UNIVERZITA PARDUBICE
Fakulta elektrotechniky a informatiky

Penetrační testy zabezpečené sítě pomocí IPS

Jaroslav Brabenec

Bakalářská práce
2015

Univerzita Pardubice
Fakulta elektrotechniky a informatiky
Akademický rok: **2013/2014**

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Jaroslav Brabenec**
Osobní číslo:	**I10017**
Studijní program:	**B2646 Informační technologie**
Studijní obor:	**Informační technologie**
Název tématu:	**Penetrační testy zabezpečené sítě pomocí IPS**
Zadávající katedra:	**Katedra informačních technologií**

Zásady pro vypracování:

Autor v bakalářské práci popíše způsob nasazení systému IPS. V práci bude popsán rozsah zabezpečení sítě při použití systému IPS. V praktické části navrhne a provede penetrační testy systému IPS v laboratorním prostředí na navržené síti. Součástí práce budou přesné postupy a výsledky penetračních testů.

Rozsah grafických prací:

Rozsah pracovní zprávy:

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

Seznam odborné literatury:

SELECKÝ, Matúš. Penetrační testy a exploitace. Computer Press, 2012. ISBN 978-802-5137-529.
CARTER, Earl a Jonathan HOGUE. Intrusion prevention fundamentals. Indianapolis, IN: Cisco Press, c2006, xxiii, 287 p. ISBN 15-870-5239-3.

Vedoucí bakalářské práce: **Ing. Soňa Neradová**
Katedra softwarových technologií

Datum zadání bakalářské práce: **20. prosince 2013**
Termín odevzdání bakalářské práce: **9. května 2014**

L.S.

prof. Ing. Simeon Karamazov, Dr.
děkan

Ing. Lukáš Čegan, Ph.D.
vedoucí katedry

V Pardubicích dne 31. března 2014

Prohlašuji:

Tuto práci jsem vypracoval samostatně. Veškeré literární prameny a informace, které jsem v práci využil, jsou uvedeny v seznamu použité literatury.

Byl jsem seznámen s tím, že se na moji práci vztahují práva a povinnosti vyplývající ze zákona č. 121/2000 Sb., autorský zákon, zejména se skutečností, že Univerzita Pardubice má právo na uzavření licenční smlouvy o užití této práce jako školního díla podle § 60 odst. 1 autorského zákona, a s tím, že pokud dojde k užití této práce mnou nebo bude poskytnuta licence o užití jinému subjektu, je Univerzita Pardubice oprávněna ode mne požadovat přiměřený příspěvek na úhradu nákladů, které na vytvoření díla vynaložila, a to podle okolností až do jejich skutečné výše.
Souhlasím s prezenčním zpřístupněním své práce v Univerzitní knihovně.

V Pardubicích dne 18. 4. 2015

Jaroslav Brabenec

Rád bych poděkoval vedoucí práce Ing. Soni Neradové za vstřícný přístup a cenné rady při zpracovávání bakalářské práce. Zvláště při odborných částech síťové bezpečnosti.

ANOTACE

Práce se zaměřuje na penetrační testování sítí zabezpečené pomocí systémů IPS. Principy použité při testování, ale také pohled ze strany útočníka. Hlavní část je věnována tvorbě pravidel pro zabezpečení simulovanými útoky.

KLÍČOVÁ SLOVA

IPS, IDS, Snort, Exploitace, Penetrační testy

TITLE

Penetration testing networks secured by IPS

ANNOTATION

The thesis focuses on penetration testing of networks secured by IPS. It also deals with the testing principles and the hacker's point of view. The main part concerns creation of security rules by means of simulated attacks.

KEYWORDS

IPS, IDS, Snort, Exploit, Penetration testing

OBSAH

SEZNAM OBRÁZKŮ

ÚVOD

Každodenní rozvoj v oboru informačních technologií přináší nové, propracovanější zařízení, metodiky kladoucí důraz na zabezpečení systému. S příchodem těchto prvků však vznikají i nové způsoby, které mohou vést k bezpečnostním hrozbám. Zanedbání tohoto faktoru může vést k nevyčíslitelným škodám, ať již znepřístupněním služby či ztrátou citlivých dat.

Většina uživatelů si ani neuvědomí, jaká rizika přináší připojení k internetu. Proto je dobré nebrat zabezpečení na lehkou váhu.

Cílem uvedené práce je zaměření se na bezpečnostní zařízení v podobě detekujících a prevenčních systémů.

První kapitola se zabývá základními prvky penetračního testování a používanými principy. Rozsáhlost tématu je široká, proto je zaměřena pouze na základní části.

Velice zajímavou část pro administrátora nebo jeho protivníka – hackera tvoří exploitace. Možné postupy a způsoby prolomení systému jsou důležité i pro správce sítě. Nejlepší cestou, jak tvořit dostatečného zabezpečení, je hledání dosavadních mezer obranného systému.

Předposlední kapitola je věnována IPS systémům neboli systémům prevence průniku. V dnešní době jsou pro běžné uživatele neznámé, ale v případě dobrých znalostí tvorby pravidel a způsobů útoků je možné dosáhnout celkového přehledu nad komunikací uvnitř sítě.

Využití uvedených aplikací pro základní kroky penetračního testování tvoří poslední část.

1 PENETRAČNÍ TESTOVÁNÍ

Hlavním úkolem penetračních testů je praktické ověření bezpečnosti sítě nebo systému. Průběh testování je založen na simulaci útočníka s cílem využít zranitelnost prvků pro napadení sítě. Penetrační testování (PT) je prevence před možnými útoky, zjištění chyb, sledování stavu bezpečnosti a v neposlední řadě zjištění optimalizace na dostatečné zabezpečení. Je to jediný způsob, jak odhalit bezpečnostní mezery v síti.

Mezi první kroky PT patří mapování informačního systému a zjištění největšího množství informací o topologii sítě, její infrastruktuře a využitých systémů. Scanning – neboli skenování se využívá ke zjištění dat na síťové a transportní úrovni, které nám umožní zmapovat aktivní zařízení. Sběr dat o testovaném informačním systému je velice důležitý, protože každou novou informací se může naskytnout další nezabezpečený přístup do systému.

Hlavním rozdělením PT je typ přístupu k informačnímu přístupu. Ve většině případů jsou útoky vedeny z Internetu, tedy z oblasti mimo testovanou síť, jsou označovány jako externí. Testování pouze útoku zvenčí by ale nemělo značného významu, kdyby byl útočník uživatelem testovaného systému, a tím měl i přístup za firewall nebo výstupní zařízení komunikující ze sítě. Jednalo by se z pohledu útočníka o interní útok. Tyto dva druhy testování se od sebe liší, ať už využitými prostředky, tak způsobem provádění testování.

1.1 Typy testů dle metodik

Penetrační testování obsahuje více druhů metodik, které jsou rozděleny na určité fáze, obvykle obsahují 4 - 7 částí. K cíli testování budou dostatečné 4 fáze.

1.1.1 Určení cílů testování

V prvním kroku je důležité určení cílů testování a směr dosažení výsledků. Není z praktického hlediska možné otestovat všechny možnosti. Proto je nutné si v prvním kroku vybrat dané cíle, které mohou zahrnovat prvky od stability sítě, zabezpečení přístupu až po omezení provozu.

1.1.2 Sběr informací

Před exploitací a skenováním je potřeba zjistit řadu informací o přístupu do sítě, odkud budeme síť testovat (grey-box, black-box, white-box). Dle daného přístupu se volí typy penetračních aplikací pro ideální využití. Během této fáze je zapotřebí zjistit o systému nejvíce obecných informací (jaké využívá zařízení, operační systémy či strukturu sítí). [3]

1.1.3 Exploitace & scanning

Nejrozsáhlejší fáze není pro všechny systémy jednotná a obsahuje velké množství možností, jaké kroky zvolit pro nejlepší výsledky. Prioritně se zaměřuje na získání přístupu do sítě nebo systému, ať už v podobě získání důvěrných informacích o uživatelích, údajů k přihlášení nebo až do míry znepřístupnění plněné služby.

Během stálého vývoje informačních technologií se zlepšuje zabezpečení, ale také vznikají i možnosti prolomení daného systému. Nekvalitní zabezpečení může vést k nevyčíslitelným škodám v podobě získání dat neoprávněnou osobou, znepřístupnění služby a spousty dalších.

Obecně je možné o této fázi mluvit jako o testování zabezpečení systému.

1.1.4 Sumarizace výsledků

Posledním krokem je shrnutí výsledků všech předchozích fází. Při firemních zakázkách obsahuje ve většině případů návrh řešení pro vyřešení zjištěných problémů.

1.2 Typy testů dle provedení

1.2.1 Manuální

Jsou prováděny testerem nebo jejich skupinou, která dokáže zpracovat kvalitu testů do více přijatelné podoby. Tuto možnost nám automatizované testy ve většině případů nenabídnou. Výhodou můžeme označit také způsob zpracování, jelikož tester musí detailně znát způsob provádění testů a principy, na kterých testování probíhá. Report z testu tak dokáže zpracovat a popsat problematiku jiným vrstvám podniku, bez kompletní znalosti z daného segmentu. Mezi nevýhody jsou zařazeny nutná rozsáhlá znalost testerů a vysoká časová náročnost.

1.2.2 Automatizované

Na rozdíl od manuálních testů mají výhodu ve zpracování a rychlejším zpracování. Jsou zde používány ověřené nástroje přímo určené pro testování nebo exploitaci. Pro osobu provádějící testování je jednodušší způsob využít přímo připravených aplikací a procedur, než provádět každý krok manuálně. Tím se testy stávají mnohem méně časově náročné. Zde je však důležité mít alespoň základní znalost o testech.

1.2.3 Semiautomatizované

Jedná se o kombinaci automatizovaných a manuálních testů, kdy jsou skloubeny výhody a nevýhody pro ideální využití testů.

1.3 Typy testů dle úrovně znalostí o informačním systému

1.3.1 Black-box

V překladu „černá skříňka“ už označuje případ simulace přístupu útočníka, který zná z počátku pouze možné vstupy do sítě či aplikace. Tento nejpoužívanější typ testů je označován pro testera v případě nevědomosti o vnitřních strukturách informačního systému a topologii. Není zapotřebí znalost programovacího jazyka ani zdrojových kódů. Každý test se však liší s důvodem rozdílnosti sítí.

1.3.2 White-box

Testování vnitřní struktury sítě je značně komplikované, protože se využívá znalosti všech interních informací, a tím se rozsáhlost testovaných částí značně rozšiřuje. Od black-box testů se liší dostupností všech vstupních informací do sítě.

1.3.3 Grey-box

Během testování se využívá znalostí vnitřní struktury, ale z pohledu vnějšího útočníka (testera). Je to kombinace White-box a Black-box testů. [3]

1.4 Firewall

V překladu „bezpečnostní brána“, je hardwarový nebo softwarový prvek odstraňující nepotřebný provoz mezi sítěmi. Komunikaci odděluje na základě vstupních nebo výstupních pravidel. Definicí těchto pravidel odstraní přístup neoprávněných uživatelů do sítě. Některé druhy firewallů umožňují monitorování komunikace, detekci a upozornění na nežádoucí provoz. Instalací firewallu společně s antivirovým softwarem je jedním z nejzákladnějších kroků pro vytváření zabezpečení systému ať už ve firemní tak soukromé síti.

Hraniční firewall ve většině případů odvrátí útoky z vnější sítě, ale v dnešní době hackeři využívají technik, přes které dokáží obejít i toto zabezpečení.

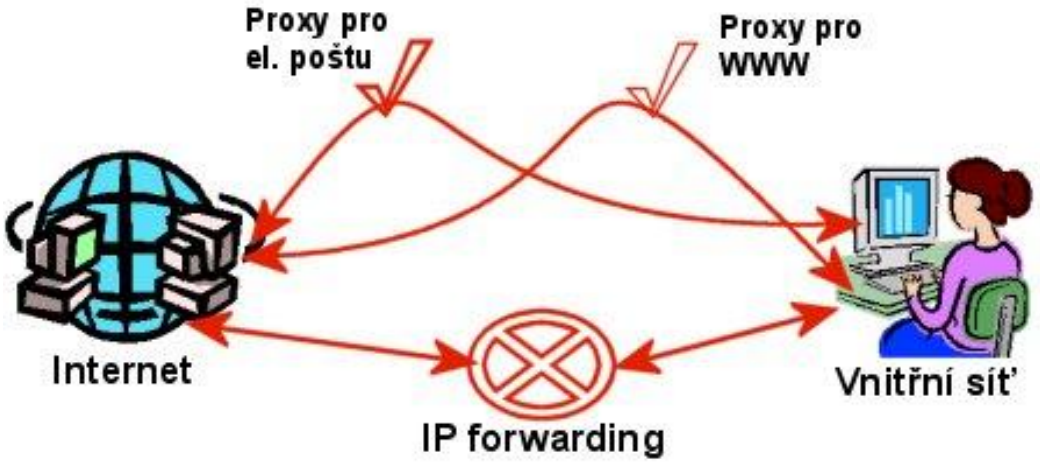
Obrázek 1 Firewall

Zdroj: (CloneGuard, 2013)

1.4.1 Paketové filtry

Paketové filtry představují nízkou úroveň zabezpečení, jelikož kontrolují pouze zdrojovou a cílovou IP adresu s porty. Pracují na třetí a čtvrté vrstvě OSI modelu. Nevýhodu slabého zabezpečení nahrazují vysokou rychlostí, proto se používají jako hraniční, kdy odfiltrují většinu nepovolených přístupů. Zástupcem paketových filtrů je například ACL, jenž bude představen v další části.

