Zabezpečení podnikové sítě ve společnosti INPOST, spol. s r.o., Uherské Hradiště

Corporate network security in INPOST Ltd., Uherské Hradiště

Bc. Martin Píštěk

Diplomová práce
2011

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2010/2011

ZADÁNÍ DIPLOMOVÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Bc. Martin PÍŠTĚK**
Osobní číslo:	**A09765**
Studijní program:	**N 3902 Inženýrská informatika**
Studijní obor:	**Informační technologie**
Téma práce:	**Zabezpečení podnikové sítě ve společnosti INPOST, spol. s r.o., Uherské Hradiště**

Zásady pro vypracování:

1. **Proveďte literární rešerši na téma bezpečnosti podnikových informačních systémů.**
2. **Analyzujte současný stav podnikové sítě společnosti INPOST, spol. s.r.o.**
3. **Navrhněte formou projektu vhodný způsob zabezpečení dle zadání.**
4. **Realizujte a ověřte navržená opatření.**
5. **Proveďte vyhodnocení celého projektu.**

Rozsah diplomové práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. **EUGENE, Schultz ; JIM, Mellander ; CARL, Endorf . Hacking – detekce a prevence počítačového útoku . Praha :GRADA, 2005. 356 s. ISBN 80-247-1035-8.**
2. **JIROVSKÝ, Václav. Kybernetická kriminalita . Praha : GRADA, 2007. 288 s. ISBN 978-80-247-1561-2.**
3. **SCAMBRAY, Joel; MCCLURE , Stuart; GEORGE, Kurtz. Hacking bez záhad. Praha : GRADA, 2007. 520 s. ISBN 978-80-247-1502-5.**
4. **PUŽMANOVÁ, Rita. Bezpečnost bezdrátové komunikace . Brno : Computer Press, 2005. 184 s. ISBN 80-251-0791-4.**
5. **LOCKHART, Andrew. Bezpečnost sítí na maximum : 100 tipů a opatření pro okamžité zvýšení bezpečnosti vašeho serveru a sítě. Brno : Computer Press, 2005. 280 s. ISBN 80-251-0805-8.**
6. **RAK, Roman . Biometrie a identita člověka : ve forenzních a komerčních aplikacích. Praha : GRADA, 2008. 664 s. ISBN 978-80-247-2365-5.**
7. **SZOR , Peter. Počítačové viry : analýza útoku a obrana . Brno : Zoner press, 2006. 608 s. ISBN 80-86815-04-8.**

Vedoucí diplomové práce: **doc. Mgr. Roman Jašek, Ph.D.**
Ústav informatiky a umělé inteligence

Datum zadání diplomové práce: **24. února 2011**

Termín odevzdání diplomové práce: **18. května 2011**

Ve Zlíně dne 24. února 2011

L.S.

prof. Ing. Vladimír Vašek, CSc.
děkan

doc. Mgr. Roman Jašek, Ph.D.
ředitel ústavu

ABSTRAKT

Obsahem práce je zabezpečení stávající podnikové sítě pomocí určitých metod a postupů. Pro tento účel je využito několik programů NAGIOS, SNORT, NESSUS. Cílem práce bylo vytvořit bezpečnou a spolehlivou počítačovou síť, odhalit slabá místa v systému a navrhnout patřičné kroky k zvýšení bezpečnosti sítě jako celku. Na základě požadavků vzniklých růstem firmy byly navrženy bezpečnostní postupy, které potvrdily rezervy současného řešení a naznačily další směr vývoje managementu a zabezpečení podnikové sítě.

Klíčová slova: IDS, IPS, Firewall, Routerboard, Honeypot, VPN, TCP/IP, Nessus, Nagios, Snort

ABSTRACT

The contents of my thesis deal with the protection of existing company network using certain methods and procedures. Several programmes, such as NAGIOS, SNORT, NESSUS, are used for this purpose. The objective of my thesis was to create a safe and reliable computer network, identify weak points in the system and suggest appropriate steps to enhance the network security as a whole. Pursuant to the requirements arisen due to the growth of the company, security procedures were proposed that confirmed the reserves of the existing solution and outlined the trend of development of the company network management and security.

Keywords: IDS, IPS, Firewall, Routerboard, Honeypot, VPN, TCP/IP, Nessus, Nagios, Snort

Rád bych touto cestou poděkoval panu doc. Mgr. Romanu Jaškovi, PhD. za obětavý přístup a za ochotu při vedení mojí diplomové práce.

Prohlašuji, že jsem na diplomové práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků, je-li to uvolněno na základě licenční smlouvy, budu uveden jako spoluautor.

Ve Zlíně …….

Podpis diplomanta

ÚVOD

Zabezpečení dnešních podnikových sítí jako celek se zejména v dnešní době stává nezbytnou součástí moderních sítí. Zejména v rozlehlých sítích, kde jsou budovy od sebe vzdáleny a kde jako přenašeč slouží veřejný internet, je velmi důležité zabránit různým útokům, intervencím, které mohou ohrozit samotný chod podnikové sítě nebo citlivá data podnikové sítě. Pro IT manažera moderní počítačové sítě existuje pestrá škála metod a technologií, které umožňují jednak komplexně síť sledovat, vytvářet spolehlivou a více úrovňovou ochranu a zajistit bezproblémový a plynulý chod sítě, mimo jiné i v kritických situacích. V posledních letech vznikly nástroje, které umožňují IT manažerovi dokonce testovat simulovanými útoky hackera, a dokonce vytvářet určité umělé pasti, které simulují nechráněná místa v infrastruktuře sítě, a tím se zdokonalovat v rozpoznávání konkrétních reálných útoků. Tato práce si klade za cíl popsat základní principy a metody instalace a konfigurace těchto nástrojů, provést jejich reálné nasazení, otestování následné úrovně zabezpečení. Důležitou součástí toho zabezpečení je zabezpečení připojení vzdálených prodejen do firemní sítě. V případech, kdy je to reálné a žádoucí, jsou dalším cílem této práce návrhy na změnu současného řešení a hledání různých řešení optimalizace variant. Praktická realizace je provedena a situovaná do prostředí velké potravinářské firmy s mnoha podnikovými prodejnami a několika pobočkami. Dle mého názoru se proto jedná o optimální prostředí, kde je možné testovat všechny tyto nástroje a metody na reálných útocích a pokusit se dosáhnout cílů stanovených v této práci.

I. TEORETICKÁ ČÁST

1 HROZBY PRO BEZPEČNOST SÍTÍ

V dnešním světě je ohrožení počítačových sítí obrovské. Vzhledem ke globální povaze komunikační sítě roste počet míst přicházejících útoků a neustále musíme čelit novým formám těchto útoků. Starý vtip, který koluje mezi správci sítí: „Co je nejbezpečnější počítač na světě?" „Ten, který není zapnutý." A toto platí ještě více i dnes. Proto musíme dosáhnout určité rovnováhy mezi použitelností počítačové sítě a bezpečnostními kontrolami, které používáme.[9]

Ohrožení bezpečnosti sítě jsou obecně rozděleny do dvou základních typů, vnější a vnitřní. Co se týče vnějších útoků prakticky každý podnik dnes je připojen k Internetu. Dokonce i některé vojenské počítačové sítě jsou připojeny k Internetu. Dnes jsme schopni chránit naše sítě pomocí firewallů, systémů prevence narušení, pomocí přístupových seznamů, ovládacích prvků na 2. vrstvě IOS/OSI[1] modelu, aplikační vrstvy firewally, proxy serverů a dalších systémů, které zajistí hloubkovou prevenci a ochranu sítě.

1.1 Vnější hrozby

Vnější hrozby přicházejí od někoho mimo síť, útočník se snaží dostat dovnitř. Mohou mít mnoho různých forem. Jedná se o lidi s různými motivy a dovednostmi. Zároveň pořád vznikají nové způsoby útoků. Následující seznam popisuje některé z prostředků, které jsou používány k pokusu porušení obvodu sítě.[1]

1.1.1 Sociální inženýrství

Napadení nemusí být nutně technologicky založený útok, sociální inženýrství rozhodně může být kvalifikováno jako útok proti důvěrnosti. Typický útočník představuje někoho z technického personálu v podniku, kde buď oběť pracuje, nebo útočí tam, kde by mohli mít účet, např. banky. Útočník se bude snažit sbírat osobní informace od oběti, aby je mohl zneužít. Například by se mohl útočník pokusit získat přístup k online bankovnímu účtu nebo zjistit nějaké citlivé heslo, např. k účtu v kanceláři.[1]

[1] ISO/OSI - standardizovaný síťový model zpracovaný organizací ISO. Úlohou referenčního modelu je poskytnout základnu pro vypracování norem pro účely propojování systémů. Zdroj: [http://cs.wikipedia.org/wiki/Referen%C4%8Dn%C3%AD_model_ISO/OSI].

1.1.2 Odmítnutí služby (DoS)

To je útok, který může vyřadit nebo ochromit systém. Obvykle se jedná jen o obrovské zatížení pakety směřující k cíli. Dále se jedná o zneužití chyby v operačním systému nebo v kódu. Popřípadě to mohlo být použití nesprávně formátovaných dat. Existuje několik specifických typů popření servisních útoků:

- SYN flood - SYN záplavy, je výsledkem použití protokolu TCP three-way hand[2], který způsobuje odmítnutí služby. Útočník posílá mnoho vytvořených paketů s falešnou zdrojovou IP adresou hostitele nebo zařízení jako jsou například firewall nebo směrovač. Útok vyčerpá všechny prostředky směrovače nebo brány firewall, aby to mělo vliv na odmítnutí služby.[1]
- Smurf attack - V tomto útoku jediný host používá falešnou zdrojovou IP, pošle záplavu pingů na vysílací adresu. Je to forma odmítnutí služby. Ovšem dnešní firewally nebo hostitelé jsou obvykle nakonfigurovány tak, aby nereagovaly na tento typ útoků.[1]
- Distribuované odmítnutí služby (DDoS) útoky Botnet[3] je to velmi aktuální téma, kdy jsou počítače zasaženy např. trojskými koni. Poté mohou sloužit pro rozesílání emialu. Tato služba se dá i koupit, poté platíte za klik napadeného uživatele, a tímto botnet jsou velmi výnosné.
- Man-in-the-middle (MITM) útok. Jedná se o klasický útok, při němž útočníci se vloží sebe do středu komunikace, kde mohou sledovat provoz, který jde z jednoho počítače do druhého. Data se mohou tak jednoduše sledovat, či manipulovat s nimi.
- Session hijacking - To je podobné jako man-in-the-middle útok, ale útočník může převzít relaci od oběti a vystupuje jako oběť na trhu. Útočník se snaží získat přístup k ID relace, která je v provozu, zatímco uživatel je připojen.
- Brute force attack – tento způsob útoků používá hrubý výkon zařízení, zkouší všechny možné kombinace, dokud nenalezne ten správný. To platí pro hesla, šifrovací klíče a podobně. Příklad tohoto typu útoku se vyskytuje v bezdrátových sítích. Při zabezpečení bezdrátových sítí, a to pomocí technologie WEP.[18]

Toto jsou jen některé z rostoucího počtu způsobů, jak zaútočit na síť, počítač, nebo aplikaci a jak mohou být zneužity.

---

[2] TCP three-way hand – Dvě TCP zařízení se synchronizují pomocí 3 fazového potřesem rukou (3 – way handshake) Zdroj:[http://www.omnisecu.com/tcpip/tcp-three-way-handshake.htm].

[3] Botnet - je skupina počítačů, které jsou ohroženy, tak že mohou být ovládány třetí osobou. Zdroj:[http://cs.wikipedia.org/wiki/Botnet].

1.2 Vnitřní hrozby

Vnitřní ohrožení sítě - ve kterém je průnik do sítě nebo odcizení dat prováděné lidmi uvnitř vaší organizace. Tyto útoky jsou obecně považovány za nejnebezpečnější druh ohrožení, protože lidé uvnitř vaší organizace mají lepší přístup a více znalostí o síti a zařízeních na sítě. Vnitřní ohrožení může být, když někdo nainstaluje na počítači spolupracovníka keylogger[4] a poté krade hesla pro přístup do systému.[1] Vnitřní hrozby bývají často úspěšné z několika důvodů:

- Nesprávné záplatování
- Výchozí konfigurace a výchozí přednastavená hesla
- Nenásledování doporučení výrobců
- Programovací techniky nezohledňují bezpečnost
- Laxní správcovské postupy.

1.3 Zabezpečení aplikací

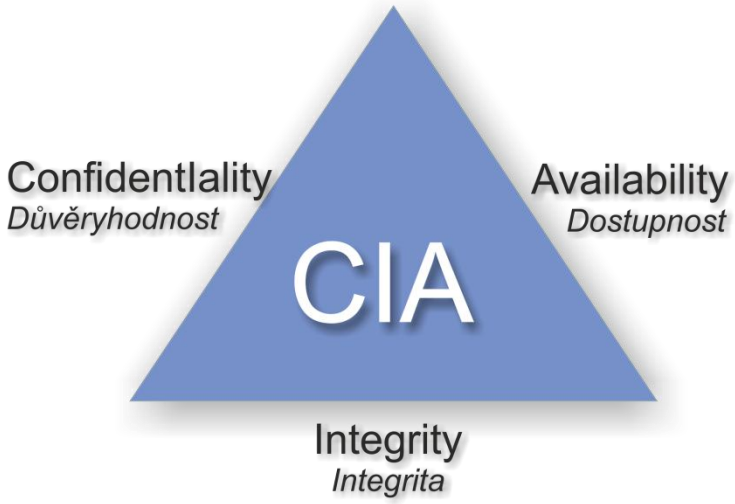
Aplikační útoky jsou pokusy získat kontrolu nad počítačem prostřednictvím sítě nebo nad konkrétní aplikací, často se jedná o webový prohlížeč nebo e-mailovou aplikaci. Aplikační útoky si zaslouží zvláštní zmínku, protože se říká, že představují 75 % všech útoků provedených v dnešním síťovém prostředí. Bývají často úspěšné v důsledku řady faktorů: Nedostatečně rozšířené bezpečnostní programovací praktiky. Programátoři jsou obvykle pod palbou doručit hotový kód co nejrychleji, takže bezpečnost je často zanedbána.

Není firewall, který by ubránil prolomení. Přes veřejné webové služby jsou aplikace přístupné útokům. Existuje stále větší počet bezpečnostních nástrojů a aplikací, které jsou postaveny specificky proti webovým útokům. A mají poměrně snadné použití.[5]

[4] Keylogger - Zaznamenávající stisky je akce sledování (nebo protokolování) kláves úderů na klávesnici. Zdroj: [http://en.wikipedia.org/wiki/Keylogger]

2 ZABEZPEČENÍ SÍTĚ CÍLE

V diskusi o principech bezpečnosti v podnikové sítě se nevyhnutelně dostáváme do styku s trojádou CIA přijde (viz obr. 1.2). CIA je zkratka pro (confidentality) důvěryhodnost, (integrity) integritu a (availability) dostupnost. Tyto jsou známé jako cíle pro zabezpečení sítě. Zde obrázek č.1 CIA trojice [1]



Obr. 1. CIA trojice

2.1 Důvěrnost

Ať už jsou naše data v klidu nebo v pohybu, musíme rozlišovat jejich důvěryhodnost. Šifrování je jedním ze způsobů ochrany důvěrnosti údajů. Například je vhodné při zadávání údajů o kreditní kartě na webu, je lepší využívat protokol HTTPS.

2.2 Integrita

Tato část CIA odkazuje na úsilí, aby zajistila, že odeslaná data dorazí na místo určení beze změny. Jednou z metod kontroly integrity je provádět kontrolu dat pomocí hašovací funkce. Kryptografická hash funkce je definována jako při řetězci proměnné délky na vstupu a pevnou-délka hashe na výstupu. Tyto kontroly pomohou určit, že data, která byla původně odeslána, jsou stejná jako data, která přišla. [1]

2.3 Dostupnost

Jsou data dostupná? Již mnohokrát se stalo, že nebyly dostupné velké e-mailové nebo webové servery. Stali jsme se datově orientovanou společností, a to je znepokojivé, pokud naše údaje nejsou k dispozici.

