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

ZABEZPEČENÍ PODNIKOVÉ SÍTĚ TECHNOLOGIÍ IPS

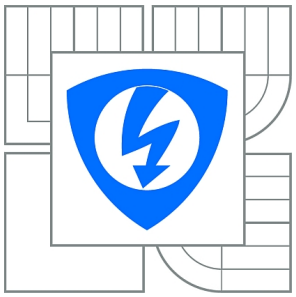
BAKALÁŘSKÁ PRÁCE
BACHELOR'S THESIS

AUTOR PRÁCE VOJTĚCH JAKAB
AUTHOR

BRNO 2012

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

ZABEZPEČENÍ PODNIKOVÉ SÍTĚ TECHNOLOGIÍ IPS

ENTERPRISE NETWORK IPS SECURITY

BAKALÁŘSKÁ PRÁCE

BACHELOR'S THESIS

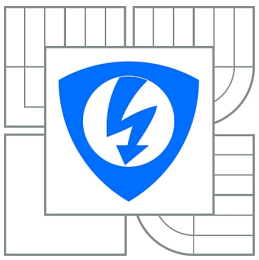
AUTOR PRÁCE — VOJTĚCH JAKAB

AUTHOR

VEDOUCÍ PRÁCE — Ing. VLADIMÍR ČERVENKA

SUPERVISOR

BRNO 2012



VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

Fakulta elektrotechniky a komunikačních technologií

Ústav telekomunikací

Bakalářská práce

bakalářský studijní obor
Teleinformatika

Student:	Vojtěch Jakab	***ID:***	125461
Ročník:	3	***Akademický rok:***	2011/2012

NÁZEV TÉMATU:

Zabezpečení podnikové sítě technologií IPS

POKYNY PRO VYPRACOVÁNÍ:

Cílem práce je zhodnotit současné možnosti útoků a zabezpečení firemní sítě. Detailně popsat technologii IPS a rozebrat její výhody. Pro dané bezpečnostní brány vypracovat návrh optimálního zabezpečení s využitím veškerých dostupných obranných mechanizmů, které budou testovány simulací vybraných útoků. Úspěšné průniky budou analyzovány, odůvodněny a doplněny o návrh dalších kroků pro omezení těchto hrozeb.

DOPORUČENÁ LITERATURA:

[1] KENNEDY, David. Metasploit : the penetration tester's guide. San Francisco, Calif : No Starch Press, 2011. s. ISBN 159327288X.
[2] WILKINS, Sean; SMITH, Franklin H. CCNP security secure 642-637 official cert guide. Indianapolis, IN : Cisco Press, 2011. s. ISBN 1587142805.
[3] BURNS, David, et al. CCNP Security IPS 642-627 official cert guide. Indianapolis, IN : Cisco Press, 2011. s. ISBN 1587142554.
[4] HUCABY, David, et al. CCNP Security Firewall 642-617 official cert guide. Indianapolis, IN : Cisco Press, 2011. s. ISBN 1587142791.

Termín zadání:	6.2.2012	***Termín odevzdání:***	31.5.2012

Vedoucí práce: Ing. Vladimír Červenka
Konzultanti bakalářské práce:

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

ABSTRAKT

Tato bakalářská práce se zabývá problematikou zabezpečení lokálních počítačových sítí LAN. Náplní práce je prozkoumat možnosti jejich zabezpečení a představení několika z mnoha možný útoků, které mohou tyto sítě ohrozit. Hlavním cílem ovšem je pokusit se navrhnout maximální zabezpečení testovací firemní sítě. K dispozici byl firewall od firmy Fortinet a směrovač od firmy CISCO. K zabezpečení jsou využity veškeré potřebné funkce, které nabízí jejich operační systémy. Pomocí příslušných nástrojů je prozkoumána konfigurace IPS na firewallu a případné možnosti jeho obcházení. V posledním kroku jsou provedeny konkrétní útoky na navrženou síť, jsou rozebrány a proti úspěšným útokům jsou navržena další opatření.

KLÍČOVÁ SLOVA

Bezpečnost, firewall, IPS, směrovač, LAN, útoky, ARP, poisoning, spoofing

ABSTRACT

This bachelor's thesis addresses the local area network security. The scope of this thesis is to explore the possibilities of security of these networks and introduction of some attacks which can threaten these networks. The main goal, however, is to design maximum security measures of testing network. CISCO router and Fortinet's firewall are available. Their configuration is limited by possibilities of their operating systems. By the appropriate programms the configuration of IPS configured on firewall is examined and they are used to try to evade this component. The last part of this work deals with executing particular network attacks. They are alaysed and agains successful attacks are proposed apropriate countermeasures.

KEYWORDS

Security, firewall, IPS, router, LAN, network attacks, ARP, poisoning, spoofing

JAKAB, Vojtěch *Zabezpečení podnikové sítě technologií IPS*: bakalářská práce. Brno: Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, Ústav telekomunikací, 2011. 68 s. Vedoucí práce byl Ing. Vladimír Červenka,

PROHLÁŠENÍ

Prohlašuji, že svou bakalářskou práci na téma „Zabezpečení podnikové sítě technologií IPS“ 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.

Brno ....

(podpis autora)

Rád bych poděkoval mému vedoucímu semestrální práce Ing. Vladimíru Červenkovi za odbornou a metodickou pomoc při tvorbě této bakalářské práce a za ochotu a velmi cenné rady při řešení dané problematiky. Dále také panu Ing. Zdeňku Homolkovi za zprostředkování a zapůjčení zařízení potřebných pro uskutečnění práce.

OBSAH

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

ÚVOD

Počítačové sítě jsou dnes již nedílnou součástí téměř všech větších či menších firem. Velmi usnadňují práci jejich zaměstnancům, ale je třeba také počítat s tím, že existuje plno způsobů, jak do sítě proniknout.

Pokud je bezpečnost sítě oslabena, může to mít za následek krádeže dat, hesel i ztrátu soukromí. Aby se tomuhle scénáři předešlo, je nutné sítě udržet chráněné. Takovýto krok je stále obtížnější, protože útoky na sítě se vyvíjí spolu s novými technologiemi a jsou čím dál více dokonalejší. Dochází k nekonečnému soupeření mezi hackery snažícími se proniknout do sítě a návrháři bezpečnostních systémů, které by měly tyto útoky zastavit.

Jelikož je důležité, aby sítě mohly mezi sebou navzájem komunikovat, je nutné poskytnout jistou otevřenost sítě, ale také dostatečně chránit důležitá data uvnitř [1]. Nejdůležitějším krokem je promyšlení efektivní bezpečnostní politiky firmy a následná implementace prvků ochrany [1].

Cílem této bakalářské práce je seznámení s firemními sítěmi a možnostmi jejich zabezpečení s použitím hardwarových bezpečnostních prvků jako firewall či IPS. Dalším záměrem práce je návrh dostačujícího zabezpečení sítě, představení možných útoků na firemní síť a zrealizováním vybraných útoků následně ověřit funkčnost bezpečnostních prvků a případně poukázat na slabá místa zabezpečení.

1 AKTIVNÍ PRVKY OCHRANY

1.1 Antivirový program

Pokud je počítač připojen k sítí internet, je antivirová ochrana téměř nezbytná. Antivirový program slouží k detekci, následnému odstranění elektronických virů a napravení souborů těmito viry poškozenými.

Tento program pracuje s různými metodami pro rozpoznávání škodlivých kódů. Mezi základní metody patří [2]:

- detekce na základě rozpoznání signatury - jde o porovnávání kódu daného programu se signaturami, obsahujícími část škodlivého kódu,
- heuristická analýza - virtuální spuštění programu a jeho analýza,
- detekce rootkit programů - na základě dvojího scanování systému.

1.1.1 Instalace antivirové ochrany

Aby ochrana proti virům byla co nejintenzivnější, je důležité vybrat místo, kam program nainstalovat. Instalace může být provedena na:

- koncové stanice,
- servery,
- vstupní brány.

Pokud se jedná o podnikovou síť bez přístupu na internet nebo k dalším externím sítím, není nutné instalovat antivirové programy na aktivní síťové prvky, jako jsou např. směrovače, či firewally. Vir se do takovéhle sítě může dostat pouze na přenosných zařízeních. Proto je dostačující antivir běžící pouze na koncových stanicích. Jedná se převážně o experimentální sítě.

Pro existenci většiny firem je téměř nezbytné připojení k internetu. Většina současných virů využívá ke svému šíření tří významných protokolů - HTTP, FTP, SMTP [2]. Z toho vyplývá potřeba instalace antivirové ochrany nejenom na konkrétní počítače, ale i na prvky, které oddělují síť od internetu. Antivir na vstupních branách síť chrání před viry, které mohou do sítě proniknout z internetu. V případě, že škodlivý program z důvodu nedostatečného výkonu zařízení projde do sítě, je vhodné chránit koncové stanice vlastní instancí antivirového programu.

1.2 Antispam

S rozšířením elektronické komunikace také roste nutnost kontrolovat příchozí poštu a filtrovat žádoucí zprávy od nežádoucích. Spamem se rozumí jakékoliv nevyžádaná

zpráva či sdělení především reklamního rázu [3]. Tato pošta je většinou posílána robotem z neexistujících e-mailových adres.

Částečnou obranu proti spamu by měly poskytnout antispamové filtry. Antispam musí kontrolovat jak příchozí, tak odchozí poštu. V případě odchozí pošty by měl být schopen detekovat zdroj nežádoucích zpráv a zablokovat ho. Výhodou je, že v tomto případě se spam nedostane ven z interní sítě [3].

Kontrolu příchozí pošty zajišťuje sada různých filtrů. Filtry pracují s databází slov, která se velmi často objevují ve zprávách spamu [3].

Další nedílnou součástí filtrů jsou tzv. černé listiny (DNS blacklist), což je seznam IP adres, o kterých se ví, že z nich chodí spam [3]. Pokud přijde zpráva z této domény, je okamžitě vyhodnocena jako spam.

1.3 Firewall

Firewallem rozumíme bezpečnostní bránu, která odděluje provoz mezi sítěmi, jež spolu komunikují[6]. Tedy např. lokální síť a internet. Firewall na základě předdefinovaných pravidel filtruje provoz jak do sítě, tak ven z ní. Respektive se povolí služby, které jsou nutné pro provoz, a ostatní se zakážou. Řešen může být buď hardwarově, softwarově, případně kombinací obou možností.

Firewally můžeme rozdělit do tří základních skupin[6]:

- paketový firewall,
- aplikační brána,
- stavový firewall (SMLI brána).

1.3.1 Paketový firewall

Jedná se o nejstarší a nejjednodušší formu ochrany [6]. Je charakterizována vysokou rychlostí, ovšem nízkou mírou zabezpečení. Paketový filtr funguje převážně na síťové vrstvě a většinou bývá implementovaný na směrovačích [6]. Kontroluje příchozí i odchozí pakety na základě údajů v hlavičce - zdrojová, cílová IP adresa a zdrojový, cílový port. Nedokáže však zapisovat do logu události, upozornit administrátora, ani nepovolí autentizaci na úrovni uživatele.

Paketové filtry je vhodné používat na vysokorychlostních linkách s přenosem velkého množství dat, např. páteřní linky [6]. Vhodné je zmíněnou ochranu také použít tam, kde není vyžadována velká přesnost kontroly dat a důkladná analýza [6]. Jedná se především o domácí sítě, a proto většina směrovačů určená pro domácí použití má tento firewall integrovaný.

Tab. 1.1: Výhody a nevýhody paketových firewallů

Paketové firewally	
výhody	nevýhody
- nízká cena - rychlé a nenáročné - integrované na většině routerů - transparentní pro uživatele	- nízký stupeň ochrany - snadná chyba při konfiguraci - nepodporují autentizaci

1.3.2 Aplikační brána

Takto řešené firewally jsou mnohem bezpečnější než paketové, ovšem také pomalejší[6]. Jsou omezeny pouze na určité služby, které kontrolují. Pokud situace vyžaduje přidání další služby, je zpravidla nutné napsat proxy aplikaci. Jedná se o aplikaci, která kontroluje veškeré pakety pro danou službu a pracuje jako „prostředník“ mezi uživatelem a serverem[6]. Když uživatel vznese požadavek na server, ten je nejprve zpracován právě proxy a až následně předán dál. Díky tomu je možné komunikaci monitorovat či blokovat. Jak již vyplývá z názvu, aplikační brány pracují na 7. vrstvě ISO-OSI modelu.

Tyto brány se využívají jen velmi zřídka. Poskytují sice velkou ochranu, ale vzhledem k jejich nedostatkům se dnes od jejich využívání ve větších firmách v dnešní době odstupuje a nahrazují se stavovými firewally[6].

Tab. 1.2: Výhody a nevýhody aplikačních bran

Aplikační brány	
výhody	nevýhody
- vysoký stupeň ochrany - logování uživatelských aktivit - umožňují autentizaci	- poměrně nákladné - vyžadují vysoký výkon firewallu - nutná konfigurace na každém koncovém počítači - nejsou pro koncového uživatele transparentní

1.3.3 Stavové firewally

Stavové firewally pracují na podobném principu jako paketové filtry. Jejich hlavní výhodou je, že jsou schopné ukládat si informace o spojeních, která byla již jednou povolena. Když přijde do firewallu paket, srovná se pouze se stavovou tabulkou, a pokud byla komunikace již jednou z tohoto směru povolena, je puštěn do sítě bez toho, aby se vykonávala sada nadefinovaných pravidel pro každý paket [7]. Z toho vyplývá, že se jedná o velmi rychlou kontrolu.

Nevýhoda tohoto filtrování tkví opět v nižší bezpečnosti v porovnání s aplikačními branami [7]. V rámci kompenzace zmíněného nedostatku se stavové firewally používají společně s technologií Intrusion Detection System (IDS), která je schopna detekovat útoky a nahlásit je firewallu [7].

Stavové firewally jsou ve velké míře využívány ve větších firmách, kde je kladen důraz jak na hloubkovou kontrolu dat, tak na relativně rychlé zpracování[8].

Tab. 1.3: Výhody a nevýhody stavových firewallů

Stavové firewally	
výhody	nevýhody
- vysoký stupeň ochrany - neomezují ani nezpomalují provoz na síti - transparentní pro koncového uživatele	- nutná odborná konfigurace - poměrně nákladné

1.4 Pokročilé metody prevence

Firewall představuje sice nutnou, ale dnes již ne zcela dostačující ochranu před útoky. Protože útoky často využívají chyby v určitých programech a maskují se jako povolený provoz, firewall je nedokáže odhalit. Je tedy nutné použít další prvky, které hrozbu na aplikační vrstvě zachytí a eliminují. Tento krok mají na starosti zařízení s implementovaným systémy Intrusion Detection System (IDS) a Intrusion Prevention System (IPS). Obě dvě technologie můžou být implementovány do hardwarového firewallu, řešeny softwarově, nebo mohou existovat jako samostatné hardwarové sondy [9]. Jedná se o prvky, na které je směrován veškerý síťový provoz a které mají za úkol detekovat útoky a zabránit jejich dopadu na cílové stanice.

1.5 Systémy detekce a prevence průniku

Dané systémy mohou být realizovány jak softwarově, tak hardwarově. Jedná se o systémy, jejichž cílem je detekovat nežádoucí činnost na síti a následně ji blokovat. Všeobecně platí, že nežádoucí aktivity je vhodnější přímo blokovat. Toto je klíčová vlastnost všech zařízení IPS, které by měly být implementovány v každé firemní síti obsahující důvěrná data.

1.5.1 Architektura

Architektura je jedním z nejkritičtějších aspektů v prevenci proti narušení [9]. Nejvýhodnější je ta, kdy každá entita vykonává svou činnost a vykonává ji efektivně. Členění na různé skupiny se děje především v závislosti na komunikaci entit a jejich činností [9].

Jednovrstvá architektura

Jedná se o nejzákladnější a nejjednodušší architekturu [9]. Každý prvek tohoto řešení provádí sběr a vyhodnocování dat samostatně. Jednotlivá nasbíraná data nejsou tedy přeposílána dalším skupinám komponent a vyhodnocování provozu probíhá bez jakékoliv další komunikace s další komponentou viz obr. 1.1. Tato architektura se využívá především u systémů detekce a průniku realizovanými softwarově [9].

Obr. 1.1: Schéma jednovrstvé architektury

Jejímu použití nahrává nízká cena řešení a jeho jednoduchost. Ovšem bez možnosti komunikace s dalšími komponenty a prvky sítě se přichází o výhody komplexnějšího řešení bezpečnostních problémů [9]. V současnosti se od tohoto řešení ustupuje a nahrazuje ho vícevrstvá architektura [9].

Vícevrstvá architektura

Vícevrstevná architektura (orb. 1.2) obsahuje entity, které mezi sebou mohou komunikovat, předávat si potřebná data a následně je vyhodnocovat (1.2). Mezi základní prvky patří:

- senzory,
- agenti neboli analyzátory,
- manažeři.

Senzory

Senzory sbírají data. Jedná se o sběr buď na aktivních síťových prvcích, nebo mohou být realizovány programem, který zachytí veškerý provoz na daném síťovém rozhraní počítače [9]. Pracují převážně na čtvrté vrstvě modelu ISO-OSI.

