal ani jeden ADSL smerovač a ani jeden zo smerovačov neposkytoval možnosť obrany voči tomuto útoku. Tieto smerovače možno považovať hárdverovým výkonom za rovnocenné. Keďže ďalej tieto smerovače slúžili ako prístupové body v bezdrôtových sieťach a boli vystavené útokom založené na odpočúvaní paketov, možno ich porovnať aj z takéhoto hľadiska. V tabuľke 5.2 vidno, že smerovač Vigor 2700VG ponúka oproti smerovaču DSL-2641R navyše funkciu filtrovania MAC adries, ale inak oba smerovače ponúkajú štandardné funkcie a aj šifrovanie prostredníctvom WPA2 kľúča.

Tabuľka 5.2: Vzájomné porovnanie použitých bezdrôtových smerovačov.

Smerovač	skrytie SSID	filtracia MAC adries	WEP	WPA / WPA2
D-Link DSL-2641R	podporuje	nepodporuje	podporuje	podporuje
DrayTek Vigor 2700VG	podporuje	podporuje	podporuje	podporuje

V porovnaní ďalších dvoch smerovačov, RouterBOARD 433 a Cisco 2821 CE, lepšie vyšiel smerovač Cisco 2821 CE, ktorý pri DoS útoku nevykazoval mimo požadovanú činnosť, pričom RouterBOARD 433 vykazoval vyššiu odozvu, ktorá napríklad spôsobila výpadky pripojenej IP kamery. Voči útoku typu „brute-force“ oba smerovače ponúkli zabezpečenie s rozdielom, že v smerovači RouterBOARD 433 bolo potrebné zložitejšie nastavovanie zabezpečenia voči nežiadúcim pokusom o prihlásenie, narozdiel od smerovača Cisco 2821 CE, kde bolo toto zabezpečenie primárne implementované a do prevádzky sa dalo jednoduchým nastavením. Z tohto porovnania možno vyplýva to, že tieto smerovače sú na rovnkej úrovni, ale nie je to tak. Z globálneho pohľadu, ide ale o dva rôzne smerovače, pretože ich hárdverový výkon je diametrálne odlišný. Smerovač Cisco 2821 CE je viacej vhodný na náročnejšiu prevádzku než smerovač RouterBOARD 433.

6 ZÁVER

Riziko napadnutia počítačovej siete je v súčasnej dobe pomerne dosť veľké. Svedčí o tom všeobecne početné množstvo útokov, ktoré môžu byť realizované len jedným útočníkom s cieľom získania rozličných informácií či masou v podobe zneužitia určitého počtu nič netušiacich napadnutých strojov.

Bakalárska práca je zameraná na väčšinu všeobecne dostupných bezpečnostných mechanizmov, ktoré smerovač poskytuje voči napadnutiam siete. Ďalej je zameraná na vyhodnotenie kladných ale i negatívnych stránok, vybraných podrobnejšie spracovaných bezpečnostných techník, pretože každá z nich prináša svoje výhody či nevýhody. Pri akejkoľvek negatívnej vlastnosti daného mechanizmu je uvedené, akým spôsobom či akou formou útoku je možné toto negatívum zneužiť. Nesmieme však zabudnúť nato, že s príchodom novšej IPv6 niektoré staršie útoky strácajú na svojom význame a opodstatnenosti, pretože sú realizovateľné iba pod IPv4.

Smerovač môže slúžiť ako primárne, jediné bezpečnostné zariadenie s implementáciou rôznych doplňujúcich funkcií. Napríklad vďaka často krát základne implementovanej funkcii ACL, smerovač chráni sieť filtrovaním paketov, či vďaka technológii NAT chráni pred nežiaducim pohľadom na vnútornú schému adries. Pomocou rozširujúcich technológií, na smerovač môžeme preniesť napríklad funkciu primárneho Firewallu alebo pomocou CBAC dosiahneme stavovú inšpekciu paketov. Ak je smerovač súčasťou hĺbkovej ochrany môže napomáhať napríklad pri chránení kvality služieb QoS. Keďže smerovač má nepochybne významnú úlohu v zabezpečení počítačovej siete, musíme tiež klásť dôraz na bezpečnosť samotného smerovača. Môžeme tak zabrániť rozšíreniu informácií, ktoré by mohli byť zneužité napríklad ovládnutím zariadenia cudzou osobou.

Na základe výsledkov praktickej časti v kapitole 5.8, možno tvrdiť, že dnešné moderné smerovače, ktoré slúžia ako prístupové či centrálne zariadenia, na ktoré sú kladené vysoké nároky, dokážu odolať útokom typu DoS a taktiež útokom typu „brute-force“. Z pohľadu bezpečnosti smerovačov v bezdrôtových sieťach, možno tvrdiť, že s využitím všetkých dostupných mechanizmov, ktoré smerovače ponúkajú, sú smerovače pomerne bezpečné, ale zároveň je tu stále pomerne veľké množstvo prvkov, ktoré ponúkajú zneužitie.

Skutočná efektivita a využitie potenciálu smerovača ako bezpečnostného prvku siete spočíva v jeho samotnej konfigurácii, umiestnenia, využitia všetkých možných dostupných bezpečnostných prostriedkov a v neposlednom rade i spoluprácu s inými možnými bezpečnostnými technológiami. Iba dôkladne spravovaný a zodolnený smerovač sa môže stať základným prvkom v zabezpečení počítačovej siete. V otázke bezpečnosti smerovačov a aj ďalších aktívnych prvkov v počítačových sieťach, a to ethernetových či bezdrôtových, bude do budúcna vždy čo skúmať a vylepšovať.