1.4.2 Aplikační brány



Obrázek 2 Proxy brána

Zdroj: (Pctuning, KUCHAŘ Martin, 2005)

Také nazývány jako proxy brány pracují na aplikační vrstvě. Na rozdíl od paketových filtrů veškerou komunikaci přebírá firewall. Po principiální stránce si můžeme proxy bránu představit jako klienta a server v jednom. Při komunikaci z vnitřní sítě uživatel vyšle požadavek směrem do veřejného Internetu. Vyslaná komunikace je zpracována firewallem, který si zprávu převezme a vyšle ji na cílenou adresu jako svůj požadavek. Po odpovědi ji firewall příjme, zpracuje a opět vyšle, tentokrát původnímu uživateli vnitřní sítě. Použitím proxy brány je značně vysoká bezpečnost sítě i přes značnou pomalost zařízení. Při komunikaci tedy server či venkovní uživatel nezná IP adresu žadatele, ale pouze IP adresu firewallu. Tento krok vede i k podstatně náročnějšímu skenování sítě a zjištění její topologie. Aplikační brána tedy pracuje i jako NAT.

1.4.3 Stavové paketové filtry

Pracují podobně jako klasické paketové filtry s rozdílem logování informací. Tato data pak používá k rozhodnutí, zda je již spojení povoleno nebo musí pakety znovu projít přes filtr. Stavové paketové filtry těží z rychlosti paketových filtrů a logování, které tvoří bezpečnostní část. Na rozdíl od aplikační brány nejsou tak bezpečné, ale s lehčí konfigurací.

1.4.4 Stavové paketové filtry s IDS

Systémy pro detekci útoku fungují velice podobně antivirům a s používáním signatur mohou odhalit i detailnější útoky. Nabízí vysokou bezpečnost i s přijatelnou rychlostí, i když jsou pomalejší než klasické stavové paketové filtry. [1, 2, 3, 4]

1.5 Cisco IOS Firewall

Chránění uživatelů a interních sítí je hlavním úkolem firewallu. Existuje nespočetné množství společností zabývající se bezpečností a firewallů. V našem případě preference patří firmě Cisco, která pokrývá většinové množství bezpečnostních zařízení po celém světě, jako jsou Cisco IOS firewall.

Cisco IOS Firewall (Cisco's Internetwork Operating System)

Nese označení operačního systému pracujících na většině sitchů a routrů společnosti Cisco. IOS je zpracován přímo na dané zařízení s rozsáhlými konfiguračními možnostmi. K základní konfiguraci se převážně využívá CLI – Command Line Interface (příkazová řádka). Pro přístup ke konfiguraci se často využívá konzolového portu. V případě doplňující konfigurace je možné přes telnet nebo ssh, případně přes webové rozhraní.

Rozhraní pro přístup k určitým pravomocem je rozděleno do čtyř módů:

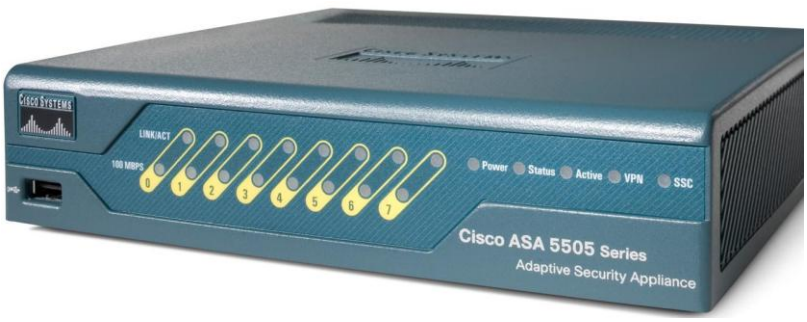
- uživatelský Switch> omezený, umístění při přihlášení

- privilégovaný Switch# výchozí mód pro konfiguraci, umožňuje zobrazení nakonfigurovaného nastavení
- globální konfigurační Switch(config)# konfigurační režim pro celý systém zařízení
- konfigurace interace Switch(config-if)# konfigurace daného interface.[5, 6, 7]

1.6 Cisco ASA (Adaptive Security Appliance)

Společnost Cisco se zabývá bezpečnostními síťovými prvky po celém světě. Mezi tyto prvky patří již zmiňovaný ASA. Je to bezpečnostní zařízení nabízející ochranu informačního systému. Použitím zařízení je tedy možné využívat jeho funkcí firewallu, VPN, antivir, antispyware a v neposlední řadě IPS. Nabízené jsou i další služby, které je v případě potřeby možné dokoupit. Moduly řady 5500 pokryjí uživatelské požadavky od základních verzí 5505, která je určena pro malé části firmy, až po super výkonnou verzi 5585. S rostoucím výkonem a vylepšenými bezpečnostními prvky se také rapidně zvyšuje cena zařízení. Cisco ASA zařízení jsou rozdělena do edic, které se zaměřují na určitou činnost v systému. (bezpečnostní brány, IPS, VPN, anti-X kontrolující emaily a weby). Podstatnou výhodu tvoří ucelením více potřebných prvků na jedné platformě. Konfigurace může probíhat pomocí ASDM (Adaptive Security Device Manager) dostupného přímo na zařízení nebo přes příkazovou řádku, která je velice podobná konfiguraci Cisco IOS. ASA pracuje ve dvou základních režimech, routovacím a transparentním. Transparentní pracuje pouze na vrstvě L2, na které filtruje provoz. V routovacím je ASA přiřazena IP adresa, přes kterou je routována komunikace zařízení v síti. V tomto režimu lze zpřístupnit funkce VPN, NAT, dynamický routing.

Ve velkém množství případů se Cisco ASA VPN používá pro vzdálený přístup do vnitřní sítě, ať už v podobě zaměstnanců firmy, tak jako Site-to-Site propojující například firemní sítě.



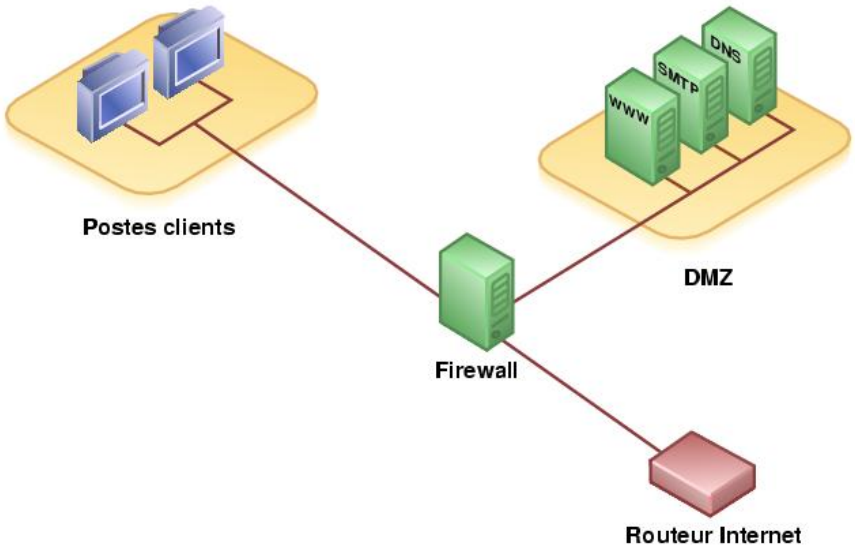
Obrázek 3 Cisco ASA

Zdroj: (Cisco)

Cisco ASA je plnohodnotným bezpečnostním prvkem, který při správné konfiguraci a návrhu sítě zajistí bezpečnost na vysoké úrovni. [9, 10, 11, 13]

1.6.1 Demilitarizovaná zóna (DMZ)

Demilitarizovaná zóna určuje rozdělení počítačové sítě za účelem zabezpečení. Do DMZ jsou ukládány zařízení provozující služby přístupné z vnější sítě Internet. Bezpečnostní hledisko zabraňuje útočníkovi přístup do dalších částí sítí. Základem je firewall, který má za úkol chránit ostatní sítě z DMZ. [12, 13, 14, 15]



Obrázek 4 Demilitarizovaná zóna

Zdroj: (Benj, 2015)

V praktickém použití se demilitarizovaná zóna používá k umístění serverů.

1.6.2 IDS (Intrusion Detection System)

Společně jako IPS, které bude představeno v další části, slouží IDS k detekování nepovolené komunikaci v systému.

Detekční systémy jsou z pravidla tvořeny těmito částmi:

- **senzory** – slouží ke snímání dat na síti, dle určeného rozhraní ke kontrole. Implementace je možná pomoci aktivních zařízení nebo softwarově. Obvykle pracují na čtvrté vrstvě OSI modelu;
- **konzole** – sesbíraná data jsou předána konzoly monitorující a shromažďující informace o veškerých síťových aktivitách;

- **jádro systému** – samotný program s vyhodnocujícími algoritmy pro zpracování. Každý nasnímaný prvek je hodnocen a porovnáván s pravidly pro třídění provozu sítě a následným generováním výstražné zprávy při neoprávněné aktivitě.

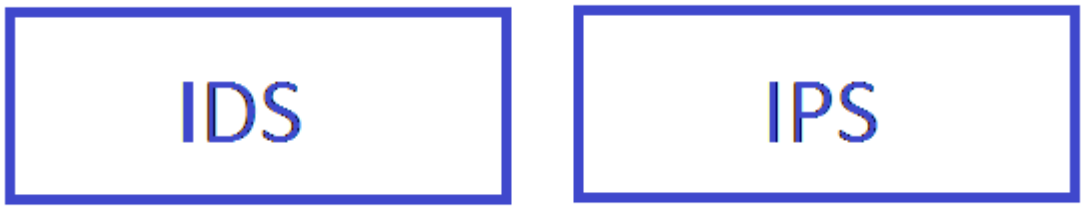
Rozdělení IDS prvků je převážně u hardwarového zařízení, kde každá jeho část splňuje přímo svoji aktivitu. Na rozdíl od softwarového řešení mohou být tyto části implementovány do jedné aplikace. Značnou výhodou SW řešení je použití volné licence. Avšak ve většině případů je systém méně kvalitní a pomalejší.

Pro domácí použití obvykle stačí antivirus s dobře nakonfigurovaným firewallem, ale pro systémy s nutností většího zabezpečení, jako jsou firemní či státní sítě a mnohé další, je potřeba odhalit případné útoky hackerů dříve, než vzniknou případné škody napadením či ukradení citlivých dat. IDS systémy jsou schopny detekovat průnik nebo jeho pokus i ve formě škodlivých kódů, které mohou přes firewall projít. Velkým krokem k vyšší bezpečnosti systému je způsob monitoringu sítě. IDS systémy totiž zkoumají komunikaci v interní síti. Takže útočník, který se dostal přes vnější zabezpečení sítě, nemá zdaleka jistotu přístupu k citlivým datům.

Architektura IDS/IPS systémů je základním stavebním kamenem při tvoření zabezpečení sítě, a to bez ohledu na její velikost. Nejlepší řešení tvoří složením individuálních zabezpečovacích prvků, aby každý pracoval na své funkci, a poté rozesílal nasbíraná data do určených skupin. Tato řešení jsou finančně náročná, proto se často kombinují.

1.7 Architektura IDS

1.7.1 Jednovrstvá



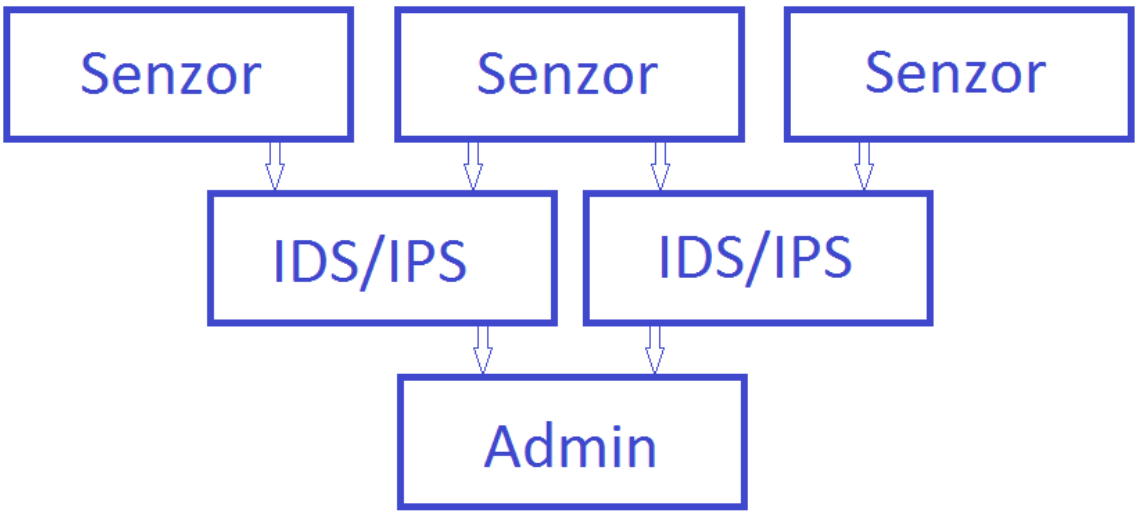
Obrázek 5 Jednovrstvá architektura

Zdroj: vlastní

Zařízení pracující v jedné vrstvě si samy zpracovávají a vyhodnocují data. Nevzniká zde komplexní ochranný systém, který je schopen sbírat data od více bezpečnostních prvků, a tím zajišťovat i vyšší zabezpečenost. Typickým příkladem je softwarové řešení prevenčního systému. Nabízí nejlevnější řešení. Existují i volně dostupné instalace pro Windows, převážně však pro unixové distribuce.

1.7.2 Vícevrstvá

Jak je popsáno u IDS systémů, realizace je tvořená senzory, konzolami, jádrem systému a dalšími doplňkovými částmi. Tyto části mohou být rozděleny po celé infrastruktuře sítě a vzájemně mezi sebou komunikovat. Výsledné zpracování přechází do komplexního opatření, jako jsou výpis administrátorovi, uložení dat do logu nebo databáze.