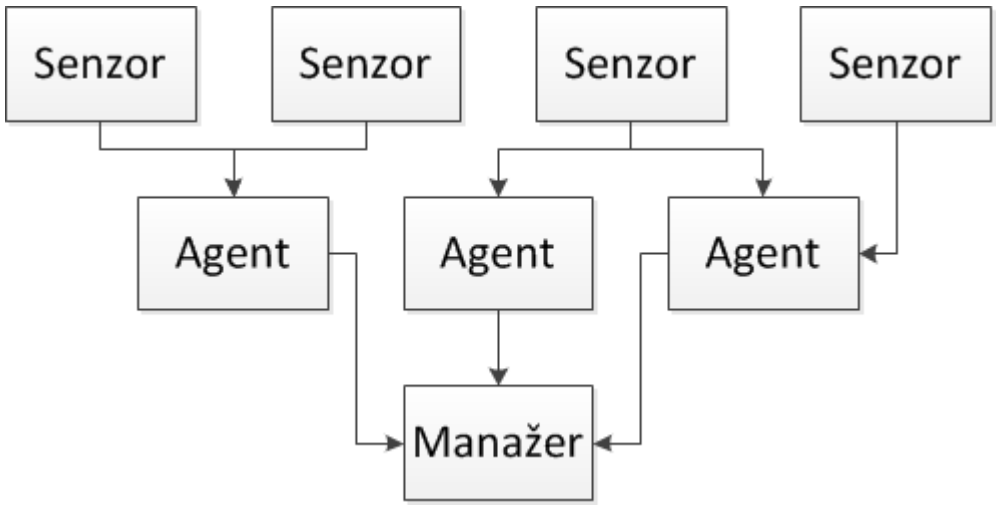
Agenti

Přijímají data od senzorů a jejich činností je monitorování aktivity nežádoucích uživatelů [9]. Zpravidla platí, že každý agent provádí pouze jednu činnost (kontrola UDP provozu, kontrola HTTP požadavků atd.).

Manažeři

V případě nežádoucí aktivity vyšle agent zprávu manažerovi, který na základě rizika a předchozího nastavení může provést určité opatření [9]. Jedná se především o:

- výpis varování na konzoli,
- zápis do databáze,
- zaslání informací směrovači nebo firewallu, z důvodu změny přístupových pravidel,
- poskytnutí rozhraní k řízení manažerské komponenty.



Obr. 1.2: Schéma jednovrstvé architektury

Vícevrstvá architektura je převážně stromovitého charakteru viz obr. 1.2. Základ tvoří senzory. Pro jejich správnou činnost je zapotřebí zvolit vhodné rozmístění v rámci kontrolované sítě [9]. V případě podezřelého chování sítě předají senzory nashromážděná data vyšší vrstvě, která je tvořena agenty. Nejvyšší vrstvu tvoří

komponenta manažera, která na základě informací obdržených od agentů a provede vhodné opatření.

Výhody vícevrstvé architektury zahrnují mnohem větší účinnost a hloubku analýzy [9]. Toho je dosaženo tak, že každá entita provádí pouze svoji předem definovanou činnost. Díky vhodnému rozmístění senzorů je možné vytvořit komplexní obraz bezpečnostních podmínek na jednotlivých uzlech sítě. Nevýhodou jsou náklady potřebné na vytvoření tohoto druhu architektury [9].

Peer-to-Peer architektura

Architektura využívá komunikace „rovný s rovným“. Komunikují mezi sebou tedy dvě rovnocenné entity, které analyzují provoz, každá svými vlastními prostředky (obr. 1.3) [9]. Neexistuje tedy žádný nadřazený řídící prvek. V praxi se jedná převážně o spolupracující firewally, na které mohou být následně vázány směrovače či přepínače. Detekované nebezpečí způsobí předání dat a instrukcí komponentě, která chrání určitou část sítě, na niž byl potencionální útok směrován [9].

Obr. 1.3: Schéma architektury Peer-to-Peer

Mezi výhody tohoto řešení patří jednoduchost a vyšší míra ochrany než u jednovrstvého modelu [9]. Ovšem k správné činnosti jsou zapotřebí vzájemně spolupracující prvky (firewally, směrovače).

1.5.2 Analýza

Analýza probíhá na základě rozboru dat, které zachytily jednotlivé senzory umístěné v síti. Jedná se o data, u nichž je podezření, že obsahují nežádoucí pakety. Na základě těchto informací systémy mohou vygenerovat čtyři základní zprávy [5]:

- **True positive** - Nezávadné pakety jsou pouštěny do sítě (1. požadovaný stav).
- **False positive** - IPS vyhodnotí škodlivé pakety jako nezávadné a pustí je do sítě. K tomu dojde, když pravidla pro rozpoznávání signatur jsou příliš obecná.
- **True negative** - Škodlivé pakety jsou správně odfiltrovány a nedostanou se do sítě (2. požadovaný stav).
- **False negative** - Nezávadné pakety jsou vyhodnoceny jako škodlivé, a nejsou tedy puštěny do sítě. Tohle mají za následek příliš striktní pravidla pro rozpoznávání signatur.

Podle typu prováděné analýzy se systémy dělí na systémy provádějící detekci [10]:

- na základě rozpoznání signatury,
- na základě nastavených pravidel,
- na základě rozpoznání anomálie,
- za využití Honeypot.

Detekce na základě rozpoznání signatury

Zařízení pracující se signaturami jsou velmi přesná a jejich začlenění do sítě není obtížné [10]. Metoda rozpoznání nežádoucí činnosti spočívá v porovnávání struktury paketů s databází známých útoků. V případě, že paket obsahuje vzor konkrétního útoku, je označen za škodlivý a následuje příslušná vygenerována zpráva.

Pakety se převážně označují za podezřelé v případě, že jsou přidružené k určité službě nebo určeny pro konkrétní port [10]. Toto opatření přispívá ke zrychlení činnosti systému. Není tedy nutno kontrolovat veškerý provoz. Ovšem dochází také k propouštění paketů, které nejsou určeny pro známé porty [10].

Výhodou této metody analýzy je vysoká rychlost, přesnost kontroly a jednoduché začlenění do sítě [10]. Problém nastane tehdy, pokud není databáze signatur udržována aktualizovaná. V případě, že systém není nakonfigurován na požadavky sítě, zařízení generuje větší množství false positive zpráv [10].

Detekce na základě pravidel

V těchto systémech musí být senzory zařízení nakonfigurovány podle konkrétních požadavků dané sítě [10]. Jakýkoliv provoz, který neodpovídá těmto pravidlům, bude generovat poplašné zprávy, případně bude blokován.

Algoritmus k rozpoznání signatury pracuje na základě statistického vyhodnocování toku dat [10]. Poplašná zpráva je generována tehdy, když je překročena nastavená prahová hodnota, např. požadavků o TCP spojení.

Nevýhoda tohoto řešení spočívá v nutnosti znát podrobné požadavky na síťový provoz a v důkladném odladění konfigurace senzorů [10]. V opačném případě budou zařízení hlásit velké množství zpráv false positive a blokovat legitimní provoz.

Detekce na základě rozpoznání anomálie

Jedná se o systémy, které kontrolují běžný provoz a v případě, že je zachycen datový tok, který vybočuje z nadefinovaného chování sítě (nesprávné využití protokolu, chybná segmentace paketů atd.), vygenerují opět poplašnou zprávu [10].

Klíčem je tedy definování standardního chování sítě. Definice lze provést několika způsoby [10]:

- vlastním definováním legitimního provozu,

- výrobcem definovaného legitimního provozu,
- vlastním vyhodnocením legitimního provozu na základě dlouhodobějšího pozorování.

Největší problém představuje poslední metoda. Po začlenění senzoru do sítě je síť i nadále nechráněna z důvodu právě dlouhodobého pozorování [10]. Pokud proběhne konkrétní útok v této době, zařízení jej přiřadí k povolenému provozu. Nedokáže jej dále samovolně rozpoznat.

Využití Honeypot

Honeypot systémy využívají ke své činnosti speciální server obsahující bezpečnostní trhliny, jehož cílem je odvrátit útočníka od síťových prvků, které obsahují důvěrná data [10]. V případě nebezpečí, je možno provést analýzu, aktualizovat databázi signatur a také rozpoznat nové modifikace již známých útoků.

Tab. 1.4: Porovnání jednotlivých analýz

	Výhody	Nevýhody
Signatury	- jednoduchá konfigurace - méně false positive reakcí	- Nemožnost detekovat neznámé signatury - nutnost udržovat databázi signatur aktualizovanou
Pravidla	- jednoduché a spolehlívé - možnost vlastní konfigurace - detekce neznámých útoků	- vyžadována znalost provozu sítě - důkladné odladění konfigurace
Anomálie	- jednoduchá implementace - detekce neznámých útoků	- nutná definice standartního provozu
Honeypot	- odvrácení útočníka od skutečného cíle - získání informací o útoku	- vyžadován nedůvěryhodný server

1.6 Intrusion Prevention Sysem - IPS

Systém IPS vychází ze staršího IDS. Hlavní nedostatkem IDS je již zmíněná neschopnost blokovat probíhající útoky. Z toho důvodu byla vyvinuta zařízení IPS. Jedná se o aktivní prvek sítě, který využívá ke kontrole provozu stejné metody jako IDS, avšak v případě odhalení nežádoucí činnosti má možnost ji blokovat. Kontrola

provozu probíhá v reálném čase, a systém musí mít tedy dostatečnou propustnost, aby nedocházelo k nežádoucímu zpoždění.

1.6.1 Požadavky na IPS

K důkladné kontrole provozu by měly být dodrženy následující požadavky. V opačném případě by mohlo dojít ke zpoždění, případně k selhání zařízení a úspěšnému průniku do sítě [11].

- Analýza v reálném čase - pouze v případě, že systém pracuje v reálném čase, je možné zachytit veškeré nežádoucí pakety a blokovat podezřelý provoz.
- Spolehlivost a dostupnost - je důležité pokusit se minimalizovat selhání systému, v opačném případě zůstane síť nechráněná a význam zařízení v síti je minimální. Systém také musí zůstat v činnosti i při aktualizaci databáze signatur a po jejím úspěšném dokončení by neměl být vyžadován restart.
- Pružnost - pokud již dojde k výpadku systému, je nutné provoz přesměrovat na další aktivní prvek, který by měl být schopen zajistit aspoň částečnou ochranu.
- Malé zpoždění - systém IPS by měl pracovat dostatečně rychle, aby zvládal analyzovat veškerý provoz v reálném čase. Zpoždění IPS by mělo přibližně odpovídat zpoždění které nastává na směrovačích či přepínačích.
- Vysoký výkon - rychlost zařízení by měla být dostatečná, aby bylo možné s rezervou kontrolovat veškerý provoz na síti i při značném vytížení linky.
- Přesnost detekce - Systém prevence by měl generovat co nejmenší počet false positive poplachů. K tomu dochází např. v důsledku neaktualizované databáze signatur. Chybějící signatury by měly být doplňovány s dostatečnou rychlostí a bez nutnosti restartovat senzor, případně celé zařízení.
- Různorodá kontrola - systém by měl být schopen rozeznat, zdali se podezřelý provoz týká již konkrétního útoku, porušení pravidel nebo chyby na úrovni uživatele.
- Schopnost upozornění - v případě detekce nebezpečného provozu musí být zařízení schopno včas a důkladně informovat pověřenou osobu (výpis do konzole, uložení záznamu do databáze atd.)

1.6.2 Rozdělení IPS

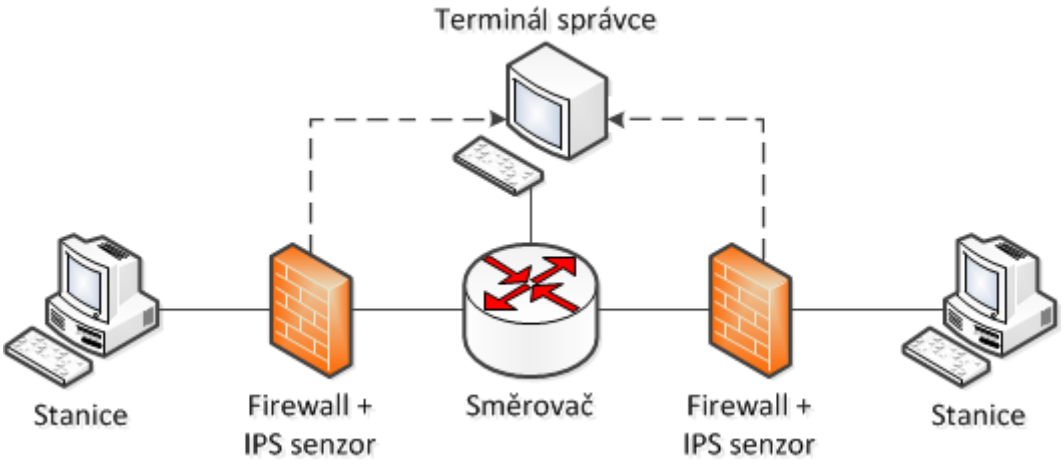
Podle typu zařízení a umístění senzorů v rámci sítě se systémy klasifikují do tři základních skupin[11] [12]:

- Network-based Intrusion Prevention System - NIPS,
- Host-based Intrusion Prevention System - HIPS,
- Wireless-based Intrusion Prevention System - WIPS.

Network-based Intrusion Prevention System

Síťově orientovaný IPS zahrnuje rozmístění monitorovacích zařízení na potřebných místech, za účelem vytvoření komplexního obrazu dění na síti, bez ohledu na pozici cíle útoku (obr 1.4)[11]. Převážně se jedná o zařízení kombinující schopnosti standardního IPS a firewallu. Operační systém, na kterém je spuštěn IPS, je ochuzen o veškeré nepotřebné služby a hardwarové vybavení obsahuje pouze tři základní komponenty[12]:

- minimálně 2 síťové rozhraní,
- procesor,
- paměť.



Obr. 1.4: Zjednodušené schéma umístění NIPS

Síťově orientovaný monitorovací systém je schopen jednoduše zaznamenat i útoky, které probíhají na jiném segmentu sítě, než na kterém je umístěná sonda[12]. Jelikož probíhá analýza provozu na samostatném prvku, není nutné aby NIPS obsahovalo operační systém kompatibilní se systémem na koncových stanicích.

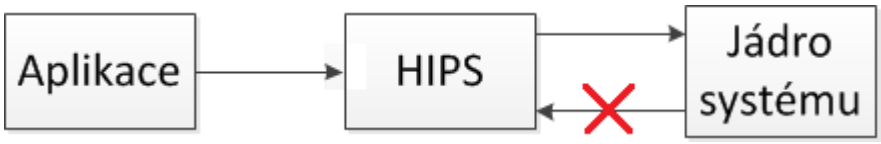
Nedostatky jsou patrny při kontrole šifrovaného provozu. Šifrovaný datový tok je pro NIPS zařízení průhledný a nelze jej vyhodnotit[12]. Tento nedostatek lze však efektivně vyřešit implementováním HIPS na koncové stanice.

Při začlenění NIPS do větší sítě nemusí být systém schopen kontrolovat veškerý provoz. V tomto případě je vyžadováno další obdobné zařízení.

Host-based Intrusion Prevention Sysem

Systémy mají své senzory i agenty umístěny přímo na koncové stanici. Výraznou výhodou takto realizovaného řešení je možnost komunikace přímo s jádrem systému (viz obr 1.5)[10]. HIPS využívá pravidla ke kontrole operačního systému a činnosti

na síťovém rozhraní stanice či serveru. V případě zaznamenaného nebezpečí jsou zakázány adekvátní služby a dochází k úpravě registrů za účelem řízení síťového provozu. To má za následek, že při probíhajícím útoku nemůže stanice navazovat např. FTP spojení, případně se ani na útoku podílet.



Obr. 1.5: komunikace s jádrem operačního systému

Značnou výhodou HIPS je kontrola šifrované komunikace[12]. Není analyzována přímo šifrovaná komunikace, ale díky svázání s jádrem k ní má systém přístup v místě, kde šifrována není. To zaručuje mnohem větší míru bezpečnosti a nahrává k umístění HIPS také na servery, ke kterým je třeba přistupovat pomocí zabezpečeného protokolu.

Hlavní nedostatek HIPS tvoří neschopnost vytvořit komplexní obraz o stavu celé sítě[10]. Jelikož pracuje pouze lokálně na stanici, není možno v případě nutnosti koordinovat činnost s dalšími systémy. Aby byla umožněna komunikace mezi jádrem operačního systému u HIPS, je důležité dbát na vzájemnou kompatibilitu.

Wireless-based Intrusion Prevention Sysem

Jedná se o přístupové body, do nichž je integrovaný systém prevence průniku[14]. K jejich nadstandardní činnosti patří rozpoznání neoprávněných WLAN sítí a bezdrátových zařízení. Dále jsou schopny odhalit bezpečnostní trhliny ve WLAN sítích.

Bezdrátové zařízení se skládá ze čtyř základních entit:

- bezdrátový senzor - monitoruje a analyzuje provoz,
- server obsahující manažera - přijímá data od senzoru a provádí důkladnou analýzu,
- server s databázemi - tvoří databáze všech vygenerovaných zpráv od senzoru nebo manažera,
- konzole - konfigurační rozhraní.