LITERATÚRA

[1] *Aircrack-ng.org* [online]. 2009-2010 [cit. 20010-05-12]. Dostupné na internete: <http://aircrack-ng.org>.

[2] BARRETT, BYRNES, SILVERMAN. *SSH: The Secure Shell* [online]. 2001-2009 , 2008-10-01 [cit. 2009-11-30]. Dostupné na internete: <http://www.snailbook.com/faq/ssh-1-vs-2.auto.html>.

[3] *Cisco IOS Login Enhancements (Login Block)* [online]. August 2005, August 26, 2009 [cit. 2010-05-12]. Dostupné na internete:<http://www.cisco.com/en/US/docs/ios/sec_user_services/configuration/guide/sec_login_enhance.pdf>.

[4] *CISCO IOS SOFTWARE RELEASE 12.4 FEATURES AND HARDWARE* [online]. Júl 2006 [cit. 20010-05-12]. Dostupné na internete: <http://www.cisco.com/warp/public/cc/general/bulletin/software/general/2852_pp.pdf>.

[5] *Cisco Router Guide* [online]. 2007 [cit. 20010-05-12]. Dostupné na internete: <http://www.cisco.com/en/US/prod/collateral/routers/ps5855/prod_brochure0900aecd8019dc1f.pdf>.

[6] BOUŠKA P. *Cisco QoS 1 – úvod do Quality of Service a Diffserv* [online]. 2005 - 2009 [cit. 2009-11-01]. Dostupné na internete: <http://www.samuraj-cz.com/clanek/cisco-qos-1-uvod-do-quality-of-service-a-diffserv>.

[7] *Common Vulnerabilities and Exposures (CVE)* [online]. 1999 , December 01, 2009 [cit. 2009-11-25]. Dostupné na internete:<http://cve.mitre.org/>.

[8] DOSTÁLEK, L.; et al. *Velký průvodce protokoly TCP/IP: Bezpečnost.* 2. aktualiz. vyd. Praha : Computer Press, 2003. xvi, 571 s. ISBN 80-7226-849-X.

[9] ENDORF, C.; MELLANDER, J.; SCHULTZ, E. *Hacking - Detekce a prevence počítačového útoku.* Praha : Grada, 2005. 356 s. ISBN 80-247-1035-8.

[10] HANK, A. *Detekcia narušenia počítačovej siete.* Brno : FIT VUT v Brně, 2007. 43 s.

[11] *Internet byl napaden silou 40 Gbps* [online]. 13. 11. 2008 [cit. 2010-05-12]. Dostupné na internete: <http://www.root.cz/zpravicky/internet-byl-napaden-silou-40-gbps/>.

[12] *Katalóg zariadení - DSL WiFi router* [online]. [cit. 2010-05-12]. Dostupné na internete: <http://www.t-com.sk/Default.aspx?CatID=1438&Section=home&ktzcat=356&ktzid=817>.

[13] KURTZ, G.; MCCLURE, S.; SCAMBRAY, J. *Hacking bez záhad.* Praha : Computer Press, 2005. 592 s. ISBN 978-80-247-1502-5.

[14] LYON, G. *.Org - Nmap Free Security Scanner, Tools and Hacking resources* [online]. 2001-2009 , 2008-10-01 [cit. 2009-11-30]. Dostupné na internete: <http://insecure.org/>.

[15] MANDIA, K.; PROSISE, Ch. *Počítačový útok : Detekce, obrana a okamžitá náprava.* [Praha : Computer Press, 2002. xxii, 410 s. ISBN 80-7226-682-9.

[16] *Medusa Parallel Network Login Auditor* [online]. 2010 [cit. 20010-05-12]. Dostupné na internete: <http://www.foofus.net/jmk/medusa/medusa.html>.

[17] MOLNÁR, K. *Směrování v datových sítích (bez korekcí)* [online]. Brno : FEKT VUT v Brňe, 25.9.2006 [cit. 25.10.2009]. Dostupné na internete: <http://www.utko.feec.vutbr.cz /˜ molnar/bhws/ smerovani-nedokoncene.doc>.

[18] MOLNÁR, K. *Úvod do problematiky směrování* [online]. Brno : FEKT VUT v Brňe, 25.9.2006 [cit. 25.10.2009]. Dostupné na internete: <http://www.utko.feec.vutbr.cz/˜ molnar/bhws /P11.ppt>.

[19] MOLNÁR, K. *Vnitřní architektura směrovačů* [online]. Brno : FEKT VUT v Brňe, 25.9.2006 [cit. 25.10.2009]. Dostupné na internete: <http://www.utko.feec.vutbr.cz/˜ molnar/bhws/P12.ppt>.

[20] *Najväčší DDoS útok na svete so silou 17 Gbit/s smeroval na Slovensko* [online]. 14. 9. 2007 [cit. 2010-05-12]. Dostupné na internete: <http://www.zive.sk/spravy/najvacsi-ddos-utok-na-svete-so-silou-17-gbits-smeroval-na-slovensko/sc-30-a-273909/default.aspx> ISSN 1335-806X.

[21] *New DoS attack tool released (stream.c, raped.c, ACK)* [online]. 21. 1. 2000 [cit. 20010-05-12]. Dostupné na internete:<http://www.securiteam.com/unixfocus/5YP0I000DG.html>.

[22] NORTHCUTT, S.; et al. *Bezpečnost počítačových sítí : Kompletní průvodce návrhem, implementací a údržbou zabezpečené sítě.* Brno : Computer Press, 2005. 592 s. ISBN 80-251-0697-7.

