Univerzita Pardubice

Fakulta ekonomicko-správní
Ústav systémového inženýrství a informatiky

Bezpečnost v prostředí počítačové sítě

Lukáš Pešek

Bakalářská práce
2013

PROSTOR PRO ZADÁVACÍ LIST

PROHLÁŠENÍ

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

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

Souhlasím s prezenčním zpřístupněním své práce v Univerzitní knihovně.

V Pardubicích dne 30. 4. 2013 Lukáš Pešek

PODĚKOVÁNÍ:

Tímto bych rád poděkoval svému vedoucímu práce Ing. Oldřichu HORÁKOVI za jeho odbornou pomoc a cenné rady, které mi pomohly při zpracování bakalářské práce. Dále bych rád poděkoval manželce a dcerám za trpělivost.

ANOTACE

Bakalářská práce s názvem Bezpečnost v prostředí počítačové sítě, obecně popisuje stávající bezpečnostní hrozby v kyberprostoru a dostupné nástroje pro monitorování sestavených modelových situací lokálních počítačových sítí malého rozsahu.

Cílem je vytvoření přehledu základních skupin bezpečnostních incidentů v prostředí počítačové sítě, dostupných nástrojů pro monitoring a odhalovaní nežádoucích činností uživatelů sítě.

KLÍČOVÁ SLOVA

Kyberprostor, bezpečnostní incident, domácí počítačová síť malého rozsahu, monitorování

TITLE

Safety in the environment of computer network

ANNOTATION

Bachelor thesis titled Safety in the environment computer network, generally describes the existing security threats in cyberspace and the tools available for monitoring assembled model situations LANs small scale.

The aim is to create an overview of the basic groups of security incidents in the computer network environment, the tools available for monitoring and detecting undesirable activities of network users.

KEYWORDS

Cyberspace, security incident, home office local area network, monitoring

OBSAH

SEZNAM TABULEK

SEZNAM OBRÁZKŮ

SEZNAM ZKRATEK A ZNAČEK

ACK	Acknowledgement
AP	Access Point
BIOS	Basic Input Output System
CD	Compact Disc
CERT	Computer Emergency Response Team
CIA	Confidentiality Integrity Availability
CSIRT	Computer Security Incident Response Team
CSV	Comma Separated Values
DDoS	Distributed Denial of Service
DNS	Domain Name System
DoS	Denial of Service
Gb	Gigabit
GHz	Gigahertz
GNU	GNU's Not Unix
GPL	General Public License
GPS	Global Positioning System
HTML	HyperText Markup Language
HTTP	HyperText Transfer Protocol
HTTPS	HyperText Transfer Protocol Secure
HW	Hardware
ICMP	Internet Control Message Protocol
ICQ	I Seek You
ICT	Information and Communication Technologies
IEEE	Institute of Electrical and Electronics Engineers
IP	Internet Protocol
IRC	Internet Relay Chat
ISO	International Organization for Standardization
IT	Information Technologies
LAN	Local Area Network
MAC	Media Access Control
MAN	Metropolitan Area Network

Mb	Megabit
NAS	Network Attached Storage
NAT	Network Address Translation
NBÚ	Národní bezpečnostní úřad
NMAP	Network Mapper
OS	Operating System
PAN	Personal Area Network
PC	Personal Computer
PoE	Power over Ethernet
RAID	Redundant Array of Independents Disks
RSSI	Received Signal Strength Indication
SMS	Short Message Service
SNMP	Simple Network Management Protocol
SOHO	Small Office, Home Office
SSID	Service Set Identifier
SW	Software
SYN	Synchronize
TCP	Transmission Control Protocol
TP	Twisted Pair
TXT	Text
UDP	User Datagram Protocol
VoIP	Voice over Internet Protocol
WAN	Wide Area Network
WEP	Wired Equivalent Privacy
Wi-FI	Wireless Fidelity
WLAN	Wireless Local Area Network
WPA	Wi-Fi Protected Access
XML	eXtensible Markup Language

ÚVOD

Cílem této bakalářské práce je vytvoření přehledu základních skupin bezpečnostních incidentů v prostředí počítačové sítě, dostupných nástrojů pro monitoring a odhalovaní nežádoucích činností osob, zneužívajících počítačovou síť.

První kapitola se věnuje možným bezpečnostním incidentům v kyberprostoru - ve světě počítačových sítích. Kybernetická bezpečnost, vyjadřuje schopnost odolávat úmyslně i neúmyslně vyvolaným hrozbám a v případě škodlivého zásahu dosáhnout opětovného bezpečného stavu v rámci kyberprostoru [1]. Dále jsou zde zmíněny bezpečnostní funkce v oblasti informační bezpečnosti. Popis osob zneužívajících kyberprostor a nástin jejich možných nástrojů či aktivit. Ke konci této kapitoly jsou zmíněny uživatelům doporučení, jak preventivně eliminovat hrozící nebezpečí.