Jelikož se pásmo jednotlivých bezdrátových technologií dělí na kanály a k přístupu do sítě lze využít jakýchkoliv z nich, je žádoucí, aby WIPS zařízení byla schopná kontrolovat provoz na všech kanálech[13]. Senzory jsou limitovány vždy pouze na jeden konkrétní kanál[13]. Tento nedostatek řeší metoda „channel scanning“ sledující provoz na jednotlivých kanálech několikrát za vteřinu. K rozšíření

této metody je vhodné využít senzory, které obsahují více radiových modulů a jsou schopny analyzovat provoz na více kanálech současně[13].

Zařízení wireless IPS pracují ve dvou režimech. První tvoří přístupový bod, druhý je systém prevence[14]. Mezi těmito dvěma režimy zařízení přepíná. Je tedy zřejmé, že zařízení v případě, kdy se nachází v režimu přístupového bodu, není schopné poskytnout dostatečnou ochranu[14]. Problém nastává při moderních útocích, které jsou schopny tyto intervaly využít.

Tab. 1.5: Porovnání NIPS, HIPS, WIPS

	Výhody	Nevýhody
NIPS	- komplexní obraz o dění na síti - transparentní pro ostatní síťové prvky - nezávislé na OS jiných zařízení	- vysoká cena - neumožnuje analyzovat šifrovaný provoz
HIPS	- umožňuje analyzovat šifrovaný síťový provoz - úzké spojení s jádrem operačního systému - umožnuje kontrolu všech aplikací	- vyžaduje kompatibilitu s OS koncové stanice - nutná instalace na všech koncových stanicích
WIPS	- podpora standardů 802.11	- nízká míra ochrany - neumožňuje kontrolovat více kanálů současně

1.6.3 Možnosti IPS

Na základě nadefinovaných pravidel můžou IPS systémy při odhalení škodlivých dat provést jedny z následujících protiopatření [10]:

- Blokování útočníka v reálném čase - děje se tak na základě IP adresy stanice, ze které je útok prováděn. V případě správného rozpoznání útoku je daná IP adresa zařazena do databáze zakázaných adres a zařízení z ní nadále blokuje veškerý provoz. Z důvodu false positive zpráv je využit časovač, po jehož vypršení se záznam z databáze vymaže a zařízení je znovu povolen přístup do sítě.
- Blokování spojení v reálném čase - nastane blokování všech paketů z konkrétního TCP spojení.
- Zahození paketů v reálném čase.
- Logování podezřelých paketů.
- Generování poplašných zpráv.

- Zaslání požadavku o blokaci konkrétní linky nebo stanice.
- Vynucení restartu TCP spojení.

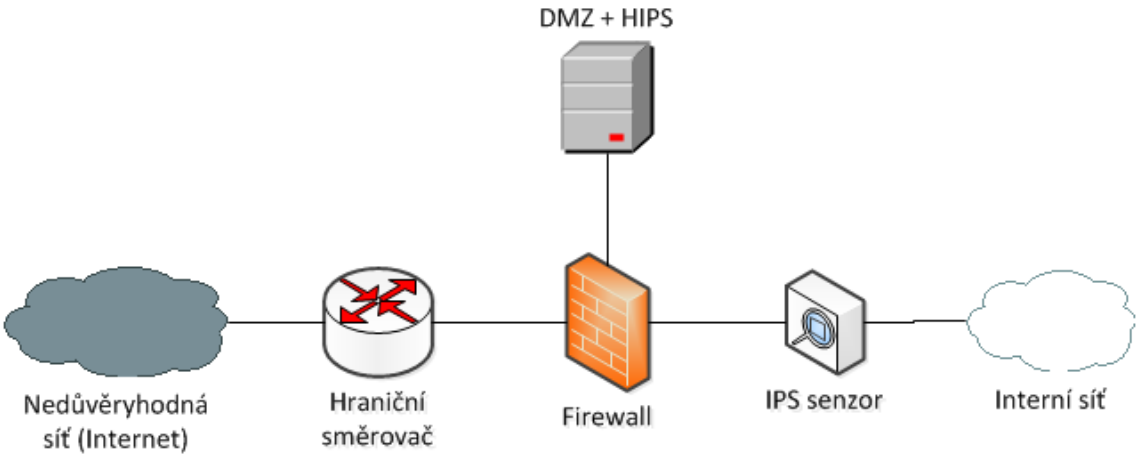
1.6.4 Umístění IPS

Pro maximální míru zabezpečení sítě je nutné zvolit správný druh IPS zařízení a vhodně jej umístit. Ve většině firemních sítí existují tzv. zúžená místa, která představují vhodný prostor pro implementaci síťově orientovaných IPS.[15] Jedná se např. o linku mezi směrovačem představujícím bránu do internetu a hlavním firewallem.

V případě, že infrastruktura firemní sítě obsahuje farmu serverů - místo, pro potencionální útok, za účelem získání důvěrných dat, je vhodné tyto servery chránit pomocí host-based IPS, která poskytují větší míru zabezpečení a jsou schopna pracovat i na aplikační vrstvě modelu ISO-OSI.

Umístění za firewall

Typické zúžené místo představuje právě linka mezi hraničním směrovačem a firewallem [15]. V případě, umístění IPS zařízení za firewall (viz obr. 1.6). již firewall



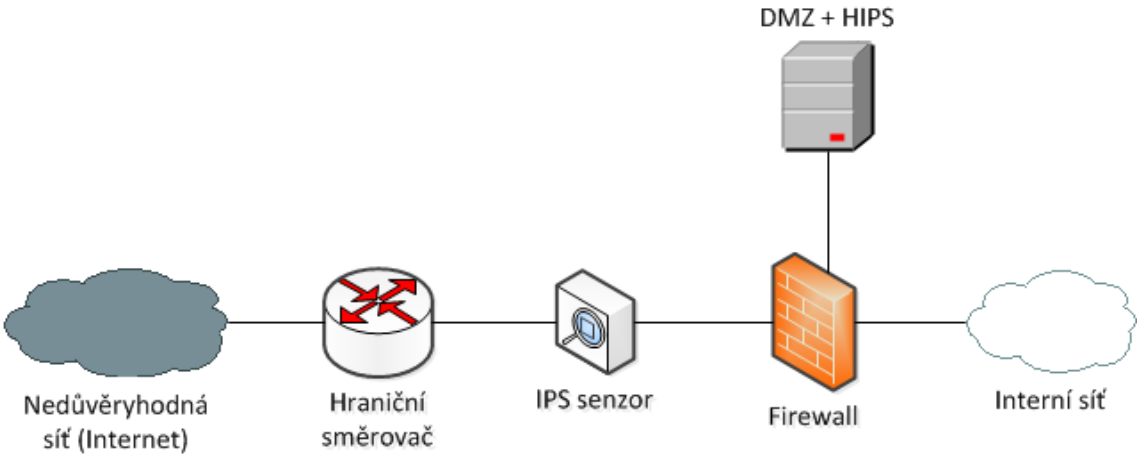
Obr. 1.6: Umístění IPS zařízení za firewall

blokuje určitý nežádoucí provoz a analýza datového toku je mnohem účinnější, neboť IPS zařízení nemusí analyzovat veškerý tok přicházející z nedůvěryhodné sítě.

Hlavní nevýhodou takto realizovaného řešení je neschopnost kontrolovat provoz směrovaný do demilitarizované zóny a ven z ní[15]. Tento nedostatek odstraní instalace HIPS systému na stanice uvnitř demilitarizované zóny. Cenově náročnější řešení činí instalace další sondy za firewall směrem do demilitarizované zóny.

Umístění před firewall

V opačném případě může být IPS zařízení umístěno před firewall (obr 1.7). Výhoda spočívá v možnosti analýzy provozu přicházejícího do demilitarizované zóny[15]. Není tedy nutné implementovat další prevenční systémy.

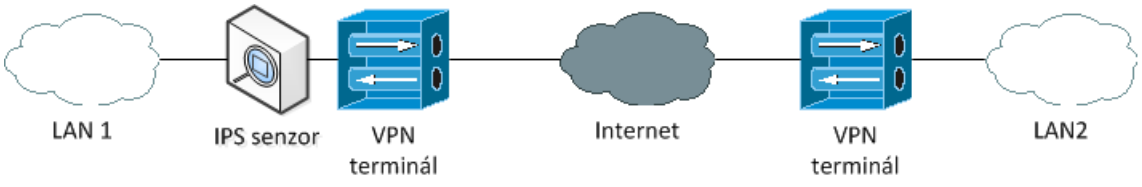


Obr. 1.7: Umístění IPS zařízení před firewall

Nedostatek vyplývá z umístění zařízení. Jelikož se analyzuje veškerý příchozí provoz z internetu, je nutné do této pozice umístit zařízení s dostatečným výpočetním výkonem a propustností. V opačném případě bude docházet ke zpoždění a potencionální průniky do sítě mohou být úspěšné. Je tedy vhodné nastavit pravidla tak, aby systém nekontroloval ta data, která by firewall nepropustil. Pro správnou činnost systému je nutná detailní konfigurace a odladění veškerých chyb[15].

Umístění mezi různé LAN

Předchozí příklady braly v úvahu jako zúžené místo pouze hranici místní sítě. Pokud firma vyžaduje vzdálený přístup pomocí VPN tunelu, je nutné dbát na prevenci i v tomto směru[15].

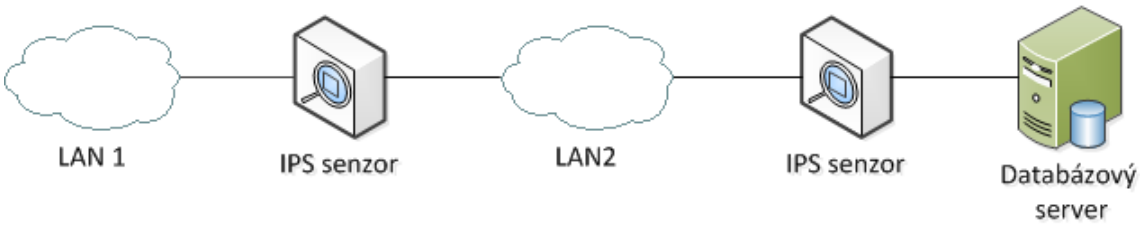


Obr. 1.8: Umístění IPS před VPN tunel

Ve většině případů se toto řešení kryje s předchozím případem, jelikož VPN spojení poskytuje firewall, případně hraniční směrovač. V opačném případě je vhodné umístit IPS před zařízení tvořící jeden konec VPN tunelu (obr. 1.8).

Umístění mezi segmenty LAN

V případě je lokální síť rozdělena na segmenty, linky mezi nimi tvoří vhodné zúžené místo pro umístění IPS senzoru (obr 1.9)[15].



Obr. 1.9: Umístění IPS mezi segmenty LAN

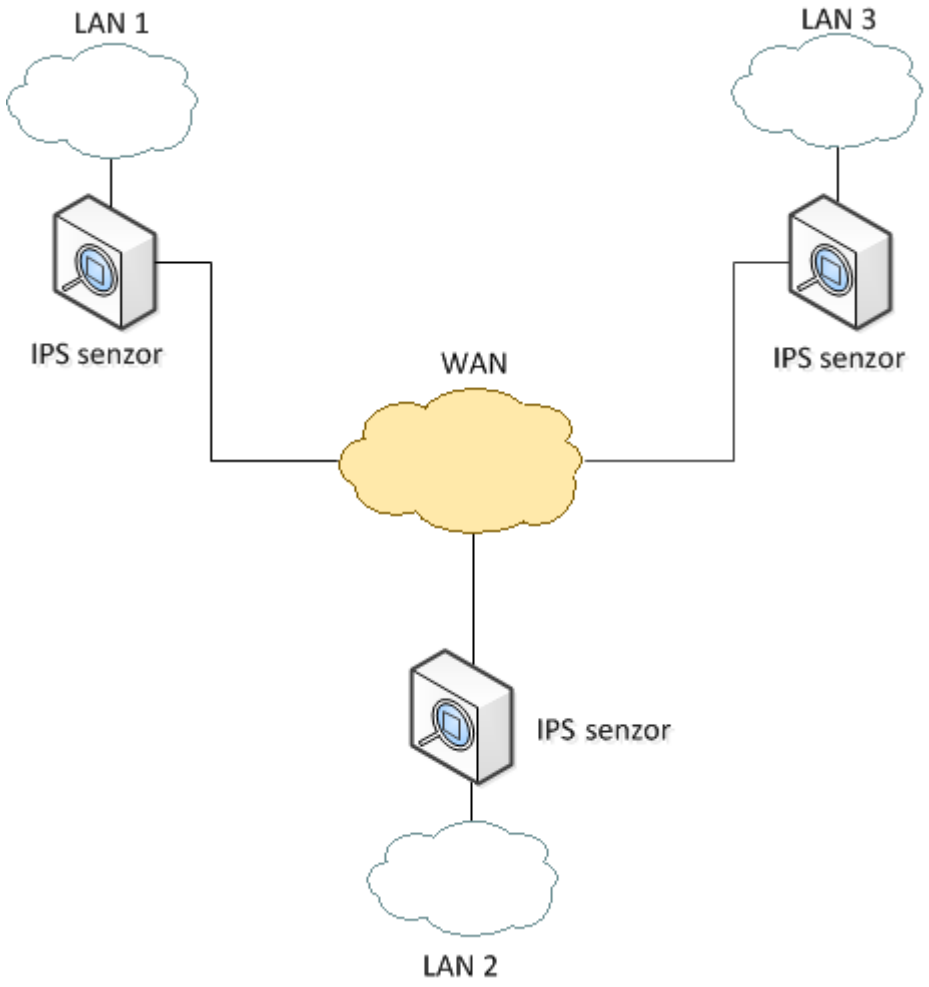
Umístění před most

Jednoduché struktury firemních sítí nemusí obsahovat žádné z již zmíněných zúžených míst. Jedná se převážně pouze o přepínané sítě. V tomto případě začlenění IPS senzoru činí problém. Situace je řešena vytvořením různých VLAN sítí a jejich přemostěním pomocí IPS senzorů (obr 1.10)[15].

Obr. 1.10: Přemostění VLAN

Umístění v infrastruktuře WAN

Problém nastává také při implementaci IPS zařízení do struktury WAN. Jediné, avšak cenově náročné řešení, spočívá v umístění IPS senzoru mezi distribuovanou lokální síť a přepínanou WAN (obr 1.11)[15].



Obr. 1.11: Umístění IPS v infrastruktuře WAN

1.6.5 Možnosti detekce útoků

Systémy prevence průniku jsou schopny zkoumat provoz a zajišťovat bezpečnost mnoha mechanizmy. Tím je zaručena poměrně velká bezpečnosti proti útokům využívajícím např. přetečení vyrovnávací paměti, skenování portů a využívání zranitelností systémů atd [16]. Mezi základní mechanizmy patří [16]:

- Důkladné dekódování provozu využívajícího konkrétní protkoly.
- Stavová kontrola provozu, kdy je zkoumán tok paketů jako celek.
- Heuristická analýza a zaznamenávání anomálií provozu.

• Zahazování poškozených, nebo upravených paketů.

Dekódováním provozu jsou systémy prevence schopny odhalit veškeré útoky, které obsahují signatury zaznamenané v databázi. Tyto útoky převážně využívají chyb a zranitelností systémů a aplikací.

Stavovou kontrolou paketů je odhalena většina útoků typu Man In The Middle, založená na různých typech spoofingu.

Heuristická analýza slouží jako prevence proti útokům založeným na krádežích relací. Před útokem je nutné analyzovat daný systém, zjistit otevřené porty, které jsou následně k útoku zneužity.

Neúplné nebo upravené pakety mohou být opět využity ke krádeži již navázaných spojení. Jedná se především o pakety s podvrženými sekvenčními čísly.

Tab. 1.6: Odhalitelné útoky různými mechanizmy IPS

Kontrola protokolu	útoky využívající chyby aplikací
Stavová kontrola provozu	IP spoofing, ARP cache poisoning, DNS spoofing
Heuristická analýza	DoS, DDoS, krádež TCP, UDP relací, útok hrubou silou
Zahazování poškozených paketů	krádež TCP, UDP relací, narušení DNS

1.6.6 Možnosti obcházení IPS

Zařízení se systémem prevence průniku mají svá omezení spočívající v tom, že jsou schopny kontrolovat pouze provoz na síti. Veškerá ostatní činnost před nimi zůstává skrytá. Nejsou tedy schopna odhalit útoky využívající chyby v programovacích jazycích. Neodhaleny také zůstanou útoky, které při komunikaci nevyužívají žádných anomálií, ani upravených paketů. Jedná se např. o krádež SSL relace (viz kapitola 2.3.2), kdy je veškerá nežádaná komunikace IPS senzorům skrytá, protože se jedná o legitimní provoz.