[23] NORTHCUTT, S.; et al. *Inside Network Perimeter Security : The Definitive Guide to Firewalls, VPNs, Routers, and Intrusion Detection Systems.* Indianapolis : New Riders, 2003. 678 s. ISBN 0-7357-1232-8.

[24] PELKA, T. *Návrh, správa a bezpečnost počítačových sítí : Počítačová cvičení.* Brno : FEKT VUT v Brňe, 2008. 82 s.

[25] POSTEL, J. *RFC792 - Internet Control Message Protocol* [online]. September 1981 [cit. 2009-10-25]. Dostupné na internete: <http://www.faqs.org/rfcs/rfc792.html>.

[26] *RB433* [online]. cit. [2010-05-12]. Dostupné na internete:<http://www.routerboard.com/pricelist.php?showProduct=43>.

[27] SCHUDEL, G., SMITH, D.J. *Router Security Strategies : Securing IP Network Traffic Planes.* Indianapolis : Cisco Press, 2008. 650 s. ISBN 978-1-58705-336-8.

[28] THOMAS, T.M *Zabezpečení počítačových sítí : bez predchozích znalostí.* Brno : Computer Press, 2005. 344 s. ISBN 80-251-0417-6.

[29] *VLC media player* [online]. 2009-2010 [cit. 20010-05-12]. Dostupné na internete:<http://www.videolan.org/>.

[30] *Wi-Fi: Najväčší technologický skok posúva hranice - Živé.sk* [online]. 21. 9. 2009 [cit. 2009-11-30]. Dostupné na internete:<http://www.zive.sk/wi-fi-najvacsi-technologicky-skok-posuva-hranice/sr-1-sc-4-a-284450/default.aspx> ISSN 1335-806X.

[31] *Winping* [online]. [cit. 20010-05-12]. Dostupné na internete: <http://www.stahuj.centrum.cz/internet_a_site/monitoring_site/winping>.

[32] *Wireshark.org* [online]. 2009-2010 [cit. 20010-05-12]. Dostupné na internete:<https://www.wireshark.org>.