Jakou metodiku používá hacker k provedení útoku? Každý útok je většinou postaven proti jednomu z těchto tří cílů CIA. Například takové jednoduché znetvoření webové stránky, útok proti integritě? Nebo někdo přidá nepravdivé informace na Wikipedii, poté to někdo čte a věří, že je to pravda? A konečně pokud se někdo dostane do databáze a ukradne údaje o kreditních kartách, došlo k útoku proti důvěrnosti.[1] V tabulce č. 1 jsou vidět různé typy útoků a určité cílé

Tab. 1. Obsahuje seznam cílů, zabezpečení sítě a některých typů útoku

Kategorie útoku	Strategie útoku
Důvěrnost	Man-in-the-middle, odchyt paketů, mapování portů
Integrita	Škodlivý kód/záměna dat, skrytý záznam kláves, proxy
Dostupnost	DDOS, SYN flood, smurf attack

3 KLASIFIKACE DAT

Klasifikace dat je jedním z prvních úkolů, které organizace musí přijmout, aby odpovídajícím způsobem chránila svá data. Musíme znát hodnotu dat, kterou se snažíme ochránit, abychom byli schopni přiřazovat vhodné kontroly?[1]

Následující seznamy ukazují důležité principy klasifikace dat:

- Všechny údaje nejsou rovny.
- Některé údaje mohou být nevhodné nebo poškozující, pokud budou zveřejněny.
- Některá dodržování opatření vyžadují určitou klasifikaci.
- Je důležité se snažit ochránit všechna data, stejně i ta méně důležitá.

Data se třídí v organizacích podle stupně tajení. Stupně utajení se v organizacích liší. Mnoho firem se snaží dodržovat systém klasifikace podobný tomu z mnoha vojenských organizací. Některé organizace necítí potřebu mít pět úrovní dat klasifikací. Mnoho organizací používá vlastní režim, který vyhovuje jejím organizačním potřebám.

4 BEZPEČNOSTNÍ KONTROLY

Bezpečnostní kontroly jsou opatření, jejichž cílem je řídit a snižovat riziko pro vaše data. Bezpečnostní kontroly jsou obecně koncentrované do tří kategorií: administrativní, technické a fyzické. Administrativní kontroly jsou obvykle spojeny s politikami a postupy. Zde jsou některé příklady administrativních kontrol:[1]

- bezpečnostní zásady a postupy
- odborná příprava
- Audity
- Skrytá kontrola zaměstnanců
- Obezřetné postupy při přijímání zaměstnanců
- Rotace úkolů
- Separace povinností

Technické kontroly jsou obvykle o hardwaru a softwaru, jako jsou následující příklady:

- Firewally
- Intrusion Prevention Systems
- Router kontroly přístupu na routery
- Virtuální privátní sítě (VPN) zařízení
- systémy Identity management, TACACS[5], RADIUS[6]
- Síťové systémy administrátorské kontroly
- čipových karet

[5] TACACS (*Terminal Access Controller Access-Control System*, česky *systém řízení přístupu k řadiči terminálového přístupu*) je vzdálený autentizační protokol používaný ke komunikaci s autentizačním serverem. TACACS umožňuje vzdálenému přístupovému serveru komunikovat s autentizačním serverem, aby se rozhodlo, zda má uživatel přístup k síti. Zdoj : [http://cs.wikipedia.org/wiki/TACACS]

[6] RADIUS - Vzdálenou autentizaci přes Uživatel služby (RADIUS) je síťový protokol , který poskytuje centralizované autentizace, autorizace a účtování (AAA) vedení pro počítače připojit a používat síťové služby. Zdoj : [http://en.wikipedia.org/wiki/RADIUS]

Fyzické kontroly jsou typicky ty mechanické. Níže jsou uvedeny příklady z fyzické kontroly:

- Zámky
- Zdroje nepřerušovaného napájení
- diesel generátory
- Pohybová čidla
- Poplachové systémy
- Trezory
- Protipožární systémy

Je třeba říci, že nestačí používat jen jeden typ těchto kontrol. Je důležité je kombinovat mezi sebou.

5 LIDSKÉ FAKTORY

Také v oblasti lidského faktoru je úkol vybudovat skvělý tým, který je schopen reagovat, když se stane nečekaná událost. Nejlepší je, vybrat lidi z mnoha oborů, takže máte zastoupení v rámci celého podniku a schopnost podívat se na daný problém s nějakou úrovní odborných znalostí.

Měli byste vytvořit organizaci systém, který může podporovat dobu odezvy na poruchu do 15 minut až 30 minut. To je z velké části na vedení společnosti, zda tolik peněz a lidských zdrojů je ochotna investovat. Máme-li incident na vzdáleném místě, a jde-li o jinou pobočku vaší organizace nebo na společnosti, musíte se rozhodnout, jestli vám tam na místě může někdo pomoci, nebo tam potřebujete poslat někoho.[1]

Několik dalších prvků, které jsou klíčové v přípravné fázi. Následující seznam obsahuje řadu doporučení:

- Vytvořit komunikační plán.
- Zřídit školení a testy.
- Koordinovat vše se správci systému.
- Mít nouzová hesla a šifrovací klíče k dispozici.
- Mít k dispozici tašku s nářadím, disky, kabely, USB klíče, náhradní baterie, a tak dále.
- Mít k dispozici bootovatelné médium s bezpečnostními nástroji a notebook. Mít k dispozici mobilní telefony a seznamy pro technickou podporu.

5.1 Etika

Etika se odkazuje na soubor norem a zásad, které jsou považovány za správné jako chování v dané situaci. Určité skupiny průmyslových profesí obvykle mají etický kodex a očekávají, že jejich členové nebo složky se budou tímto kodexem řídit. V rámci komunity informační bezpečnosti existuje celá řada etických kodexů vypracovaných organizacemi působícími v odvětví:

- Mezinárodní bezpečnost informačních systémů certifikace Consortium (ISC) 2 etický kodex
- Globál Information Assurance certifikace (Giac) etický kodex
- Informační systémy Security Association (ISSA) etický kodex
- Informační systémy pro audit a kontrolu Association (ISACA) kodexu profesionální etiky
- Internet Architecture Board (IAB)
- obecně uznávaných zásad zabezpečení systému (Gaasp)
- Počítačové Etika ústavu

6 MONITORING PODNIKOVÉ SÍTĚ A NAGIOS

Nagios je open source projekt založený na Unixové platformě. Tento software umožňuje sledovat pakety běhající po síti. Pomocí Nagios je možné sledovat aktivity, jako jsou servery, síťová zařízení a aplikace, v podstatě jakékoli zařízení nebo službu, která má IP adresu a může být kontaktována přes TCP / IP protokol.

Je možné sledovat počítače se systémem Microsoft Windows, Unix /Linux, Novell NetWare, a další operační systémy. Také může být nakonfigurován pro práci přes firewally, VPN tunely, přes SSH tunely a přes internet. Nagios je open source projekt založený na Unixové platformě. Tento software umožňuje sledovat pakety běhající po síti. Pomocí Nagios je možné sledovat aktivity, jako jsou servery, síťová zařízení a aplikace v podstatě jakékoli zařízení nebo službu, která má IP adresu a může být kontaktována přes TCP / IP protokol. Je možné sledovat počítače se systémem Microsoft Windows, Unix /Linux, Novell NetWare, a další operační systémy.[4]

Také může být nakonfigurován pro práci přes firewally, VPN tunely, přes SSH tunely a přes internet. Pomocí Nagiosu je možné sledovat celou řadu atributů na stanicích v síti. Jako jsou provozní aktivity, systémové atributy, jako je procesor, disk a využití paměti pro aplikace, soubory a databáze. Dále může sledovat celou řadu síťových protokolů, včetně HTTP, SNMP a SSH. Nagios může také přijímat SNMP pasti, také se snadno integrovat vlastní kontroly prováděné pomocí různých jazyků, včetně C, Perl a shell skriptů. Nástroj Nagios může být nasazen v distribuovaném modelu s více servery, shromažďování údajů o IT struktuře a podávání zpráv na centrálním serveru, který je ideální pro organizace z různých zeměpisných oblastí, které jsou řízeny z centrálního místa nebo síťového operačního střediska.

Pomocí Nagiosu je možné sledovat celou řadu atributů na stanicích v síti, jako jsou provozní aktivity, systémové atributy, jako je procesor, disk a využití paměti pro aplikace, soubory a databáze. Dále může sledovat celou řadu síťových protokolů, včetně HTTP, SNMP a SSH. Nagios může také přijímat SNMP pasti, také se snadno integrovat vlastní kontroly prováděné pomocí různých jazyků, včetně C, Perl shell skriptů. Nástroj Nagios může být nasazen v distribuovaném modelu s více servery, shromažďování údajů o IT struktuře a podávání zpráv je na centrálním serveru, který je ideální pro organizace z různých zeměpisných oblastí, které jsou řízeny z centrálního místa nebo síťového

[7]operačního střediska. Nagios může být také konfigurován jako redundantní robustní monitoring infrastrukturu, která je schopná obnovy po havárii a failover[8] režimy provozu.

Nagios je vyvíjen jedním vývojářem, Ethan Galstad jako open source projekt. To znamená, že doba mezi vydáváním nových verzí může být dlouhá, ale celkový produkt je pečlivě a rozsáhle testován.

6.1 UMÍSTĚNÍ NAGIOS SERVERU

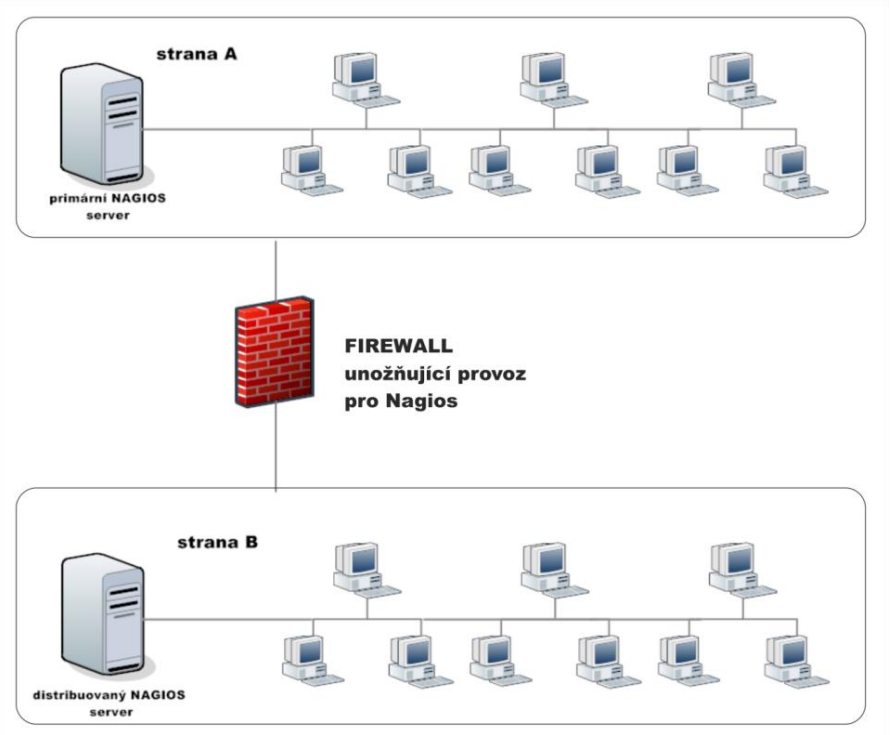
Před samotnou instalací Nagios serveru se musí rozhodnout, kde umístit Nagios server. Kde se nasadí Nagios server nebo servery je důležitou součástí implementace Nagios. Nagios používá Transmission Control Protocol , Internet Protocol (TCP / IP) pro sledování hostí a zařízení. Proto je nutné nasadit Nagios server nebo servery tam, kde mají síťovou viditelnost hostitelů a zařízení, které mají být sledovány.[10]

Máte-li v síťi firewall, síťová nebo filtrační zařízení mezi serverem Nagios a hostitelé mají být monitorováni, pak pravděpodobně není viditelnost hostitelů. Například používáte Internet Control Message Protocol (ICMP) ping pro sledování přítomnosti hostitele, musí zasahovat do síťových zařízení umožňujících ICMP provoz. Pokud tato síť není viditelná, dá se nasadit další server nebo více dalších serverů pro sledování těchto hostitelů.[4]

Nejlepším modelem pro nasazení je další server nebo servery v distribuované konfiguraci, kde výsledky vzdálených serverů Nagios jsou zaslány zpět na centrální server. To znamená, že stačí sledovat pouze jednu webovou konzolu a máte pak jen jednu sadu oznámení. Tato konfigurace vyžaduje možnost konfigurace firewallu nebo jiné síťové zařízení mezi centrálním serverem a distribuovaným serverem. Nagios servery si mezi sebou předávají informace z oddělených sítí. Můžete vidět tuto konfiguraci na obr. 2.

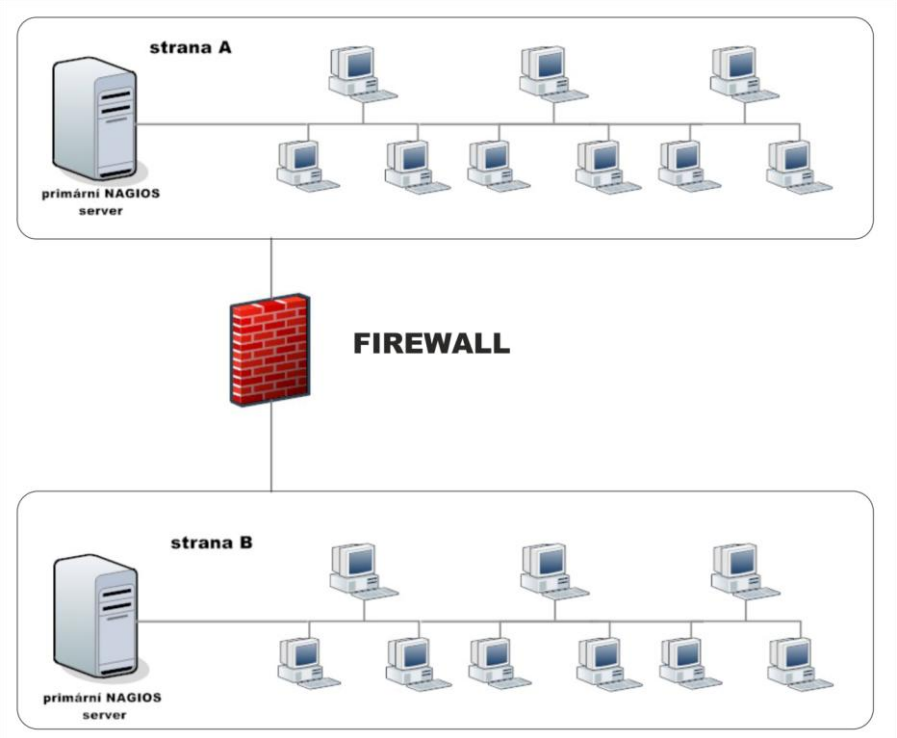
[7] Protokol TCP/IP (Transmission Control Protocol/Internet Protocol) - je standardní sada protokolů navržená pro rozsáhlé sítě segmenty, které jsou propojené pomocí směrovačů. Protokol TCP/IP je základní sadou protokolů používanou v Internetu. Zdroj: [http://technet.microsoft.com/cs-cz/library/cc732974(WS.10).aspx]

[8] Failover – schopnost počítače přejít automaticky do pohotovostního režimu.
Zdroj: [http://en.wikipedia.org/wiki/Failover]



Obr. 2. Servery Nagios v distribuované distribuce

Pokud se nedá konfigurovat firewall nebo síťová zařízení tak, aby tento provoz mezi servery Nagios nefungoval, je třeba je nakonfigurovat jako nezávislé servery. Potom však budou mít Nagios servery svou vlastní webovou konzolu, která by musela být monitorována a potenciálně mít vlastní oznámení o infrastruktuře. Tato konfigurace je patrná na obr. 3.



Obr. 3. Servery Nagios v klasické distribuci

Nasazení serverů Nagios sebou nese bezpečnostní a výkonové důsledky. Nejvíce je to patrné, když jsou monitorovaní hostitelé geograficky vzdáleni a připojeni přes internetové připojení k Nagios serveru. Zejména pokud jsou tyto segmenty sítě připojeny pomalým internetovým připojením nebo nespolehlivým, pak to sebou nese určitá rizika v podobě nedoručených výstrah např. o nefungujících službách monitorovaných serverů.

6.1.1 Výběr software a hardware

Nagios je navržen tak, aby primárně běžel na operačním systému Linux. Neexistuje žádná zvláštní Linux distribuce, kterou se dá doporučit jako platforma operačního systému pro Nagios, a neměl by mít žádné problémy běžet na preferované platformě Linuxu. Měl by úspěšně fungovat na platformě Rudém Hat, Debian, Mandrake, SuSE, Gentoo a distribuce, dále Unix, včetně Sun Solaris, IBM AIX, Mac OS X, a HP-UX. Je poté vybrat si operační systém, který vyhovuje danému prostředí. Nicméně obecně se doporučuje platforma Linux. Většina dokumentace a podporované zdroje, jako jsou internetová fóra,

obvykle nabízí poradenství a podporu informací, které předpokládá, že používáte Linux. Jako hardware doporučuji platformu Intel, protože zaručuje vysokou spolehlivost a relativně nízkou cenu a velkou dostupnost.[10]

6.1.2 Dimenzování kapacity

Dimenzování serveru Nagios je velmi závislé na prostředí a úmyslu, co chceme sledovat. Protože počet hostitelů a služby, které chceme sledovat a kontrolovat, to má velký vliv na výkonnost hostitele pro server Nagios. Existuje několik základních pravidel pro přesné určení, kolik služeb a počítačů můžete sledovat na určité hardwarové konfiguraci. Stejně jako u většiny aplikací, tři hlavní faktory ovlivňující výkonnost Nagios jsou CPU, velikost operační paměti RAM a volné místa na disku HDD.[1]

Tabulka 3 obsahuje některé údaje o počtu hostitelů, můžete sledovat s konkrétní konfigurací.