Mezi útoky, které je velmi obtížné detekovat, patří:

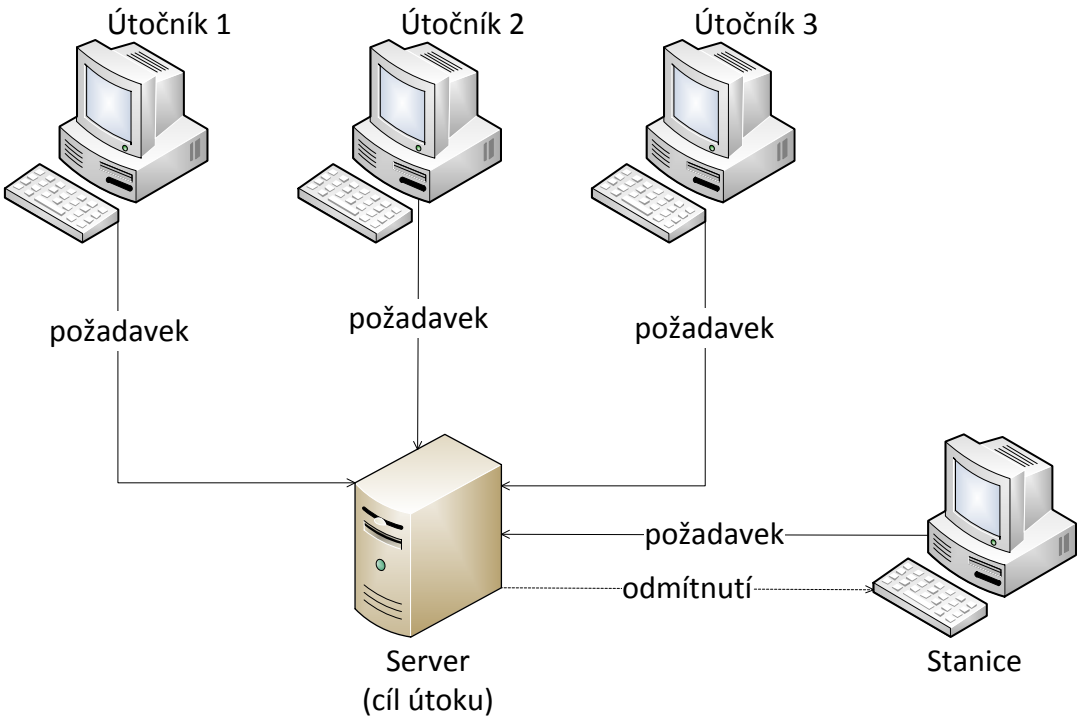
- cross-site request foregery,
- cross-site scripting,
- SQL injection,
- krádež SSL relace atd.

2 ÚTOKY NA SÍŤ

2.1 Denial of Service, Distributed Denial of Service

Útoky Denial of Service (DoS) brání v přístupu legitimním uživatelům ke konkrétním službám běžícím na serverech či v přístupu k internetovým stránkám [17]. Jejich cílem je ochromit síťovou komunikaci a znepřístupnit služby pro ostatní uživatele [17]. V případě úspěšného útoku dojde k:

- zahlcení sítě nepotřebným provozem, a tedy omezení šířky pásma sítě
- obrovskému zatížení CPU serveru
- odmítnutí služeb uživatelům
- odmítnutí přístupu k internetovým stránkám.



Obr. 2.1: Schéma DDoS útoku

Útoky využívají nejběžnějších síťových protokolů HTTP, TCP, UDP a ICMP. Jedná se o zahlcení cíle požadavky, které není schopen v reálném čase zpracovat, a tak se stává nedostupným (obr 2.1) [17]. Podle použitého protokolu existují různé typy DoS útoků, které jsou uvedeny v tabulce 2.1 [31] vč. jejich četnosti výskytu.

Tab. 2.1: Četnost typů DDoS útoků platná k 2. čtvrtletí 2011 [17]

typ útoku	výskyt [%]
HTTP flood	89
TCP SYN flood	5,5
UDP flood	2,5
ICMP flood	2
ostatní	1

Také rozlišujeme, zda je útok veden z jednoho počítače - DoS nebo z mnoha stanic současně, to znamená, že se jedná o Distributed Denial of Service (DDoS).

2.1.1 HTTP flood

Nejrozšířenější forma útoků DoS, DDoS bývá ta, kdy je na webový server vzneseno během krátkého časového intervalu mnoho požadavků http [17]. Jedná se o upravené požadavky, které je těžké rozpoznat a filtrovat.

2.1.2 TCP SYN flood

Typ útoku využívající protkol TCP. [17] Před přenosem dat musí zřízeno spojení mezi účastníky. To probíhá pomocí tzv. three–way–handshake.

První fáze obsahuje vyslání požadavku – TCP paketu, který v hlavičce obsahuje synchronizační příznak SYN. Cíl po obdržení SYN vrací klientovi druhý paket obsahující SYN+ACK, který signalizuje rozpoznání jeho požadavku. Spojení je ustanoveno v momentě zaslání ACK opět na server.

Útok využívá zasílání SYN paketů na server, které obsahují neplatnou zdrojovou IP adresu [17]. Jakmile server tento paket obdrží, vyšle zpět žadateli potvrzení ACK+SYN a očekává obdržení ACK, aby ustanovil spojení. V případě, že potvrzení neobdrží, v tabulce TCP spojení je udržována nekompletní cesta. Vysláním mnoha (řádově stovky až tisíce) podvržených SYN paketů je tabulka zaplněna.

Pokud legitimní uživatel vznese požadavek na server, nebude možné vytvořit nové TCP spojení a dojde k odepření služeb.

2.1.3 ICMP flood

Jedná se o zahlcení cíle pakety ICMP echo. Napadené počítače pod kontrolou útočníka (tzv. zombie počítače) začnou směrem k cíli vysílat téměř nepřetržitý tok paketů [17]. Modifikací velikosti odesílaného paketu lze zhroucení cílového systému

zapříčinit i jediným paketem.

2.1.4 Ochrana sítě proti odepření služeb

Proti útokům s odepřením služeb se brání velmi obtížně, jelikož k činnosti využívají legitimní provoz, který by neměl být blokován.

Jako hlavní prevence slouží sledování rychlosti určitého druhu provozu [19]. Jedná se převážně o pravidla na firewallu , kde je povolený pouze určitý počet dotazů na danou službu.

Vhodně zvolená anti-spoof pravidla omezí propouštění paketů s podvrženou zdrojovou IP adresou. [19] Když směrovač obdrží paket, je prozkoumán, a pokud jeho zdrojovou adresu není možné dohledat přes interface (u cisco zařízení např. služba unicast Reverse Path Forwarding – RPF), kterým dorazil, je zahozen.

Implementací QoS a nastavením vhodných pravidel pro provoz se omezí prioritní zpracování podvržených požadavků. Měla by být přidělena maximální priorita komunikaci administrátora s danými sítěmi, aby i v případě útoku mohl s nimi nadále komunikovat.

Jako první krok prevence proti útoku DoS je nutné začlenit do topologie sítě firewall nejlépe podporující technologii IPS. IPS kontroluje každý paket. Snaží se zjistit, jaký má záměr, z jakého zdroje pochází, a v případě podezření na útok jej dokáže odvrátit.

V případě, že prevence selže a útok proběhl, je nezbytné jej detekovat. K nalezení stop průniku je doporučeno kontrolovat logy firewallu i směrovačů a také pátrat po zombie [19]. V případě zombie se jedná většinou o nečinné procesy, které běží na serverech a čekají na „povel“ k zahájení útoku.

2.2 SQL injection

SQL injection využívá bezpečnostních trhlin na databázové vrstvě aplikací, které umožní útočníkovi zobrazit obsah databázových tabulek. K útoku dojde v případě vsunutí kódu do databáze, jež je později předán instanci SQL serveru, která jej analyzuje a spouští[20]. Pokud je syntaxe vloženého škodlivého kódu správná, server tyto dotazy vždy spustí.

Proces vkládání kódu funguje na principu předčasně ukončeného textového řetězce, za kterým následuje další příkaz.

Tab. 2.2: Operátory v jazyce SQL

Operátor	význam
;	oddělení požadavku
’	označení textového řetězce
- -	komentář
/* ... */	komentář

Existují 4 hlavní typy útoku SQL injection:

- SQL manipulace,
- vsunutí kódu,
- modifikace SQL funkce,
- přetečení bufferu.

2.2.1 SQL manipulace

Manipulace je proces, kdy jsou modifikovány SQL příkazy za pomoci operátorů (tab. 2.2)[20]. Útočník se snaží modifikovat SQL příkaz WHERE přidáním parametrů, nebo rozšířením pomocí odpovídajících operátorů.

V případě požadavku na vyplnění uživatelského jména část kódu vypadá následovně:

```
$name = ’name’;
$query = "SELECT * FROM users WHERE username = ’$name’";
echo . $query .;
```

Po zadání uživatelského jména `Roman` požadavek server zpracuje korektně a budou vybrány veškeré údaje, které obsahují uživatelské jméno Roman, tedy `$name = ’Roman’`. Požadavek, bude mít podobu

```
SELECT * FROM users WHERE username = ’Roman’
```

Využitím operátorů (viz tab. 2.2) je vložen za regulérní příkaz další, který ’je při správné syntaxi také proveden. V případě vložení `Roman’ OR ’1` je na server vznesen požadavek

```
SELECT * FROM users WHERE username = ’Roman’ OR ’1’
```

Jelikož část logického součtu `OR ’1’` je vždy pravdivá, bude vybrán veškerý obsah dané databázové tabulky[20].

2.2.2 Vložení kódu

SQL příkaz je pomocí operátoru „;“ ukončen a následně je vložen další. Při správné syntaxi budou postupně vykonány všechny uvedené příkazy. Útok využívá SQL příkazu EXECUTE.

Vložením `Roman';DROP TABLE uzivatele; --` bude předán serveru požadavek

```
SELECT * FROM users WHERE username = 'Roman';DROP TABLE users; --';,
```

který zapříčiní smazání veškerého obsahu tabulky s názvem „users“.

2.2.3 Modifikace SQL funkce

Jedná se o metodu, při které jsou vloženy funkce do zranitelného SQL příkazu SELECT, UPDATE, DELETE nebo INSERT. Ty následně mohou manipulovat s databází případně s databázovým systémem. Zavedením škodlivého kódu umožní útočníkovi

- zasílání informací z databáze vzdálené stanici
- měnit přístupové údaje
- spouštět další útoky

Struktura správné SQL funkce je následující:

```
SELECT TRANSLATE('user_input'
'prvni_parametr_funkce'
'druhy_parametr_funkce)'
```

Vložením kódu `UTL_HTTP.REQUEST('http://192.168.1.3')` bude nyní změněná funkce požadovat data z webového serveru. Útočník tak může manipulovat s řetězci URL za účelem obdržení užitečných informací z databáze a následnému zaslání zpět na webový server ve formě URL[20].

2.2.4 Přetečení bufferu

Přetečení bufferu lze dosáhnout pomocí modifikace SQL funkce. Pro většinu databázových systémů už ovšem existují opatření, která přetečení vyrovnávací paměti zabrání[20].

2.2.5 Ochrana databází

Útoky založené na SQL injection mohou být jednoduše odfiltrovány správnou konfigurací a údržbou databázového serveru. Veškeré dynamické SQL příkazy musí být chráněny. Z toho důvodu je vhodné zavést tzv. Bind proměnné.

Jedná se o proměnné, které musí být nahrazeny přesnou hodnotou nebo adresou předtím, než než se SQL příkaz úspěšně vykoná. Tyto proměnné by měly být použity v každém SQL příkazu. Jelikož je struktura zadávané hodnoty přesně nadefinovaná, není možné využít vložení modifikace či dalšího příkazu.

Jestliže není možné z jistého důvodu využít těchto proměnných, veškerá zadaná data musí být ověřena. Všechny znaky sloužící jako operátory v jazyce SQL (tab 2.2) k řetězení příkazů a řetězců musí být zakázány nebo při spouštění příkazu odstraněny.

Databáze by měla obsahovat pouze nezbytné funkce. Oddělením SQL dotazů od uživatelských dat, která jsou předávána jako parametry, se omezí možnost napadení dané SQL funkce.

V případě vyslání nesprávného požadavku je vrácena chybová zpráva obsahující popis příslušné chyby. Ten obsahuje důležité informace pro útočníka v případě, že nemůže získat zdrojový kód aplikace. Vypnutím chybových hlášení vzroste míra zabezpečení.

V jistých případech je možné detekovat a zabránit SQL injection nasazením zařízení IPS. Pro správnou činnost zařízení musí být schopno kontrolovat i zabezpečený provoz. Z toho důvodu je vhodné implementovat HIPS na konkrétní databázový server.

2.3 Man in the middle

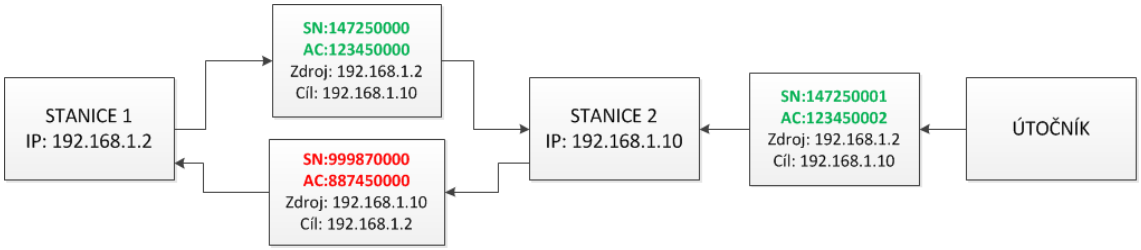
Man in the middle je jeden z nejznámějších útoků na dnešní počítačové sítě. V případě, že se útočník nachází uvnitř sítě, za může pomocí tzv. síťových snifferů odposlouchávat veškerý provoz na síti. Sniffery jsou programy, které umožní zachytit provoz na síti a podrobně ho analyzovat. Útočník tak získá údaje přenášené např. v hlavičkách jednotlivých rámců potřebných k ustanovení TCP, či UDP spojení nebo v případě použití nezabezpečeného protokolu jako je telnet, i celá uživatelská jména a hesla.

2.3.1 Narušení relací

Při „krádeži“ relace útočník využívá struktury TCP spojení[21]. Po navázání TCP spojení si stanice mezi sebou vyměňují pakety se stále rostoucím sekvenčním číslem.

To slouží k potvrzení paketů a garanci jejich přijetí ve správném pořadí.

Útočník musí nejprve tato čísla zjistit. Následně již stačí pouze odeslat paket s podvrženou zdrojovou adresou a správným sekvenčním číslem, které stanice očekává. Stanice tento paket přijme, provede zvýšení sekvenčního čísla a vyšle paket stanici na protější straně. Protože ale sekvenční číslo nesouhlasí, tato stanice paket zahodí a dojde k desynchronizaci. Oběť tak komunikuje pouze s útočníkem místo pravé stanice, která je tak z komunikace vyřazena (viz obr. 2.2 [21]).



Obr. 2.2: Princip únosu relace

Realizace únosu spojení lze dosáhnout využitím značky RST, keterá při TCP relaci signalizuje reset spojení. Při zachycení správného potvrzovacícho čísla lze vyslat podvržený paket se značkou RST a narušit tak spojení.

2.3.2 Narušení SSL relace

SSL je sada protokolů, která zajišťuje tunelové šifrování na úrovni transportní vrstvy přes nezabezpečenou síť (internet)[23]. Převážně se jedná o zabezpečenou verzi již používaných protokolů, jako jsou HTTPS, IMAPS atd.

Vytvoření spojení probíhá následovně: Klient vyšle na server požadavek s cílovým portem nezabezpečené verze protokolu. Server požadavek zachytí a vyšle zpět zprávu 30(X), která značí přesměrování cílového portu na port, který využívá zabezpečený protkol (např. HTTP-80; HTTPS-443). Po zpětném obdržení zprávy klient vznese požadavek na nový cílový port, kde je mu poskytnut certifikát, který po úspěšném ověření umožní začít šifrovanou komunikaci. V případě, že není možno z neznámého důvodu certifikát ověřit, uživatel je dotázán, zdali chce pokračovat v komunikaci i bez ověření cíle.

Útočník funguje jako proxy server mezi klientem a serverem[23]. Nejprve je nutné zachytit požadavek HTTP na server. Po odposlechu útočník sám vytvoří SSL relaci se serverem a využije služby třetí strany (např. SSLStrip), která zachytává požadavky HTTP, posílá je přes vlastní relaci serveru, vyhodnocuje jeho chování a odpovídá na uživatelské požadavky stejně jako server, avšak komunikace probíhá nešifrovaně přes HTTPS[23]. Útočník tak může vyčíst potřebné přístupové údaje.

Útok může detekovat sám uživatel. Je pouze nutné kontrolovat, jestli např. prohlížeč používá k přenosu na zabezpečených stránkách stále protokol HTTPS. V případě změny se může jednat o útok.

Další preventivní opatření by mělo poskytnout zabezpečení přístupu do sítě a nasazení Host-based IDS nebo IPS na klientskou stanici.

2.3.3 ARP cache Poisoning

Adress Resolution Protokol (ARP) se používá pro překlad adres mezi druhou a třetí vrstvou ISO-OSI modelu, tzn. překlad mezi MAC adresou a IP adresou. Překlad probíhá díky dvěma paketům – ARP požadavku a ARP odpovědi. Požadavek se skládá ze zdrojové IP a MAC adresy a z IP adresy zařízení, se kterým je třeba se spojit. Jako odpověď, pokud je vše v pořádku, dojde paket, který obsahuje IP a MAC adresu cíle.