ZOZNAM SKRATIEK

ACK príznak paketu TCP s potvrdením prenosu

ACL Access Control List

ARP Address Resolution Protocol

BotNet sieť nezávislých počítačov topologicky a geograficky decentralizovaných

CBAC Context-Based Access Control

CRC Cyclic Redundancy Check

DHCP Dynamic Host Configuration Protocol

DiffServ Differentiated Services

DNS Domain Name Server

DSL Digital subscriber line

EAP Extensible Authentication Protocol

FFS Firewall Feature Set

FTP File Transfer Protocol

GRE Generic Routing Encapsulation

HTTP Hypertext Transfer Protocol

ICMP Internet Control Message Protocol

IDS Intrusion Detection System

IETF Internet Engineering Task Force

IP Internet Protocol

IPv4 Internet Protocol verzia 4

IPv6 Internet Protocol verzia 6

IPSec Internet Protocol Security

ISO International Organization for Standardization

LAN Local Area Network

LEAP Lightweight Extensible Authentication Protocol

LSA Link State Agreement

L2F Layer 2 Forwarding

L2TP Layer 2 Tunneling Protocol

MAC Media Access Control

MGCP Media Gateway Control Protocol

MSRPC Microsoft Remonte Procedure Call

NAT Network Address Translation

NBAR Network Based Application Recognition

NIC Network Interface Card

NTP Network Time Protocol

OSI Open System Interconnection Reference Model

OSPF Open Shortest Path First

PAT Port Address Translation

PKI Public Key Infrastructure

PPPoE Point-to-Point Protocol over Ethernet

PPTP Point-to-Point Tunneling Protocol

PSK Pre-Shared Key

QoS Quality of Service

RIP Routing Information Protocol

RTSP Real Time Streaming Protocol

SMTP Simple Mail Transfer Protocol

SNMP Simple Network Management Protocol

SSH Secure Shell

SSID Service Set Identifier

SYN príznak paketu TCP s výzvou k začiatku komunikácie

TCP Transmission Control Protocol

TLS Transport Layer Security

TTLS Tunneled Transport Layer Security

TFTP Trivial File Transfer Protocol

UDP User Datagram Protocol

VLAN Virtual Local Area Network

VPN Virtual Private Network

WAN Wide Area Network

WEP Wired Equivalent Privacy

Wi-Fi Wireless-Fidelity

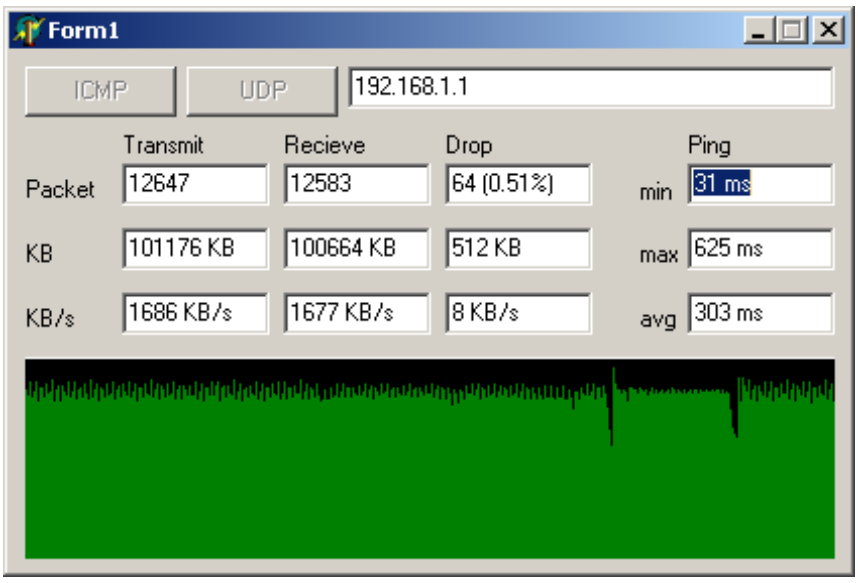
WLAN Wireless Local Area Network

WPA Wi-Fi Protected Access

ZOZNAM PRÍLOH

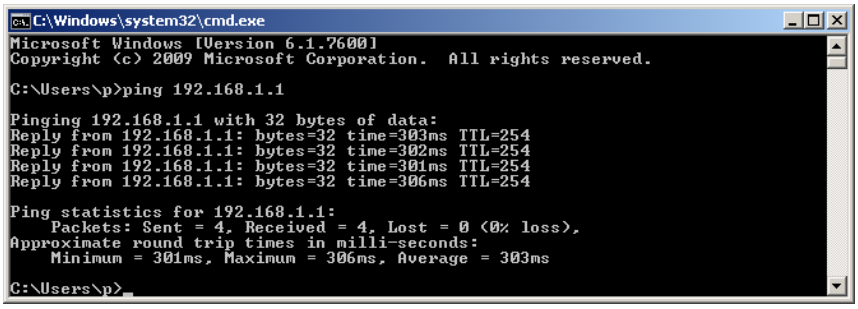
A PRVÁ PRÍLOHA

A.1 Ukážka programu NetTester



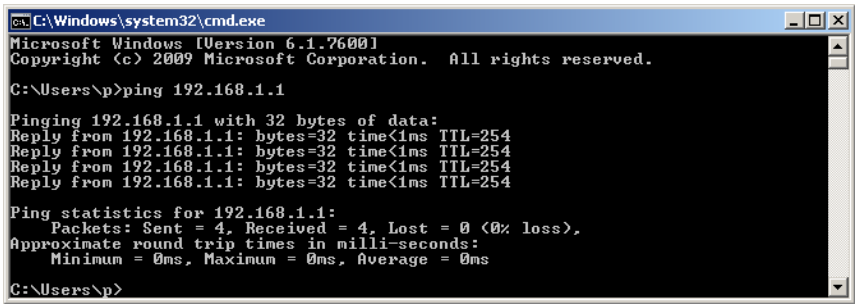
Obr. A.1: Posielanie veľkých ICMP paketov na smerovač s adresou 192.168.1.1 .

A.2 Odozva počas zaťaženia smerovača programom NetTester



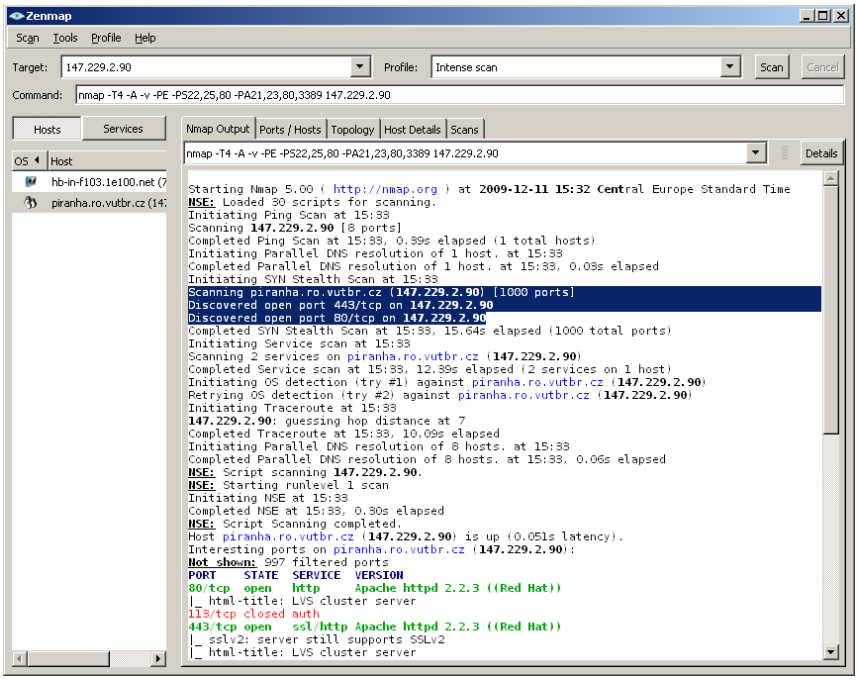
Obr. A.2: Odozva smerovača na požiadavok ping počas zaťaženia ICMP paketami.

A.3 Odozva bez zaťaženia smerovača



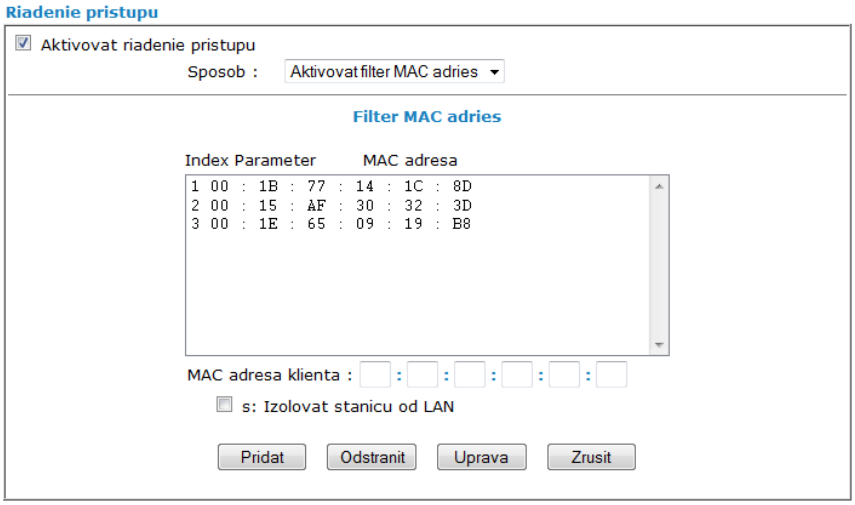
Obr. A.3: Odozva smerovača na požiadavok ping bez zaťaženia.