Tab. 2. Výkonové specifikace podle počtu uživatelů Nagios

Počet připojených Hostů	Počet CPU	Kmitočet CPU	Operační paměť RAM	Kapacita HDD
< 100	1	800MHz+	512MB+	5GB+
100–500	1	1GHz+	1GB+	10GB+
500–1000	1+	3GHz+	1GB+	20GB+
> 1000	1+	3GHz+	2GB+	40GB+

6.1.3 Instalace softwaru Nagios

Nagios zařízení se skládají ze dvou hlavních částí Nagios serveru a Nagios plug-inů. Nagios server je jádrem řešení Nagios a plní vykonávané funkce, jako je tlumočení konfigurace, spuštění webové konzole a zasílání oznámení a kontroly.[4]

Nagios plug-iny poskytují rozhraní pro počítače, zařízení a aplikace a umožní je sledovat, například plug-in balíček obsahuje plug-in nazvaný check_mysql, který vám umožní sledovat stav databáze MySQL[9]. Dále také obsahuje plug-inů, kterými lze zkontrolovat

[9] MySQL - je relační databázový systém (RDBMS) od společnosti Microsoft.
Zdroj: [http://en.wikipedia.org/wiki/MySQL]

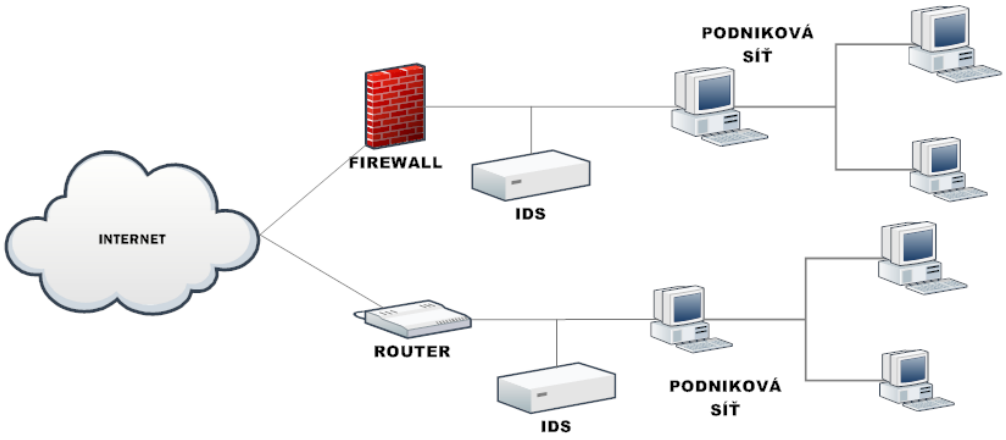
společně síťové služby přes TCP, User Datagram Protocol (UDP), nebo ICMP. A další, které umožňují sledovat lokální zdroje, jako je CPU, paměť RAM a volné místo na disku.

6.1.4 Předpoklady pro instalaci softwaru Nagios

Nejdříve je potřeba provést kompilaci ze zdrojových kódů, budete potřebovat kompilátor C pro vytvoření, jak pro server Nagios i plug-iny. Pokud instalujete na server a plug-iny z balíku, jako RPM, není potřeba kompilátor. Pokud chceme používat webovou Nagios konzoli, musíme nainstalovat: webový server, doporučuji server Apache a GD knihovnu, která se používá pro zobrazení grafů a různých výstupů. Po instalaci C kompilátoru je třeba nainstalovat Apache Web Server.[10]

7 SYSTÉMY IDS

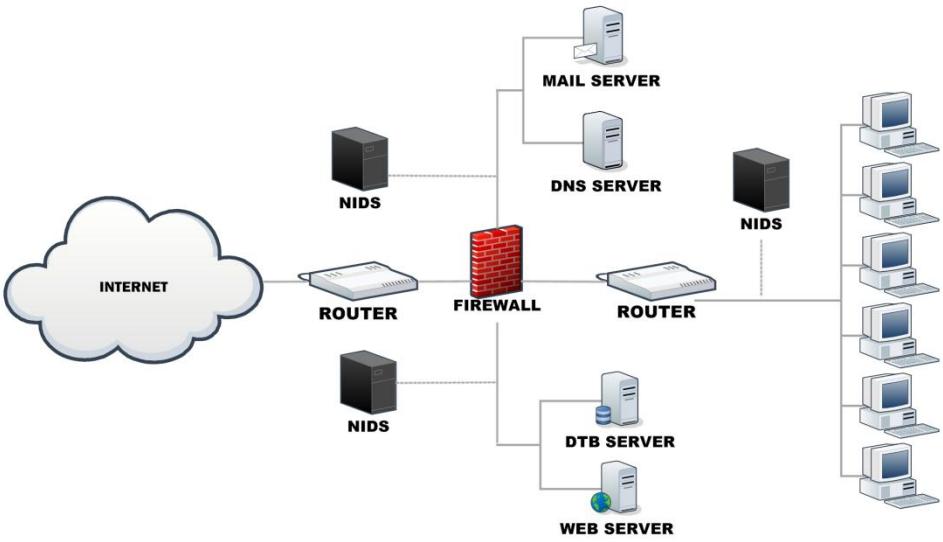
Zabezpečení podnikové sítě je dnes velký problém pro všechny sítě a v dnešním podnikovém prostředí provedli útočníci a hackeři mnoho úspěšných pokusů, a tak dokázali shodit spoustu sítí ve velkých společnostech a webových službách. Proto byly vyvinuty metody pro zajištění síťové infrastruktury a komunikace přes internet, mezi nimi je i používání firewallů, šifrování a vizualizace privátních sítí. Detekce narušení bezpečnosti je poměrně nový přírůstek do těchto typů datových technik. Detekce narušení bezpečnosti se začaly objevovat během několika posledních let. Používání detekce narušení bezpečnosti umožňuje shromažďovat informace o běžných typech útoků a zjistit, pokud se někdo snaží zaútočit na síť nebo na konkrétního hostitele. Informace shromážděné tímto způsobem mohou být použity k upevnění zabezpečení sítě, rovněž také pro právní účely. Komerční i open-source jsou k dispozici v hojné míře. Na trhu je také široká paleta nástrojů pro hodnocení zranitelnosti podnikové sítě, které dokážou odhalit a poté posoudit různé typy bezpečnostních děr.



Obr. 4. Ukázka zapojení IDS v podnikové síti

7.1 NIDS

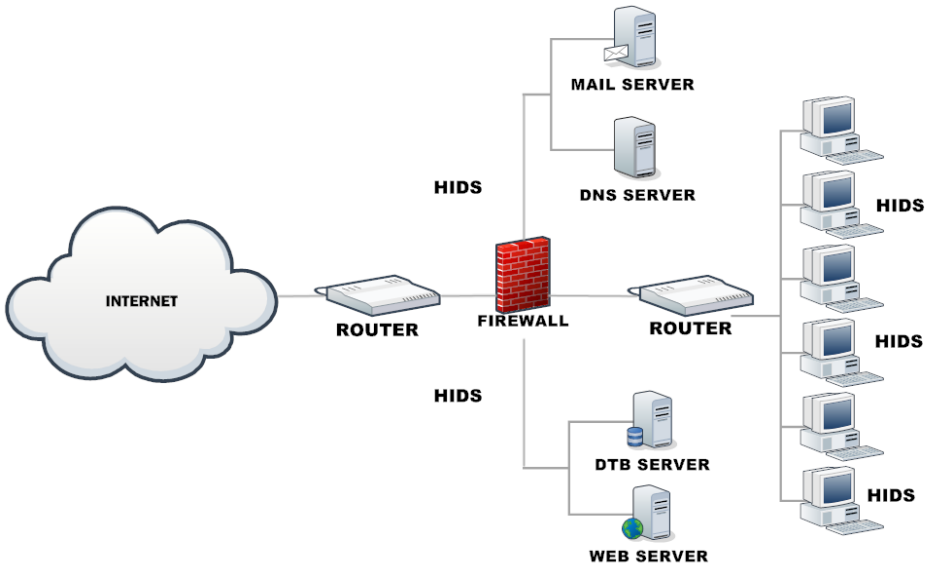
Network IDS jsou systémy narušení bezpečnosti, kde pakety zachytí data na cestách mezi síťovými medii (kabely, bezdrátové připojení) a následně přiřadí k databázi signatur. V závislosti na tom, zda-lije poket označen s podpisem vetřelce, je zaznamenán do databáze. [7] Zapojení NIDS v síti znázorňuje Obr. č. 5.



Obr. 5. Umístění NIDS v síti

7.2 HIDS

Host-based systémy detekce průniku jsou instalovány jako agenti na hostitelských stanicích. Tyto systémy detekce průniku nahlíží do systémových souborů a do aplikačních logů a zjišťují případné činnosti vetřelce. Některé z těchto systémů jsou reaktivní, což znamená, že vás informují pouze tehdy, kdež se něco stalo. Některé host-based IDS jsou aktivní a mohou kontrolovat síťový provoz na konkrétní počítač, na kterém je nainstalován HIDS a upozorní vás v reálném čase. [11] Zapojení HIDS v síti znázorňuje Obr. č. 6.



Obr. 6. Umístění HIDS v síti

7.2.1 Záznamy

Záznamy jsou určitým druhem oznámení vetřelcově činnosti. Když IDS detekuje vetřelce, má tato služba poslat upozornění a informovat tím správce zabezpečení o tomto útoku. Záznamy existují ve formě pop-up oken, logování do konzole, posílání emailů a jiných. Záznamy se ukládají do log souborů nebo databází, kde jsou poté zpřístupněny bezpečnostním odborníkům. Snort může také generovat upozornění o mnoha formách narušení systému díky výstupním pluk- inů. Snort může také poslat určitý záznam do více destinací. Například je možné do log záznamů, log do databáze a přitom generovat SNMP pasti a vše současně. Některé modely plug-in můžou být také upraveny, aby obtěžování hostů bylo blokováno na firewallu nebo hlavním routeru.[12]

Zprávy protokolu jsou obvykle uloženy v souboru. Ve výchozím nastavení ukládá Snort tyto zprávy do adresáře /var/log/snort. Nicméně lze umístění těchto zpráv měnit v příkazovém řádku při spuštění. Zprávy bývají uloženy v různých databázových serverech, kde jsou pak vyhodnocovány buď ručně uživatelem, nebo specializovaným programem například Prelude.[10]

[10] Prelude – Používá se v kombinaci ze Snort jak HIDS Zdroj: [http://www.dusatko.org/cs/node/121]

8 IDS SNORT

Snort je program, který patří do kategorie programů systémů detekce průniku. Snort je vyvíjen jako open-source. Jeho hlavní funkce je odposlech v síti a detekci útoků. Na základě rozpoznání různých vzorků útoků v síti provádí různé akce bez toho, aniž by nějakým způsobem narušil síťový provoz. Snort byl vyvinut tak, aby podporoval různé operační systémy. Proto jde bez problému nainstalovat na platformy Windows NT/2000/XP[11]

8.1 Režimy Snortu

Snort ke své funkci může běžet ve třech různých módech. Jako network introstution systém móde (režim detekce narušení systému). Sniffer móde (režim slídění) a nakonec režim pocket dogger móde (režim záznamníku).

- Network intrusion detection systém mode – Tento mód je nejvýznamnější u snortu. Snort v tomto režimů sleduje síťový provoz, odchytává síťová data, poté provádí jejich analýzu. Výsledky této analýzy porovná s uživatelem definovanými profily a na základě této analýzy Snort může provádět určité akce.[7]
- Sniffer mode – V tomto módu Snort zachytává pakety, které procházejí sítí a zobrazuje je uživateli na jeho obrazovku. Tento mód je jen informativní, žádné akce Snort neprovádí.
- Packet dogger mode – Jedená se o rozšířený sniffer mode, data jsou ale zaznamenávány do logu[15]
- Inline - tento mód získává tapety s ip adres na základě konfigurovaných pravidel rozhodne o zahození či povolení paketů. Pokud pracuje v tomto modu, pracuje s velkým HIDS.[2]

8.2 Komponenty Snortu[7]

Program Snort je rozdělen na komponenty, tyto komponenty spolu pracují a detekují útoky a generují z něj výstupy v určitém formátu. Snort jako IDS se skládá z následujících hlavních komponent:

- Jednotka paketového záchytu
- Zásuvné moduly preprocesoru
- Detekční jednotka
- Systém logování a výstrah
- Výstupní zásuvné moduly

9 PENETRAČNÍ TESTOVÁNÍ

V bezpečnostní analýze bezpečnosti vnitrofiremní sítě jsou penetrační testy velmi důležitou součástí. Používají se zde různé nástroje, kterými jsou prováděny pokusy o proniknutí k různým částem informačního systému. Penetrační testy prakticky simulují chování hackera, který se snaží proniknout do naší sítě. Tyto útoky mohou být z vnější sítě, kdy je útok směřován z vnější strany firewallu, zpravidla to bývá z Internetu na servery umístěné za firewallem. Nebo jsou tyto útoky směřovány z vnitřní sítě na infrastrukturu sítě a servery. Tento průnik do systému je buďto fyzicky realizován přítomným hackerem, který připojil vlastní počítač do interní sítě, nebo má přístup k počítači v napadené síti. Existuje ale také ještě způsob, kdy hacker nachytá uživatele, poté mu přednastaví spustitelný kód a potom převezme vládu nad jeho počítačem. Tímto způsobem může zcizit citlivá data, popřípadě z tohoto počítače vést další útoky. V současné době vzhledem ke komplexnosti operačních systémů je nacházeno stále více bezpečnostních děr (security holes). Určité skupiny lidí hlavně z Internetu využívají bezpečnostních děr a tvoří programy, které jsou schopny napadnout informační systém společnosti. Tyto programy jsou pak volně dostupné na Internetu a někteří uživatelé již nepotřebují žádné speciální znalosti, stačí jim pouze využít tyto volně dostupné programy. Dle statistik 90% všech uskutečněných útoků provádějí vlastní zaměstnanci organizace.

9.1 Jak vypadají útoky a jaké mohou způsobit škody

Útoky, které mohou způsobit škody na informačním systému společnosti, se projevují takto:

9.1.1 Odmítnutí služby

Nebo taky DoD (Denial of Service), DDoD (Distributed Denial of Service). Odmítnutí služby, nebo distribuované odmítnutí služby. Jedná se o způsob útoku hackera na internetové služby HTTP, FTP, kdy je služba, popřípadě server, přehlcen požadavky od útočníka až do fáze, kdy dojde k pádu systému. Poté dojde k nefunkčnosti, a tudíž nedostupnosti pro uživatele, kteří chtějí např. vidět aktuální ceník služeb na vašem webu. Útočník tímto útokem na informační systém sleduje hlavně tyto cíle: První je narušení komunikace mezi klientem a serverem, aby následná komunikace byla pomalá anebo se stala úplně nefunkční. Druhý cíl útoku je opakované resetování cílového serveru.[7]

9.1.2 Neoprávněný přístup

Útočník v tomto případě získává přístup k serveru, službám, datům. Ten toto využije k provedení neautorizovaných změn v konfiguraci, mazaní souborů, modifikaci souborů a jiným změnám. Většinou bývá toto zařízení či server používán jako výchozí bod pro provádění dalších útoků na jiná zařízení.

9.1.3 Získání důvěryhodných informací

Cílem tohoto útoku je získávání citlivých informací, většinou firemního charakteru. Zahrnuje většinou různé seznamy uživatelských jmen a hesel, dat z účetnictví, databáze mezd, různých interních ceníků apod.[12]

9.2 Průběh samotného testování

Při vlastní analýze tohoto útoku se test spouští na jednotlivé stanice, servery i aktivní prvky. A v případě vnějšího testování jsou testovány všechny prvky, které jsou viditelné z externí sítě.[16]

Před samotným testováním je třeba zvážit, zda se do testu zařadí také již zmíněné DoS útoky. Je možné, že v průběhu testování budou určitá zařízení dočasně vyřazena z provozu, nebo budou vyžadovat restart. Testy se provádějí tak, aby nebyl narušen provoz systému na uživatelské úrovni. Testy se provádí ve shodě s normami ČSN ISO/IEC TR 13335 a ČSN ISO/IEC 17799. Útočníci se snaží používat postupy či nástroje, které hledají slabá místa v systému.