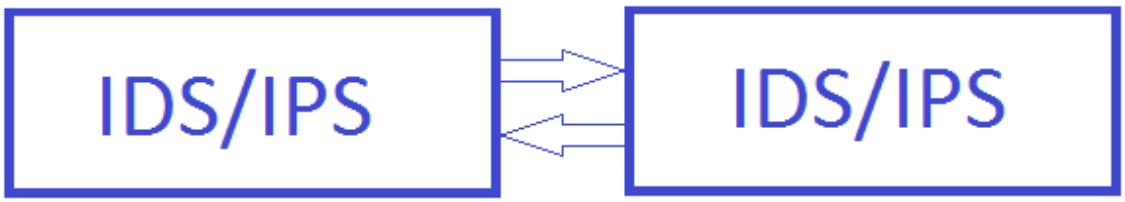


Obrázek 6 Vícevrstvá architektura

Zdroj: vlastní

1.7.3 Peer-to-peer

Bezpečnostní prvky spolupracují na stejné úrovni. Žádné ze zařízení není zvýhodněno. V reálném způsobu použití je tato architektura tvořena převážně firewally se spoluprací routrů.



Obrázek 7 Peer-to-Peer

Zdroj: vlastní

1.8 IPS (Intrusion Prevention System)

Velice blízký název napovídá podobnost IDS systémům, avšak rozdíl mezi funkcionalitou je značný. Systém prevence proniknutí neboli IPS vyniká blokováním nežádoucího přístupu, na rozdíl od IDS. Používají také rozdílné metodiky a technologie. V samotném jádru IPS dokáže rozeznat pokusy hackerů o napadení sítě nebo detekovat škodlivý kód, na které dokáže dle nastavených pravidel okamžitě reagovat a znemožnit útok v prvních částech napadení. Proto IPS systémy jsou schopny pracovat přímo se škodlivými pakety, které dokáží v daném okamžiku zpracovat. Tuto funkci nám samotné IDS nenabízejí.

IPS zařízení nemá IP ani MAC adresu, ale přitom dokáže bez přerušení či zpomalení komunikace analyzovat veškerá spojení. Reakce systémů se pohybuje v řádech mikrosekund.

Ideální IPS systém by měl defaultně obsahovat nastavené filtry v počtu několika tisíc. Filtry rozpoznávají provoz a třídí komunikaci i aplikací, která je ověřená, jelikož útočník může skrývat svůj provoz za některou z nich.

Během spuštění IPS do ostrého provozu by neměla následovat žádná konfigurace či ladění. Pouze nastavení administrátorských oprávnění a systém by měl dostatečně síť chránit. Kvalitní IPS obsahují tzv. „ karanténní část“, jenž blokuje neoprávněný přístup, ale i pracuje se zařízením generujícím škodlivý kód. Každá firma starající se o vývoj bezpečnostních systémů se liší druhy IPS, a tím i nabízí různorodost těchto zařízení. Podstatu karanténní činnosti mají však stejnou. Informovat uživatele sítě, ze které útoky mohou přicházet, blokování portů nebo přepnutí do virtuálního karanténního režimu sítě a závěrem se postarat o léčebné složky. Všechny úkony ochrany by měly pracovat automaticky bez pomoci administrátora, který dostane pouze upozornění na případný útok. Důležitou částí, která by neměla být jistě opomenuta, je aktualizace filtrů a následné uvedení do provozu bez jakékoli úpravy či výpadku zabezpečení.

Kvalitní IPS systém obsahuje při zakoupení certifikaci sloužící k ověření funkcí, které má splňovat.

1.9 Lokace IDS/IPS zařízení

Výběr správného umístění senzorů IDS/IPS je stěžejní pro správné zabezpečení systému. Nevhodné umístění může vést k bezpečnostním hrozbám sítě. Rozložení senzorů je důležité pro části obsahující kritická místa. Pro správnou funkci IPS zařízení je nutné, aby pracovala v inline módu, jenž umožňuje procházení komunikace skrze dané zařízení. Ve

všech případech je nutné pomyslet na rozsáhlost sítě včetně redundatních spojení a zvážit počet a rozložení senzorů pro snímání provozu.

1.9.1 IPS před firewall

Řešení IPS mezi vnější sítí a firewallem je výhodné pro kontrolování veškerého přístupu z internetu a odepření nežádoucího přístupu ještě před vstupem do sítě. Chráněn je tak celý prostor vnitřní sítě včetně demilitarizované zóny. Konfigurace je však značně obtížná a může vést k blokování povoleného přístupu. Ke kontrole celkového provozu je třeba velkého výpočetního výkonu. I přes tuto nevýhodu se toto schéma často používá skrze celkovou kontrolu vstupních a výstupních spojení.

1.9.2 IPS za firewallem

Velice blízkým řešením předešlé architektury je umístění prevenčního zařízení za firewall. Není nutné kontrolovat tolik dat, jelikož většinu komunikace zpracuje samotný firewall, je také možné nakonfigurovat přísnější pravidla pro přístup. IPS zařízení se tedy může zaměřit přímo na kontrolování provozu do interní sítě.

1.9.3 IPS mezi firewally

Firewallem směřujícím do externí sítě je filtrován provoz z vnější sítě. Provoz schválený přes vnější firewall je dále předán přes IPS na vnitřní firewall a vpuštěn do interní sítě. Interní firewall slouží k blokování nežádaného provozu z obou směrů vnitřní sítě. Jedná se o kombinaci dvou firewallů, s kterou značně roste i pořizovací cena.

1.9.4 VPN s IPS

Kontrolování provozu z externí sítě neboli internetu není vždy účelem IPS systému. V případě rozsáhlé firemní sítě je potřebné mít přehled o datových tocích procházejících přes VTP tunely či mosty sloužící pro propojení různých LAN sítí používaných pro spojení různých firemních poboček a center. [16, 17]

1.10 Rozdělení IPS

1.10.1 Network-based Intrusion Prevention (NIPS)

IPS systém pracuje na síťovém provozu a kontroluje rozsáhlou část sítě. NIPS umožňuje jednoduše monitorovat celou síť podle rozmístění sledovacích zařízení. Útoky vedené na jinou než monitorovanou síť však tento systém může také odhalit. Důvodem je snímání a kontrola síťových prvků, na které se útočníkova komunikace s větší

pravděpodobností dostane. Síťově založené IPS systémy nejsou schopny rozlišit šifrovaný tok dat, proto se často používají v kombinaci s HIPS.

1.10.2 Wireless Intrusion Prevention System (WIPS)

Podobně jako síťově založené prevenční systémy pracují i WIPS, s rozdílem podpory standartu 802.11, který slouží pro bezdrátovou komunikaci. Kontrola bezdrátového spojení je značně rozsáhlá. Na rozdíl od pevného připojení probíhá bezdrátová komunikace na různých kanálech. Senzory snímající aktivity se postupně přepínají na určitý kanál a snímají jejich komunikaci. Na podobném principu pracují i vyhledávače wifi zařízení nebo přístupových bodů. Přepínání může pomoci útočníkovi, který je schopen využít časového limitu, během jehož napadení není WIPS senzor přepnutý na hackerův kanál. Dostačujícím řešením zabezpečení je zařízení obsahující více bezdrátových modulů.

1.10.3 Host-based Intrusion Prevention (HIPS)

Zařízení má přístup přímo k jádru operačního systému, který umožňuje kontrolovat šifrovaný datový tok. Zabezpečenou komunikaci kontroluje na úrovni jádra, kde už data šifrovaná nejsou. HIPS se díky této vlastnosti instalují na servery používající zabezpečené síťové protokoly. Uvedený systém pracuje v rozsahu určeného zařízení a není tedy schopen analyzovat další síťovou komunikaci.

1.10.4 Network Behavior (NBA)

Patří mezi nejméně používané bezpečnostní systémy. Specializuje se na detekci různých anomálií. V případě rozpoznání ohrožujícího útoku je přístup blokován. Mezi nejběžnější anomálie můžeme zařadit IP/MAC spoofing, IP/MAC duplicita.

1.11 Signatury

Pojem Signatura může být lehce zavádějící. Signatura je popis a způsob detekující hrozbu. Jednodušeji řečeno – obsahuje prvky zjišťující přítomnost škodlivého kódu. Signatury však neřeší, jakým způsobem se bránit exploitaci. Proto se tento pojem využívá hlavně u systémů IDS.

1.12 Filtry

Programátor filtrů klade důraz na nejmenší zátěž systému, aby nedocházelo ke zpomalení systému a na zvyšování odolnosti proti útočníkům. Náročnost programování

a flexibilita jsou jedním z nejdůležitějších prvků potřebných pro tvoření filtrovacích algoritmů.

U IPS systémů se spíše vyskytuje slovo filtr, jenž obsahuje kombinaci signatur, tedy detekce hrozeb a zároveň i blokaci či bezpečnostní krok pro jejich zpracování. Důležitým pojmem u filtrací je „pruning“, jehož významem je odstranění paketů za přímého provozu na síti. V našem případě blokování paketů útočníka.

„Při psaní filtrů pro blokování musí být dodržena dvě pravidla:

- *žádná falešná pozitiva. Nikdy, za žádných okolností nesmí IPS blokovat legitimní provoz. Toto pravidlo má vždy nejvyšší prioritu.*
- *žádná falešná negativa. Nenechte projít útok, ani když se útočník intenzivně snaží vyhnout detekci. Toto má vysokou prioritu.*

Tvůrce filtrů musí mít stále na paměti tato dvě pravidla a jejich relativní prioritu. Klíčový rozdíl v přístupu k psaní signatur mezi IPS a IDS spočívá ve vzájemném pořadí těchto dvou cílů. Umění tvorby filtrů pro blokovací zařízení spočívá v co největším zobecnění logiky detekce tak, aby bylo dosaženo pravidla 2, bez porušení pravidla 1.“(SvětSítí, WEBER Filip, 7. listopad 2007)

Při vytváření filtrů se programátor musí vžít do role hackera a najít dostatek informací potřebných k úspěšnému útoku, kombinací různých metod a obměněním prvků k průniku. Všechny části jsou ukládány krok po kroku při každé změně. Seznam výsledných průniků je vyhodnocen a podle kritérií zpracován. Každý možný útok je tak popsán i s veškerými podmínkami pro možný průnik do sítě. Postupů a principů je ale mnohem více, zvláště při různorodosti IPS zařízení, pro které bude filtr určen.

Programátor musí široce rozumět technikám používaných pro útoky a předvídat, na jaké části by mohl být útok vytvořen. Plně funkční filtr vyžaduje zařízení, které je schopné pracovat ve vysoké rychlosti, aby bylo schopné analyzovat zranitelné protokoly, na kterých komunikace probíhá.

V případě útoku z vnitřní sítě z napadeného zařízení není dostačující pouze zablokování. Nutným krokem je uvést zařízení do karantény a následně odstranit škodlivý kód.

Firemní administrátoři využívají principů karantény například i pro zablokování uživatelských aplikací, které nejsou firmou schváleny. Mezi blokované obvykle patří peer-to-peer aplikace nebo různé druhy messengerů.

1.13 Kontrola paketů

Během kontroly paketů a rozhodování o přístupu do sítě mohou nastat 4 druhy výsledků, podle nichž se rozhodne o doručení paketů:

- pravdivá pozitiva – po zkontrolování je legitimní paket předán k příjemci,
- nepravdivá pozitiva – paket škodlivého kódu je vpuštěn do sítě, jelikož ho IPS nerozeznal. Stav propuštěné útočníkovi komunikace vzniká často volbou špatných signatur,
- nepravdivá negativa – uživatelsky povolený přístup je IPS systémem zamítnut,
- pravdivá negativa – útočníkovi pakety jsou úspěšně rozpoznány za závadné a zablokovány.

1.13.1 Analýza paketů dle stavových značek

Pakety jsou analyzovány a porovnávány s předem vytvořenými signaturami útoků. Zařízení paket příjme a rozeznává podle značek, zdali se nejedná o škodlivý kód. Kontrolují se hlavně pakety dle určitých portů, na které jsou poslány. Nutností systému je pravidelná aktualizace signatur, aby nedocházelo k nebezpečnému propuštění paketů. Kontrola paketů pomocí signatur je velice přesná a rychlá.

1.13.2 Analýza paketů dle definovaných pravidel

Méně používaný postup, který s kombinací dle signatur tvoří komplexnější ochranu před napadením. Pravidla jsou tvořena přímo na určitý druh útoků, jako je přetečení bufferu. V případě odhalení napadení jsou generovány zprávy. Vyžaduje vysokou přesnost na nastavení, jinak hrozí rizika označení zamítnutí komunikace legitimnímu uživateli nebo generování nespočetného množství upozorňujících zpráv.

1.13.3 Honeypot

Principem honeypot ve volném překladu „medová past“ je vytvoření „neexistujícího“ serveru. Náhodní útočníci se snaží dobýt službu, která není dostupná. Použitím popisované metody se snáze odfiltruje nepotřebný přístup neboli „šum“ a také je možné sledovat postup hackera snažící se server napadnout. [18, 19, 20, 21, 22, 23]

2 EXPLOITACE

2.1 Kali linux

Jedná se o speciální distribuci linuxu BackTrack, která je založena na operačním systému Debian, sloužící pro pokročilé penetrační testování a bezpečnostním kontrolám systému. Přestože byl vyvinut pro ověření zabezpečení sítě, je často používán pro nelegální činnost hackerů. Obsahuje více než 600 nástrojů a aplikací sloužící k testování. Utility jsou rozděleny do skupin dle svého využití typu sniffing/spoofing.

Kali linux je volně šiřitelný pod licencí open source. Uživatel může doladit nebo přebudovat jeho zdrojové kódy. Podobně jako většina linuxových distribucí je a vždy bude zdarma. Mezi priority operačního systému patří zaměření na bezdrátové zařízení. Podporuje pro ně velké množství ovladačů a skriptů, ať už provozovaný přes wi-fi nebo bluetooth. Penetrační testování bezdrátových sítí je mnohem rozsáhlejší díky nepotřebné přímé konektivitě do sítě.