A.4 Ukážka program Zenmap



Obr. A.4: Vyhľadanie otvorených portov na adrese 147.229.2.90 .

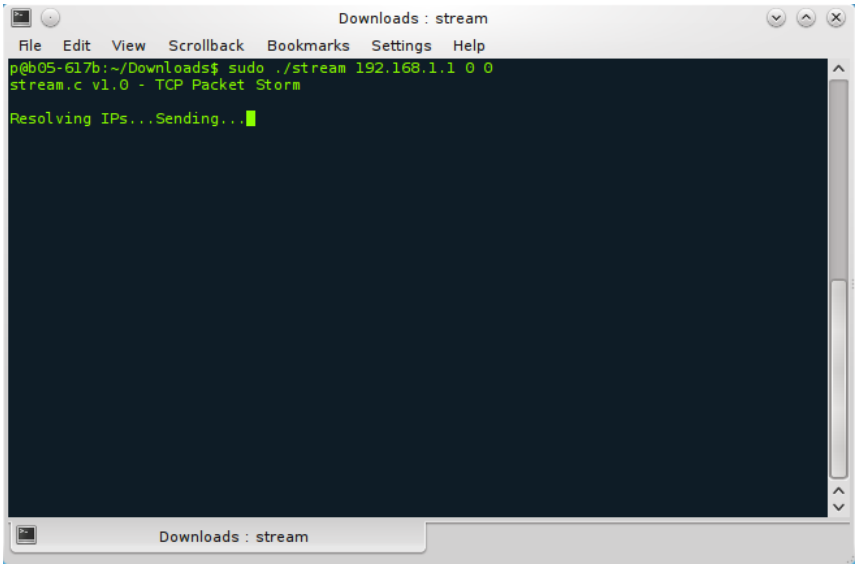
A.5 Ukážka riadenia prístupu pomocou MAC adresies



Obr. A.5: Riadenie prístupu do bezdrôtovej LAN pomocou filtrácie MAC adries v smerovači.

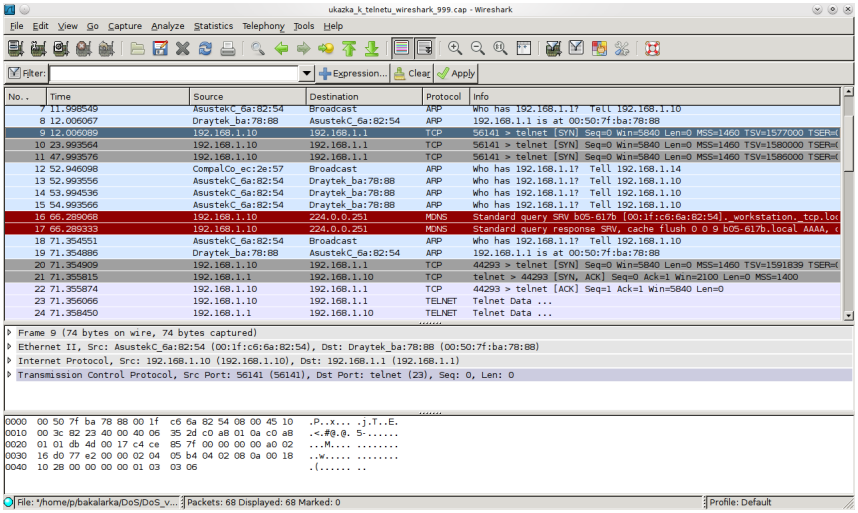
B DRUHÁ PRÍLOHA

B.1 DoS útok na smerovač D-Link DSL-2641R



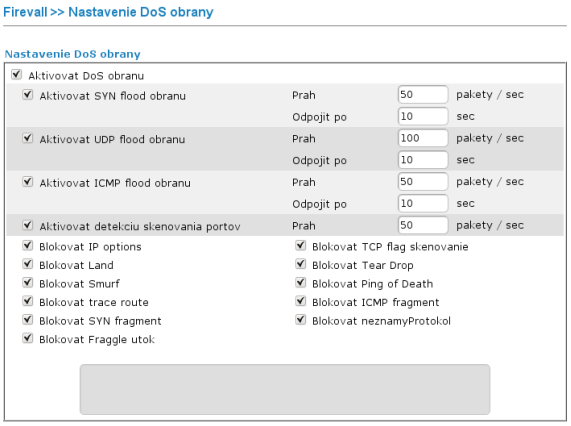
Obr. B.1: Spustenie exploitu stream.