Během penetračního testování se na zařízeních detekují následující metody:

- Firewally

Slouží k oddělení lokální sítě od okolních hrozeb. Musí čelit rozsáhlému množství specifických zranitelností, jako jsou DoS útoky, změny směrování apod.

- Backdoory

Škodlivý kód – napsaný program, který umožní hackerovi získat přístup ke stroji, na kterém ty program již běží. Může zde také provádět změny prostřednictvím vzdálené administrace. Tento program se na počítač dostane bez vědomí uživatele, například prostřednictví nebezpečné přílohy u obdrženého e-mailu.[12]

- Mailové systémy

Většina systémů emailové komunikace má velké množství závažných bezpečnostních chyb, útočník pak může využít mail server k posílání vlastních zpráv z cizího poštovního serveru. Takto se projevuje spam.

- DNS systémy

Tato služba nebo server se stará o převod jmenné adresy počítače, nebo síťového zdroje, například utb.fai.cz do formátu číselné IP adresy. Pokud je DNS špatně nakonfigurováno, existují zde možnosti zneužití této služby. Projevuje se předstíráním identity síťového zařízení.

- FTP systémy

FTP - File Transfer Protocol. Tyto systémy využívají nebo poskytují službu, která umožňuje přenos souborů. Jsou ohroženy velkým množstvím různých potenciálních zranitelností v souvislosti s operačním systémem a verzí FTP serveru.[12]

- Síťové odposlouchávání

Zde existuje nebezpečí v lokálních počítačových sítích, a tím je problém síťového odposlouchávání. Kterýkoliv uživatel v této síti může bez problému stáhnout z Internetu volně dostupný program, který mu umožní monitorovat jednotlivé pakety s daty. Takže potom může sledovat jednu určitou osobu a u ní vystopovat zadávání hesel, příchozí a odchozí poštu, jaké webové stránky si osoba prohlíží apod.

- CGI sripty

Jde o skript nebo taky skupinu příkazů, které provádějí určitou činnost, obvykle bývají umístěny na www serverech. Útočník tímto způsobem získává vládu nad www serverem.

- LDAP

Systémy LDAP jsou systémy, které využívají adresářovou službu LDAP (Lightweight Directory Access Protocol). Při použití této služby hrozí riziko zneužití neoprávněnými uživateli.

- NFS systémy

Network file systém je používán nejčastěji v systémech UNIX. Tato technologie zpřístupňuje data na síti lokálním uživatelům. Bezpečnostní riziko zde spočívá v možném neautorizovaném přístupu k síťovým diskům.

- Systémy založení na RPC

Remote procedure call - využívá vzdálené volání procedur. Útočník při napadení získává plného přístupu k zařízení

- Systémy na sdílení zdrojů

Tyto systémy jsou využívány ke sdílení dat mezi uživateli lokální sítě, např. diskový prostor. Používá se zde technologie samba apod. Riziko spočívá v možnosti neautorizovaného přístupu útočníka.

- SNMP systémy

Simple Network Management Protocol se využívá pro vzdálenou správu aktivních prvků sítě. Útočník při útoku může např. změnit adresaci celé sítě.

- X WINDOW systémy

Grafická nadstavba operačních systémů UNIX. Existuje určitá množina zranitelností. V důsledku může útočník např. monitorovat komunikaci mezi X serverem a stanicí.[12]

10 HONEY POTS

Honey pots neboli hrnce medu jsou systémy používané k návnadě hackery tím, že vystaví známým typům zranitelností úmyslně. Poté co hacker nalezne Honey pot, je velmi pravděpodobné, že se zde nějakou chvíli zdrží. Během této doby si můžeme zjistit jeho činnosti a odhalit jeho akce a techniky. Tyto informace nám poté pomohou při zabezpečení podnikové sítě. Existují různé způsoby, jak nastavit místo pro Honeypoty.[14]

Honey pot by měl běžet společně s ostatními službami. Tyto společné služby zahrnují Telnet server (port 23), Hyper Text Transfer Protocol (HTTP) server (port 80), File Transfer Protocol (FTP) server (port 21) a tak dále. Honey pot by měl být umístěn někde v blízkosti důležitých serverů tak, aby ho hackeři považovali za skutečný server. Například pokud servery budou mít IP adresy 192.168.10.21 a 192.168.10.23, můžete tak přiřadit IP adresu 192.168.10.22 k Honey potu.[17]

Můžete také nastavit firewall nebo router a přesměrovat tak provoz na některých portech k Honey potu tam, kde si vetřelec myslí, že je připojen skutečný server. Měli bychom být opatrní při vytváření výstražného mechanismu, když je ohrožen váš Honey pot, musí být toto napadení okamžitě oznámeno. Je také dobré, aby logovací soubory byly na jiném zařízení tak, aby když je ohrožena Honey pot, aby hacker neměl možnost odstranit tyto soubory. Proč by se tedy měly ve firemních sítích instalovat Honey poty? Odpověď závisí na různých kritériích, včetně následujících:

- Honey poty by se měly instalovat, pokud organizace má dostatek zdrojů na to, aby mohla vystupovat s hackery. Tyto zdroje zahrnují jak hardware, tak
- personál. Pokud nejsou tyto zdroje, není třeba instalovat Honey poty.
- Honey pot je užitečný pouze tehdy, pokud chcete použít informace shromážděné z těchto útoků k vylepšení zabezpečení podnikové sítě
- Honey poty se také dají použít, chceme-li stíhat hackery tím, že sbíráme svědectví o jejich činnosti.

II. PRAKTICKÁ ČÁST

11 POPIS ZADÁNÍ A POŽADAVKŮ NA ZABEZPEČENÍ SÍTĚ

Pro popis praktického řešení zavedení systémů pro zvýšení bezpečnosti jsem využil zkušeností a znalostí při údržbě a samotné realizaci podnikové sítě ve společnosti INPOST, kde působím 6 rokem jako IT manažer a zároveň technická podpora v oboru Informační technologie. Společnost INPOST, spol. s r.o. patří k nejvýznamnějším producentům masných výrobků v České republice a také v Evropské unii. Má několik středisek a rozsáhlou síť maloobchodních prodejen, včetně osmi prodejen ve Slovenské republice. Podniková síť společnosti INPOST, spol. s r.o. tedy představuje klasickou rozlehlou infrastrukturu, která je permanentně vystavena spoustě útoků na narušení bezpečnosti a spolehlivosti. Je tedy nutné zajistit spolehlivý chod, stalý automatizovaný dohled a bezpečnost celé sítě. Vše ovšem při využití dostupných prostředků a zachování transparentnosti celého systému.

Tato práce může sloužit jako jakási šablona pro zabezpečení firemní sítě, a tím pádem je v obecném měřítku použitelná pro jakoukoli firmu či organizaci nezáleže na velikosti. Cílem je tedy nalézt a popsat princip a postup při řešení, který zůstává stejný, protože se dané řešení dá různými způsoby modifikovat, upravovat kapacitně, a tím přizpůsobovat velikosti, výkonnosti daného rozsahem určité dané sítě. Ať už jsou požadavky složitějšího charakteru, a tím i spojených požadavků finančních nároků na realizaci.

Vrátíme-li se tedy zpět k základnímu požadavku pro vybudování bezpečné podnikové sítě ve společnosti INPOST, spol. s r.o., nejprve tedy bude nutné analyzovat současné problémy a definovat zadání, které se dá rozdělit do pěti základních kategorií:

1. Vytvoření managementu podnikové sítě kvůli zajištění globálního sledování procesů a stability aktivních síťových prvků, samotných stanic i počítačových periferií
2. Zajištění spolehlivého VPN připojení podnikových prodejen a zajistit spolehlivý chod i při výpadcích
3. Nastavit několika stupňový firewall, který oddělí síť prodejen, oddělí síť firmám v podnájmu využívající stejné internetové připojení
4. Vytvořit silný systém detekce průniku kvůli zabezpečení proti útokům na síť
5. Provést bezpečností audit a odhalit tak slabá místa jednotlivých řešení

12 FIREWALL A JEHO NASTAVENÍ

O funkci firewalu se ve společnosti INPOST stará produkt české společnosti XtendLan, typ XRT-570, který běží na platformě x86.Operační systém na něm běží RouterOS. Jedná se o hlavní router ve společnosti INPOST. Vzhledem k rychlému růstu firmy, zejména otevření nových prodejen, nahradil původní model XRT-504, který měl ovšem omezený výkon a taky následnou spolehlivost. Rovněž také měl omezený počet licencí na připojení vzdálených poboček do VPN.

Nové XRT-570 nabízí také svobodnější možnost konfigurace, a tím také větší možnosti nastavení sítě, hlavně v oblasti zabezpečení. Jak již bylo zmíněno na XRT-570 je nainstalován RouterOS[11] od lotyšské firmy Mikrotik[12]. Díky této platformě nabízí velmi svobodné nastavení pomocí různých inteface. Defakto každý port ze sedmi portů se dá nastavit dle libosti. Můžu například jednomu přiřadit WAN, druhému switch funkce a na další třeba port mirroring. Toto nastavení nenabízí žádná platforma včetně lídrů CISCO systém, RIT technologies a hlavně je tato platforma volně šiřitelná.

Obr. 7. XRT 570 od společnosti XtendLan

Configurace zařízení a vlastně všech zařízení se systémem RouterOS se děje několika způsoby. Přes webovou konzoli, Winbox popřípadě přímými příkazy v bashi RouterOS. Já pro svou konfiguraci využívám Winbox[13]. Zejména kvůli rychlému přístupu i z prostředí Windows a přehlednosti a možnosti konfigurace.

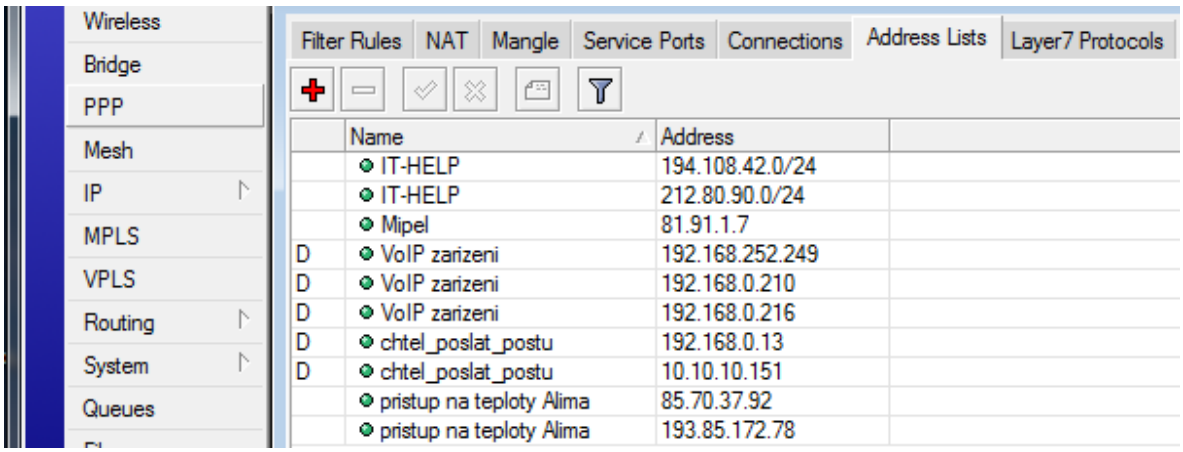
[11] RouterOS je operační systém zejména pro platformu RouterBOARD. Umí funkce směrování, firewall, řízení šířky pásma, bezdrátový přístupový bod, páteřní spojení, hotspot brána, VPN server a další. Zdroj: [http://www.mikrotik.com/software.html]

[12] Mikrotik - MikroTik byla založena v roce 1995 k rozvoji bezdrátových směrovačů a ISP systémů. Tato společnost vznikla v roce 1995. V roce 2002 vytvořila vlastní hardware, RouterBOARD. Zdroj: [http://www.mikrotik.com/index.html]

[13] Winbox - Winbox je konfigurační nástroj, který lze připojit k routeru přes MAC nebo IP protokolu. Zdroj: [http://wiki.mikrotik.com/wiki/Manual:First_time_startup]

12.1 Adress List v nastavení Firewallu

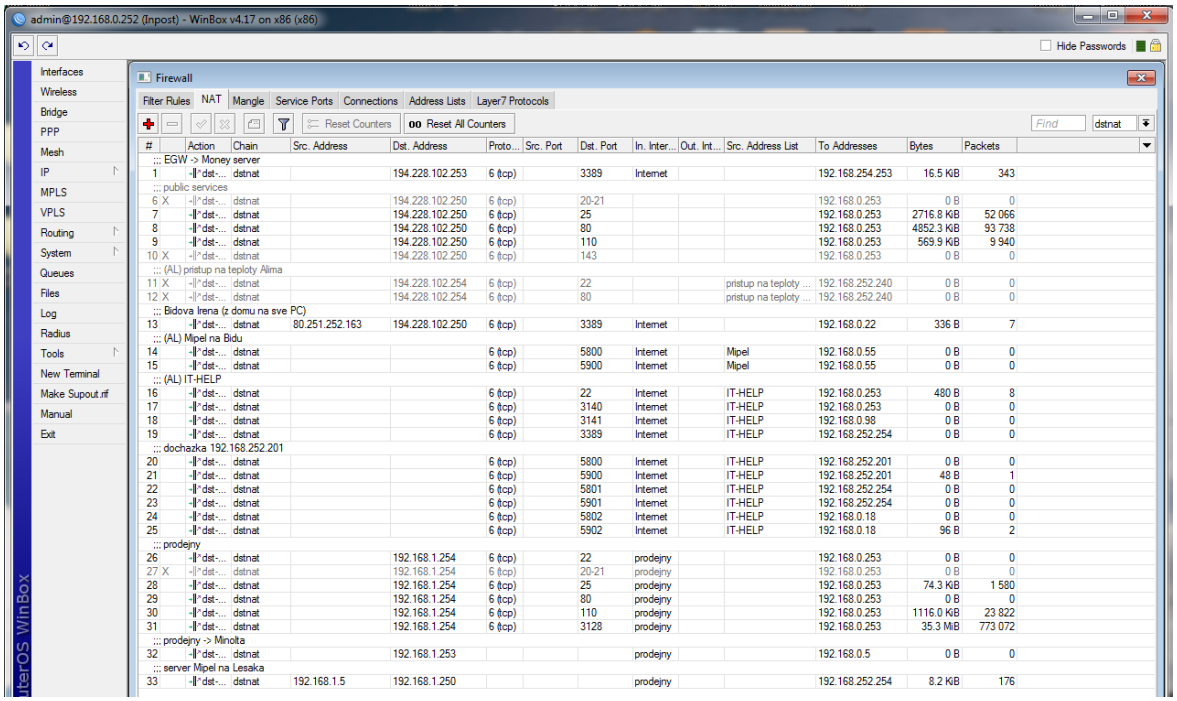
Adress List je použit zejména k nastavení určitých rozhraní firewallu, v případě INPOST, spol, s r.o. je využit zejména pro přístup různých outsourcingových firem, které zajišťují chod např. POS systému či databázových programů. Dále jsou zde nastaveny webové servery pro přístup na systémy zaznamenávající teploty v chladnicích a mrazicích zařízeních. Zadává se zde veřejná IP adresu například z Brna a ve firewallu je nastaveno, kam tyto adresy směrovat a kam je vlastně v síti pustit, děje se tam díky různým pravidlům a povolováním určitých portů.



Obr. 8. Winbox – Adress List

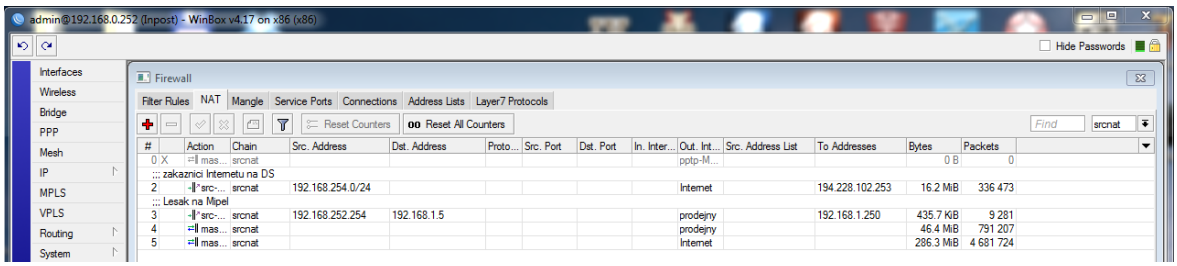
12.2 Nastavení NAT ve Firewallu

Nastavení NAT se skládá ze dvou základních sekcí destination NAT a source NAT. Ve společnosti INPOST se zadávají hlavně destination NAT, kde jsou vlastně zakotveny veškerá pravidla pro přístupy různých outsourcingových firem. Jsou zde také nastavena pravidla pro směrování serverů a pro připojení (kapitola 14). Obrázek č 15 ukazuje snímek z konfigurace destination NAT.