Developeři Kali linux nabízí komerční kurzy penetračních testování využitím jejich operačního systému a přístupných nástrojů. Splněním kurzu uživatel získá certifikát OSCP (Offensive Security Certified Professionals), který je celosvětově vysoce uznávaný.

2.2 Počítačové útoky a bezpečnostní hrozby

Využití bezpečnostních aspektů sítě pro úmyslné prolomení zabezpečení k získání citlivých dat nebo znepřístupnění služby můžeme nazývat temnou stranou testování. Způsobů napadení je nespočetné množství.

2.2.1 Útok na aplikační vrstvě

Na rozdíl od hybridních/síťových útoků není využití aplikační vrstvy tolik rozsáhlé, ale vzhledem k možným vzniklým škodám o to více závažné. Útoky jsou zaměřeny přímo na určité aplikace běžící na síti, např.: HTTP, FTP, DHCP a další. Vyřazení z provozu některé ze služeb aplikační vrstvy může mít za následek nefunkčnosti celé sítě.

2.2.2 Autorooters

Jedná se o aplikace, které automaticky provádí hackování systému. Během průběhu jsou hledána napadnutelná místa s nejnižším zabezpečením. Při testování se do zařízení instaluje rootkit, skrze který je možné bez dalších kroků hackera proniknout do dalších zařízení. Tento typ útoků umožňuje hackerovi napadnout velké množství systémů v krátkém čase.

2.2.3 Zadní vrátka (Backdoor)

Backdoor je předem připravená metoda pro přístup do systému umožňující vyhnout se autentizaci. V některých případech jsou zadní vrátka vytvářena přímo tvůrci softwaru pro následující přístup, například při vzdáleném připojení servisu. Představuje ovšem velké bezpečnostní riziko. Útočník tak má přístup do systému, dokud není tato hrozba odstraněna. Tato cesta do zařízení se velmi často využívá pro přístup k soukromým datům, vytváření DoS útoků a mnoha dalších. Pokud není systém důkladně zabezpečen, může být tento exploit zpřístupněn pomocí malware, virů nebo červů.

2.2.4 Man in the middle - „prostředník“

Útočník se snaží zachytávat komunikaci mezi objekty použitím sniffer nástrojů. Pro sledování komunikace a následný odposlech je potřebný přístup k síti. Obvykle se jedná o zaměstnance poskytovatele internetového připojení (ISP). Jak už název napovídá, uživatel zachytává pakety odesílatele a následně je posílá příjemci. Tím si zajistí přístup k předávaným informacím, aniž by přerušil komunikaci daných objektů.

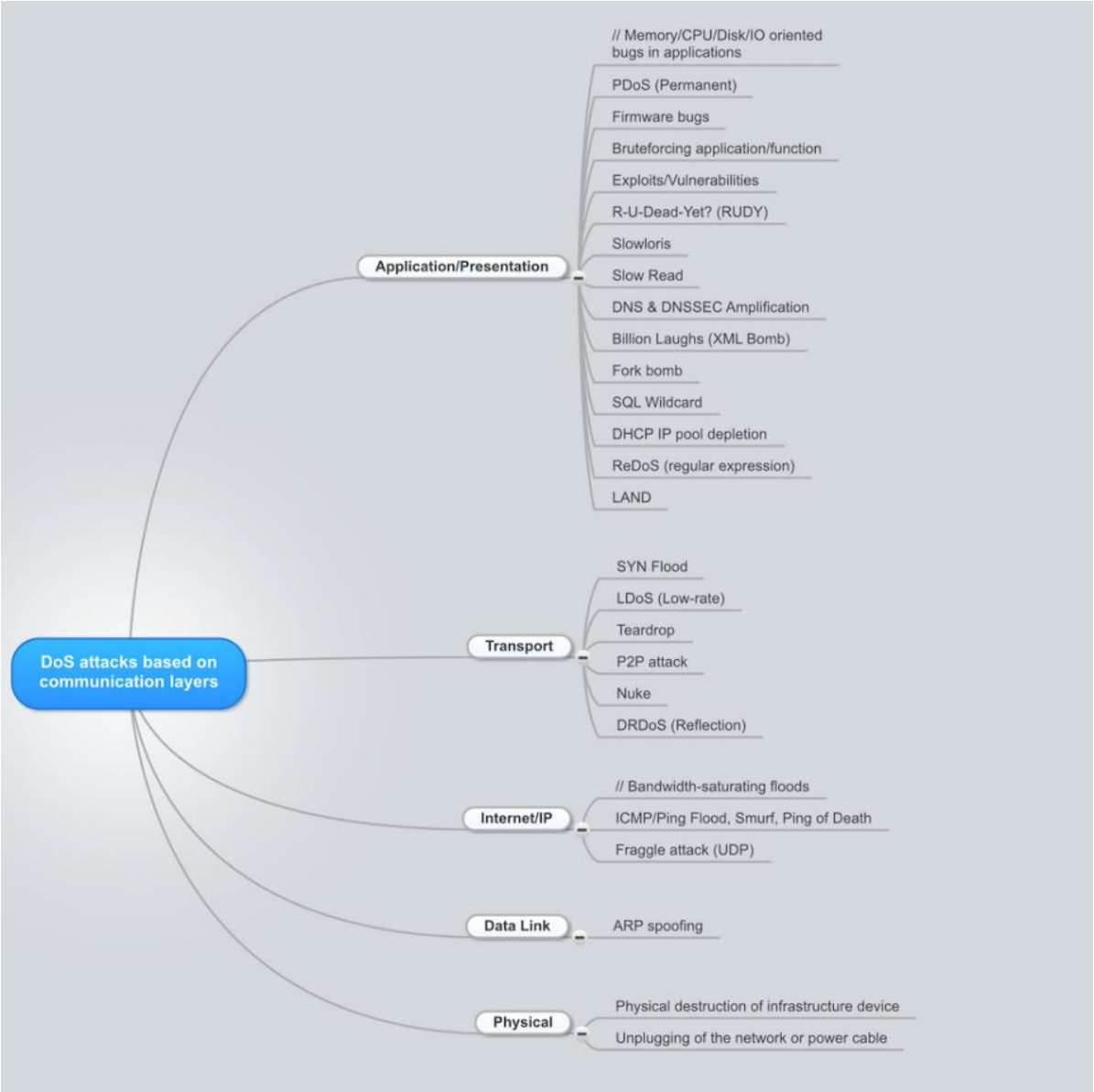
2.2.5 Podvržení IP

Podvržení neboli IP spoofing je druh přístupu do sítě, kdy hacker použije IP adresu s povoleným přístupem do systému. Útočník tedy podvrhuje adresu a napadaný systém předpokládá, že se jedná o uživatele s povoleným přístupem. Útok podvržení IP adresy bývá většinou vstupním klíčem k následné exploitaci systému.

2.2.6 DoS (denial of service) / DDoS (distributed denial of service)

Hlavním cílem útoku je zpomalení nebo znepřístupnění služby. Uvedené DoS a DDoS útoky se od sebe liší pouze zdroji, z kterých útok přichází. DoS je provozován od jednoho uživatele na rozdíl od Distribuovaného DoS, který může pocházet až od statisíců zařízení. Provozování útoků na nižší síťové vrstvě (na rozdíl od aplikační) je méně náročné a pro daný systém více problematické. Příkladem můžeme uvést znepřístupnění hraničního zařízení, zahlcení serveru nebo databáze a mnoha další. Existuje velké množství typů DoS útoků, proto jsou uvedeny ty nejpoužívanější.

2.2.7 DoS



Obrázek 8 Seznam DoS útoků dle vrstev

Zdroj: (Security-portal, 2013)

- **Záplava TCP SYN paketů**

Z počátku útoku vypadá komunikace mezi útočníkem a napadeným systémem bezproblémově. Uživatel otevře spojení TCP a pošle na daný server SYN zprávu, který odpoví SYN-ACK uživateli a následně potvrdí spojení ACK. Na rozdíl od vytvoření kompletního spojení je napadané zařízení zasypáno „na půl“ otevřeným spojením, které vede k nepoužitelnosti zařízení.

- **Smrtící ping (Ping of death)**

Příkaz ping se nejčastěji využívá k otestování konektivity zařízení. Ping má maximální velikost packetu 65536 bajtů u protokolu IP. Této vlastnosti je možné využít posláním příliš velkého paketu. Tato hrozba může vést k následnému pádu zařízení, které na ping reaguje. Hrozba tohoto typu je už více méně zastaralá.

2.2.8 DDoS

- **TFN (Tribe flood Network)**

Nástroj pro synchronizaci útoků DoS od více počítačů. Tím se stává obrana proti této hrozbě náročnější. Při této technice se často využívá falšování IP adresy. Útočník konstruuje a přeposílá informace na zařízení dostupné k útoku, které vytvoří DoS útok.

- **Stacheldraht**

Německy pojmenovaná hrozba s překladem „ostnatý drát“ je kombinací více druhů DoS útoků, mezi něž patří i TFN. Hlavní rozšířením od TFN je použití šifrování. Samotný proces exploitace je rozdělen na dva druhy kroků. V prvním se inicializuje komunikace s ostatními počítači, kteřé budou tvořit útok. Druhou částí je DoS útok na jeden nebo více cílů. Využití více cílů je vhodné například pro napadení hraničních zařízení sítě nebo pro využití více proxy bran pro lepší zabezpečení.

2.2.9 Zkoumání sítě

V první části útoku na síť je pro hackera důležité vědět o síti co nejvíce informací, proto je potřeba prozkoumat síť. Každá nová informace může vést k novým napadnutelným cestám systému. Nejvyužívanější techniky pro průzkum jsou skenování portů, rozesílání příkazů ping a komunikace s DNS.

2.2.10 Packet Sniffing

Packet Sniffing neboli sledování paketů, je softwarový nástroj umožňující sledovat běžící pakety v síti. Sniffery mohou sloužit jak už pro hackery, tak i pro administrátory pro zvýšení zabezpečení své sítě. Funkce analyzování síťového provozu pracuje na principu síťového adaptéru nastaveného do promiskuitního režimu, zachytává pakety a odesílá je použitému softwaru, který dokáže odposlechnout komunikaci. Tím se útočník může dostat k citlivým informacím, zvláště uživatelským loginům a heslům.

2.2.11 Promiskuitní mód

Síťová karta přijímá všechnu komunikaci na síti, aniž by řešila MAC adresu cílového zařízení.

2.2.12 Útoky na hesla

Existuje více způsobů, jak může hacker získat citlivé údaje. Hesla se mohou vyskytovat v hashové podobě, která nabízí lepší zabezpečení než hesla uložená v klasické textové podobě. Účelem této části je získání uživatelských hesel, aby se hacker mohl vydávat za oprávněného uživatele.

2.2.13 Útoky hrubou silou (brute force attack)

Jedná se o způsob expoiltace bez vědomosti šifry zaheslování. Mezi tyto způsoby můžeme zařadit jak už vytvoření zadních vrátek, tak i především testování možných kombinací. Útočník se snaží vyhnout uživatelskému ověření.

2.2.14 Útoky přesměrování portů

Principem přesměrování portů je zpřístupnění komunikace přes firewall a přenášení dat, která by firewall zablokoval. K této technice je však nutný přístup zařízení připojeného do napadané sítě.

2.2.15 Trojský kůň

Název odpovídající řecké báji představuje podobný princip při dobití Tróji. Trojský kůň je škodlivý software, který se tváří jako uživatelem nebo systémem používaná aplikace. Exploitace udávaného typu má mnoho podob, kterých je použito při popisovaných útocích. Nejčastějším rozšiřováním trojských koní bývá otevření neověřených příloh e-mailové pošty nebo přístupem na webové stránky, které obsahují škodlivý obsah. Jak už bylo řečeno, široké využití je možné rozdělit mezi 4 základní rozdělení týkající se vzdáleného přístupu, hledače hesel, keyloggery a v neposlední řadě aplikace s destruktivním přístupem k zařízení.[3, 19]

2.3 Aplikace pro penetrační testování

2.3.1 Hping3

Hping je testovací nástroj využívající TCP, UDP, ICMP a RAW-IP protokoly. I přes hlavní účel analýzy zabezpečení je většinou uživatelů používán k napadení zařízení. Hping dále nabízí pokročilé skenování portů, testování firewallu či sítě pomocí různých protokolů a další.

Podporované platformy jsou: Linux, FreeBSD, NetBSD, OpenBSD, Solaris, MacOs X, Windows.[24]

2.3.2 Nmap

Síťový skener pro hledání aktivních zařízení v síti. Obrovskou výhodu Nmapu tvoří předem definovaná pravidla ke zjišťování informací ze sledované sítě. Na rozdíl od ostatních programů používajících jednoduché pingy k rozeznání aktivních zařízení Nmap bere ohled na různé stavy sítí, včetně zahlcení sítě či kolísání latence. Postupem času se aplikace rozrostla do úrovně komplexního nástroje. Poslední verze dokáže určit operační systém nalezeného zařízení, verze a názvy služeb, dobu od puštění systému i typy zařízení.

Grafickou nadstavbu tvoří tzv. Zenmap.

Mezi podporované platformy patří: Linux, Solaris, BSD, Windows, MacOS X, AmigaOS. [8]

3 SNORT

Snort je volně šiřitelný software pro analýzu síťového provozu vyvíjený pro unixové distribuce společností Sourcefire. Aplikace Snort v základním režimu pracuje jako NIDS (Network Intrusion Detection System), který je podporovaný i na platformách Windows. V režimu IDS umožňuje pouze detekovat veškerou komunikaci, která bude zobrazována dle pravidel nebo rozpoznaných anomálií. Způsob kontroly prvků použitím seznamu pravidel se nazývá signature-based. Dalším podporovaným režimem je NIPS (Network Intrusion Prevention System) pracující v inline módu, který umožňuje nejen detekovat, ale také blokovat nepovolenou komunikaci. Správné použití Snort IPS vyžaduje více rozhraní s účelem procházení veškeré sledované komunikace skrze IPS/IDS zařízení.