Výměna těchto zpráv není ovšem nijak zabezpečená. Pokud zařízení přijme paket s ARP odpovědí, vždy si zapíše nové hodnoty do tabulky. Následným vysláním pouze ARP odpovědi s útočníkovou MAC adresou si cílové zařízení aktualizaci okamžitě zapíše. [24] To má za následek, že si napadená stanice myslí, že komunikuje přímo s další stanicí, ovšem ve skutečnosti se jedná o útočníka, který až posléze přeposílá data skutečnému cíli.

Obrana proti tomuto typu útoku není snadná. Výměna ARP paketů probíhá víceméně automaticky, bez velké možnosti zásahu do tohoto procesu [24]. Jedinou možností tedy zůstává udělat z dynamického průběhu překladu IP adresy na MAC částečně statický. Pokud existuje podezření, že se útočník snaží proniknout mezi dvě zařízení, je nutno kontrolovat výměnu ARP paketů programem třetí strany. Toho je možné docílit buď softwarově, případně za použití zařízení IDS nebo IPS [24].

2.3.4 DNS spoofing

DNS spoofing je obdobou výše zmíněného ARP poisoningu. Útok spočívá v poskytování falešných DNS informací oběti, ta je pak místo své požadované webové stránky přesměrována na jinou, kterou mohl navrhnout útočník tak, aby získal např. hesla nebo jiné citlivé informace [25].

Hlavním problémem DNS spoofingu je, že se velmi obtížně detekuje. Většinou útok poznáme až v případě, když jsme přesměrováni na jinou stránku, než jsme chtěli. Částečnou prevenci poskytne důkladné zabezpečení všech síťových prvků proti přístupu, jelikož útoky pochází většinou zevnitř sítě. [25] Velmi dobře poslouží opět zařízení IDS, případně IPS, která jsou schopna zachytit valnou většinu DNS

spoofingu [25].

2.3.5 Způsob ochrany

Všeobecně platí, že pokud k útokům typu MITM dojde a útočník naslouchá komunikaci, je již pozdě. Proto je nezbytné klást důraz na dostatečnou prevenci. Už kvůli spoustě modifikací útoku neexistuje žádné jednotné pravidlo, jak útoku předejít [26].

Za částečnou prevenci se dá považovat šifrování. Ať už se jedná o šifrování dat uložených na počítači, nebo šifrování provozu na síti. Jelikož valná část komunikace probíhá nezabezpečeně, dá se k šifrování využít veřejného klíče [26]. Vhodné je také používat zabezpečené protokoly, jako je např. SSH, místo telnetu.

Protože určité útoky se provádí většinou interně - ze sítě, nesmí se opomenout důkladně zabezpečit veškeré síťové prvky proti nežádoucímu přístupu [26]. Částečnou prevenci by měla poskytnout implementace protokolu 802.1x na přístupové prvky. Tím rozumíme vynutit zadání hesla pro přístup k síťovým prvkům (směrovače, přepínače), přiřazení maximálního počtu MAC adres na port přepínače (případně přidělení určité MAC adresy na určitý port) a veškeré nevyužité porty je vhodné vypnout [26].

Ovšem největší ochranu poskytnou zařízení IDS, IPS. Ta jsou schopná při správném nastavení ve velké míře rozpoznat různé modifikace útoku MITM a zabránit jim.

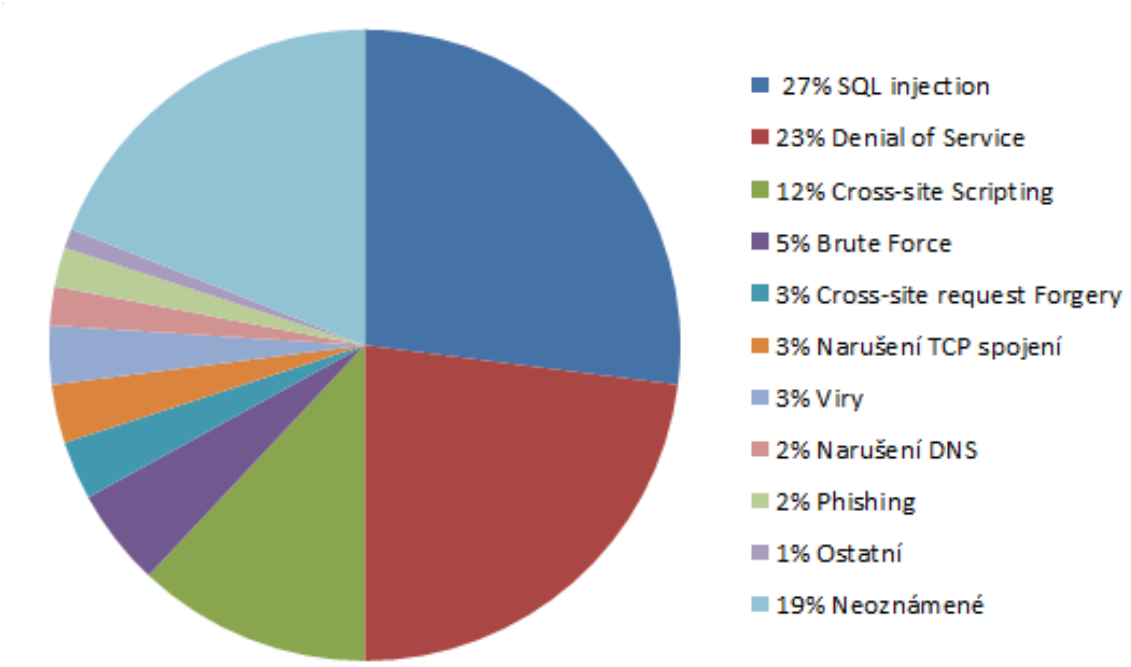
2.4 Současné ohrožení sítí

Kvůli současným možnostem ochrany sítí počet jakýchkoliv útoků využívajících narušení spojení klesl na minimum (viz obr 2.3). Velká část pokusů o útok ovšem zůstala nenahlášena[27].

Současné útoky se snaží převážně využívat chyb v programovacích jazycích a následně využít vlastní škodlivý kód[27]. Hlavním důvodem je větší anonymita útočníka a přístup k mnohem většímu množství citlivých dat. Při úspěšném útoku na databázový systém se útočník může dostat k uloženým osobním i přihlašovacím údajům mnoha uživatelů.

V současné době byly zachyceny nejčastěji útoky se znaky SQL injection viz kapitola 2.2 a Cross-Site request forgery, scripting (útok do internetových aplikací za pomoci skriptovacích jazyků)[28]. Nárůst také zaznamenaly útoky na databázové systémy hrubou silou.

Druhou skupinou útoků s velkým procentuálním zastoupením tvoří útoky typu Denial of Service[28]. Jejich nárůst je zapříčiněn velmi jednoduchým provedením a



Obr. 2.3: Procentuální zastoupení útoků v roce 2011

využitím při protestních akcích. Nejvyužívanějším typem je zahlcení serveru požadavky HTTP[31].

Ochrana dnešních serverů spočívá v zavedení speciálního směrování tzv. anycast [29]. Instance stejné služby v tomto případě sdílí stejnou IP adresu. Pokud je vyslán např. DNS požadavek, je zpracován serverem, který je topologicky nejblíže zdroji zpráv [29]. Při úspěšném DoS útoku, tedy vypadne pouze topologicky nejbližší server, avšak ostatní mohou nadále odpovídat na vznášené požadavky uživatelů.

Analýzou sítí, na nichž byly konkrétní útoky úspěšné, byly zjištěny hlavní nedostatky současných sítí, které průnikům napomohly, nebo obsahovaly slabinu, kterou bylo možné potencionálně k útoku využít. Jednalo se převážně o[28]:

- slabá nebo žádná administrátorská hesla,
- zasílání nechráněných citlivých dat přes nedůvěryhodnou síť,
- nedostatečné zabezpečení bezdrátového přístupu (např. využití WEP),
- chybná přístupová pravidla na směrovačích a firewallech,
- umístění citlivých dat mimo chráněnou zónu.

2.4.1 Advanced Persistent Threats

Společně s vývojem bezpečnostních návrhů sítí se také vyvíjí druhy malware a v dnešní době právě tyto škodlivé programy představují největší nebezpečí pro firemní sítě [27]. Prioritou využívaného malwaru je umožnit útočníkovi vzdáleně manipu-

lovat se systémy v napadené síti, ale současně zůstat neviditelný pro standardní obranné mechanizmy. Programy, které toto umožňují, jsou nazývány Advanced Persistent Threats (APT) [27].

Detekce APT programů je velmi obtížná, jelikož jsou napsány tak, aby jejich signatury nebylo možno zaznamenat žádnými ochrannými systémy. Neexistuje žádné hardwarové či softwarové řešení, které by bylo schopno APT odhalit [27].

Hlavním cílem není přímo identifikování konkrétního APT programu, ale odlišení běžného malwareu od APT. Odhalení probíhá až s odstupem času po dlouhodobém vyhodnocování veškeré síťové činnosti [27].

2.4.2 Online hrozby

Podle výzkumů je denně ohroženo více než 30 000 webových stránek a více než 85% všeho malwaru ohrožující dnešní sítě pochází právě z těchto stránek [30]. Hlavní problémy představují převážně [30]:

- přímé stahování,
- sociální inženýrství,
- botnet software.

Útoky za pomoci přímého stahování využívají neopravených zranitelností konkrétního internetového prohlížeče [30]. Jakmile uživatel navštíví nedůvěryhodnou stránku, je bez jeho vědomí stažen a spuštěn software, který umožní útočníkovi získat potřebné údaje. Nejčastějším typem tohoto softwaru jsou tzv. černé díry využívající zranitelností v java a flash aplikacích [30].

Jedná se o neustále se měnící škodlivý kód, za účelem obcházení antivirového programu. Tento sofware nejčastěji pracuje jako [30]:

- botnet malware (rozesílání spamu),
- rootkit,
- backdoor,
- falešný antivirus.

Převážná většina online hrozeb využívá chyb uživatele. Částečnou prevenci v současnosti poskytují vhodně zvolená pravidla pro filtrování přístupu na konkrétní webové stránky [30]. Odfiltrovat ale všechny škodlivé není možné. V případě, že uživatel podezřelou stránku navštíví, stahování a šíření škodlivého kódu ve většině případů zabrání antivirus nebo systém IPS. Útoky tohoto typu představují nebezpečí převážně na menší firemní sítě, ve který není z finančních důvodů možné nasadit pokročilejší metody prevence útoků [30].

2.4.3 Systémové a softwarové hrozby

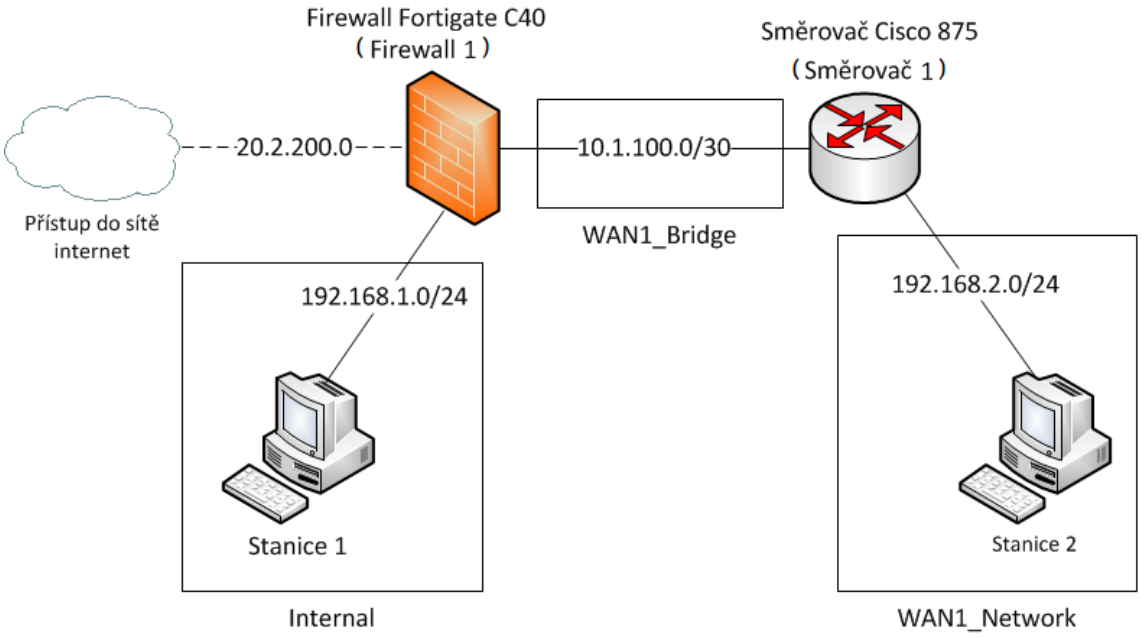
Z důvodu rostoucí bezpečnosti operačních systémů a rychlému vydávání aktualizací opravujících nově objevené zranitelnosti, počet útoků mířených konkrétně na operační systémy výrazně ubývá [30]. Mnohem více nezabezpečeného prostoru poskytují právě aplikace, které pod těmito systémy běží.

Nejčastěji jsou útoky směřovány na aplikace napsané v jazyku java, dále na PDF software a flash z důvodu jejich frekventovaného využití téměř na každém počítači [30].

Velký podíl na narušení bezpečnosti také nesou webové aplikace, v nichž nejsou naprogramována dostatečná bezpečnostní opatření [30]. Frekventované jsou útoky SQL injection a cross-site scripting [30].

3 ZABEZPEČENÍ SÍTĚ

3.1 Návrh sítě



Obr. 3.1: Návrh testovací sítě

3.1.1 Použitá zařízení

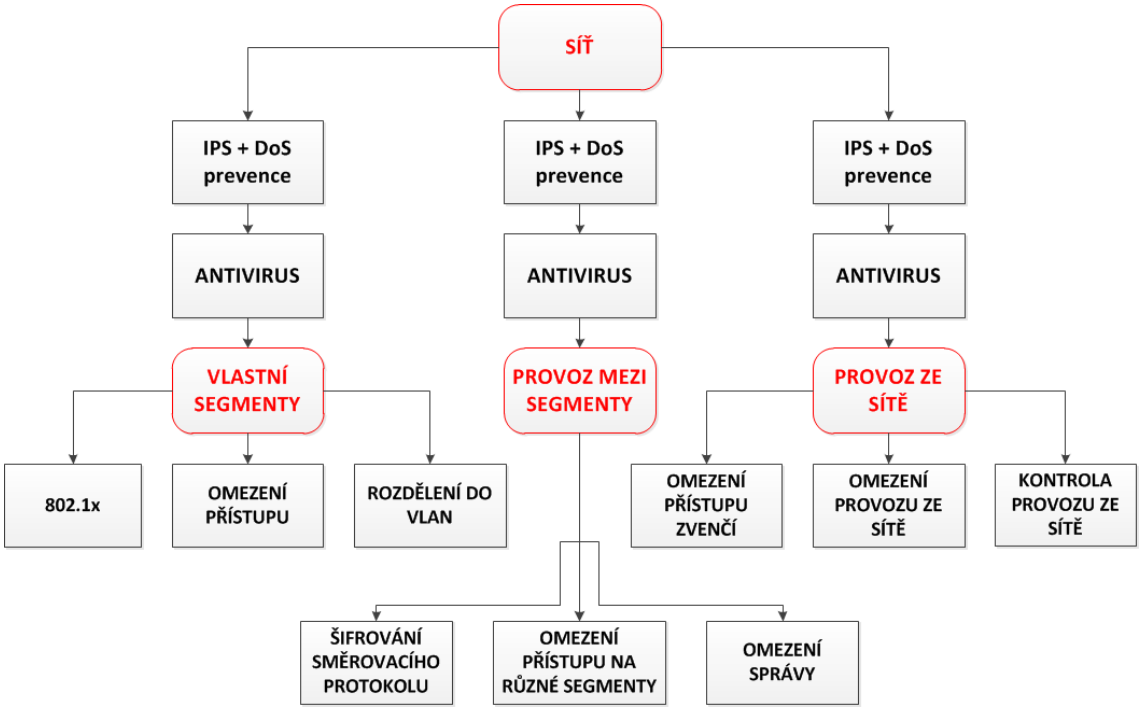
Směrovač Cisco 875:

- IOS v12.2,
- podpora šifrování,
- podpora protkolu 802.1x,
- podpora stavového firewallu,
- access list (ACL) s podporou VLAN.

Servisní gateway firewall Fortigate C40:

- firewall s výkonem 600Mbps,
- IPS s výkonem 135Mbps,
- podpora instalace antivirové ochrany,
- 2x10/100/1000 WAN porty, 5x10/100/1000 porty pracující na 2. vrstvě.

3.2 Návrh zabezpečení



Obr. 3.2: Návrh zabezpečení testovací sítě

Navržená testovací síť byla rozdělena na tři segmety (viz obr.3.1):

- segment *internal*,
- segment *WAN1_Bridge*,
- segment *WAN1_Network*.