Obr. 9. Winbox – nastavení destination NAT

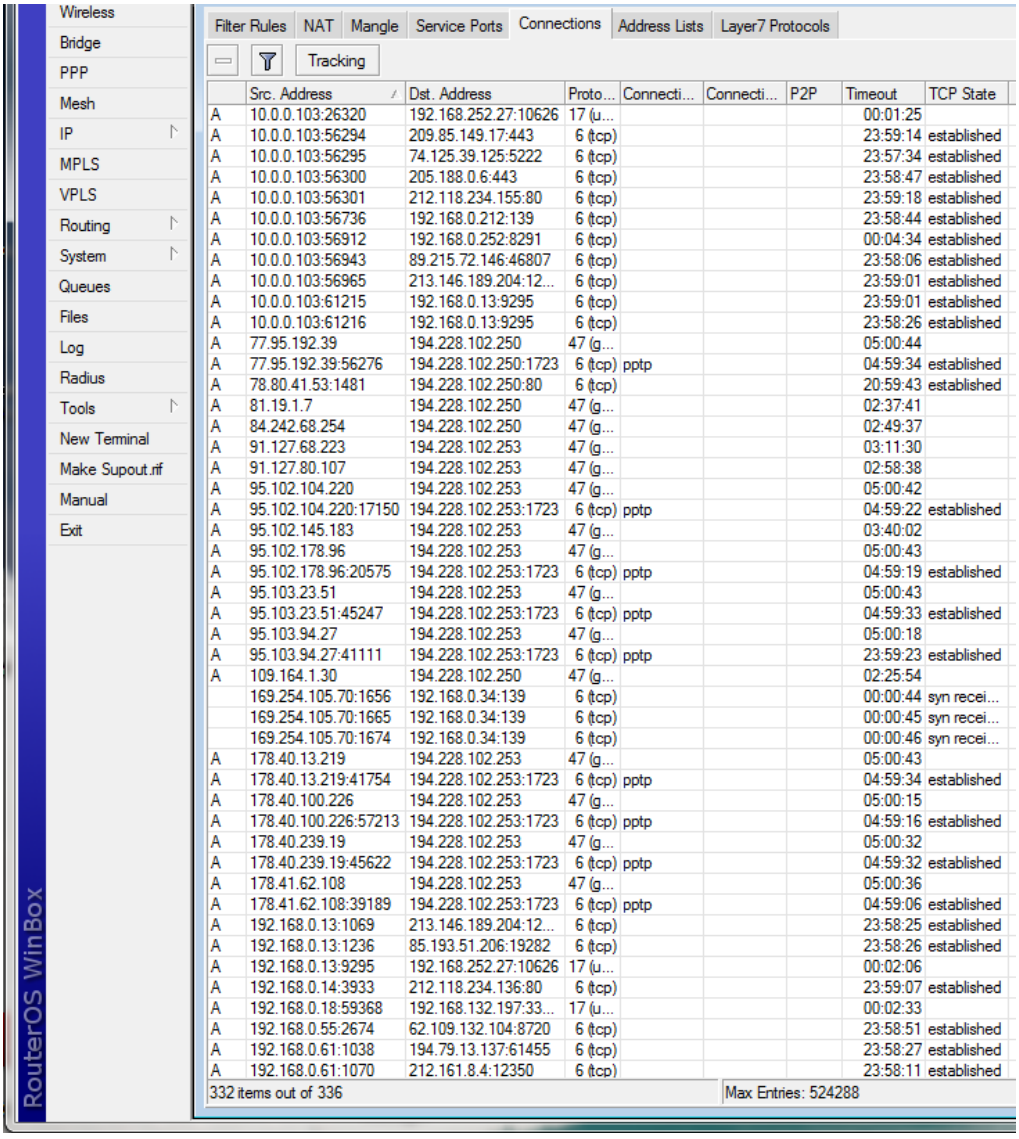
V nastavení source NAT najdeme jen nastavení pro zákazníky využívající Internet na distribučním středisku a směrování databázového serveru se serverem prodejen, kvůli jiné adresaci – tedy kvůli bezpečnosti. Oddělení některých sítí je jedním ze základních pravidel pro nastavení firewallu. Například síť prodejen je oddělená od lokálních sítí například obchodního oddělí, a tak se velmi omezí šíření škodlivých dat i přístupu nežádoucích osob mezi sítěmi. Nastavení source NAT v INPOST, spol s r.o. zobrazuje obrázek č. 15.



Obr. 10. Winbox – nastavení source NAT

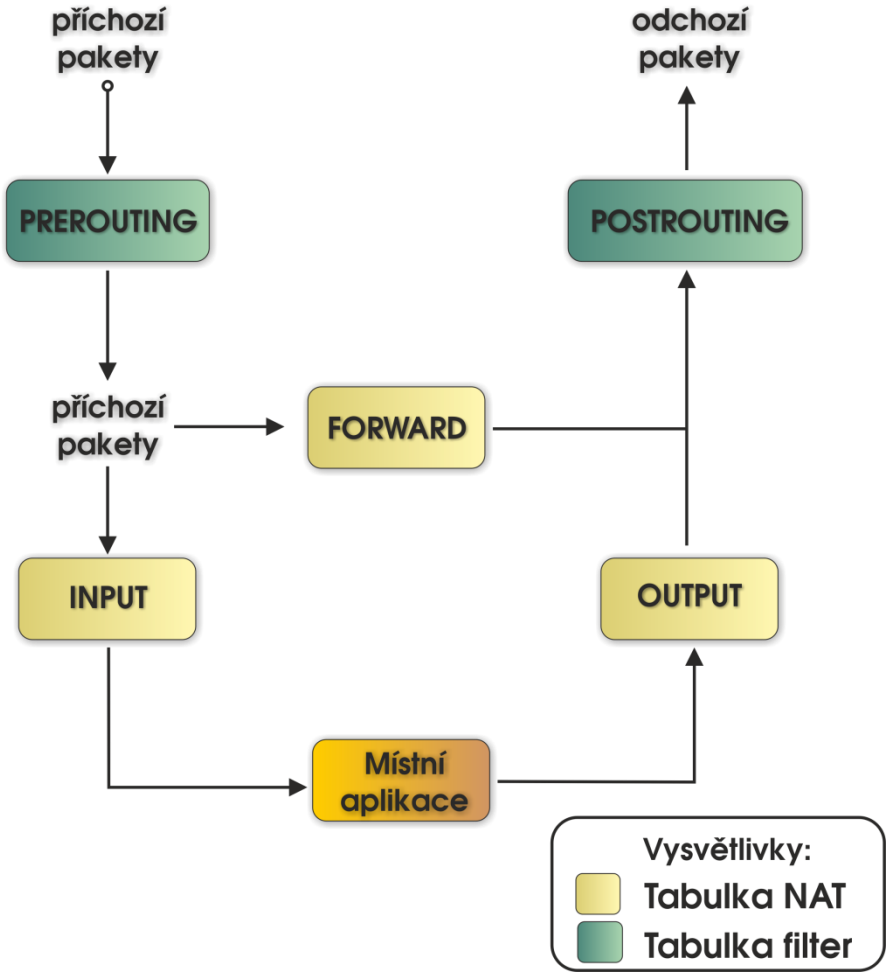
V sekci „connection“ můžeme vidět veškerý provoz procházející přes XRT 570 (Obr. 7.) Je zde k vidění:

- Source Address – venkovní adresa, ze které přichází spojení nebo požadavek
- Destination Address – cílová adresa, na kterou jsou jednotlivá spojní směrována
- Protokol – tato položka ukazuje použitý protokol
- Timeout – jedná se o časovou odezvu
- TCP State – dle protokolu ukazuje status připojení



Obr. 11. Winbox – zobrazení všech připojení

Celkové fungování firewallu jsem zobrazil na následujícím schématu (Obr. 12). Je to lepší pro pochopení postupu přes různé parametry firewallu. Skutečné schéma by ovšem bylo velmi složité, některá pravidla ve firewallu jsou nastavena tak, že data se několikrát firewallem protočí a jsou různě vracena do různých sekcí.



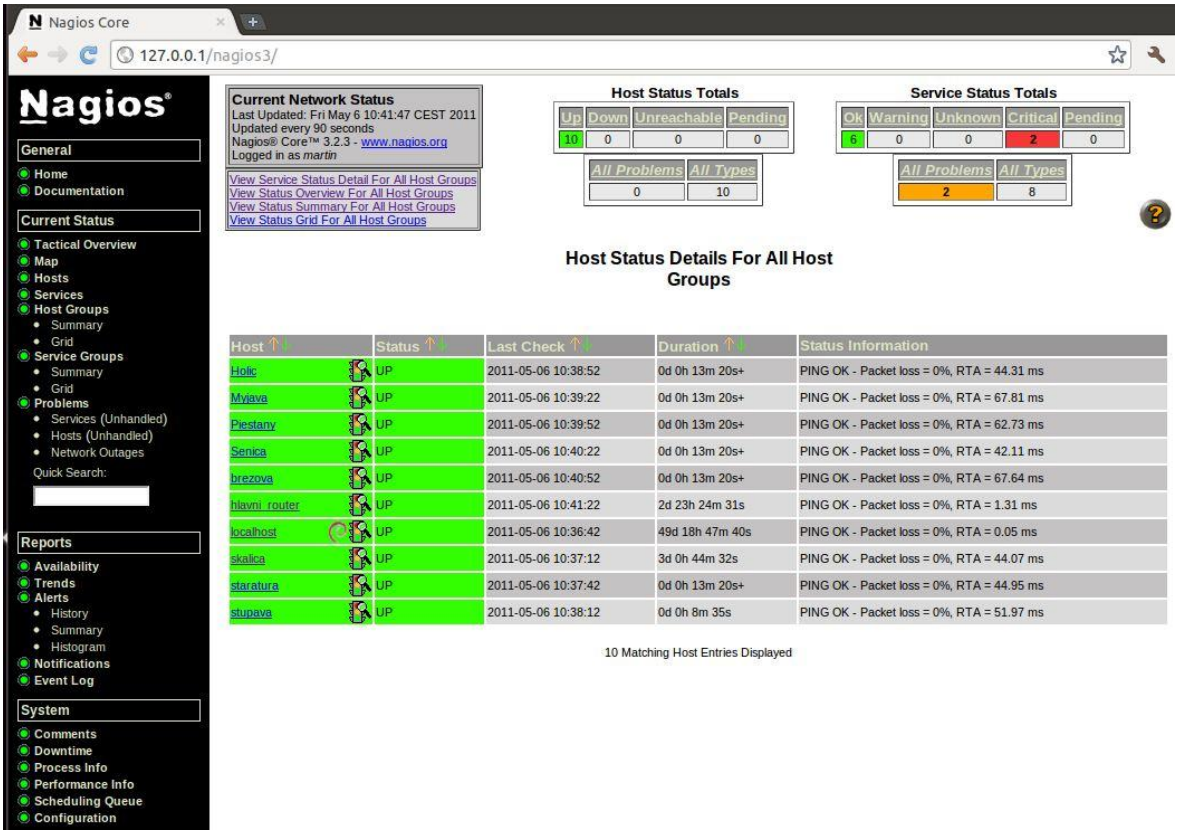
Obr. 12. Schéma fungování firewallů na RouterOS

13 VYTVOŘENÍ MANAGEMENTU SÍTĚ A SYSTÉM NAGIOS

Jako prvním krokem bylo vytvoření managementu sítě a implementace do sítě. Jako management sítě jsem opět kvůli finanční nenáročnosti vybral produkt NEGIOS. Systém Nagios velmi napomohl k monitoringu sítě. Na webové konzoly mohu jako správce hned od příchodu do zaměstnání monitorovat důležitá místa v síti INPOST, spol. s r.o. Je to důležité zejména při monitoringu nejdůležitějších aktivních komponent v síti. Mezi sledované patří hlavní routery a administrovatelné switche ve firmě, samozřejmě všechny servery, protože ty při výpadku serveru se většinou zhroutí celý segment sítě nebo služba nutná například pro distribuci nových ceníků do maloobchodní sítě prodejen. Monitoruje ale také hlavní tiskárny na jednotlivých střediscích a také monitoruje pokladní systémy všech prodejen, protože se vždy jedná o poruchu na vzdáleném místě od centrály, proto je třeba se o poruše dozvědět velmi rychle, ne od obslužného personálu při ověřování funkčnosti služeb. Nagios také umožňuje sledování funkčností různých služeb běžících na počítači, také umí sledovat volné prostředky a volné místo na pevném disku počítače. Ovšem tyto služby již vyžadují nainstalované agenty na samotných monitorovaných stanicích. Z tohoto důvodu v současné době monitoruji jen 2 stanice i s těmito službami, popravdě řečeno v praktické administraci nevyžaduji monitoring těchto služeb, navíc již zmíněný monitoring služeb vyžaduje nainstalovaného agenta, který ovšem bere určitý výkon daného zařízení.

13.1 Instalace NAGIOS

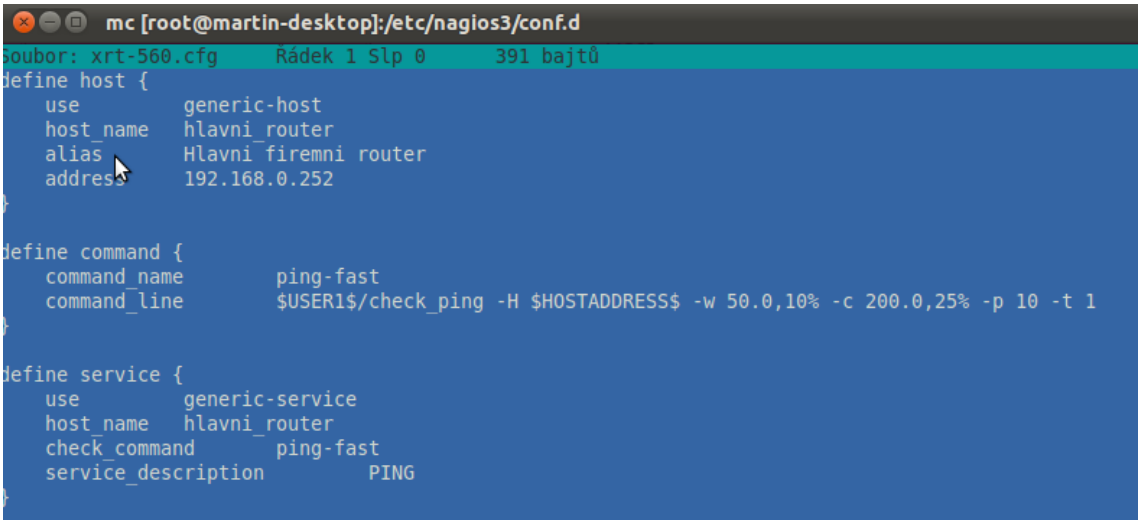
Pro samotnou instalaci byl vybrán opět Pc, na který jsem nainstaloval opět systém Ubuntu ve své poslední verzi. Nejnovější verzi využívám také z důvodů bezpečnosti a výkonu systému. Instalace proběhla z balíku klasicky pomocí příkazu apt-get a získal jsem s ní nejnovější verzi 3.0. Ovšem pro zprovoznění webové konzole jsem potřeboval na serveru zprovoznit Apache server. Apache server jsem nainstaloval vzhledem k aktuálnosti z centra software v Ubuntu. Po restartu jsem nastavil v adresáři /etc/nagios3/ editací nakonfiguroval soubor apache2.conf a nastavil Apache na adresu 127.0.0.1 a nastavil další jednoduché parametry. Poté jsem již ve webovém prohlížeči zadal adresu 127.0.0.1/nagios3/ a spustil jsem webovou konzoly, ovšem s nezadanými stanicemi. Ještě bylo nutné tato monitorovaná místa nakonfigurovat.