Sourcefire se zaměřuje na bezpečnostní prvky a nabízí komerční zpracování zabezpečení jak na hardwarové, tak softwarové úrovni.

Detekce a prevence na základě pravidel vyžaduje často aktualizované signatury vydávané týmem VRT (Vulnerability Research Team) z téže společnosti. Společnost Sourcefire nabízí k dispozici řadu pravidel, které spadají pod placenou licenci. K dispozici jsou i neplacené signatury, které jsou implementovány ke starším verzím nebo novější s menším pokrytím bezpečnostních hrozeb. Signatury vyvíjené pro Snort jsou velice často používány pro řadu dalších IDS systémů.

Jedná se o softwarově nejpoužívanější IDS/IPS systém po celém světě.

3.1 Rozdělení:

Systém je možné rozdělit do 4 skupin, dle základních funkcí.

3.1.1 Sniffer

Slouží k zachytávání veškerých paketů probíhajících přes dané rozhraní. Sniffer aplikaci můžeme na internetu najít nespočetné množství, jelikož jsou hlavním klíčem k bezpečnostním hrozbám. Ať už použitím administrátora, tak i hackera.

3.1.2 Preprocessor

Funkce nutné pro práci s pakety zařizuje preprocessor. Dekódováním protokolů na vyšších vrstvách napomáhá k plynulejšímu srovnávání paketů. Hlavním účelem můžeme označit uspořádání dat do proudů, dle jednotlivých vrstev ISO/OSI modelu, a tím i značně zrychlit funkcionalitu systému.

3.1.3 *Detection*

Nejdůležitější prvek celého zařízení. Přijatá data od preprocessoru jsou porovnána se signaturami a následně vyhodnocena podle předem určených kroků. Od propuštění paketu a uložení do databáze přes odeslání požadavku na přeposlání nového paketu až po blokování systémem IPS.

3.1.4 *Output*

Přehlednost o veškerém dění aplikace Snort se stará poslední funkční vrstva. Defaultní logování je možné rozšířit o řadu doplňků. Ukládání do databáze patří mezi nejčastější použití Snortu v rozsáhlejších pracovních oblastech. K dispozici jsou i webové nadstavby jako je například Snorby umožňující přes webový prohlížeč dostatečnou kontrolu nad systémem.

3.2 Instalace

Důležitým krokem je výběr operačního systému podporující správnou funkčnost softwaru Snort a výběrem režimu použití jako IDS nebo IPS. Uvedený postup je určen a otestován operačním systémem Ubuntu.

3.2.1 *Stažení*

Aplikace Snort je multiplatformní. Na oficiálních stránkách jsou dostupné odkazy na uvedený software pro unixové distribuce, ale také pro Windows. Jednoduchou instalací pro OS Windows můžeme dosáhnout kvalitního IDS systému. Není zde potřeba instalace dodatečných knihoven, jelikož jsou v instalaci implementovány. Hlavní nevýhodou Snortu instalovaným na Windows je neschopnost aplikace pracovat v inline režimu. Není doposud implementován, a tak může pracovat pouze jako IDS.

Stažení aplikace je možné na oficiálních stránkách www.snort.org nebo příkazem na platformě Ubuntu.

```
wget https://snort.org/downloads/snort/snort-2.9.7.2.tar.gz
```

3.2.2 *Instalace knihoven*

V základu jsou potřebné nástroje pro sestavení programů. Balíček build-essentials je možné nainstalovat následujícím příkazem:

```
sudo apt-get install -y build-essential
```

Snort vyžaduje řadu dodatečných knihoven potřebných pro běh programu jako IPS. Dostupné v repozitářích pro Ubuntu:

pcap (libpcap-dev)

PCRE (libpcre3-dev)

Libdnet (libdumbnet-dev)

```
sudo apt-get install -y libpcap-dev libpcre3-dev libdumbnet-dev
```

Vytvoření složky snort_src pro přehlednost instalovaných balíků.

```
mkdir ~/snort_src
cd ~/snort_src
```

Knihovna flex potřebná pro inline mod.

```
sudo apt-get install -y bison flex
```

DAQ (Data AcQuisition Library)

Stažení a instalace poslední verze DAQ je možná ze stránek Snort. Následné kroky umožní stažení a instalace knihovny DAQ. Doposud nejnovější verzí je 2.0.4.

```
wget https://www.snort.org/downloads/snort/daq-2.0.4.tar.gz
tar -xvzf daq-2.0.4.tar.gz
cd daq-2.0.4
./configure
make
sudo make install
```

3.2.3 Instalace Snort

Upozornění: v případě instalace starší verze je potřeba ověřit kompatibilitu knihoven s použitou verzí aplikace.

Instalace dodatečné knihovny zlibig.

```
sudo apt-get install -y zlib1g-dev
```

Pokud jste doposud nestáhli instalaci Snort, pokračujte následujícími dvěma řádky. V opačném případě tento krok přeskočte.

```
cd ~/snort_src
wget https://www.snort.org/downloads/snort/snort-2.9.7.2.tar.gz
```

```
tar -xvzf snort-2.9.7.0.tar.gz
cd snort-2.9.7.0
./configure --enable-sourcefire
```

```
make
sudo make install
```

Aktualizace knihoven. V případě přeskočení aktualizací následuje při spuštění aplikace chybové hlášení.

```
sudo ldconfig
sudo ln -s /usr/local/bin/snort /usr/sbin/snort
```

Ověření nainstalovaných částí je možné příkazem:

```
sudo snort -V
```

Vytvoření složky s pravidly, do které je potřeba zkopírovat konfigurační soubor snort.conf a do složky rules stažené signatury. Signatury lze instalovat pomocí softwaru Oinkmaster nebo manuálním způsobem.

```
mkdir /snort/
mkdir /snort/rules
```

Před spuštěním je nutné nastavit iptables pro řazení komunikace do front

```
./iptables -A INPUT -j QUEUE
./iptables -A FORWARD -j QUEUE
```

3.2.4 Konfigurace základního souboru

Konfigurační soubor snort.conf je rozdělen do určitých kroků. Většina důležitých a používaných konfigurací je uvedena v konfiguračním souboru pouze za komentujícím znakem #.

- **Nastavení proměnných pro síť**

Proměnná #var HOME_NET any slouží pro určení adresy sítě, která je kontrolována IDS/IPS zařízením. Ukazatel any určuje analýzu veškeré dostupné komunikace. Pro snímání paketů sítě lze nastavit přímo adresou sítě.

```
var HOME_NET 192.168.1.0/24
```

Další proměnnou je #var RULE_PATH /cesta/ umožňující definovat základní cestu k dalším konfiguračním souborům a signaturám.

```
Var RULE_PATH /snort/rules/
```

- **Konfigurace preprocessoru**

Velice široká konfigurační část obsahující SID popisující typ analyzovaného toku, nastavení upozornění a další. Pro základní konfiguraci není potřeba měnit.

- **Konfigurace výstupních pluginů**

Nastavení logů, ukládání do souborů.

- **Dodatečná konfigurace**

Možnost ignorování určitých portů, které není třeba analyzovat.

- **Nastavení pravidel**

Nejdůležitější částí konfiguračního souboru je přístup pravidel použitých k provozu. Použitý odkaz RULE_PATH v prvním kroku uvádí umístění signatur.

Prvním uvedeným pravidlem je local.rules, který se používá pro vlastní nastavení pravidel.

3.2.5 Spuštění a základní parametry

- **A** rychlý výpis upozornění
- **b** logování paketů využitím tcpdump
- **c** cesta k základním pravidlům.
- **d** zahození paketů aplikační vrstvy
- **D** spuštění Snortu na pozadí
- **F** načtení filtrů
- **h** nastavení domácí sítě
- **i** nastavení použitého interface
- **K** logovací mód
- **l** logování do složky
- **M** ukládání upozorňujících zpráv do logu
- **N** vypnutí logu, upozorňující zprávy pořád pracující
- **p** vypnutí módu Sniffování
- **Q** zapnutí v inline módu
- **T** testovací mód
- **U** použití časových známek
- **V** zobrazení verze a instalovaných potřebných balíčků
- **y** přidává rok do logu a upozornění

Parametry knihovny DAQ –daq afpacket předají programu zdroj paketů.

Výběr –daq-mod inline zpřístupní režim v inline módu a tedy možnost funkce IPS. Samotné spuštění v inline modu jako IPS

```
sudo snort -c /snort/snort.conf -A console -y -i eth0:eth1 –daq afpacket –daq-mod inline -Q
```

Parametrem -c je nastavena cesta k souboru se základní konfigurací snort.conf. Každé zařízení má individuální cestu dle umístění. [26, 27]

3.3 Tvorba vlastních pravidel

Snort používá velice flexibilní jazyk pro tvorbu vlastních pravidel. Většina pravidel je tvořena jedním řádkem. Každé pravidlo je rozděleno na dvě části. První hlavičková část obsahuje způsob přístupu k paketům, použitý protokol, zdrojovou a cílovou adresu s maskou a v neposlední řadě vstupní i výstupní čísla portů. Druhá sekce pravidel je nastavovací obsahující oznamující zprávy, části zkoumaných paketů a značení typů komunikace.

Příklad:

```
alert icmp any any → 192.168.1.0/24 any (msg:“Prichozi ping zaznamenan“;)
```

Výše uvedené pravidlo oznamuje veškerou komunikaci icmp protokolu na síť 192.168.1.0/24 na jakýkoliv port. V logu se objeví IP adresa, ze které je posílaný ping s oznamující zprávou.

Hlavičková část pravidel popisuje kdo, kde, jaký paket a jakým způsobem ho zpracoval.

První řetězec označuje akci vyvolanou při detekování paketu. Pravidla pro Snort v IDS režimu jsou téměř shodná s rozdílem, že IPS umožňuje odmítnutí či blokování paketů na rozdíl od IDS.

3.3.1 Možné reakce na pakety:

- **alert** Vygeneruje upozornění na vybraný paket a uvede jej do logu.
- **log** Přidá informaci do logu.
- **pass** Ignoruje paket.
- **activate** Upozorní a přepne na další dynamické pravidlo.
- **dynamic** Nečinný, dokud není předem využito aktivní pravidlo. Následně se používá log.
- **Drop** Zablokuje paket a uloží informaci do logu.
- **Reject** Zablokuje paket, uloží do logu a pokud se jedná o TCP nebo ICMP protokol je zažádáno o resetování komunikace.
- **Sdrop** Zablokuje paket bez logování.

3.3.2 Protokoly

Řetězec následující po reakci na paket určuje, jaký typ komunikace má Snort analyzovat. Základní protokoly schopné detekovat jsou TCP, UDP, ICMP a IP. Dle

dostupných informací bude následující verze umožňovat detekovat protokoly ARP, IGRP, GRE, OSPF, RIP a další.

3.3.3 IP adresy a porty

Po výběru protokolu následuje IP adresa sítě nebo zařízení, z kterého je komunikace vysílána. V případě přijetí veškerých informací, nehledě na IP adresu, lze nahradit slovem „any“. Po zdrojové IP adrese následuje zdrojový port, který je také možný nahradit slovem „any“. U zdrojových portů se obvykle tento řetězec nechává na hodnotě „any“, protože rozesílat pakety z různých portů není nijak složité.

Stejná pravidla jako u zdrojových adres a portů platí i pro cílová. Konfigurací těchto informací značně zpřehledníme sledovaný provoz.

Použitím negace ve tvaru „!“ je možné invertovat pravidla či rozsah adres.

Mezi zdrojovými a cílovými informacemi jsou umístěny ukazatele určující směr komunikace (<-, →,<>).

```
Drop tcp !192.168.1.0/24 any → any any(msg:“TCP spojení z adresy sítě bylo zablokováno 192.168.1.0“;)
```

3.3.4 Hlavní stavy pravidel

Slouží k upřesnění pravidel, dle kterých je reagováno na přijatý paket.

- **msg** Nastavení zprávy zobrazené při výpisu nebo uložení do logu.

```
msg:“Tato zprava bude zobrazena.“;
```

- **sid** Parametrem sid jsou označovány pravidla. Při použití velkého množství pravidel je možno přehledněji kontrolovat komunikaci na základě jednoho pravidla. Identifikační čísla jsou rozdělena do rozmezí:
  <100 Rezervované pro budoucí pravidla
  100-999999 Použitá identifikační čísla společností Sourcefire.
  >=1000000 Určená pro vlastní pravidla.

```
Sid:“1000008 “;
```

- **rev** Klíčové slovo rev upřesňuje o jaké pravidlo se jedná. Společně používané s atributem „sid“.

Tvorba dodatečný pravidel je prakticky nekonečná. Kombinací různých druhů zabezpečení a veškerých dostupných parametrů lze dosáhnout kompletního přehledu nad

veškerou komunikací v síti. Soupis veškerých rozšiřujících parametrů lze najít v oficiálním manuálu.