B.2 Odpoveď smerovača Vigor 2700VG na požiadavku Telnet



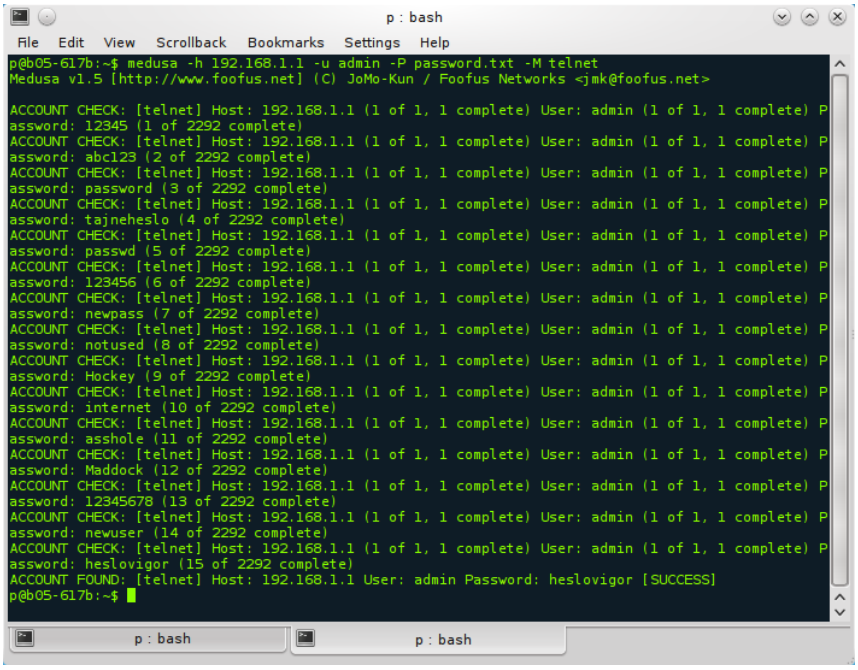
Obr. B.2: Neúspešný a úspešný pokus o pripojenie klienta k smerovaču.

B.3 Obrana smerovača Vigor 2700VG proti DoS útokom



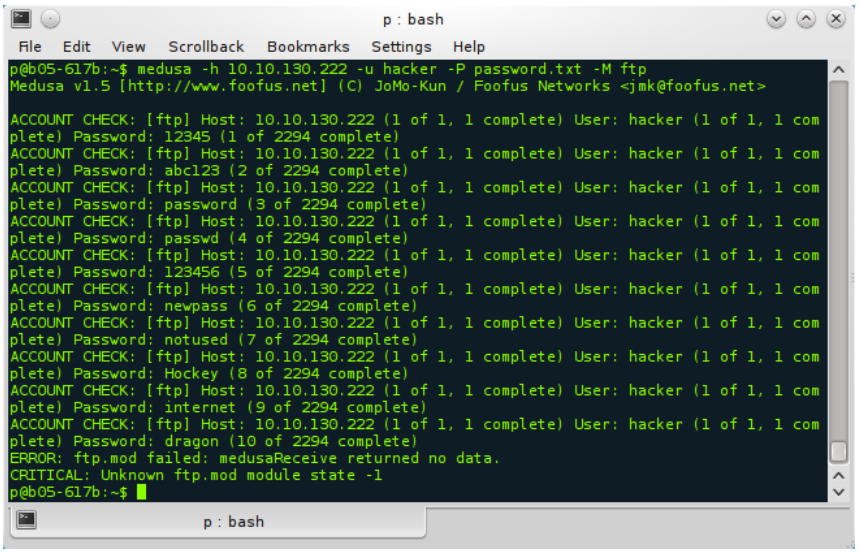
Obr. B.3: Zapnuté všetky možnosti obrany proti DoS útokom.

B.4 „Brute-force“ útok na smerovač Vigor 2700VG



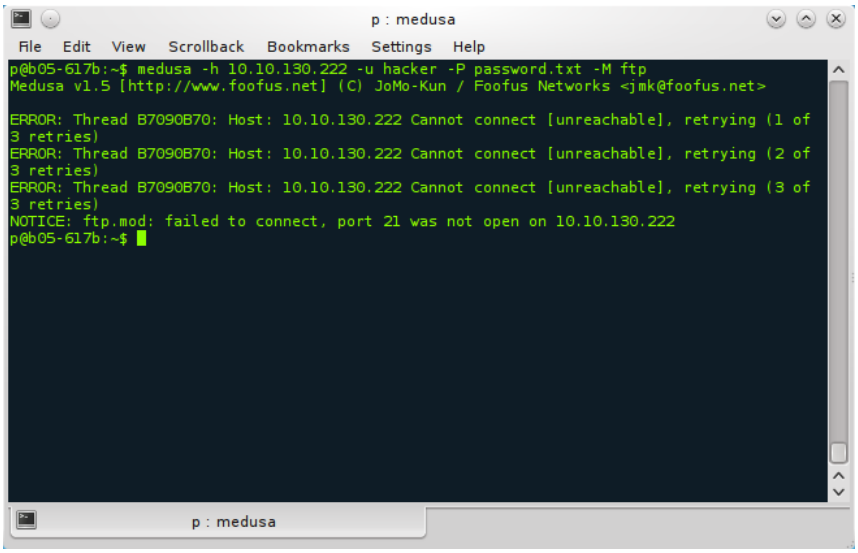
Obr. B.4: Odhalené prístupové heslo k smerovaču.