Návrh zabezpečení byl rozdělen do tří sekcí (viz obr 3.2). Byla vytvořena bezpečnostní pravidla pro provoz v jednotlivých segmentech sítě (obr. 3.1), pro provoz mezi segmenty sítě a pro provoz na rozhraní testovací sítě a sítě internet. Pro každou sekci byla navržena vhodná bezpečnostní pravidla, která by měla zabránit nežádoucímu provozu na síti a detekovat možné útoky a zabránit jim (viz kapitola 3.3).

Jelikož navrženou síť nebylo možné v době testování připojit k internetu, pravidla týkající se právě tohoto provozu byla navržena tak, aby při následném připojení poskytla již dostatečnou bezpečnost.

Následující konfigurace IPS/IDS, kontroly aplikací a antiviru byla možná pouze na firewallu 1.

3.2.1 Konfigurace IPS

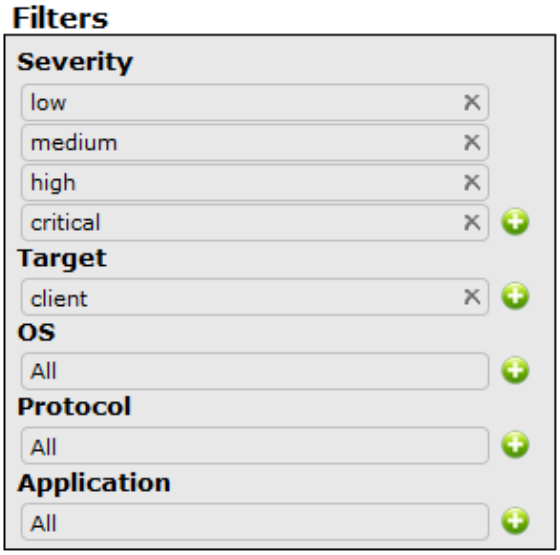
Jelikož Intrusion prevention system představuje hlavní bezpečnostní prvek navržené sítě, senzory byly umístěny tak, aby bylo možné kontrolovat co největší část síťové

komunikace. Vytvořenými pravidly je sledován veškerý provoz, mimo interní komunikaci v síti 192.168.2.0.

Jelikož předdefinované signatury definují útoky na cílové stanice a servery, byly vytvořeny dva různé filtry.

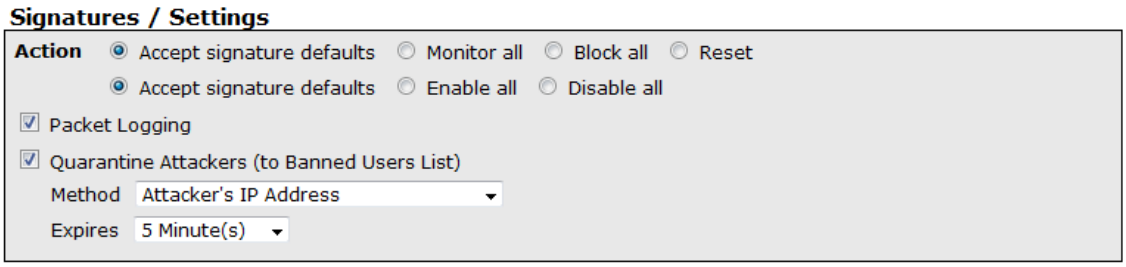
Ochrana cílové stanice

První filtr definuje veškeré útoky vedené na cílové stanice s jakýmkoliv operačním systémem. IPS senzor s tímto filtrem bude kontrolovat všechny dostupné protokoly i aplikace, které směřují k vybrané cílové stanici (viz obr. 3.3)



Obr. 3.3: Nastavení filtrace signatur pro ochranu koncové stanice

V případě, že je rozpoznán útok, událost se zapíše do seznamu, který je uložen v paměti brány firewall 1. Pokud je útok veden ze segmentu internal nebo WAN1_Network, způsobí blokaci útočníkovy IP adresy po dobu pěti minut (obr. 3.4).

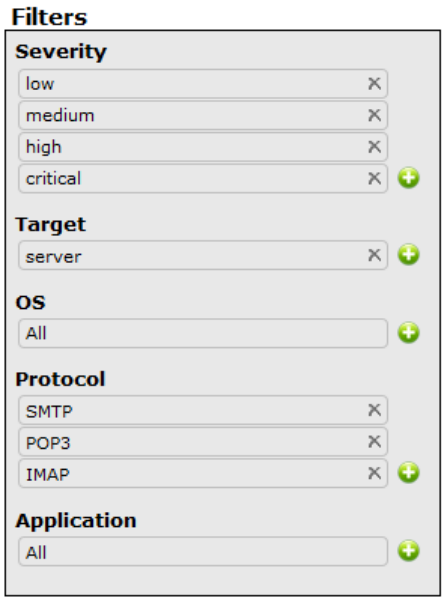


Obr. 3.4: reakce při detekci útoku

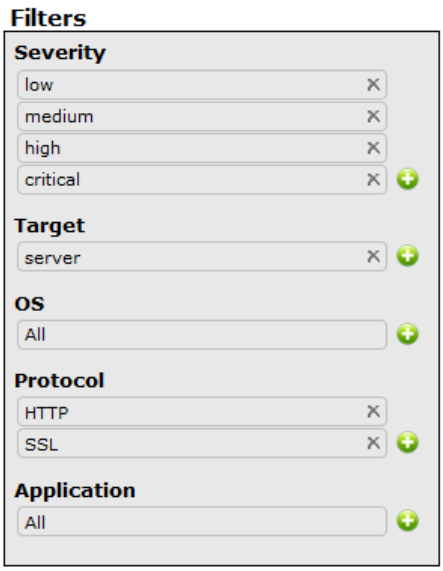
Tato doba je zvolena pouze pro testovací účely, ve skutečnosti by měla být mnohonásobně vyšší. Další možností odpojení útočníka je vypnutí portu, přes který škodlivá data přišla. Tohle řešení ovšem není vhodné, jelikož by neškodné stanice v zónách internal a WAN_Network mezi sebou nemohly dále komunikovat.

Ochrana serverů

Pro případ rozšíření sítě o nové servery (web server, mail server) byly vytvořeny dva obdobné filtry. Funkcí prvního filtru je ochrana poštovního serveru, tedy kontroluje veškerý provoz, který zajišťují protokoly STMP, POP3 a IMAP (obr. 3.5). Druhý filtr slouží pro http server, je tedy nutné kontrolovat veškerý provoz směřující na port 80 a 443 (https) viz obr. 3.6. Jelikož dané servery mohou obsahovat důležité informace, byl pro maximální bezpečnost filtr nastaven tak, aby byl schopen detekovat i méně nebezpečné útoky.



Obr. 3.5: Nastavení filtrace signatur pro mail server



Obr. 3.6: Nastavení filtrace signatur pro web server

Obdobně jako u předchozího filtru v případě, kdy dojde k útoku, bude útočníkova IP adresa přidána do seznamu zakázaných IP adres po dobu pěti minut.

Omezení

Omezení spočívá v nemožnosti kontroly provozu, který přes jednotlivé senzory neprochází. Jedná se převážně o komunikaci v rámci jedné VLAN sítě, která není žádným způsobem směrována. O veškerý provoz se starají pouze přepínače.

V případě testovací sítě se jedná o segment WLAN1_network (síť 192.168.2.0), jelikož rozhraní přes, která je připojena stanice2 pracují pouze na druhé vrstvě ISO/OSI modelu. Vznik tohoto problému také hrozí v případě rozšíření zóny internal o nový přepínač. Komunikace bude procházet pouze přes přidaný přepínač a nebude využívat trunk linky mezi přepínačem a bránou firewall, která už kontrolována bude.

Řešením tohoto problému je umístění IPS senzoru na místo, kde může plnit svoji funkci. Vhodná by tedy byla instalace host-based IPS na konkrétní stanice a přiřazení potřebných stanic do různých VLAN sítí, aby provoz musel procházet přes zařízení s funkčním IPS. Toto řešení ovšem zvýší provoz na síti a zatížení brány firewall, která by jako páteřní prvek měla být schopna zpracovávat data s co nejmenší prodlevou.

3.2.2 Konfigurace DoS filtru

K detekci a zastavení útoků typu odepření služeb slouží jednoduchý filtr, který kontroluje počet příchozích datových jednotek jednotlivých protokolů. V případě, že dojde k překročení nastavené hraniční hodnoty, přestane firewall 1 požadavky se zdrojovou adresou útočníka propouštět a v útoku nebude možné dále pokračovat. požadavky legitimních uživatelů je však možné dále zpracovávat.

Name	Enable	Logging	Action	Threshold
tcp_syn_flood	☑	☑	Block	2000
tcp_port_scan	☑	☑	Block	1000
tcp_src_session	☑	☑	Block	5000
tcp_dst_session	☑	☑	Block	5000
udp_flood	☑	☑	Block	2000
udp_scan	☑	☑	Block	2000
udp_src_session	☑	☑	Block	5000
udp_dst_session	☑	☑	Block	5000
icmp_flood	☑	☑	Block	250
icmp_sweep	☑	☑	Block	100
icmp_src_session	☑	☑	Block	300
icmp_dst_session	☑	☑	Block	1000
ip_src_session	☑	☑	Block	5000
ip_dst_session	☑	☑	Block	5000

Obr. 3.7: Limitní hodnoty zvolených anomálií

Limitní hodnoty se v závislosti na požadavcích pro různé sítě mohou značně

lišit. Hodnoty pro testovací síť uvedené na obr. 3.7 jsou zvoleny tak, aby bylo možné funkčnost filtru jednoduše otestovat.

Omezení

V případě, že rozsah DDoS útoku překročí maximální rychlost firewallu, kterou je schopen kontrolovat příchozí provoz, budou útočníkovy požadavky do sítě propouštěny. Proti distribuovaným útokům DoS neexistuje žádná stoprocentní ochrana. Částečného omezení lze dosáhnout umístěním dostatečně výkonného firewallu před místa v síti, kde existuje podezření, že sem bude útok směřován.

3.2.3 Konfigurace antiviru

Antivirus byl nastaven tak, aby kontroloval data. Jejich přenos zajišťují všechny dnes používané protokoly pro přístup na web, odesílání a příjem pošty a přenos dat (obr. 3.8). Když dojde k odhalení viru, soubor, který jej obsahuje, bude smazán. V testovací síti je kontrolován pouze přenos dat, jelikož síť neobsahuje připojení do internetu. Ostatní nastavení se projeví až v případě, že jsou přidány poštovní a http servery, nebo je zavedeno připojení k internetu.

	Web		Email						File Transfer		
	HTTP	HTTPS	SMTP	SMTPS	POP3	POP3S	IMAP	IMAPS	FTP	FTPS	IM
Virus Scan and Removal	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑
Quarantine	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐

Obr. 3.8: Kontrolované protokoly antivirem

Omezení

Jediným omezením zvoleného řešení je nedostatečný výkon antiviru na hraničním firewallu 1. V Případě většího množství dat nebude schopen kontrolovat všechen potřebný provoz.

Tento nedostatek odstraňují nainstalované antivirové programy na koncových stanicích a serverech.

3.2.4 Kontrola aplikací

V testovací síti jsou povoleny všechny druhy aplikací kromě zvolených aplikací poskytujících peer-to-peer spojení. Z testovacích důvodů byla zakázána aplikace DC++ a všichni klienti obsažení v databázi firewallu 1, kteří umožňují stahování torrentů. Nebezpečí těchto aplikací spočívá v tom, že uživatel nezná identitu uživatele, ke

kterému je připojen. Není tedy ani zaručena neškodnost přenášených dat. V případě stažení infikovaného souboru bude narušena bezpečnost celé sítě.

Na servisní bráně běží filtr, který veškeré tyto aplikace blokuje. Činnost ostatních povolených aplikací je pouze monitorována systémem IPS, detekujícím možné anomálie provozu.

3.2.5 Zabezpečení segmentů

Implementace protokolu 802.1x

Na všech portech obou síťových zařízení (firewall 1 a směrovač 1 viz obr. 3.1) pracujících pouze na druhé vrstvě ISO/OSI modelu byl implementován protokol 802.1x. Jeho cílem je ověřit totožnost uživatele a teprve po úspěšném zadání přihlašovacích údajů mu umožnit přístup do sítě.

Autentizace uživatele může probíhat dvěma způsoby:

- lokálně - přímo z databáze uložené na přepínači nebo směrovači,
- vzdáleně - pomocí protokolů RADIUS nebo TACACS+, kdy k ověření dochází na příslušných serverech.

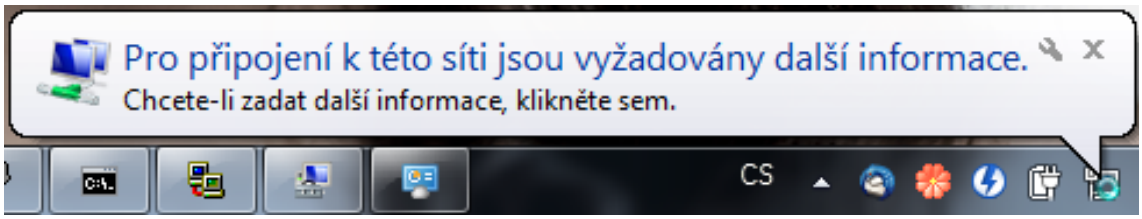
Z důvodu omezení sítě byla zvolena pouze lokální autentizace. Databáze uložená na směrovači 1 obsahuje následné údaje:

Tab. 3.1: Přihlašovací údaje v lokální databázi

uživatelské jméno	heslo
guest	guest
JanNovak	Novak
PetrDohnalek	D0hNá1€K

Pro připojení počítače do sítě, je nutné, aby v jeho operačním systému běžela služba 802.1x supplicant. Teprve po jejím spuštění je možné si od uživatele vyžádat přihlašovací údaje (obr. 3.9). Pro šifrování a přenos kontrolních údajů byl zvolen protokol PEAP. Po zadání jakýchkoliv údajů z tabulky 3.1 je uživateli umožněn přístup do sítě.

Problém protokolu 802.1x spočívá v nutnosti mít pro každého uživatele konkrétní přihlašovací údaje a v případě vzdáleného ověřovaní také přístup na RADIUS server. Proto je jeho implementace vhodná spíš do sítí, kde není kladen důraz na neomezený přístup. Jde převážně o bezdrátové sítě.



Obr. 3.9: Vyžádání přihlašovacích údajů

VLAN sítě

Z důvodu větší míry bezpečnosti byly stanice testovací sítě na obou síťovým prvcích přesunuty ze standardní sítě VLAN1 do vyšších VLAN sítí, konkrétně VLAN150. Po případném rozšíření sítě je vhodné nové stanice přiřadit do dalších VLAN sítí. Dosáhne se tak omezení provozu v jednotlivých sítích a je zajištěna možnost kontroly provozu pomocí IPS.

Omezení přístupu a služeb na směrovači 1

K zabránění nežádoucímu přístupu k síťovým zařízením bylo nutné nastavit administrátorské přihlašovací údaje. Nastavena byla hesla pro lokální přístup (konzole), tak vzdálený (telnet, SSH). Zapnutím služby password-encryption se znemožní vyčtení těchto údajů z výpisu konfigurace směrovače 1.

V Jednotlivých segmentech běží na síťových prvcích služby, které je z bezpečnostního hlediska lepší vypnout, případně existují služby, které by měly být zapnuty.

GLOBÁLNÍ SLUŽBY SMĚROVAČE 1:
Z globálních služeb byl vypnut protokol Finger, který může poskytnout nežádoucí osobě údaje o tom, kdo a odkud je ke směrovači 1 přihlášen.

Vypnuty byly také malé UDP a TCP servery. Dané servery pracují na portech 19 a níže a poskytují prostor k útoku DoS. Jedná se o zastaralou službu, která by měla být vypnuta na všech směrovačích.

Zakázána byla služba Gratuitous ARP. Jde o službu, kdy je poslána zpráva gAPR pokaždé, když klient obdrží IP adresu přes spojení point-to-point. Tohoto mechanismu se využívá u většiny starších ARP poisoning útoků.

Povolením služby TCP keepalives in/out a TCP synwait-time jsou kontrolovány veškeré pokusy o navázání TCP spojení. Keepalive pakety mají za úkol ověřit, zda je TCP spojení stále aktivní. V případě netypicky ukončeného spojení tato spojení směrovač ze své tabulky vymaže. TCP synwait-time byl nastaven na 10s. Jedná se o časový interval, ve kterém je možno navázat TCP spojení.

Z globálních služeb byl vyřazen také protokol CDP.

Kvůli omezení nežádoucího přístupu ke směrovači 1 byla povolena služba Password encryption, která zašifruje použitá hesla, a následně tedy není možné vyčíst z konfigurace směrovače 1.

SLUŽBY BĚŽÍCÍ NA ROZHRANÍCH SMĚROVAČE 1:
Služby, které ovlivňují chování jednotlivých rozhraní, může využít útočník k mapování celé sítě a k následnému provedení útoku.

Vypnuta byla služba IP redirects, kdy ICMP zpráva informuje stanici, který směrovač má použít při cestě do vzdálené sítě. Dále také služba IP unreacheables, která informuje stanici o snaze vytvořit spojení s nedosažitelnou IP adresou. Vypnutím služby IP mask replies se zamezí rozesílání informací o masce sítě použité na rozhraních.