Příklad jednoduchého zablokování přístupu na webovou stránku seznam.cz.

```
drop tcp any any -> any any ( content:"www.seznam.cz ;msg:"Pokus o pristup na stranku www.seznam.cz zamitnut"; sid:10000006; rev:1;)
```

[27]

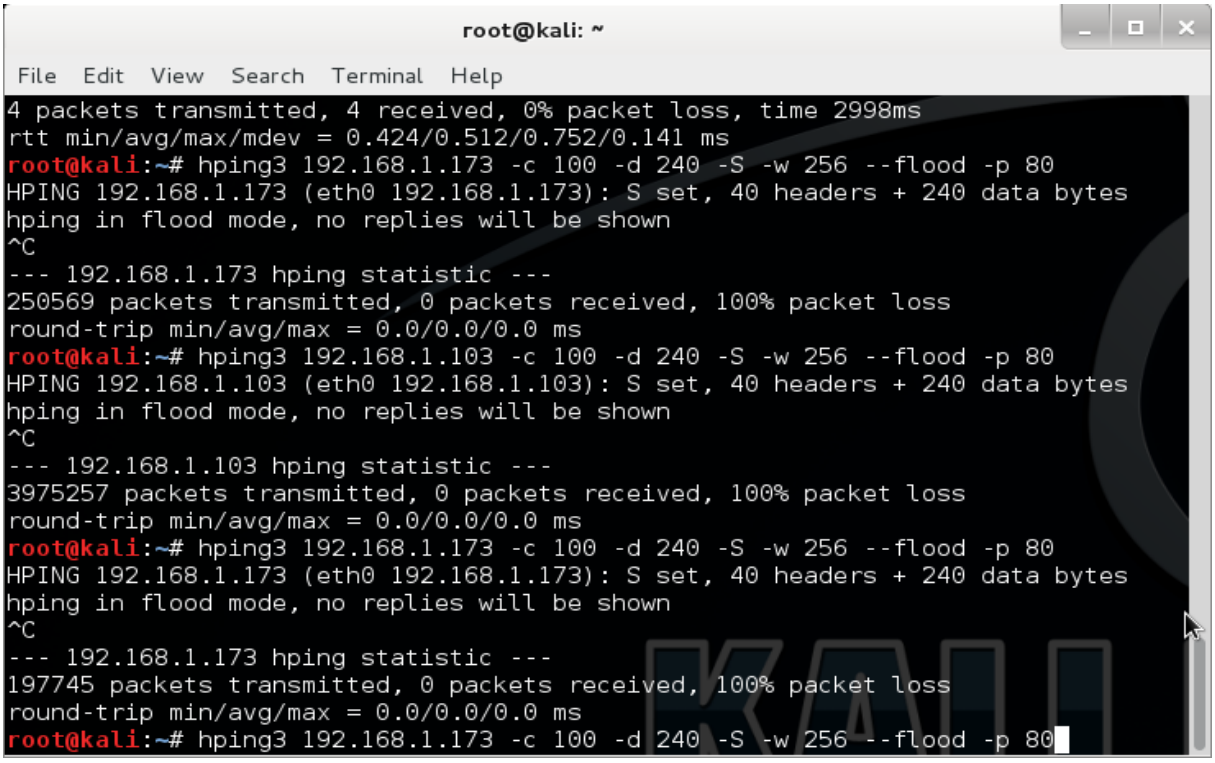
4 TESTOVÁNÍ

Pravidla používaná IDS a IPS zařízeními jsou značně rozsáhlá a striktní i v nejzákladnější volně šiřitelné verzi. Proto se zaměříme na detekování veškerého přístupu následným vytvořením vlastních pravidel.

4.1 Praktické použití Hping3

4.1.1 IPS uvnitř sítě

Umístění prevenčního systému za firewall do vnitřní sítě umožní sledování komunikace propuštěné do interní části.

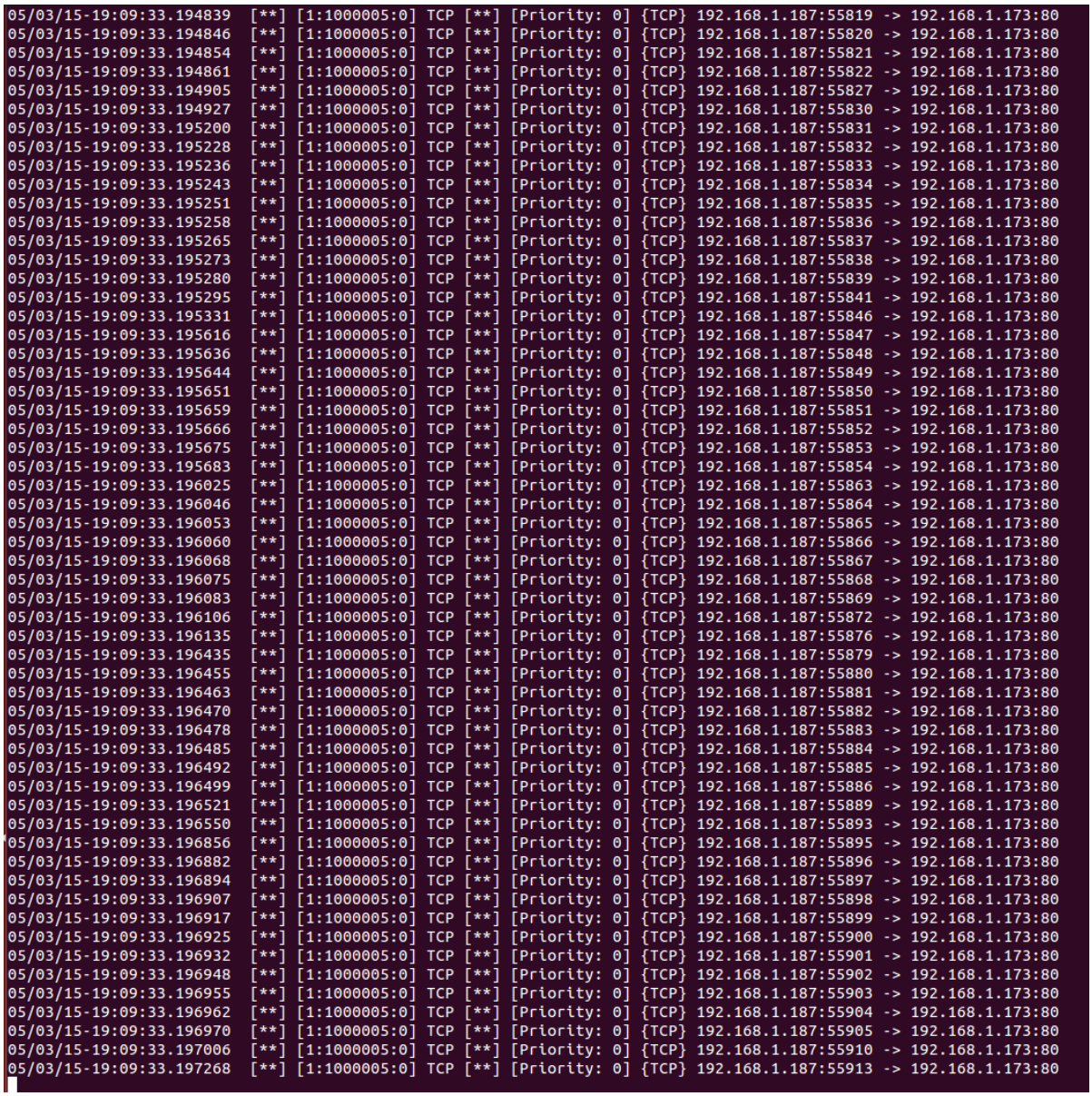


Obrázek 9 Hping3 z pohledu útočníka.

Zdroj: vlastní

Použitím aplikace Hping3 jsme docílili zaplavení zařízení TCP pakety, kterým bylo obsazeno 92% síťového provozu během pár vteřin.

Síťový provoz procházející přes Snort bez blokujících signatur podobně jako IDS detekoval veškerý provoz generovaný útočníkovou aplikací, který postupně generoval TCP pakety ze všech portů. Pakety procházely zařízením v řádu milisekund na port 80, a tím docházelo ke zpomaleným reakcím zařízení.



Obrázek 10 Detekce útoku z rozdílných portů.

Zdroj: vlastní

Po úspěšné detekci napadení je potřeba použít nebo vytvořit vhodnou signaturu pro blokování útoku. K tomu to kroku je již potřebné nastavení IPS v režimu inline, aby bylo možné „zahodit“ paket nesplňující pravidla.

Vytvořením jednoduché signatury je blokován opětovný útok a pakety se nešíří k napadenému zařízení. Útočník může volit útok z jiné adresy či portu. V tom případě je vhodné použití komerčních signatur nebo více definovat vlastní pravidla.

```
drop tcp 192.168.1.187 any -> any 80 (msg:"TCP attack packet dropped";sid:1000005;)
```

Použitím defaultních signatur dosáhneme stejného výsledku.

Obrázek 11 Zahození TCP paketů

Zdroj: vlastní

4.1.2 Umístění mimo síť

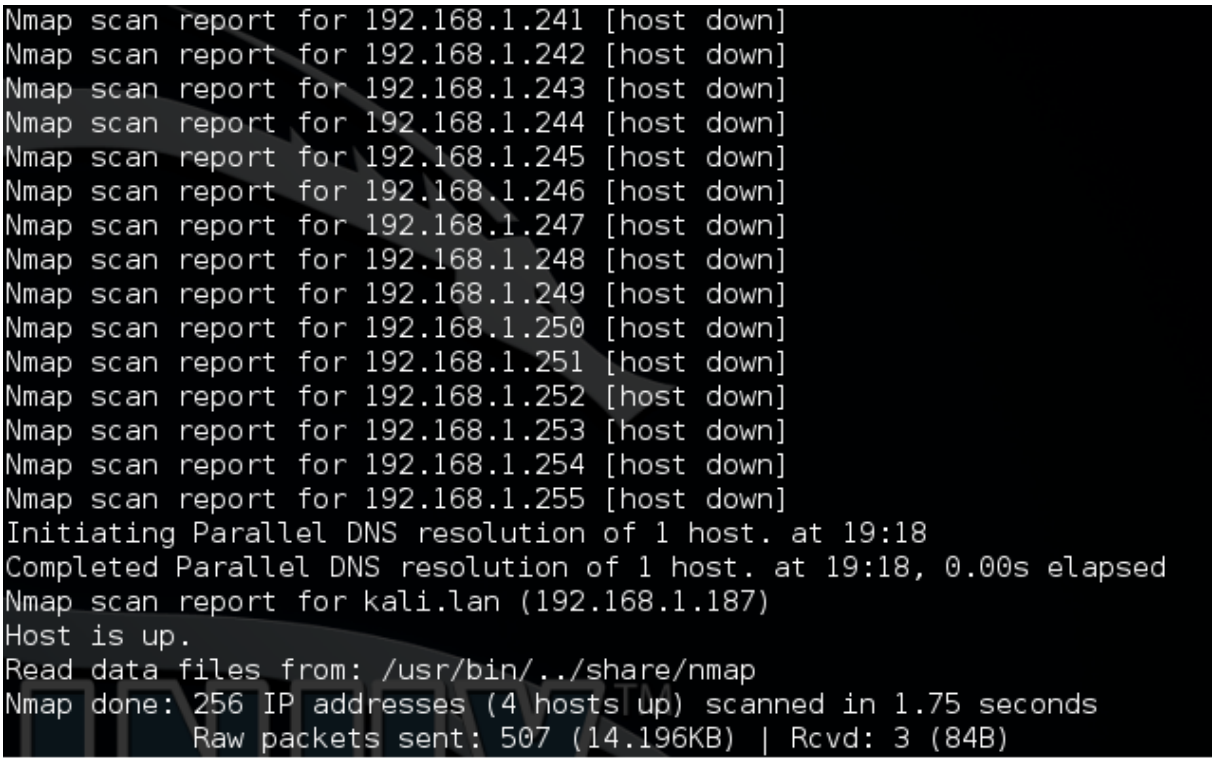
Umístěním IPS zařízení před router bylo ošetřeno napadení směrovače. Při testování domácího zařízení od společnosti TP-Link se podařilo v mžiku shodit celý router. Nedostupnost zařízení trvala do doby zapnutí blokovacího režimu. Bez přerušení útočníka by bez uvedených bezpečnostních zásahů nebylo zařízení schopné dospět do pracovního režimu.

4.2 Praktické použití NMAP

Aplikace sloužící k detekování prvků v síti. NMAP používá velké množství způsobů, které je Snort neschopen detekovat. Přes veškerou blokaci paketů byl schopen zjistit aktivní zařízení.

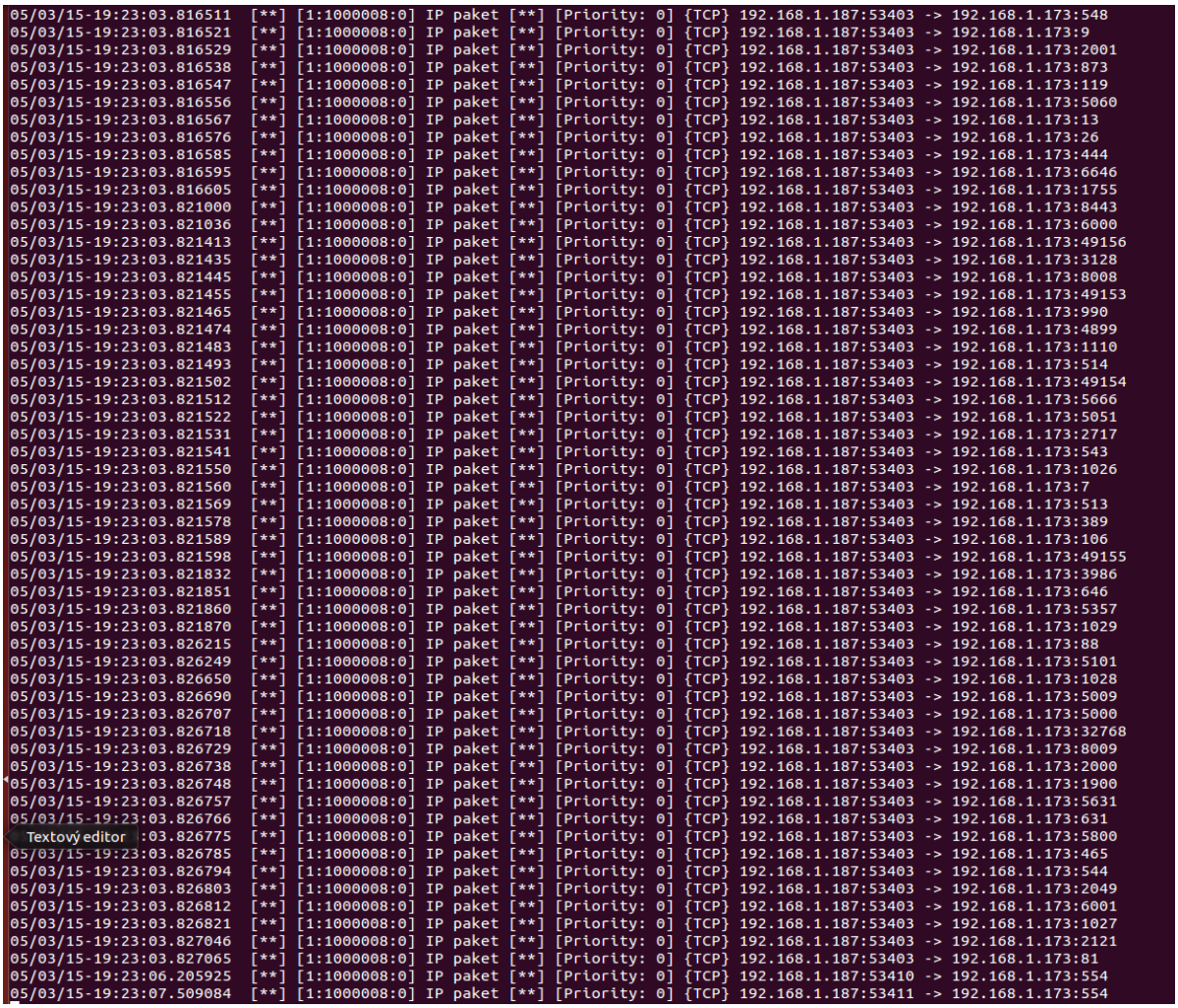
Obrázek 12 Skenování aktivních zařízení pomocí UDP protokolu.