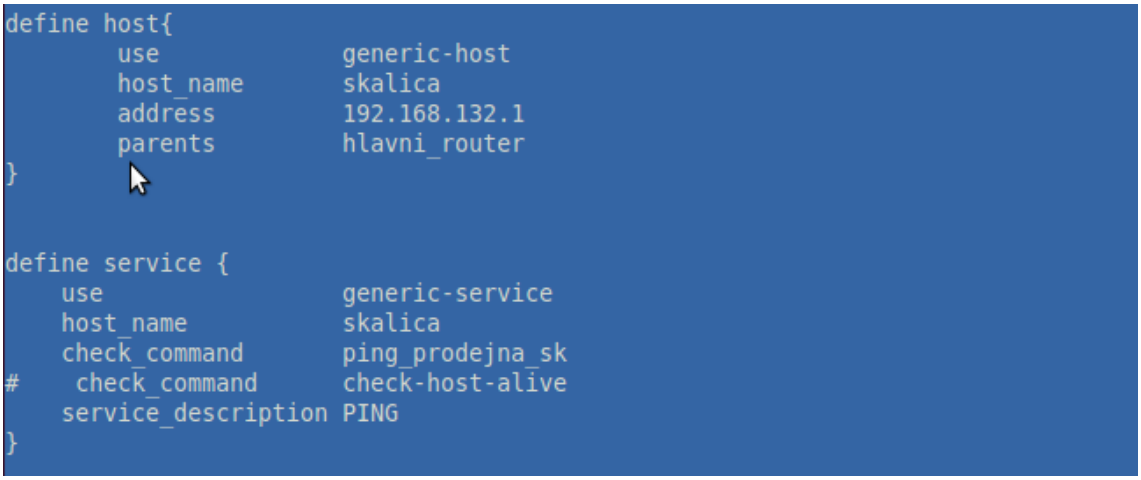
Obr. 13. Webové rozhraní NAGIOS

13.2 Konfigurace NAGIOS nastavení sledovaných míst v síti

Systém Nagios jsem konfiguroval pomocí editace souborů v adresáři /etc/nagios3/conf.d. Zde jsou umístěny soubory host.conf, service.conf, atd. Tyto soubory se dají hierarchicky rozdělit podle tiskáren, PC stanic, routerů, serverů, uživatel má zde velmi svobodnou ruku. Dále jsem nastavil jednotlivé služby, u těchto služeb jsem využíval jen službu ping na protokolu ICMP. Jak jsem již uvedl, ostatní plug – iny Nagios jsem zkoušel jen na dvou stanicích a jedna z nich byl kamerový server, u kterého hrozilo přeplnění disku video záznamem z kamer. Proto jsem musel na stanici nainstalovat agenta, který odesílal sesbírané informace serveru nagios. Ukázky editací souborů znázorňují obrázky č. 14 a č. 16, kde je zobrazen hlavní router a maloobchodní prodejna ve Slovenské republice.



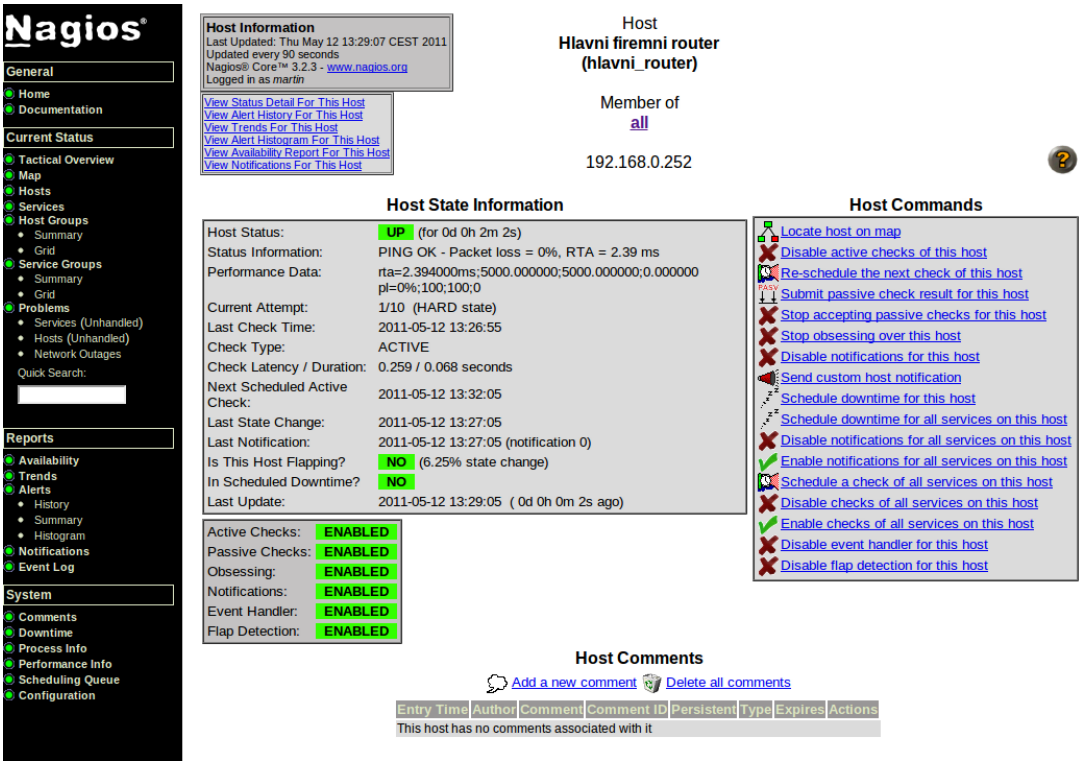
Obr. 14. Ukázka Konfigurace hlavního routeru NAGIOSu



Obr. 15. Ukázka konfigurace vzdálené prodejny ve Skalici na Slovensku

Po konfiguraci těchto souborů je nutné příkazem nagios -v ověřit správnost nastavení konfigurace. Toto se děje, pokud špatně zadáte například služby, tak Nagios se nespustí, takto se dozvíte, co jste zadali špatně.

Ve webové konzole je ještě možnost prohlížet si statistiku kontrol definovaného hosta. Jako je aktuální status, doba latence, doba odpovědi na ping, kdy Nagios naplánoval další test a mnoho dalších. Vše záleží na konfiguraci Nagios a možnosti nainstalovaných plug-inů Nagios. Tuto obrazovku s hostem můžete vidět na obrázku č. 16, kde je zobrazen hlavní router INPOST, spol. s r.o.



Obr. 16. Nagios – host Hlavní router

14 VPN PŘÍPOJENÍ FIREMNÍCH PRODEJEN

14.1 VPN ve firemní síti

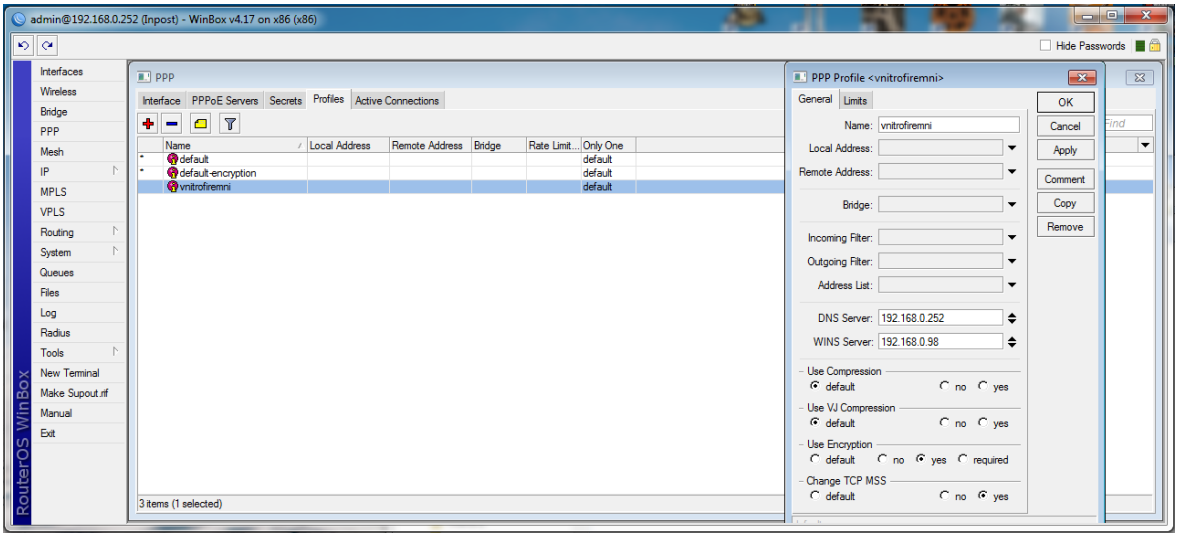
V souvislosti s vysokým nárůstem nově otevřených prodejen a zejména s masivním rozšířením vysokorychlostního Internetu bylo nutné vybudovat VPN pro prodejny jednak po území celé Moravy a jednak ve Slovenské republice. Co se týče připojení prodejen v České republice, běží tyto prodejny na službě O2 VPN lite, která byla společnosti INPOST, nabídnuta v rámci služby ADSL 8M. Na Slovensku jsou prodejny připojeny pomocí služby T-Com Internet Magic II. Obě tyto služby jsou nastaveny tak že prodejny jsou neustále v on-line režimu a dálkově posílají na centrálu data o tržbách, skladech, popřípadě stahují nové ceníky atd. Obě VPN připojení samozřejmě nabízí připojení na vzdálené plochy kas i počítačů v zázemí prodejen. Rovněž se dá sledovat, zdali jsou na prodejnách připojeny váhy, protože mají přidělenou svoji IP adresu, proto je tedy můžu sledovat pomocí systému Nagios.

14.1.1 Vzdálené připojení firemních prodejen ve Slovenské republice

Pro připojení slovenských maloobchodních prodejen jsem využil protokol PPPTP[14], tento protokol je obsažen téměř v každé vyšší verzi zařízení s nainstalovaným systémem RouterOS. Rovněž jsem tedy využil služeb naše XRT 570. Nejdříve jsem pomocí Winboxu v položce Profiles vytvořil tři typy profilů. Dva z nich jsou určeny pro připojení různých outsourcingových firem. Ale jeden z nich vnitrofiremní jsem vytvořil právě pro připojení prodejen v tomto případě na Slovensku, jak je vidět na obrázku č. 17. Je třeba také zvolit položku use encryption, která bude data kódovat pomocí technologie MPPE 128 stateless[15].

[14] PPTP - Point-to-Point Tunneling Protocol (PPTP) je metoda pro realizaci virtuálních privátních sítí. PPTP využívá řídicí kanál přes TCP a tunelu GRE provoz k zapouzdření PPP paketů.
Zdroj: [http://en.wikipedia.org/wiki/Point-to-Point_Tunneling_Protocol]

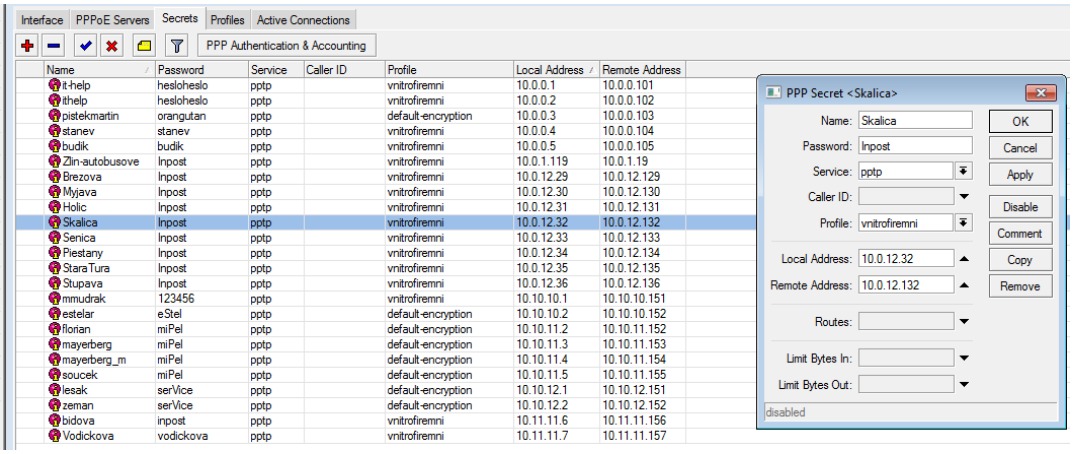
[15] MPPE 128 stateless - Microsoft Point-to-Point Encryption (MPPE) je protokol pro šifrování dat přes Point-to-Point Protocol (PPP) a virtuální privátní sítě (VPN) spojení.
Zdroj: [http://en.wikipedia.org/wiki/Microsoft_Point-to-Point_Encryption]



Obr. 17. Winbox – Profiles - nastavení profilů pro prodejny

V další fázi jsem pomocí Winboxu nastavil položku Secrets, kde jsem přidal všechny prodejny. Tady jsem nastavil:

- Název služby - z důvodů orientace, hlavně slouží jako uživatelské jméno
- Heslo pro přístup v PPTP serveru
- Profil - již vytvořený vnitropodnikový
- Lokální IP adresa
- Vzdálená IP adresa



Obr. 18. Winbox – Secret – nastavení pro jednotlivé prodejny

s ukázkou prodejny Skalica

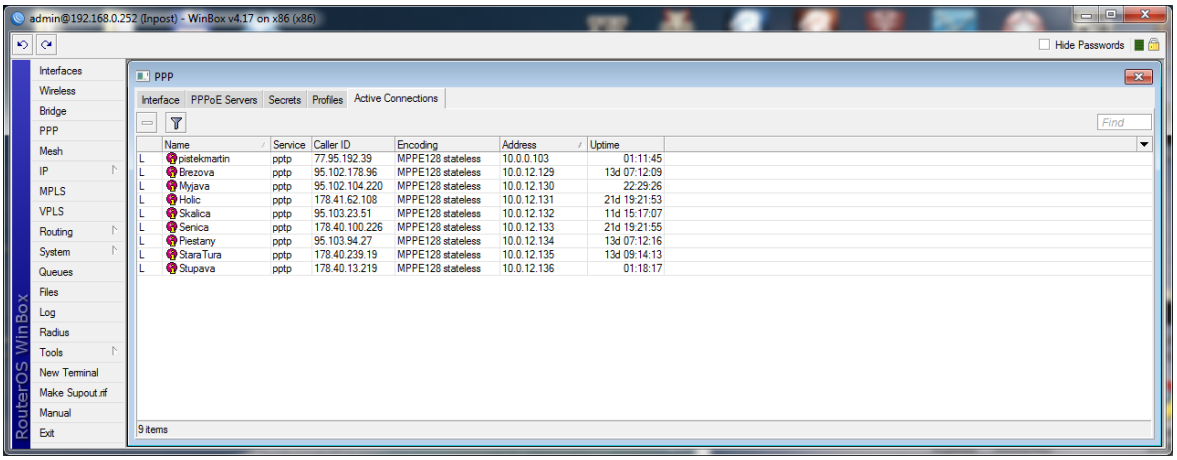
Na straně prodejen je možné se k připojení PPTP serveru samozřejmě využít klasické VPN připojení z Windows. Pomocí tunelového připojení a kódování MS-CHAP v2[16]. V našem případě jsem využil nákladu na pořízení již zmiňovaných RouterBoardů RB750 (Obr. 19). Tyto RouterBoardy jsem nastavil přímo pro toto připojení k našemu PPTP serveru.

Obr. 19. RouterBoard RB 750 pohled dovnitř zařízení

Pro tyto RouterBoardy jsem po ověření jejich stability vytvořil skript, který využívám při nastavení nových připojení prodejen. Takže na RouterBoard pustím skript a jen změním přihlašovací jméno a heslo, popřípadě IP adresu, kterou jsem nastavil v položce Secret na PPTP serveu a vše je nastaveno. Tento router se poté zapojí přímo na ADSL router od T-Comu a routerboard dále switchuje další zařízení za tímto RouterBoardem, váhy na prodejně, počítač pokladna i PC v zázemí prodejny popřípadě jednu až tři IP kamery. RouterBoard zjistí, že má připojení na Internet a okamžitě se snaží připojit k PPTP

[16] MS-CHAP v2 - MS-CHAP je verze Microsoft Challenge-Handshake Authentication protokolu CHAP Zdroj: [http://en.wikipedia.org/wiki/MS-CHAP]

serveru. Toto je obrovská výhoda oproti tunelovému připojí pomocí služeb Windows, protože zde, když vypadne Internet, tak se odpojí od serveru a po obnově spojení je třeba se připojit znovu ručně. Do budoucna se také plánuje plošné nasazení VoIP telefonie. Na toto řešení jsou RouterBoardy také připraveny porty 5050 a 5060 jdou upřednostnit například před porty 80, 25, 110, a to kvůli plynulosti hovoru po Internetu. Na obrázku je vidět soupis připojených VPN zařízení, zajímavý je Uptime neboli čas připojení, který jsou prodejny připojeny, v některých místech se celkový čas pohybuje v týdnech. U některých prodejen je třeba jen 22 hodin, toto ukazuje na nestejnorodou kvalitu ADSL služeb jako celku.



Obr. 20. Aktivní spojení VPN

14.1.2 Vzdálené připojení firemních prodejen v České republice

Pro připojení prodejen v České republice využíváme službu O2 VPN lite, která běží na službě ADSL 8M. Jelikož se jedná o outsourcingovou službu a veškeré routery (v našem případě CISCO 876 Obr. 21), jsou majetkem společnosti Telefonica O2, pro administrační rozhraní mně nejsou zpřístupněny a veškerou konfiguraci zajišťují technici O2.