B.5 Neúspešný útok typu „brute-force“ na smerovač RB433



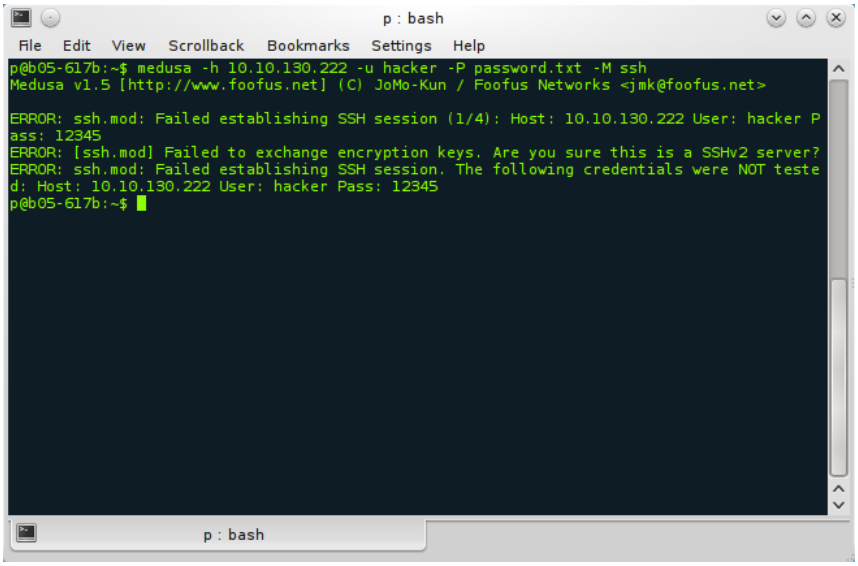
Obr. B.5: Zablokovanie prihlásenia po desiatich neúspešných pokusoch.

B.6 Zablokovaný útok typu „brute-force“ na smerovač RB433



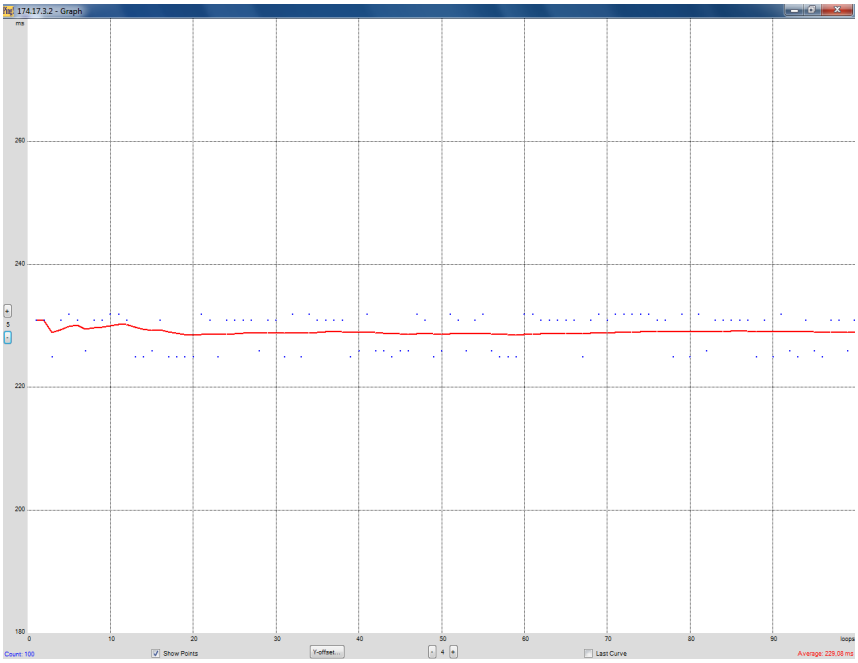
Obr. B.6: Nefunkčnost služby FTP po zablokovaní.

B.7 Pokus o útok „brute-force“ na smerovač RB433



Obr. B.7: Nefunkčnosť SSH spojenia.

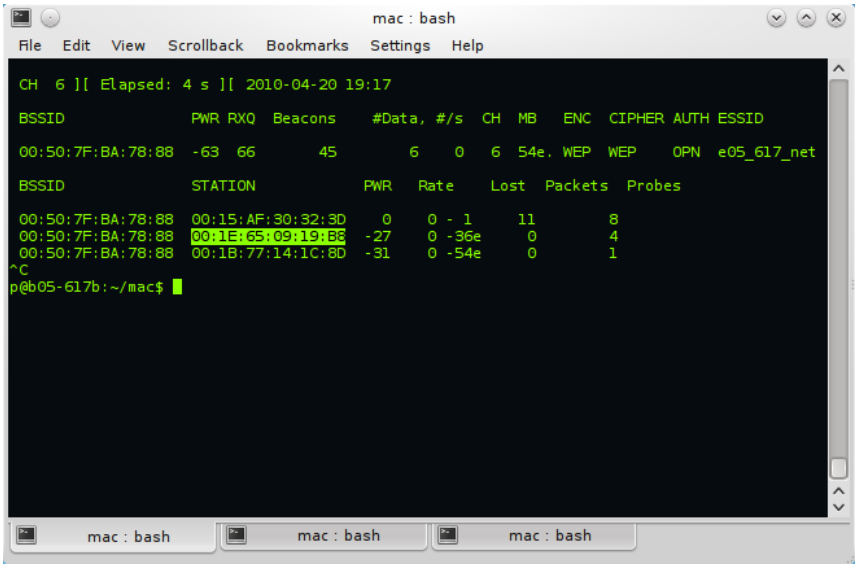
B.8 Odozva smerovača Cisco 2821 CE



Obr. B.8: Grafické znázornenie odozvy na žiadosť *ping*.