Zdroj: vlastní



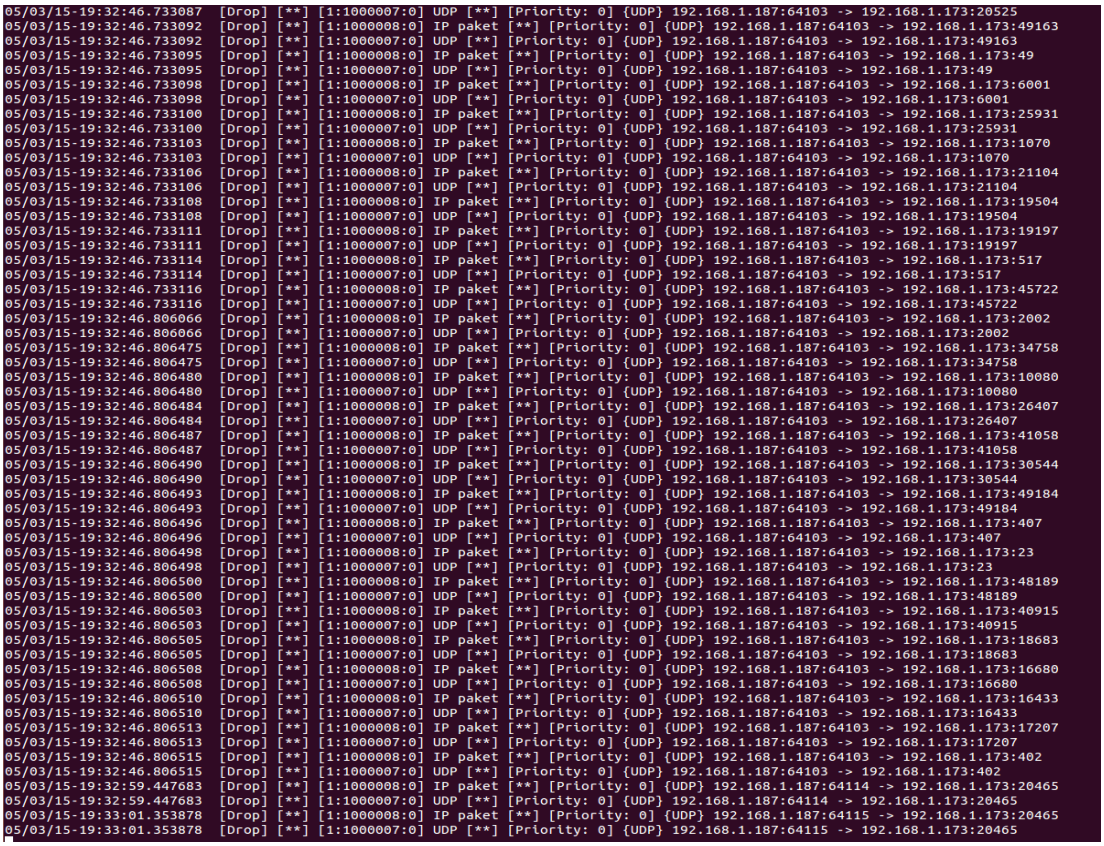
Obrázek 13 Skenování využitím DNS

Zdroj: vlastní



Obrázek 14 Zahození paketů při skenování sítě

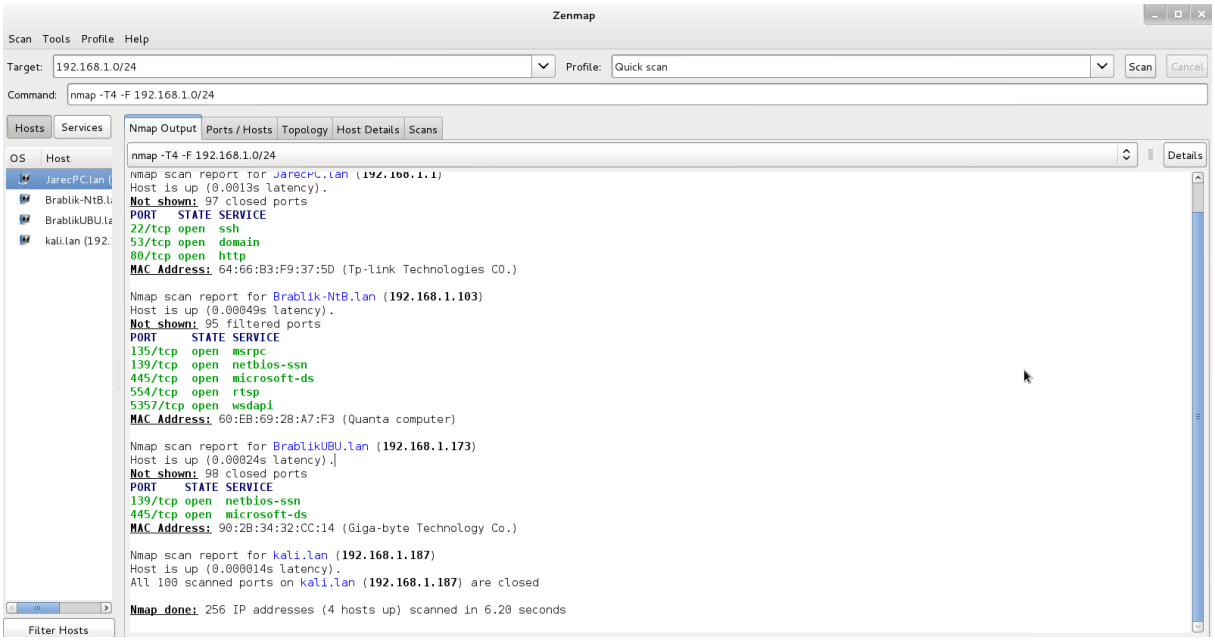
Zdroj: vlastní



Obrázek 15 Zahození IP a UDP paketů při skenování.

Zdroj: vlastní

Přes detekování a blokování IP paketů analyzujících aktivní zařízení v síti včetně otevřených portů byla aplikace schopná informace získat.



Obrázek 16 Výsledný scan

Zdroj: vlastní

4.3 Přístup na webové stránky

IPS zařízení nemusí sloužit pouze k detekci a následnému blokování útoků. Kombinací pravidel je možné dosáhnout komplexního využití. Ukázkou si předvedeme blokování přístupu k webovým stránkám. Toto pravidlo může být výhodné pro administrátory za cílem zakázat uživatelům přístup k nepovoleným stránkám.

Pravidlo začínající řetězcem „alert“ pouze upozorní administrátora, z jaké IP adresy se uživatel snaží přistupovat na stránku. Jako příklad si uvedeme přístup k „www.seznam.cz“.

```
alert tcp any any -> any any (content:"www.seznam.cz";msg:"Nepovoleny pristup";sid:100008;)
```

V případě zablokování přístupu stačí pouze zaměnit „alert“ za „drop“.

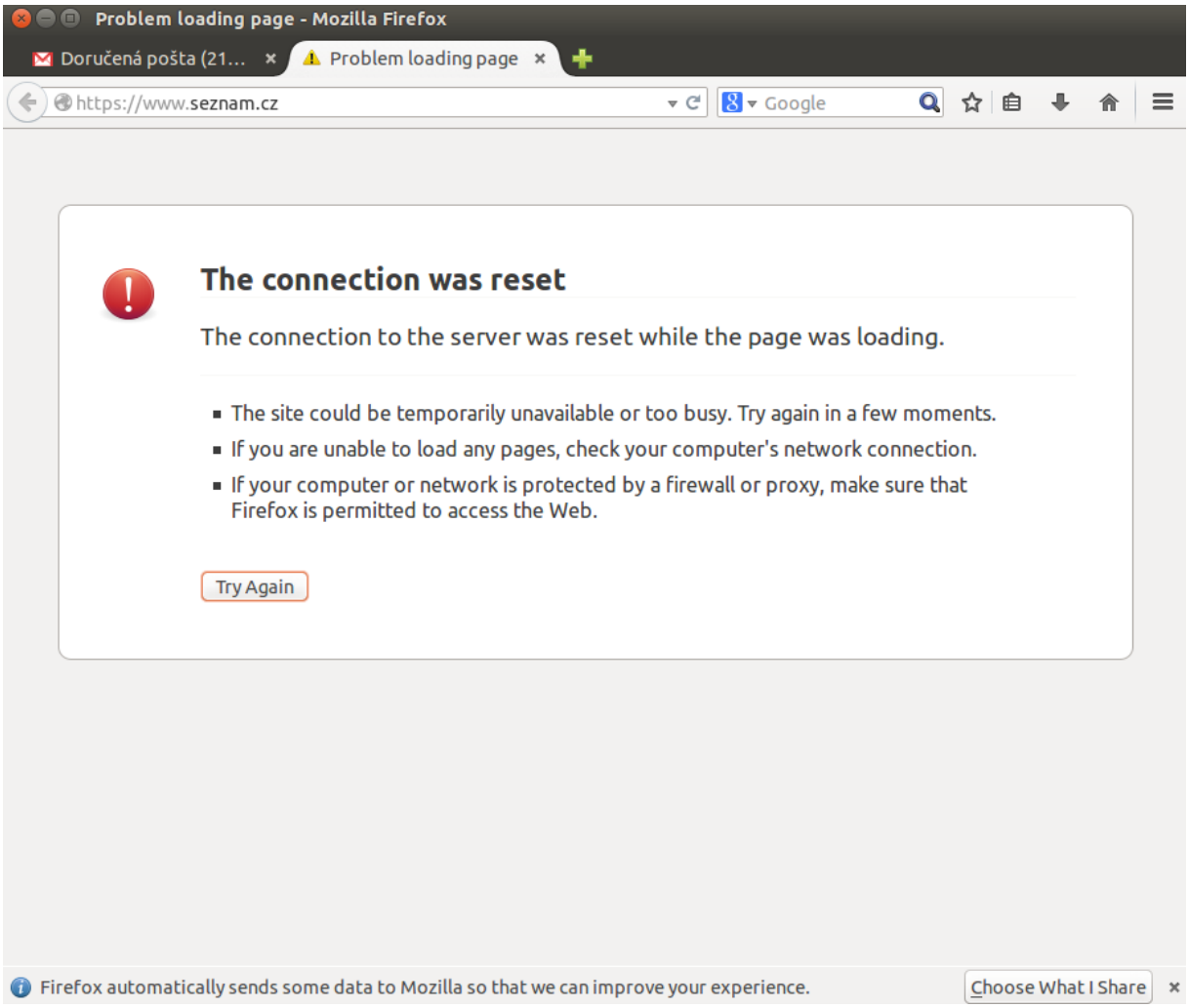
```
drop tcp any any -> any any (content:"www.seznam.cz";msg:"Nepovoleny pristup";sid:100008;)
```

Po zablokování domény pomocí IPS uživatel ztrácí možnost přístupu k uvedené stránce.

```
05/03/15-20:30:22.248921  [Drop] [**] [1:100008:0] Nepovoleny pristup [**] [Priority: 0] {TCP} 77.75.76.3:80 -> 192.168.1.173:46494
05/03/15-20:30:22.248921  [Drop] [**] [1:100008:0] Nepovoleny pristup [**] [Priority: 0] {TCP} 77.75.76.3:80 -> 192.168.1.173:46494
05/03/15-20:30:22.259754  [Drop] [**] [1:100008:0] Nepovoleny pristup [**] [Priority: 0] {TCP} 77.75.76.3:443 -> 192.168.1.173:36026
05/03/15-20:30:22.274304  [Drop] [**] [1:100008:0] Nepovoleny pristup [**] [Priority: 0] {TCP} 77.75.76.3:443 -> 192.168.1.173:36027
05/03/15-20:30:22.288575  [Drop] [**] [1:100008:0] Nepovoleny pristup [**] [Priority: 0] {TCP} 77.75.76.3:443 -> 192.168.1.173:36030
05/03/15-20:30:22.304385  [Drop] [**] [1:100008:0] Nepovoleny pristup [**] [Priority: 0] {TCP} 77.75.76.3:443 -> 192.168.1.173:36035
05/03/15-20:30:22.318248  [Drop] [**] [1:100008:0] Nepovoleny pristup [**] [Priority: 0] {TCP} 77.75.76.3:443 -> 192.168.1.173:36036
05/03/15-20:30:22.334632  [Drop] [**] [1:100008:0] Nepovoleny pristup [**] [Priority: 0] {TCP} 77.75.76.3:443 -> 192.168.1.173:36037
05/03/15-20:30:22.348499  [Drop] [**] [1:100008:0] Nepovoleny pristup [**] [Priority: 0] {TCP} 77.75.76.3:443 -> 192.168.1.173:36042
05/03/15-20:30:22.363653  [Drop] [**] [1:100008:0] Nepovoleny pristup [**] [Priority: 0] {TCP} 77.75.76.3:443 -> 192.168.1.173:36045
05/03/15-20:30:22.374604  [Drop] [**] [1:100008:0] Nepovoleny pristup [**] [Priority: 0] {TCP} 77.75.76.3:443 -> 192.168.1.173:36046
05/03/15-20:30:22.390354  [Drop] [**] [1:100008:0] Nepovoleny pristup [**] [Priority: 0] {TCP} 77.75.76.3:443 -> 192.168.1.173:36047
```

Obrázek 17 Zahození paketů seznam.cz

Zdroj: vlastní



Obrázek 18 Zablokovaná uživatelská služba

Zdroj: vlastní

ZÁVĚR

Tato bakalářská práce byla věnována penetračnímu testování využitím systémů pro detekci a prevenci průniku. V základě byly představeny veškeré části zabezpečení používané během testování.