O2 VPN Expres Lite umožňuje připojení jednoho pracoviště nebo malé LAN (lokální síť menší pobočky) do podnikové virtuální privátní sítě (VPN). V přístupové síti využívá

technologii ADSL a nabízí rychlosti až 8 a 16 Mbit/s v závislosti na délce a kvalitě přístupového okruhu. Pro připojení k VPN je využíván protokol IP Sec. V ceně služby je zahrnuto přístupové vedení a koncové zařízení (router) umístěné u zákazníka.

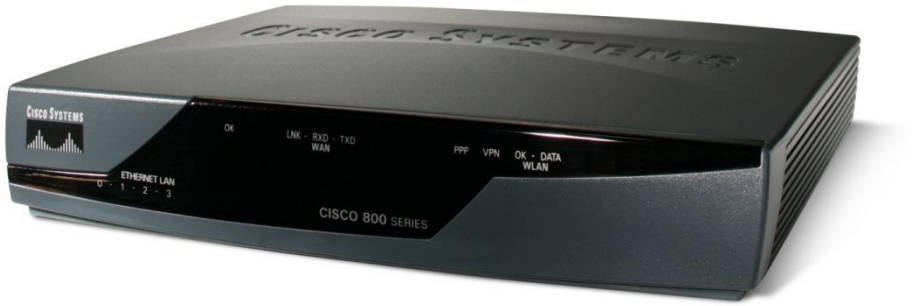
Základní parametry:

Asymetrické rychlostní profily až do 8 M/512 a 16 M/512

Agregace v páteřní síti 1:50

Zákaznické koncové zařízení (CPE): Cisco 876

Předávací rozhraní: port routeru, ethernet, RJ-45, IPv4



Obr. 21. CISCO 876 koncový router na prodejnách v ČR

15 VYTVOŘENÍ SYSTÉMU DETEKCE PRŮNIKU

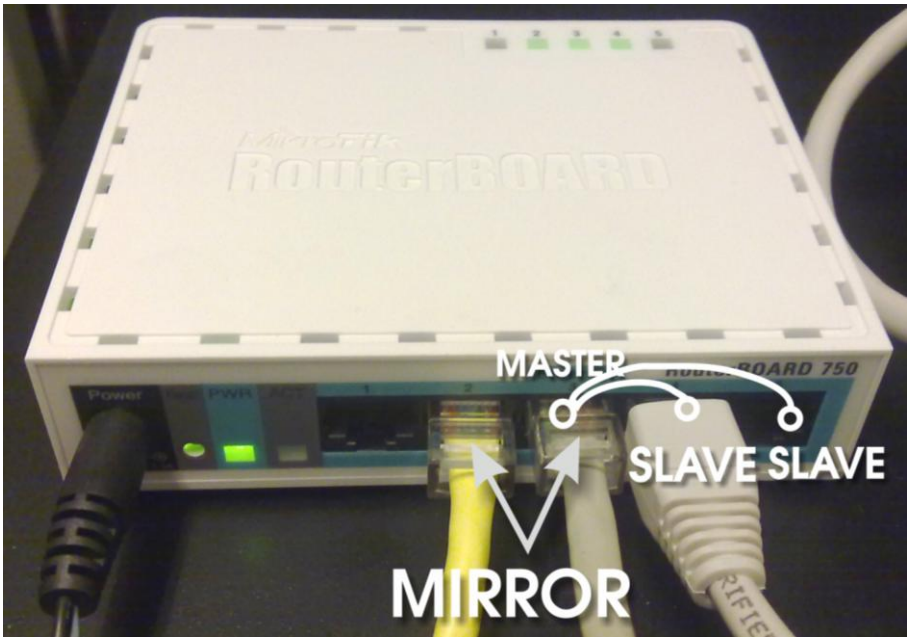
Zavedení systému detekce průniku umožní ve společnosti INPOST, spol. s r.o. mnohem intenzivněji sledovat anomálie, či dokonce samotné útoky běhající po této síti. Ve společnosti INPOST pracuje na počítačích zhruba třetina celé firmy, tedy zhruba 150 pracovních stanic. Proto není v mých silách ohlídat takové množství potencionálních útočníků na tyto stanice nebo na důležité servery, které jsou nezbytné pro samotný chod celé společnosti. Nasazení detekce průniku je proto nezbytná v takto rozsáhlé síti.

15.1 Vytvoření port mirroringu

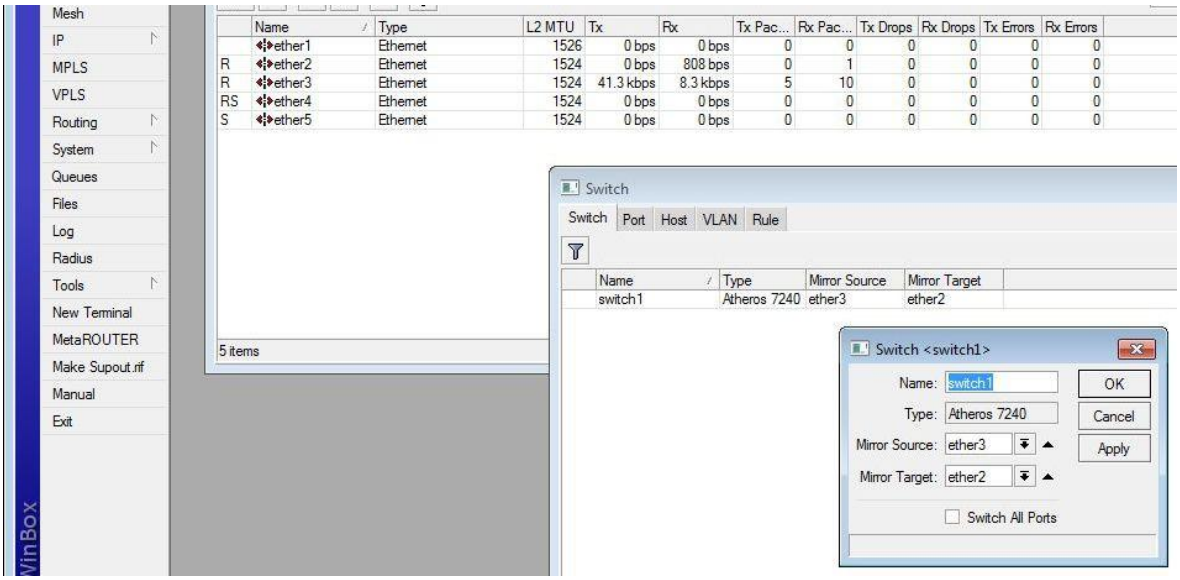
Před samotným nasazením je nezbytné upravit stávající zapojení v hlavním rozvaděči, aby detekcí neovlivňoval žádným způsobem jakékoliv parametry sítě. Pokud například všechny prodejny začnou přibližně ve stejnou dobu stahovat nové ceníky z centrály a zároveň na tento server posílat data o tržbách a kladu, je velmi dobře vidět, jak tento výkon ovlivní spoustu faktorů. Například pokud se v tu samou dobu začnou synchronizovat data z prodejen a z distribučního střediska, chvílemi se provoz zastavuje. Proto, jak jsem již uvedl, nemůžu síti odebrat další jednotky výkonu.

Tuto situaci jsem vyřešil funkcí port mirrororing[17] respektive port span od CISCO systems. Tato funkce umožňuje zrcadlit určitý port, v našem případě se jedná o hlavní port, ze kterého jsou směrovány všechna data letící do firmy a ven. K této funkci jsem přidal na tento port RouterBoard RB 750, který umožňuje díky přeinstalovanému RouterOS na něm nastavovat jednotlivé porty dle potřeby. Na tento mirroringový port napojím tento port a takto budu schcopen monitorovat celý provoz sítě bez omezení jejího výkonu. Způsob toho Routerboardu zapojení popisuje obr. Č 22, rovněž ukázku nastavení pomocí Winboxu znázorňuje obrázek č 23, na kterém je vidět způsob nastavení jednotlivých ethernetových portu Routerboardu.

[17] Port Mirroring je používán na síťový přepínač zaslat kopii sítě pakety vidět na jednom portu přepínače (nebo celá VLAN) pro monitorování sítě, připojení na jiný port přepínače. Zdroj: [http://en.wikipedia.org/wiki/Port_spanning]



Obr. 22. RouterBoard RB 750



Obr. 23. Ukázka nastavení funkce port mirroring na RouterOS

15.2 Instalace aplikace Snort

Po provedení úprav se sítí můžeme přistoupit k samotné instalaci serveru Snort. Tento server obsahuje systém Linux distribuci Ubuntu[18] ve verzi 11.04 workstation editon, po konfiguraci serveru jsem přešel k samotné instalaci Snort. Přiznám se, že samotnou instalaci jsem provedl pomocí centrum pro software, který je součásti každé verze Ubuntu. Tímto se zajistí stažení nejnovější verze, její kompilaci a zároveň nabídne i různé upgrade a plug-in, které se do Snortu dají nainstalovat a o kterých bych se možná ani nedozvěděl při provádění instalace pomocí příkazu apt-get. Takže po samotné instalaci můžeme přejít k nastavení a konfiguraci.

15.3 Konfigurace Sortu

Konfigurace aplikace Snort se provádí editací úpravou souboru /usr/locat/etc/snort.conf**.** Zde jsem nastavil tyto proměnné:

- HOME_NET
- EXTERNAL_NET
- RULE_PATH

Dále jsem poté musel nastavit a zkontrolovat cesty. Při nastavení těchto cest je třeba být obezřetný. Snort totiž při špatném nastavení nic nezahlásí a nespustí se. Pro pomoc při ladění se dá do konfiguračního souboru přidat:

output alert_syslog: LOG_AUTH LOG_ALERT

Výsledná hlášení se ukládají do souboru /var/log/messages**.** Posledním krokem je povolení spuštění Snortu. To se děje úpravou souboru /etc/rc.conf, kde jsem vložil následující dva parametry.

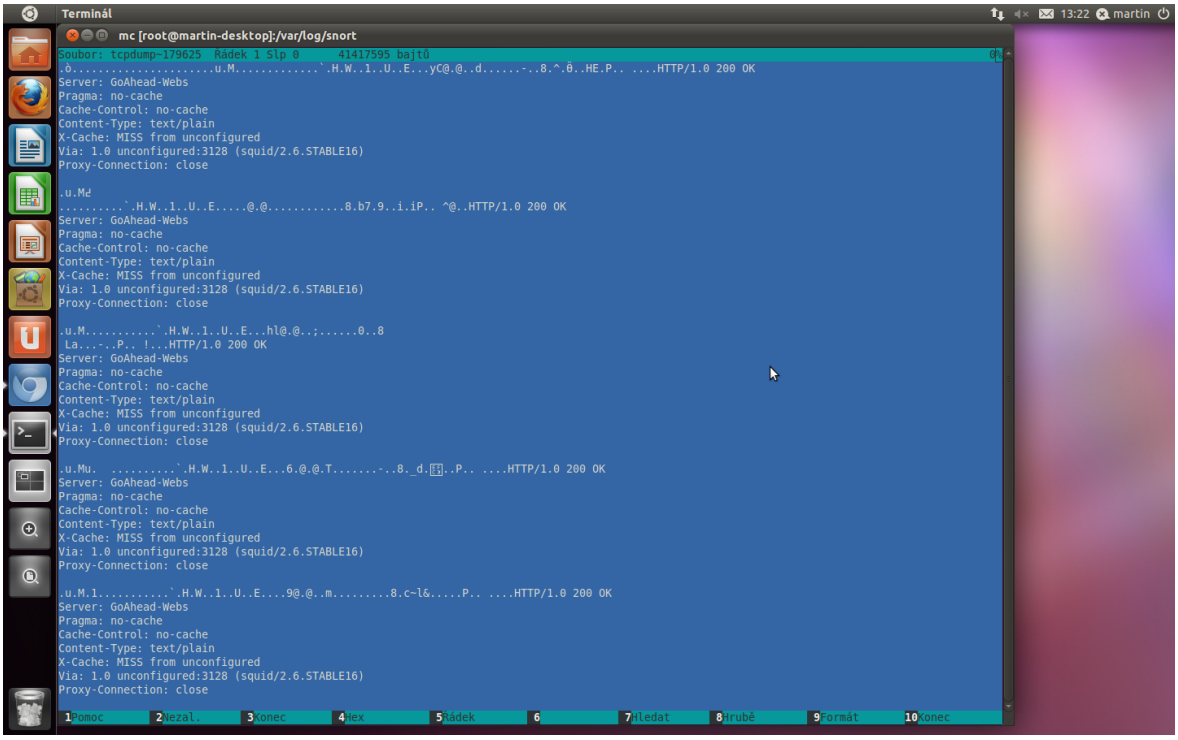
snort_enable="YES"
snort_interface="bridge0"

[18] Ubuntu – v poslední době velmi rozšířená distribuce Linuxu. Zdroj: [http://www.ubuntu.cz/]

Restartování Snortu se provádí příkazem:

/usr/local/etc/rc.d/snort restart

Kontrola se provádí v systémovém logu a dá se zjistit, kde konkrétně nastala chyba. Po odladění je možné, aby Snort přesměroval informace buď do textového souboru, do databáze nebo do programu Prelude. Ladění senzitivity Snortu se provádí buď zásahem do souborů s pravidly (rules), nebo do konfiguračního souboru. Ovšem soubory s pravidly podléhají pravidelnému update. Na začátku jsem vše povolil a postupným testováním jsem některé parametry vypnul, až jsem dospěl do fáze, kdy všechny komponenty fungovaly, jak jsem potřeboval vzhledem k povaze a členění podnikové sítě INPOST, spol. s r.o. Toto testování je velmi časově náročné a ideálním nástrojem pro toto testování je využití síťového auditu. Pro tento audit jsem použil produkt Nessus od společnosti Tenable software. Tomu se ale budu věnovat v kapitole 16.



Obr. 24. Výpis Log souboru Snort, zachycení síťového provozu

16 PROVEDENÍ SÍŤOVÝCH AUDITŮ POMOCÍ APLIKACE NESSUS

Po důkladném nastavení firewallu se můžu pustit do provedení síťových auditů. Provedení toho auditu ve společnosti INPOST, spol. s r.o., by mělo přinést odhalení slabých míst v celém systému podnikové sítě. Výsledky tohoto auditu by měly poskytnout také doporučení při záplatování těchto bezpečnostních děr. Pro provedení tohoto auditu jsem vybral software Nessus od společnosti Tenable. Jedná se o open-source projekt, které podporuje všechny známé operační systémy.

16.1 Instalace Nessus a nasazení v síti

Pro instalaci Nessus je důležité, aby samotný test byl spuštěn pokud možno z jiného místa, než je naše podniková sít, proto jsem Nessus nainstaloval domů, aby byl můj síťový audit co možná nejobjektivnější. V minulosti jsem tento audit také zkoušel provádět z počítače v síti společnosti INPOST a také jsem skutečně detekoval i kritické chyby v zabezpečení sítě. Ovšem bylo jich odhaleno mnohem méně, než při pozdější auditu spouštěném z jiného místa mimo sít společnosti INPOST.

Nejprve jsem stáhl instalační soubor z http://www.tenable.com/products/nessus/select-your-operating-system. Vybral jsem platformu Windows x86, poté jsem spustil samotnou instalaci produktu. Jedná se o velmi jednoduchou instalaci s klasickým instalačním souborem. Po instalaci je nutné se na stránkách www.tenable.com zaregistrovat, kde uvádím jen e-mailovou adresu a heslo. Toto sebou nese výhodu toho, že můžu dělat více auditu například na více firmách a stačí se jen v aplikaci Nessus přihlásit na jiný učet a nejen provádět audity, ale také prohlížet historické výsledky všech testů, které jsem na určitou IP adresu provedl.