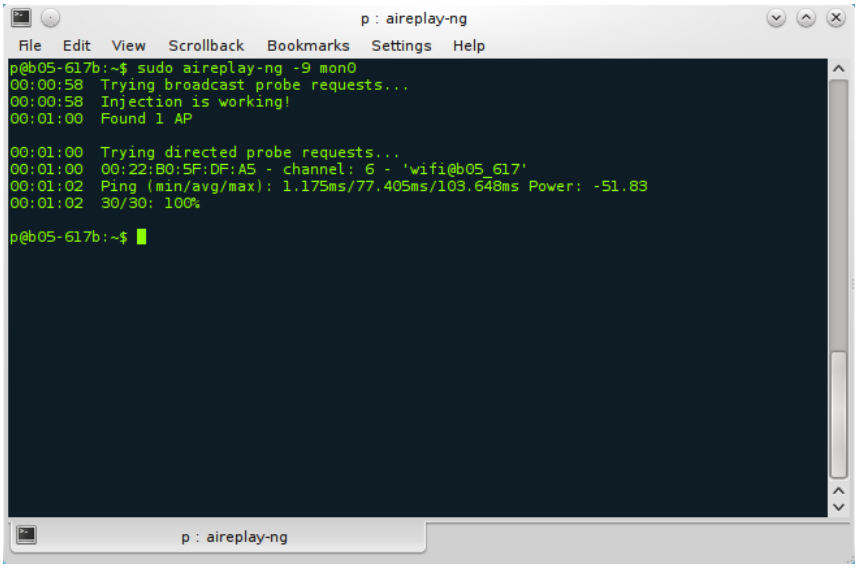
C TRETIA PRÍLOHA

C.1 Odchytávanie bezdrôtovej komunikácie



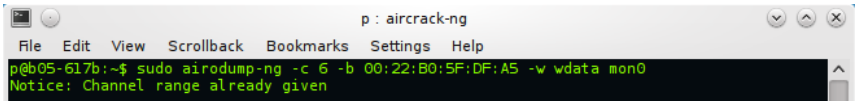
Obr. C.1: Pripojený klienti a ich MAC adresy.

C.2 Packet injection



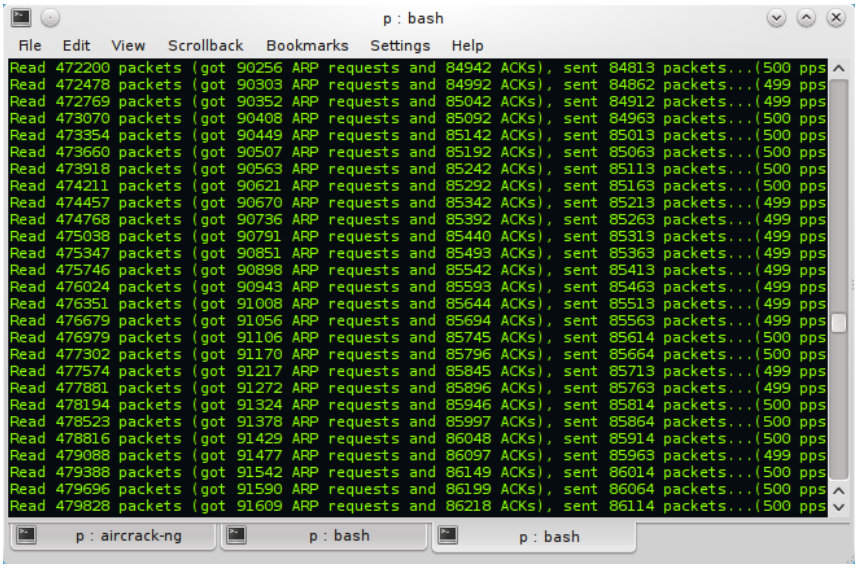
Obr. C.2: Overenie podpory *packet injection*

C.3 Spustenie odchytávania bezdrôtovej komunikácie



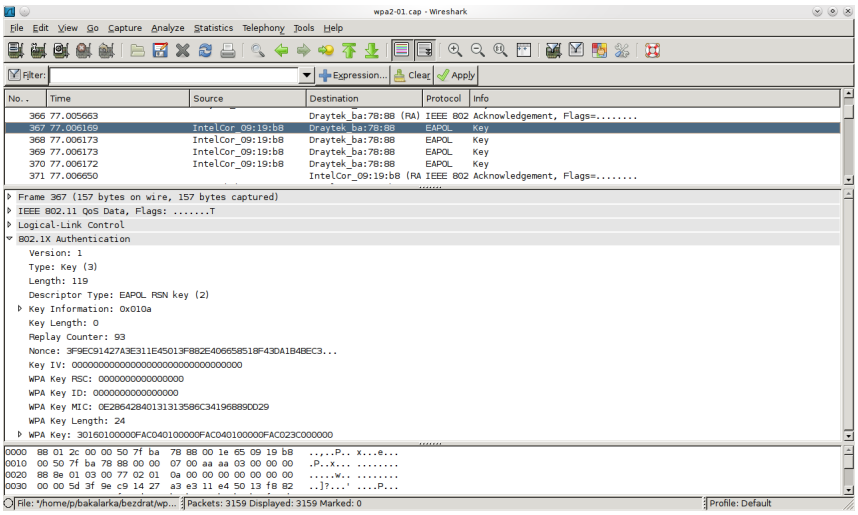
Obr. C.3: Príkaz airodump-ng s nadefinovanými parametrami.

C.4 Generovanie ARP paketov



Obr. C.4: Generovanie ARP paketov nástrojom aireplay-ng.

C.5 Štvrocestný handshake



Obr. C.5: Odchytenie štvrocestného handshaku vo Wiresharku.

D ŠTVRTÁ PRÍLOHA

D.1 Elektronická príloha - obsah CD

- bakalárska práca *bachelor_thesis_xbubel06* vo formáte .pdf
- zdrojové obrázky v priečinku *zdroje* vo formáte .svg
- použité obrázky a tabuľky v priečinku *obrázky* vo formáte .png
- použité prílohy v priečinku *prílohy* vo formáte .png
- súbory získané z jednotlivých útokov v priečinku *útoky*
- video ukážky z jednotlivých útokov v priečinku *video*
- inštalačný program VLC media player pre OS Windows v priečinku *video*
- použité softvérové vybavenie v priečinku *programy* s priloženým popisným súborom s názvom *README*