Zprovoznění prevenčního systému průniku byla stěžejní část. I přes kvalitní podporu a zpracování síťových prvků společnosti Cisco bylo zvoleno softwarové řešení Snort od firmy Sourcefire, která dává IPS volně k dispozici. Nevýhodu zde však tvořila podpora pouze unixových platforem.

Bezpečnostní prvky IPS se v minimálních případech objeví u koncových uživatelů. Jsou určeny převážně pro větší firmy nebo rozsáhlé organizace, a proto je jejich podpora ve velké míře komerční. Placené služby zaručují vyšší kvalitu zabezpečení, zároveň však znemožňují dostatečné testování při využití open source softwaru. Společnosti Cisco i Sourcefire patřící k největším společnostem, které se zabývají detekčními a prevenčními systémy a nabízejí pravidla (signatury) potřebná pro správnou funkci zařízení za nemalé finanční částky. Proto byla práce zaměřena převážně na pochopení principů zabezpečení a tvorbu individuálních doplňujících pravidel.

V detekujícím režimu bezpečnostního zařízení IDS/IPS jsme simulací útoků na vlastní síť docílili omezení provozu i samotného odstavení zařízení. Z informací získaných pomocí analýzy síťového provozu skrze Snort jsme byli schopni vytvořit vlastní pravidla pro blokování opětovných útoků. Po přepnutí IDS/IPS na prevenční režim s aplikací vlastně vytvořených pravidel byly další útoky zablokovány.

V určitých režimech skenování sítě pomocí aplikace Nmap jsme nebyli schopni analyzovat její celkový provoz, jelikož tento program využívá kombinaci různým metrik a postupů, které IDS/IPS Snort nebyl schopen detekovat.

I přes vysokou finanční náročnost pořízení IDS/IPS systému by měla každá větší společnost vlastnit alespoň jeden uvedený bezpečnostní prvek, jenž umožňuje kontrolu nad síťovým provozem, a tím i značně přispívá ke kvalitnímu zabezpečení.

POUŽITÁ LITERATURA

[1] Softwarové Firewally. *Antivirové centrum.* [online]. [2014] [cit. 2015-04-18]. Dostupné z: *http://www.antivirovecentrum.cz/firewally.aspx*

[2] PETERKA, Jiří. Proxy brány. *earchiv.* [online]. © 2011 [cit. 2015-04-18]. Dostupné z: *http://www.earchiv.cz/b01/b0100025.php3*

[3] SELECKÝ, Matúš. *Penetrační testy a exploitace*. 1. vyd. Brno: Computer Press, 2012, 303 s. ISBN 978-80-251-3752-9.

[4] BERÁNEK, Ladislav. Firewally a iptables. *eAMOS.* [online]. © 2002-2015 [cit. 2015-04-18]. Dostupné z:*http://eamos.pf.jcu.cz/amos/kat_inf/externi/kat_inf_28372/files/10.prednaska/12-firewally_a_iptables.pdf*

[5] GRYGAREK, Petr. Cisco IOS Firewall. *SPS portál.* [online]. ©2015 [cit. 2015-04-18]. Dostupné z: *http://www.cs.vsb.cz/grygarek/SPS/projekty0506/IOS-FW-IDS.pdf*

[6] PETR, Bouška. Cisco IOS 1 - úvod, příkaz show. [online]. 08.03.2007 [cit. 2015-05-02]. Dostupné z: http://www.samuraj-cz.com/clanek/cisco-ios-1-uvod-prikaz-show/. ISSN 1801-867X

[7] GRYGAREK, Petr. Konfigurace směrovačů a přepínačů s Cisco IOS . *SPS portál.* [online]. ©2015 [cit. 2015-04-18]. Dostupné z:*http://www.cs.vsb.cz/grygarek/SPS/projekty0506/IOS-FW-IDS.pdf*

[8] DOČEKAL, Michal. Správa linuxového serveru: Úvod do skenování sítí pomocí Nmap. *Linuxexpres.* [online]. 1.3.2012 [cit. 2015-04-18]. Dostupné z:*http://www.linuxexpres.cz/praxe/sprava-linuxoveho-serveru-uvod-do-skenovani-siti-pomoci-nmap*

[9] SMITKA, Vladimír. Cisco ASA. *Lint Services.* [online]. 31. 7. 2013 [cit. 2015-04-18]. Dostupné z: *http://lynt.cz/blog/predstaveni-cisco-asa*

[10] BOUŠKA, Petr. VPN 2 – Úvod do Cisco ASA a možnosti VPN. *Samuraj-cz.* [online]. 17.04.2011 [cit. 2015-04-18]. Dostupné z: *http://www.samuraj-cz.com/clanek/vpn-2-uvod-do-cisco-asa-a-moznosti-vpn/* . ISSN 1801-867X

[11] Cisco ASA. *Adaptive Security Appliance (ASA).* [online]. ©1998-2015 [cit. 2015-04-18]. Dostupné z: *http://www.atcomp.cz/downloads/cisco/asa_popis.pdf*

[12] DMZ (Demilitarizovaná zóna). *Managment mania.* [online]. 28.05.2013 [cit. 2015-04-18]. Dostupné z:*http://www.atcomp.cz/downloads/cisco/asa_popis.pdf*

[13] PETERKA, Jiří. Internet a bezpečnost. *earchiv.* [online]. ©2011 [cit. 2015-04-18]. Dostupné z: *http://www.earchiv.cz/a98/a814k180.php3*

[14] STĚPÁNEK, Pavel. Demilitarizovaná zóna DMZ – kdy použít, jak nastavit, nejčastější chyby. *Kerio Knowledge base.* [online]. 4.2.2013 [cit. 2015-04-18]. Dostupné z: *http://kb.kerio.com/product/kerio-control-cz-/demilitarizovan%C3%A1-z%C3%B3na-dmz-kdy-pou%C5%BE%C3%ADt-jak-nastavit-nej%C4%8Dast%C4%9Bj%C5%A1%C3%AD-chyby-605.html*

[15] TESAŘ, Jiří. Demilitarizovaná zóna DMZ – kdy použít, jak nastavit, nejčastější chyby. *ICT Security.* [online]. ©2011 [cit. 2015-04-18]. Dostupné z:*http://www.ictsecurity.cz/10/06/2-ids-ips-monitoring/cisco-pokud-ips-blokuje-nejaky-typ-datoveho-toku-musi-si-byt-jista-tim-proc-to-dela.html*

[16] Cisco IPS. Cisco IPS 4200 Series Sensors. [online]. ©1998-2015 [cit. 2015-04-18]. Dostupné z: *http://www.atcomp.cz/downloads/cisco/pruvodce/ips-4200-mid.pdf*

[17] MESSMEROVÁ, Ellen. Kam směrují firewally?. *Computer world.* [online]. 06.04.2015 [cit. 2015-04-18]. Dostupné z:*http://computerworld.cz/securityworld/kam-smeruji-firewally-51925. ISSN* 1210-9924

[18] How to Use CCP to Configure IOS IPS. *Cisco.* [online]. [cit. 2015-04-18]. Dostupné z: *http://www.cisco.com/c/en/us/products/collateral/security/ios-intrusion-prevention-system-ips/prod_white_paper0900aecd8066d265.html*

[19] JAKAB, Vojtěch. *Zabezpečení podnikové sítě technologií IPS* [online]. Brno, 2012 [cit. 2015-05-02]. 68 l. Dostupné z: https://www.vutbr.cz/www_base/zav_prace_soubor_verejne.php?file_id=57788. Bakalářská práce. Vysoké učení technické v Brně. Vedoucí práce Vladimír Červenka.

[20] Systémy detekce a prevence průniku. *ICT Security.* [online]. © 2010 [cit. 2015-04-18]. Dostupné z: *http://www.ictsecurity.cz/odborne-clanky/systemy-detekce-a-prevence-pruniku.html*

[21] WEBER, Filip. Systémy prevence průniků (1) – jen detekovat nestačí. *Svět sítí: Informace ze světa počítačových sítí.* [online]. 5.11.2007 [cit. 2015-04-18]. Dostupné z: *http://www.svetsiti.cz/clanek.asp?cid=Systemy-prevence-pruniku-1–jen-detekovat-nestaci-5112007*

[22] LASEK, Petr. Intrusion prevention system Nová kategorie bezpečnostního řešení. *System Online: S přehledem ve světě informačních technologií.* [online]. 1.2.2005 [cit. 2015-04-18]. Dostupné z: *http://www.systemonline.cz/clanky/intrusion-prevention-system.htm*

[23] Druhy Intrusion Prevention Systems. *bestedates: S přehledem ve světě informačních technologií.* [online]. 22.9.2014 [cit. 2015-04-18]. Dostupné z:*http://www.bestedates.com/druhy-intrusion-prevention-systems/*

[24] SANFILLIPO, Salvatore. hping. . [online]. © 2006 [cit. 2015-05-04]. Dostupné z: *http://www.hping.org/*

[25] DIETRICH, Noah. Snort 2.9.7.x on Ubuntu 12 and 14. *bestedates: with Barnyard2, PulledPork, and BASE.* [online]. 22.9.2014 [cit. 2015-01-14]. Dostupné z: *https://s3.amazonaws.com/snort-org-site/production/document_files/files/000/000/065/original/Snort_2.9.7.x_on_Ubuntu_12_and_14.pdf?AWSAccessKeyId=AKIAIXACIED2SPMSC7GA&Expires=1430564016&Signature=ogRwCkOJcg8pBLAcWHNscwvT7Zs%3D*

[26] ALSADASFEH, Moath Hashim . Configuring Snort as a Firewall on Windows 7 . *National university of Malaysia.* [online]. [cit. 2015-01-14]. Dostupné z:*http://abdnoor80.weebly.com/uploads/1/2/2/8/12282674/configuring_snort.pdf*

[27] Sourcefire, Inc.. SNORT Users Manual . *Snort manual.* [online]. ©2014 [cit. 2015-04-18]. Dostupné z: *http://manual.snort.org/*

SEZNAM ZKRATEK

ASA	Adaptive Security Appliance Adaptivní bezpečnostní zařízení
ASDM	Adaptive Security Device Manager Adaptnivní bezpečnostní manažer zařízení
DAQ	Data Acquisition Přínos dat
DDOS	Distributed Denial of Service Odmítnutí služby
DHCP	Dynamic Host Configuration Protocol Protokol pro přiřazení IP adresy
DNS	Domain Name Systém Systém pro překlad doménových jmen
DMZ	Demilitarized zone Demilitarizovaná zóna
DOS	Denail of Service Odmítnutí služby
FTP	File Transfer Protocol Protokol pro přenos souborů
HIDS	Host Intrusion Detection Systém Systém detekce průniku na koncovém zařízení
HIPS	Host Intrusion Prevention Systém Systém prevence průniku na koncovém zařízení
HTTP	Hypertext Transfer Protocol Protokol pro výměnu hypertextových dokumentů
ICMP	Internet Control Message Protocol Internetový kontrolní protokol
IOS	Internetwork Operating Systém Operační systém Cisco zařízení
IDS	Intrusion Detection Systém Systém detekce průniku
IP	Internet Protocol Internetový protokol
IPS	Intrusion Prevention Systém Systém prevence průniku
ISO	Internation Organization for Standardization Mezinárodní organizace tvorby norem
ISP	Internet Service Provider Poskytovatel internetového připojení
MAC	Media Access Control Fyzická adresa
NAT	Network Adress Translation Překlad síťových adres

NBA	Network Behavior Anomaly Síťové chování anomálií
NIDS	Network Intrusion Detection System Síťový systém detekce průniku
NIPS	Network Intrusion Prevention System Síťový systém prevence průniku
OSI	Open Systems Interconnection Propojení otevřených systémů
P2P	Peer To Peer Rovný s rovným
TCP	Transmission Control Protocol Protokol transportní vrstvy
TFN	Tribe Flood Network Zaplavení sítě
UDP	User Datagram Protocol Protokol bez záruky
VPN	Virtual Private Network Vitrtuální privátní síť
VRT	Vulnerability Research Team Tým zkoumající zranitelnost zabezpečení
WIPS	Wireless Intrusion Prevention System Bezdrátový systém prevence průniku

SEZNAM PŘÍLOH

Příloha A – Přiložené CD

Přiložené CD obsahuje konfigurační soubor s počátečním nastavením aplikace Snort a základní signatury pro blokování a detekci síťového provozu.