Vypnuta byla i služba IP direct-broadcast. IP direct broadcast je datagram zasílaný jako broadcast do sítě, která není přímo připojená. Tohoto mechanizmu využívají útočníci při provádění DoS.

UNICAST RPF:
Reverse Path Forwarding (RPF) umožňuje zařízení zjistit, zdali zdrojová IP adresa příchozího paketu je dohledatelná přes rozhraní, kterým paket dorazil. Pokud není, paket je zahozen. Tato služba byla povolena na všech rozhraních směrovače 1.

3.2.6 Provoz mezi segmenty sítě

Zabezpečení směrovacího protokolu

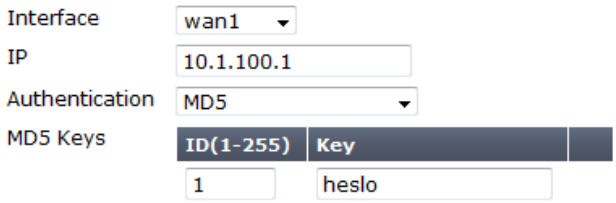
Směrovací protokol OSPF ve svém výchozím nastavení posílá veškeré zprávy nezašifrované. Na obou zařízeních je k šifrování zpráv možné použít pouze algoritmus MD5, který ale již neposkytuje maximální bezpečnost.

Příkazy:

```
ip ospf authentication message-digest
ip ospf message-digest-key 1 md5 heslo
```

je v konfiguračním módu rozhraní směrovače 1 vytvořena klíčenka s identifikátorem 1 a konkrétním heslem. Stejný identifikátor i heslo musí být zvoleno i na zařízení, se kterým je třeba vytvořit OSPF sousedství, tedy na firewallu 1 (obr. 3.10)

Po potvrzení obou údajů bylo znovu vytvořeno sousedství mezi směrovačem 1 a bránou. Tím bylo dosaženo plné konektivity mezi jednotlivými segmenty sítě (Obr. 3.11)



Obr. 3.10: Nastavení šifrování pomocí MD5 na hraniční bráně

```
     20.0.0.0/30 is subnetted, 1 subnets
O       20.2.200.0 [110/11] via 10.1.100.1, 00:04:23, FastEthernet4
     10.0.0.0/30 is subnetted, 1 subnets
C       10.1.100.0 is directly connected, FastEthernet4
O    192.168.1.0/24 [110/2] via 10.1.100.1, 00:04:23, FastEthernet4
C    192.168.2.0/24 is directly connected, Vlan100
C    192.168.3.0/24 is directly connected, Loopback0
Router(config)#
```

Obr. 3.11: Směrovací tabulka OSPF na směrovači 1

Omezení přístupu na segmenty

Na firewallu 1 byla vytvořena přístupová pravidla do jednotlivých segmentů testovací sítě (viz tabulka 3.2). Správci sítě s IP adresou 192.168.1.2 je povolen přístup na všechny segmenty. Ostatní uživatelé mohou komunikovat pouze v rámci vlastního segmentu a mezi sítěmi 192.168.1.0 a 192.168.2.0.

Tab. 3.2: Přístup do segmentů

Z | DO	Internal	WAN1_Bridge	WAN1_Network	WAN2
Internal	-	spravce	uzivatel, spravce	uzivatel, spravce
WAN1_Bridge	spravce	-	spravce	spravce
WAN1_Network	uzivatel, spravce	spravce	-	uzivatel, spravce
WAN2	nepovoleno	nepovoleno	nepovoleno	-

Jelikož provoz ze sítě 192.168.2.0 směřovaný do segmentu WAN1_Bridge nemůže být filtrován pomocí pravidel na hraniční bráně, na virtuální rozhraní VLAN100 byl v příchozím směru aplikován access-list, zakazující tuto komunikaci:

```
access-list 199 deny ip 192.168.2.0 0.0.0.255 10.1.100.0 0.0.0.3
access-list 199 permit ip any any.
```

Omezení správy

Vzdálený přístup na konkrétní zařízení je povolen pouze správci sítě s IP adresou 192.168.1.2. Běžní uživatelé na síťová zařízení nemají přístup.

V celé síti byl pro vzdálený přístup zakázán protokol telnet. Jedná se o nezabezpečený protokol, který přenáší data v nešifrované formě a je tedy vhodný převážně do menších experimentálních sítí a rozrůstajících se sítí, které neobsahují správě nakonfigurované síťové prvky. Obdobně byl také pro správu vypnut protokol http, který obsahuje stejné nedostatky jako telnet.

Pro vzdálený přístup na webové rozhraní byla povolena pouze zabezpečená verze protokolu http - https. Pro vzdálení připojení ke konzoli je nutné místo telnetu použít zabezpečený protokol SSH (obr. 3.12).

Name	IP/Netmask	Access
internal	192.168.1.99 / 255.255.255.0	HTTPS,PING,SSH
loopback	192.168.99.1 / 255.255.255.0	PING
wan1	10.1.100.1 / 255.255.255.252	HTTPS,PING,SSH
wan2 (Internet Service Provider)	20.2.200.2 / 255.255.255.252	PING

Obr. 3.12: Povolený přístup na rozhraní

V případě, že by bylo nutno např. z důvodu selhání klienta poskytujícího připojení přes SSH povolit telnet, na virtuální lince směrovače 1 je v příchozím směru aplikován access-list

```
access-list 66 permit 192.168.1.2,
```

který zakáže přístup ze sítě 192.168.2.0 (není kontrolováno firewallem 1) a povolí ho pouze správci s uvedenou IP adresou.

3.2.7 Komunikace sítě a internetu

Omezení přístupu do sítě

Jelikož je většina útoků vedena právě z internetu byla tato komunikace velmi omezena. Veškerý vzdálený přístup na jakýkoliv prvek v síti byl zakázán přes zastaralý protokol telnet, ale i bezpečnější SSH. SSH sice svou strukturou poskytuje ochranu proti IP spoofingu, modifikaci přenášených dat, avšak v případech, kdy útočník dokáže převzít přístupová práva jedné z komunikujících stanic, vznikne bezpečnostní trhlina. Pakety tedy z jakéhokoli zdroje v nedůvěryhodné síti směřované do vnitřní sítě využívající port 22 a 23 budou zahozeny (obr. 3.13). Jediný možný přístup byl ponechán přes VPN.

Seq.#	ID	From	To	Source	Destination	Service	Action	Log	IPS Sensor
8	12	wan2	any	any	any	TELNET SSH	DENY		-

Obr. 3.13: Zákaz přístupu přes telnet a ssh

3.2.8 Omezení provozu ze sítě

Pravidla byla nakonfigurována tak, aby po případném připojení do internetu, byl provoz již filtrován. Veškeré povolené služby ze segmentu internal jsou uvedeny na obr. 3.14. Aby se zabránilo uniknutí chybně směrovaných paketů v rámci lokání sítě do internetu, cílovou adresu představovala adresa na rozhraní internetu.

Seq.#	ID	From	To	Source	Destination	Service	Action	Log	IPS Sensor
11	8	internal	wan2	internal_pool	internet provider	AOL DNS FTP HTTP HTTPS ICMP_ANY PING IMAPS SMTPS POP3S TCP UDP	✓ ACCEPT		protect_host
12	15	internal	wan2	internal_pool	internet provider	ANY	DENY		-

Obr. 3.14: Povolené protkoly

Stejná pravidla platí také pro segment WAN1_Network. Za každým takto zvoleným filtrem pro konkrétní segment následuje pravidlo deny, které veškerý provoz nesplňující požadavky daného filtru zakáže a vypíše zprávu do seznamu událostí (obr. 3.14).

Aby bylo možné odpovědět na požadavek, který byl vznesen na server nacházející se v síti internet, musely být v příchozím směru povoleny stejné protokoly, jaké byly zvoleny u filtru omezujícího provoz ze sítě.

Pro veškerý příchozí i odchozí provoz byl na patřičná místa umístěn IPS senzor pro rozpoznání útoku na koncovou stanici. V případě rozšíření testovací sítě o servery, by musel být senzor změněn na senzor umožňující ochránit právě konkrétní server.

3.3 Testování sítě

3.3.1 Test antivirového programu

Pro otestování správné činnosti antiviru byly na dva počítače v různých segmentech nainstalovány FTP servery, přes které následně probíhala výměna škodlivého souboru.

Jednalo se o upravený testovací soubor, do kterého byla vnesena část kódu, kterou koncové stanice neohrozí, avšak antivirový program by ho měl rozpoznat. Následoval pokus přenést soubor z FTP serveru na segmentu WAN1_Network na FTP server běžící v segmentu Internal.

Pokus o přenesení byl zastaven, došlo k odhalení škodlivého kódu a operaci kopírovaní nebylo možno dokončit. V logu antiviru byla zapsána zpráva:

```
Sub Type: Malware
Severity: High
Message: EICAR.AV.Test.File.Transfer.
Action: Block
Filter: Antivirus_Scan
Dst port: 21
Src add: 192.168.2.2
Dst add: 192.168.1.2
```

3.3.2 Test kontroly aplikací

Konkrétně bylo testováno pravidlo pro blokování peer-to-peer spojení. Pro testování byl využit program DC++, který umožňuje offline sdílení souborů na lokální síti. Po nastavení programu a nasdílení požadovaného souboru byl proveden pokus o přenos mezi dvěma stanicemi.

Navázání spojení muselo být vedeno ze stanice s IP adresou 192.168.1.100 a směrován na adresu 192.168.2.2, jelikož peer-to-peer spojení z definovaných administrátorských adres je povoleno.

Pokus o spojení byl detekován a byla vygenerována poplašná zpráva:

```
Sub Type: Application
Severity: User-defined rule
Message: Strong.DC.++.Attempt.To.Estabilish.P2p.Connection.
Action: Block
Filter: block-p2p
Src add: 192.168.1.100
Dst add: 192.168.2.2
```

3.3.3 Denial of Services

K provedení DoS útoky byl využit program LOIC, který je schopen simulovat požadované množství virtuálních stanic, ze kterých jsou následně k cíli zasílány zvolené požadavky.

V případě testovací sítě byl útok proveden z počítače s IP adresou 192.168.1.100, připojenou do segmentu intertal a za cíl byla zvolena stanice s adresou 192.168.2.2 na segmentu WAN1_Network.

Obr. 3.15: Nastavení DoS útoku

Program vysílal neúplné požadavky na TCP spojení směrované na port 80. Tato konfigurace simuluje např. pokus o přihlášení k webovému rozhraní konkrétního síťového prvku. Počet virtuálních stanic byl nastaven na 30 (obr. 3.15).

Po zahájení útoku IPS senzor po překročení limitní hodnoty okamžitě rozpoznal, že se jedná o útok, a komunikaci zastavil. Konkrétně se jednalo o případ, kdy byla kontrolována položka ip_src_session s hraniční hodnotou 5000 příchozích požadavků o TCP spojení (viz obr 3.7).

Date	Level	UTM Type	Message	Src	Dst	Dst Port
2012-05-17		Attack	ip_src_session, 5226 > threshold 5000, repeats 53 times	192.168.1.100	192.168.2.2	80
2012-05-17		Attack	ip_src_session, 5173 > threshold 5000, repeats 172 times	192.168.1.100	192.168.2.2	80
2012-05-17		Attack	ip_src_session, 5001 > threshold 5000, repeats 6 times	192.168.1.100	192.168.2.2	80

Log location: Disk 1 / 47

Date Time	2012-05-17 04:43:12	**Date**	2012-05-17
Time	04:43:12	**Level**	alert
Sub Type	anomaly	**ID**	18432
Policy ID	0	**Serial Number**	0
Attack ID	16777322	**Severity**	critical
Carrier End Point	n/a	**Profile Name**	n/a
Sensor	stop_flood	**Src**	192.168.1.2
Message	anomaly: ip_src_session, 5226 > threshold 5000, repeats 53 times	**Identity Index**	0
Profile type	n/a	**Profile Group Name**	n/a
Attack Name	ip_src_session	**UTM Type**	Attack

Obr. 3.16: Výpis z logu firewallu 1 po rozpoznání DoS útoku

Výsledkem bylo přesunutí útočníkovy IP adresy na tzv. blacklist, seznam zakázaných IP adres, a byl mu tedy odepřen přístup do sítě.

Následně byl útok proveden současně ze dvou fyzicky přítomných stanic. Parametry útoku byly ponechány na stejných hodnotách, pouze počet virtuálních počítačů byl zvednut na 60. V tomto případě, než opět došlo k odpojení obou útočících stanic ze sítě, bylo na firewallu 1 patrné, že nezvládá kontrolovat veškerý provoz a po krátkou dobu dochází k zahlcení cílové stanice.

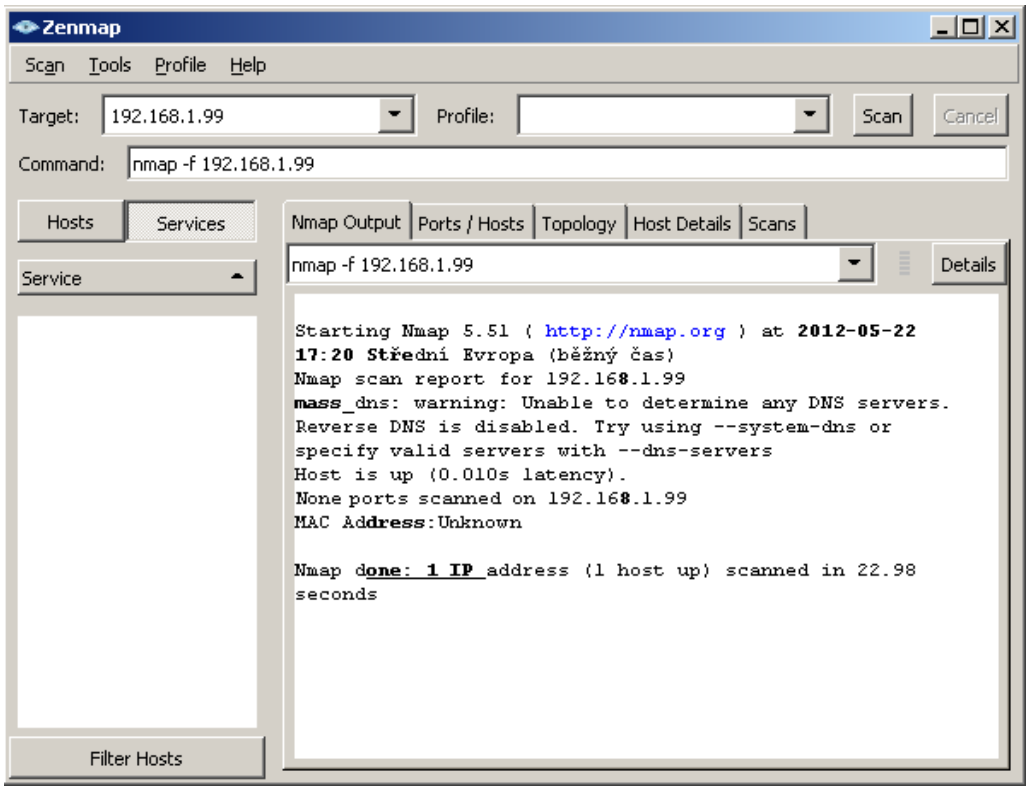
3.3.4 Mapování síťových prvků

K zmapování firewallu 1 byl použit freeware program nmap. Ten podporuje některé techniky, které mají za úkol obejít firewall a zmapovat daný prvek v síti, konkrétně jeho MAC adresu, otevřené porty a běžící služby. Příkazem

```
nmap -f 192.168.1.99
```

se provedla instrukce pro zasílaní fragmentů paketů na cílovou stanici s IP adresou 192.168.1.99 (obr. 3.17). Pokud není specifikovaný rozsah skenovaných portů, jsou zkoumány všechny.

Z obr. 3.17 je patrné, že skenování příslušných údajů nebylo možné dokončit. Intrusion prevention system tedy úspěšně odhalil pokus o zmapování a nebezpečnou akci zastavil dříve, než mohla být dokončená.



Obr. 3.17: Výsledky skenování firewallu 1

IPS běžící na firewallu 1 ovšem na tento provoz zareaguje, jelikož se jedná o anomálii, která může poskytnout potřebné údaje pro budoucí útoky. IP adresa stanice, ze které bylo skenování prováděno, je přidána na seznam zakázaných adres a vygeneruje se poplašná zpráva:

```
Sub Type: Anomaly
Severity: Medium
UTM Type: Attack
Attack ID: 2643587
Message: Detection.Network.Scan.repeats.6times.
Sensor: Protect_host Action: Block
Filter: Protect_host
Src add: 192.168.1.100
Dst add: 255.255.255.255
```

K mapování byly využity další metody:

- zasílání paketů o nestadardní velikost MTU,
- použití návnady,
- přidávání vlastní dat,

- zasílání paketů s chybným kontrolním součetem.

V každém případě došlo k odhalení činnosti programu nmap a provoz byl vždy zakázán.

3.3.5 ARP poisoning

Tento útok byl proveden dvakrát. Jednou ze segmentu internal, za využití linuxové distribuce Backtrack, a podruhé na segmentu WAN1_Network pomocí programu Cain & Abel.