16.1.1 Provedení samotného auditu

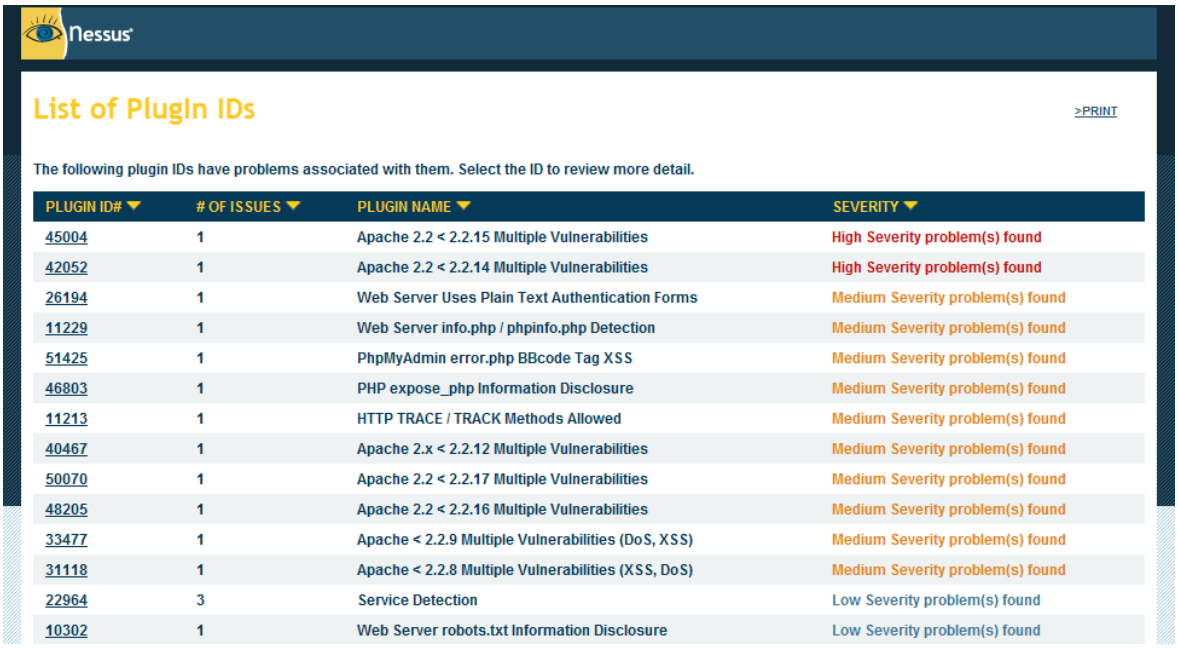
Při spuštění auditu jsem zadal veřejnou IP adresu společnosti INPOST. Nessus hned poté začne zasypávat tuto IP adresu různými simulovanými útoky, které jsou samozřejmě neškodné a nejdou do důsledků těchto simulovaných útoků. Ovšem k odhalení slabých míst v naší síti je to velmi dostatečné. Po spuštění Nessus pracuje cca. 5 minut, poté jsou zobrazeny výsledky auditu.

16.1.2 Rozbor výsledků auditu

Po skončení auditu a porovnání se všemi plug-in moduly v aplikaci Nessus vypíše výsledky testu, zároveň je uloží do naší databáze pod naše přihlašovací jméno. Zároveň také nabídne export těchto dat v mnoha formátech, také je může zveřejnit na webu ve formátu HTML.

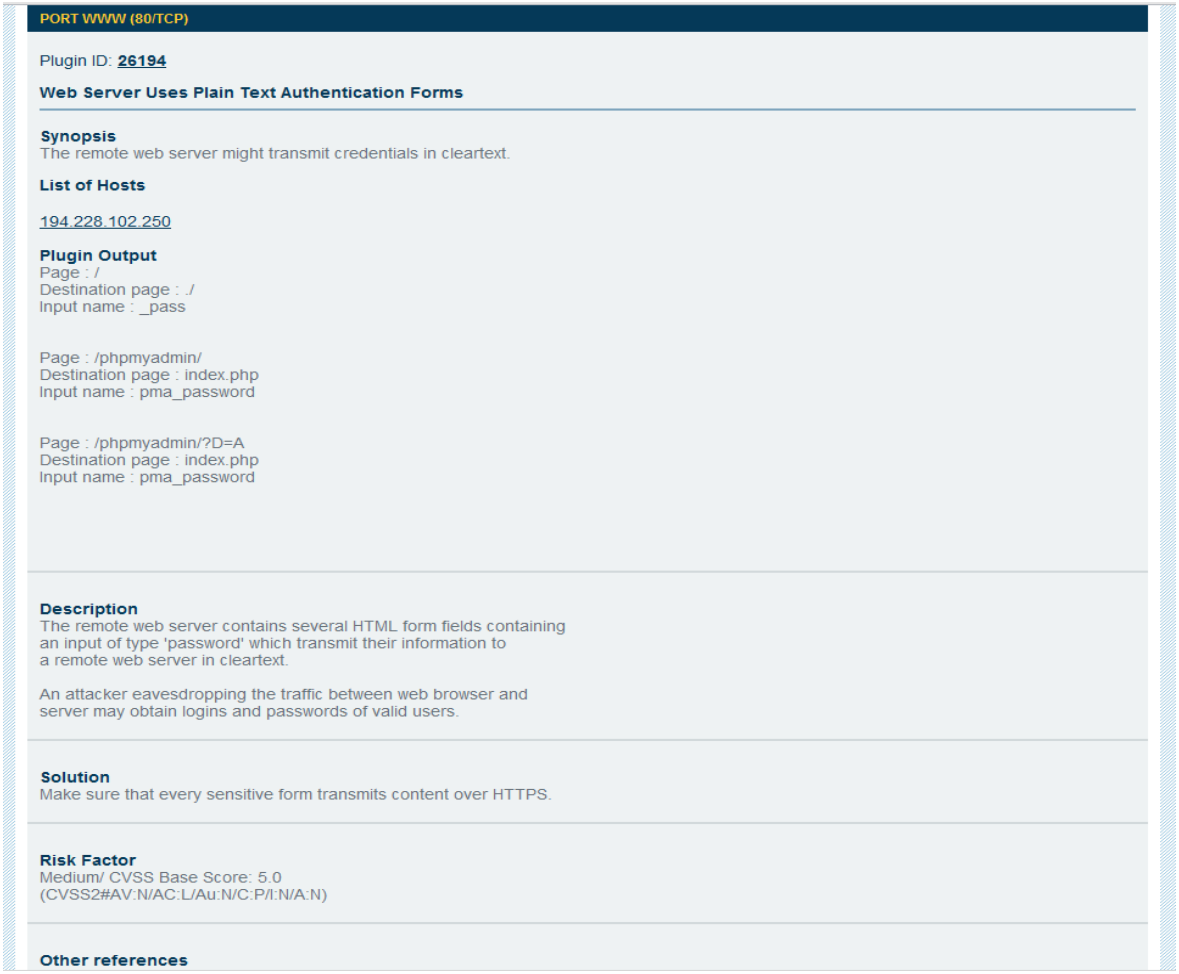
Výsledky auditu jsem rozdělil do tří hlavních kategorií podle nebezpečnosti:

- High severity problems – tato úroveň nabádá správce systému k okamžitému řešení daného problému, obvykle se jedná o závažný problém, který je dříve nebo později zneužit k provedení útoku.
- Medium severity problems – tato úroveň nebezpečnosti vypovídá o středních chybách v zabezpečení. Správce by je měl řešit okamžitě, ale při útocích na tato místa nehrozí např. znefunkčnění určité služby nebo zařízení v síti.
- Low severity problem – tato úroveň má spíše doporučující charakter.



Obr. 25. Výsledek auditů

Obr. 26. Kritická bezpečností mezera



Obr. 27. Střední bezpečnostní mezera

Z těchto výsledků bezpečnostní síťového auditu je patrné, že veškeré kritické a středně kritické chyby jsou v oblasti portu 80 a Apache na kterém běží firemní webové stránky společnosti INPOST. Z doporučení vyvozené z výsledků auditu aplikace Nessus vyplívá, že je nutné udělat upgrade Apache služeb běžících na webovém serveru. Zastaralé verze Apache neobsahují totiž bezpečnostní záplaty. Navíc na tomto serveru je nainstalována poměrně stará verze systému Linux v distribuci Mandriva a ta také není záplatována po dlouhou dobu. V budoucnu bude tento server nahrazen výkonnějším zařízením, kde plánuji použít Linuxovou distribuci Debian a to Ubuntu server a na kterém poběží již nejnovější verze Apache i PHP.

Z dalších výsledků je patrné že žádné jiné bezpečnostní chyby Nessus neodhalil, tudíž Firewall je dobře nastaven. Port 80 je určený pro web a ten na Firewallu samozřejmě zakázat nemohu, kvůli internetu ve firmě a také webovým stránkám INPOST, spol. s r.o. Myslím, že zmíněný upgrade web serveru tento problém vyřeší.

ZÁVĚR

Cílem práce bylo provést komplexní analýzu současného stavu a celkového nastavení podnikové sítě. Tuto analýzu jsem provedl na základě metody simulací různých typů útoků, kterým jsem celou síť jako celek vystavoval a současně sledoval určité typy jejího selhání a jejich závažnost. Díky této analýze jsem dospěl k řešení, které je nutné realizovat pro dosažení vysoké úrovně zabezpečení a spolehlivosti podnikové sítě. Jako nejvhodnější řešení, které vyhoví vzniklých požadavkům, jsem se rozhodl použít pro realizaci tohoto zabezpečení systém „ managementu sítě“, který umožňuje detekci průniků a útoků na síť a současně také provést síťový audit, který ověří správnost nastavení těchto systémů. Problémem ovšem bylo monitorovat síť jako celek a zajistit její bezpečnost a spolehlivost a přitom neovlivnit dostupnost a rychlost přenosu dat v síti. Tento problém jsem vyřešil vhodnou implementací těchto nástrojů do celkového systému sítě. Veškeré poznatky, které jsou v práci uvedeny a popsány, byly provedeny na reálném základě a mohou posloužit jako šablona pro podobné organizace. Pozitivum tohoto řešení vidím jednak v nízkých finančních nákladech, ale hlavně v jeho vysoké účinnosti při zabezpečení a zajištění funkčnosti všech požadovaných služeb v síti.

CONCLUSION

The objective of my thesis was to carry out a comprehensive analysis of the existing situation and setting up a complete company network. I have made this analysis pursuant to a simulation of various types of attacks to which I exposed the complete network as a whole and I was monitoring certain types of failures and their importance at the same time. Thanks to this analysis, I have come to a solution that must be implemented in order to reach a high level of security and reliability for the company network. As the most suitable solution that meets the requirements arisen, I decided to use the "network management" system for implementation of this security enabling detection of interventions and attacks to the network and execution of a network audit that checks the setting of these systems for correctness. However, there was a problem in monitoring of the network as a whole and in ensuring its security and reliability and simultaneously not affecting the availability of data and their transfer rate on the network. I have fixed this problem by a suitable implementation of these tools into the entire network system. All pieces of knowledge presented and described in the thesis were implemented on a factual basis and may serve as a template for similar organizations. I see the positive aspect of this solution in its low costs and mainly in its high efficiency along with providing all network services with security and functionality.

SEZNAM POUŽITÉ LITERATURY

[1] BOYLES, Tim. CCNA Securtiy : Study Guide. Indianapolis : Wiley Publishing, Inc., 2010. 520 s. ISBN 978-0-470-52767-2.

[2] EUGENE, Schultz ; JIM, Mellander ; CARL, Endorf . Hacking - detekce a prevence počítačového útoku . Praha : GRADA, 2005. 356 s. ISBN 80-247-1035-8.

[3] JIROVSKÝ, Václav. Kybernetická kriminalita . Praha : GRADA, 2007. 288 s. ISBN 978-80-247-1561-2. [4] PUŽMANOVÁ, Rita. Bezpečnost bezdrátové komunikace . Brno : Computer Press, 2005. 184 s. ISBN 80-251-0791-4.

[4] JOSEPHSEN, David. Building a Monitoring Infrastructure with Nagios. 1st ed. p. cm. Boston : Prentice Hall, 2007. 255 s. ISBN 0-13-223693-1.

[5] LOCKHART, Andrew. Bezpečnost sítí na maximum : 100 tipů a opatření pro okamžité zvýšení bezpečnosti vašeho serveru a sítě. Brno : Computer Press, 2005. 280 s. ISBN 80-251-0805-8.

[6] RAK, Roman . Biometrie a identita člověka : ve forenzních a komerčních aplikacích. Praha : GRADA, 2008. 664 s. ISBN 978-80-247-2365-5.

[7] RAMIREZ, Gilbert ; CASWELL, Brian ; RATHAUS, Noam . Nessus,Snort, & Ethereal Power Tools : Customizing Open Source Security Applications. Rockland : Syngress, 2005. 471 s. ISBN 1-59749-020-2.

[8] SCAMBRAY, Joel; MCCLURE , Stuart; GEORGE, Kurtz. Hacking bez záhad. Praha : GRADA, 2007. 520 s. ISBN 978-80-247-1502-5.

[9] SZOR , Peter. Počítačové viry : analýza útoku a obrana . Brno : Zoner press, 2006. 608 s. ISBN 80-86815-04-8.

[10] TURNBULL, James. Pro Nagios 2.0 : Use Nagios to monitor and report on the status of servers, network devices, nad applications. New York : Apress, 2006. 400 s. ISBN 1-59059-609-9.

[11] UR REHMA, Rafeeq . Intrusion Detection Systems with Snort : Advanced IDS Techniques Using Snort, Apache, MySQL, PHP, and ACI. New Jersey : Prentice Hall PTR, 2003. 263 s. Dostupné z WWW: <http://ptgmedia.pearsoncmg.com/imprint_downloads/informit/perens/0131407333.pdf>. ISBN 0-13-140733-3.

[12] Dusatko.org [online]. 2007 [cit. 2011-05-12]. Monitorování změn a trendů v zabezpečení. Dostupné z WWW: <http://www.dusatko.org/cs/node/100>.

[13] EINWECHTER, Nathan . Securityfocus.com [online]. 2002 [cit. 2011-05-12]. Implementing Networks Taps with Network Intrusion Detection Systems. Dostupné z WWW: <http://www.securityfocus.com/print/infocus/1594>.

[14] Insecure.in [online]. 2008 [cit. 2011-05-12]. Honeypots. Dostupné z WWW: <http://www.insecure.in/honeypots.asp>.

[15] Insecure.in [online]. 2008 [cit. 2011-05-12]. Intrusion Detection System. Dostupné z WWW: <http://www.insecure.in/ids.asp>.

[16] Linuxexpres.cz [online]. 2006 [cit. 2011-05-12]. Nessus provadime bezpecnostni audity. Dostupné z WWW: <http://www.linuxexpres.cz/software/nessus-provadime-bezpecnostni-audity>.

[17] SPITZNER, Lance. Tracking-hackers.com [online]. 2003 [cit. 2011-05-12]. Honeypots - Definitions and Value of Honeypots. Dostupné z WWW: <http://www.tracking-hackers.com/papers/honeypots.html>.

[18] Wiki.airdump.cz [online]. 2011 [cit. 2011-05-12]. Hacking WiFi sítí 2011. Dostupné z WWW: <http://wiki.airdump.cz/Hacking_WiFi_s%C3%ADt%C3%AD_2011>.

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

ADSL	Asymmetric Digital Subscriber Line - je jedna z forem Digital Subscriber Line technologie, datové komunikační technologie, která umožňuje rychlejší přenos dat
CPU	Centrální procesorová jednotka - je část počítačového systému, který provádí pokyny počítačových programů , a je primární prvek pro provádění počítačových funkcí
FTP	File Transfer Protocol - je standardní síťový protokol slouží ke kopírování souborů z jednoho hostitele na druhého přes TCP
HDD	Hard disk drive - pevný disk , počítačové zařízení, které ukládá digitálně kódovaná data
HTML	HyperText Markup Language - je značkovací jazyk pro webové stránky
HTTPS	Hypertext Transfer Protocol Secure - je kombinace Hypertext Transfer Protocol s SSL / TLS protokolu, pro bezpečnou identifikaci sítě webového serveru
ICMP	Internet Control Message Protocol - je jedním ze základních protokolů Internet Protocol Suite
PHP	PHP - je skriptovací jazyk původně určený pro vývoj webových aplikací na výrobu dynamických webových stránek
RAM	Random-access memory - paměť s náhodným přístupem. Je to forma ukládání dat počítače . Dnes, to má formu integrovaných obvodů.
ROUTER	Směrovač - aktivní síťové zařízení, přeposílá datové pakety k jejich cíli.
RPM	RPM - jedná se o formát souboru , software bývá zabalen v takových souborech pro instalaci v Linuxu
SNMP	Simple Network Management Protocol- je Internetový protokol pro správu zařízení v sítích IP
SSH	Secure Shell - je síťový protokol , který umožňuje výměnu údajů prostřednictvím zabezpečeného kanálu mezi dvěma síťovými zařízeními
TCP	The Transmission Control Protocol - je jedním ze základních protokolů z Internet Protocol Suite
Telnet	Síťový program, který umožňuje připojení a práci na vzdáleném počítači.

UDP	User Datagram Protocol - je jedním z hlavních prvků Internet Protocol Suite , sada síťových protokolů používaných pro Internet
UNIX	Unix je multitaskingový, multi-uživatelský počítačový operační systém, původně vyvinutý v roce 1969
VoIP	Voice over Internet Protocol - Technologie pro přenos digitalizovaného hlasu pře internet
VPN	virtual private network -Virtuální privátní sítě je bezpečný způsob připojení k vzdálenému místu, s využitím internetu
WAN	Wide Area Network - e počítačová síť , která pokrývá širokou oblast
WEP	Wired Equivalent Privacy - je bezpečnostní algoritmus pro IEEE 802.11 bezdrátových sítích

SEZNAM OBRÁZKŮ

SEZNAM TABULEK