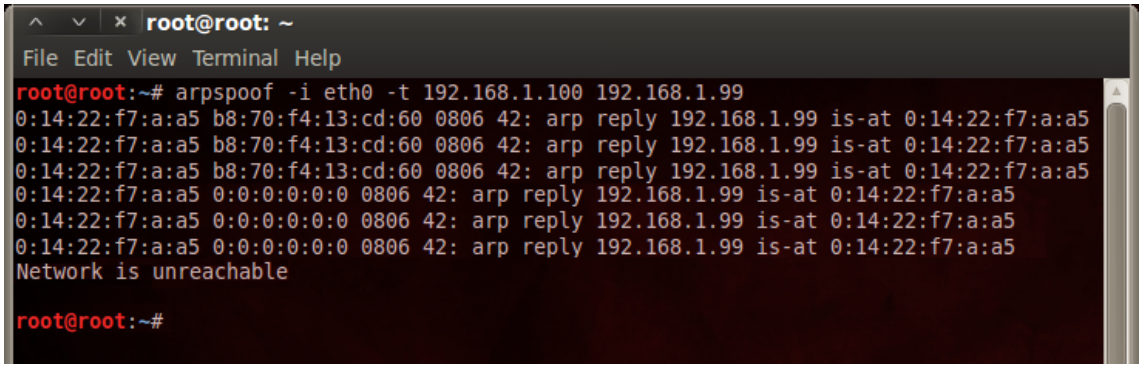
Útok ze segmentu internal byl uskutečněn pomocí skriptu arpspoof, umožňujícího přesměrovat pakety z označeného cíle, nebo cílů na další stanici na přepínané LAN síti (viz kapitola 2.3.3).

Příkaz:

```
arpspoof -i eth0 -t 192.168.1.100 192.168.1.99
```

specifikuje rozhraní, přes které probíhá odposlech provozu. Parametr -t upřesní IP adresu odposlouchávané stanice. Pakety budou zachytávány, pokud jsou směrovány na výchozí bránu, tedy 192.168.1.99.

V tomto případě by bylo možné zachytit komunikaci směřující kamkoli mimo přepínanou síť, ve které se oběť útoku nachází.



Obr. 3.18: Průběh ARP poisoningu

Z obr. 3.18 je patrné, že systém prevence podvrženou komunikaci odhalil téměř okamžitě. Výsledkem opět bylo zakázání útočníkovy IP adresy a vygenerování poplašné zprávy s parametry:

```
Sub Type: Anomaly
Severity: Critical
UTM Type: Attack
Attack ID: 1544788
Message: Invalid.ARPs.on.WAN1.repeats.4times
Sensor: Protect_host Action: Block
Filter: Protect_host
Src add: 192.168.1.100
```

Podruhé byl útok cíleně prováděn na segmentu WAN1_Network. Provoz zde není kontrolován IPS senzorem a celková bezpečnost tohoto segmentu je limitována velmi omezenými možnostmi použitého směrovače.

K provedení ARP poisoningu byl využit program Cain & Abel, který je schopen odhalit přítomné stanice v síti a nahradit jejich ARP tabulku takovými hodnotami, aby požadovaný provoz byl směrován přes útočníkovu stanici.

Status	IP address	MAC address	Packets ->	<- Packets	MAC address	IP address
Poisoning	192.168.2.1	001C0EDA3DC1	56	53	B870F413CD60	192.168.2.3

Status	IP address	MAC address	Packets ->	<- Packets	MAC address	IP address
Half-routing	192.168.2.3	B870F413CD60	1	0	001C0EDA3DC1	107.6.133.250
Half-routing	192.168.2.3	B870F413CD60	3	0	001C0EDA3DC1	195.39.12.115

Obr. 3.19: Průběh útoku ARP poisoning

Do segmentu WAN1_Network byly připojeny dvě stanice s IP adresami 192.168.2.2-3 a na směrovači 1 byl ponechán otevřený port 23 z důvodu odposlechu. Ze stanice 192.168.2.2 byl následně útok proveden.

Po úspěšném odhalení potřebných stanic je ARP tabulka stanice 192.168.2.3 nahrazena novou, kde původní MAC adresa rozhraní 192.168.2.1 (00:1C:0E:DA:3D:C1) je změněna na MAC adresu útočníkovy síťové karty, tedy B8:70:F4:13:CD:60 (viz obr. 3.19). Veškerý provoz prochází přes útočníkovu stanici a teprve následně je posílán na požadované rozhraní.

V případě vytvoření TCP spojení na portu 23 (telnet) je provoz z napadené stanice velmi jednoduché rozšifrovat, jelikož datový tok není za použití tohoto protokolu šifrován. Z vygenerovaného textového souboru je následně možné vyčíst veškeré přihlašovací údaje použité pro vzdálené přihlášení ke směrovači 1. Výpis ze souboru vypadá následovně:

```
User Access Verification(port:23 protocol:telnet)
Password: admin
Router> en
Password: admin
Router#conf t

Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# exit
Router# exit
```

Opatření

Částečnou ochranu proti změně ARP tabulky dokáže poskytnout ARP access-list. Jedná se o soubor pravidel, která jsou aplikována na konkrétní rozhraní a v nichž jsou pevně přiřazené IP adresy jednotlivých stanic k MAC adresám. Když se tyto dva údaje neshodují, je paket zahozen. Nevýhoda spočívá v tom, že nelze tento proces zvolit dynamicky. Veškeré nové údaje musí jednotlivě přidávat správce.

V případě větších sítí, je statické řešení velmi nepraktické. Vhodným opatřením je na požadované místo umístit IPS senzor, který dané anomálie provozu detekuje a zastaví.

4 ZÁVĚR

Většina dnešních firem stále preferuje nasazování pouze základních bezpečnostních mechanizmů, které představují různé druhy antivirů a firewallů. Ty jsou schopny chránit síť proti běžným a jednodušším útokům. Proti nově vznikajícím a stále modifikovanějším útokům však již síť ochránit nedokáží. Pro vytvoření komplexního bezpečnostního návrhu je proto nutné počítat i s pokročilými prvky prevence, jako jsou systémy detekce a prevence průniku.

V případě zjednodušené testovací sítě hlavní bezpečnostní prvek představoval hraniční firewall, který by následně sloužil i jako vstupní brána do sítě internet. Právě na tomto síťovém prvku běžel systém IPS.

Návrh bezpečnosti byl převážně zaměřen na ochranu proti jednotlivým útokům a úniku důležitých dat mimo lokální síť. V době testování nebylo možno navrženou síť připojit k internetu, z toho důvodu nebylo možno tato nastavení důkladně otestovat.

Testování nakonfigurovaných bezpečnostní prvků bylo prováděno odhalováním podezřelé činnosti na lokální síti. Z dosažených výsledků je patrné, že systémy prevence průniku jsou schopny valnou část nebezpečné komunikace zavčasu identifikovat a zastavit. Tímto byla dokázána nezbytnost jejich nasazení v sítích obsahujících důvěrná data.

Ovšem ani tyto systémy nejsou schopny poskytnou stoprocentní bezpečnost. Jelikož jejich činnost je zaměřena pouze na kontrolu provozu na síti, nejsou schopna odhalit útoky využívající např. chyb v programovacích jazycích. Tyto útoky nebyly testovány – jejich rozsah přesahuje zadání bakalářské práce. Protože v testovací síti neexistovalo připojení k internetu, možnosti simulování ohrožení lokální sítě zvenčí byly výrazně limitovány.

Slabý bezpečnostní článek sítě představoval použitý směrovač. I při využití obranných mechanizmů, které poskytoval, nebyl schopen odhalit jednoduchý útok Man in the middle. Jedná se o směrovač, který se svou podstatou hodí převážně k nasazení do domácích sítí. Ve rozsáhlejších firemních sítích by měl být nahrazen výkonnějším směrovačem, poskytujícím pokročilejší možnosti bezpečnostní konfigurace.

LITERATURA

[1] THOMAS, M. *Zabezpečení počítačových sítí bez předchozích znalostí*. David Krásenský. Brno : CP Books,a.s., 2005. 338 s. ISBN 80-251-0417-6.

[2] SURAPATI, Taufan. *How Antivirus Works: Signature Based Detection, Heuristic Scanning and Behavior Blocker* [online]. 13. 8. 2011. [cit. 15-10-2011]. Dostupné z: http://www.articlesbase.com/security-articles/how-antivirus-works-signature-based-detection-heuristic-scanning-and-behavior-blocker-5124641.html.

[3] BORG, Oliver. *Anti-spam and spam filtering techniques* [online]. 11. 9. 2008. [cit. 15-10-2011]. Dostupné z: http://www.allspammedup.com/anti-spam/.

[4] LASEK, Petr. *Intrusion prevention system - nová kategorie bezpečnostního řešení* [online]. 2005. [cit. 15-10-2011]. Dostupnéz: http://www.systemonline.cz/clanky/intrusion-prevention-system.htm.

[5] WILKINS, Sean; SMITH, Franklin H. *CCNP security secure 642-637 official cert guide*. Indianapolis, IN: Cisco Press, 2011. s. ISBN 1587142805.

[6] KUCHAR, Martin. *Firewall - obrňte své počítače...* [online]. 2. 2. 2005. [cit. 15-10-2011]. Dostupné z: http://pctuning.tyden.cz/software/ochrana-pocitace/4296-firewall-obrnte_sve_pocitace.

[7] DUBRAWSKY, Ido. *Firewall Evolution - Deep Packet Inspection* [online]. 2. 11. 2010. [cit. 15-10-2011]. Dostupné z: http://www.symantec.com/connect/articles/firewall-evolution-deep-packet-inspection.

[8] *Firewalls* [online]. 2002. [cit. 22-10-2011]. Dostupné z: http://www.vicomsoft.com/learning-center/firewalls/.

[9] ENDORF, F. Carl. *Intrusion Detection and Prevention* [online]. 2005. [cit. 3-2-2012]. Dostupné z: http://books.google.cz/books?id=AWYduASeDlEC&lpg=PP1&pg=PP1#v=onepage&q&f=false.

[10] PAQUET, Catherine. *Implementing Cisco IOS Nework Security*. Cisco Press, Indianapolis, 17. 4. 2009. 624 s. ISBN-10: 1-58705-815-4, ISBN-13: 978-1-58705-815-8.

[11] *Intrusion Prevention Sysem (IPS)* [online]. 1. 2004. [cit. 3-2-2012]. Dostupné z: http://hosteddocs.ittoolbox.com/BW013004.pdf.

[12] CARFONE, Karen; MELL Peter. *Guide to Intrusion Detection and Prevention Systems (IDPS)* [online]. 2. 2007. [cit. 5-2-2012]. Dostupné z: http://csrc.nist.gov/publications/nistpubs/800-94/SP800-94.pdf.

[13] TIMOFTE, Jack. *Wireless Intrusion Prevention System* [online]. 2008. [cit. 4-2-2012]. Dostupné z: http://revistaie.ase.ro/content/47/23Timofte.pdf.

[14] KAUN, Chia Chee. *Understanding Wireless Intrusion Prevention Systems* [online]. 14. 2. 2011. [cit. 4-2-2012]. Dostupné z: http://www.networkworld.com/news/tech/2011/021411-wireless-intrusion-prevention.html.

[15] DRUM, Robert. *IDS andd IPS placement for Network Protection* [online]. 26. 3. 2006. [cit. 6-2-2012]. Dostupné z: http://www.infosecwriters.com/text_resources/pdf/IDS_Placement_RDrum.pdf.

[16] *Enterprise-class IPS* [online]. 2011. [cit. 24-5-2012]. Dostupné z: http://www.paloaltonetworks.com/products/features/ips.html.

[17] WEBER, Filip. *Denial of Service* [online]. 16. 4. 2008. [cit. 17-10-2011]. Dostupné z: http://www.svetsiti.cz/clanek.asp?rid=14&cid=2121.

[18] WEBER, Filip. *Denial of Service* [online]. 9. 4. 2008. [cit. 17-10-2011]. Dostupné z: http://www.svetsiti.cz/clanek.asp?cid=2128.

[19] *Už víte, co je to DoS. Tak teď se naučte bránit* [online]. 5. 7. 2001. [cit. 17-10-2011]. Dostupné z: http://www.zive.cz/clanky/uz-vite-co-je-to-dos-tak-ted-se-naucte-branit/sc-3-a-101772/default.aspx.

[20] KOST, Stephen *An Introduction to SQL Injection Attacks for Oracle Developers* [online]. 3. 2007. [cit. 10-3-2012]. Dostupné z: http://www.integrigy.com/security-resources/whitepapers/Integrigy_Oracle_SQL_Injection_Attacks.pdf.

[21] BURDA, Karel. *Bezpečnost Informačních Systémů* [online]. Brno: VUT. 1. 11. 2005, [cit. 10-3-2012]. Dostupné z: https://www.vutbr.cz/www_base/priloha.php?dpid=23579.

[22] EVANS, Keatron. *Advanced Tutorial: Man in the Middle Attack Using SSL Strip – Our Definitive Guide* [online]. 19. 11. 2010. [cit. 10-3-2012]. Dostupné z: http://resources.infosecinstitute.com/mitm-using-sslstrip/.

[23] SANDERS, Chris. *Understanding Man-In-The-Middle Attacks - Part 4: SSL Hijacking* [online]. 6. 9. 2010. [cit. 10-3-2012]. Dostupné z: http://www.windowsecurity.com/articles/Understanding-Man-in-the-Middle-Attacks-ARP-Part1.html.

[24] SANDERS, Chris. *Understanding Man-in-the-Middle Attacks – ARP Cache Poisoning* [online]. 17. 03. 2010. [cit. 19-10-2011]. Dostupné z: http://www.windowsecurity.com/articles/understanding-man-in-the-middle-attacks-arp-part1.html.

[25] SANDERS, Chris. *Understanding Man-In-The-Middle Attacks – DNS Spoofing* [online]. 17. 03. 2010. [cit. 19-10-2011]. Dostupné z: http://www.windowsecurity.com/articles/Understanding-Man-in-the-Middle-Attacks-ARP-Part2.html.

[26] SANDERS, Chris. *Understanding Man-In-The-Middle Attacks – Session Hijacking* [online]. 05. 03. 2010. [cit. 19-10-2011]. Dostupné z: http://www.windowsecurity.com/articles/understanding-man-in-the-middle-attacks-arp-part3.html.

[27] *Cisco 2Q11 Global Threat Report* [online]. 7. 2011. [cit. 1-4-2012]. Dostupné z: http://www.cisco.com/en/US/prod/collateral/vpndevc/cisco_global_threat_report_2q2011.pdf.

[28] *Trustwave 2012 Global Security Report* [online]. 2012. [cit. 1-4-2012]. Dostupné z: https://www.trustwave.com/downloads/Trustwave_WP_Global_Security_Report_2012.pdf.

[29] UPADHAYA R. Gaurb. *Best Practices in IPv4 Anycast Routing* [online]. [cit. 25-5-2012]. Dostupné z: http://ws.edu.isoc.org/data/2006/1903640847448cf92da5f07/060515.AfNOG-DNS-anycast.pdf .

[30] *Security Threat Report 2012* [online]. 2012. [cit. 25-5-2012]. Dostupné z: http://www.sophos.com/en-us/medialibrary/PDFs/other/SophosSecurityThreatReport2012.pdf.

[31] *DDoS attacks in Q2 2011* [online]. 2012. [cit. 1-4-2012]. Dostupné z: http://www.securelist.com/en/analysis/204792189/DDoS_attacks_in_Q2_2011.

SEZNAM ZKRATEK

ACL Access list

APT Advanced Persistent Threats

ARP Adress Resolution Protokol

CPU Central Processing Unit

DDoS Distributed Denial of Service

DMZ Demilitarized Zone

DNS Domain Name System

DoS Denial of Service – Odmítnutí služby

FTP File Transfer Protocol

HIPS Host-based Intrusion Prevention System

HTTP HyperText Transfer Protocol

HTTPS HyperText Transfer Protocol Secure

ICMP Internet Control Message Protocol

IDS Intrusion Detection System

IMAP Internet Message Access Protocol

IMAPS Internet Message Access Protocol Secure

IP Internet Protocol

IPS Intrusion Prevention System

ISO-OSI International Organization for Standardization-Open Systems Interconnection

MAC Media Access Control

MITM Man In The Middle

MTU Maximum Transmission Unit–Maximální přenosová jednotka

NIPS Network-based Intrusion Prevention System

OS Operační Systém

OSPF Open Shortest Path First

PEAP Protected Extensible Authentication Protocol

POP3 Post Office Protocol v3

POP3S Post Office Protocol v3 Secure

QoS Quality of Service–kvalita služeb

RPF Reverse Path Forwarding

SMLI Stateful Multi-Layer Inspection

SMTP Simple Mail Transfer Protocol

SSH Secure SHell

SSL Secure Socket Layers

TCP Transmission Control Protocol

UDP User Datagram Protocol

VLAN Virtual Local Area Network

VPN Virtual Private Network

WIPS Wireless-based Intrusion Prevention System

SEZNAM PŘÍLOH

A OBSAH CD

- Konfigurační soubor firewallu 1
- Konfigurační soubor směrovače 1