Druhá kapitola popisuje modelové situace počítačových sítí malého rozsahu pro domácí použití či v malém právnickém subjektu, jako je firma a obecní úřad. V těchto modelových situacích často není zavedena správa sítě a tedy i dohled nad informační bezpečností. Dále je zde obecně popsána bezdrátová síť a pasivní hrozba pro bezpečnost sítě - odposlech.

Další kapitola se věnuje popisem volně dostupných nástrojů pro monitorování síťového provozu, které umožní přehled o činnosti a dále je lze využít k detekci některých bezpečnostních incidentů, tedy ke zvýšení celkové bezpečnosti systému.

Poslední kapitola popisuje v obecné rovinně doporučení uživatelům modelových situací, používání monitorovacích nástrojů zmíněných v kapitole 3.

Tato práce může přinést nové poznatky mírně pokročilým uživatelům, kteří jako neprofesionální správci sítě mají potřebu být informování o činnosti ve své počítačové síti, či předcházet možným informačním hrozbám.

1. KYBERPROSTOR A KYBERNALITA

1.1 Termín kyberprostor

Kyberprostor (angl. Cyberspace) se v současné době stává používaným termínem i v okruhu široké veřejnosti a to díky masivnímu využití informačních a komunikačních technologií. Pod pojmem kyberprostor si lze představit virtuální, nehmatatelný informační svět vytvořený moderními technologiemi, např. počítačovými sítěmi jakými je internet. Společnost využívá těchto technologií jako přirozenou součást každodenního života, to však přináší mimo značných výhod i možnost zneužití. S nárůstem užívání moderních informačních a komunikačních technologií dochází ke zvyšující se neetické, nemorální či dokonce protiprávní činnosti, nazývané též kybernetickou kriminalitou (kybernalitou)[1]. [1][2]

Dohody o kyberzločinu vypracované Radou Evropy, která třídí zločiny takto [3]:

- **Proti důvěrnosti, integritě a dosažitelnosti počítačových dat a systémů**:
  - nezákonný přístup;
  - nezákonné odposlouchávání;
  - narušování dat;
  - narušování systémů;
  - zneužití prostředků.
- **Ve vztahu k počítači:**
  - počítačové padělání;
  - počítačový podvod.
- **Ve vztahu k obsahu počítače, což je především dětská pornografie**.
- **Ve vztahu k autorským nebo obdobným právům.**

Škody, které jsou způsobeny kybernetickými incidenty, jsou srovnatelné se škodami velkých přírodních katastrof [4].

[1] Kybernetická kriminalita - jedná se o kriminalitu namířenou přímo proti počítačům, jejich HW, SW, datům apod., nebo kriminalitu, ve které vystupuje počítač či síť jako nástroj pro páchání trestného činu. Obvykle finančně motivováno. Nejčastějšími formami jsou různé malwary, viry a červi, spam, hacking, phishing, podvody, krádeže identity, pirátství/krádeže duševního vlastnictví, distribuce dětské pornografie.

Identifikace a následná postižitelnost osob páchající obecně řečeno kyberzločin je velmi komplikovaná. Náročnost nespočívá pouze v technických nárocích, odborných znalostech, ale i v legislativních rámcích. Česká republika, konkrétně Národní bezpečnostní úřad (NBÚ) má za úkol připravit paragrafové znění zákona O kybernetické bezpečnosti s účinností v roce 2015 a vybudovat národní centrum kybernetické bezpečnosti (CERT) v Brně.[5]

V současné době je národním CSIRT (Computer Security Incident Response Team) České republiky, tedy bezpečnostním týmem pro koordinaci řešení bezpečnostních incidentů v počítačových sítích provozovaných v České republice, sdružení CZ. NIC, správce české národní domény, a to na základě memoranda uzavřeného v roce 2012 s NBÚ. Cílem CSIRT.CZ je napomáhat provozovatelům internetových sítí s bezpečností, případně řešit bezpečnostní incidenty.[24]

Mezinárodně se stále dotvářejí normy pro oblast bezpečnosti informací ISO 27000. Zde je nutné si uvědomit, že osobu, která realizuje informační hrozbu či útok (bezpečnostní incident), je velmi obtížné dohledat a následně toto prokázat, tedy je vždy o krok napřed.

Hrozbou lze v tomto smyslu chápat cokoliv, co nějakým způsobem může vést k nežádoucí změně informace, chování systému nebo ovlivnit jeho parametry, případně využít slabého (zranitelného) místa k útoku. Za zranitelné místo lze označit slabinu informačního systému, kterým lze způsobit škodu či ztrátu. Útok je faktická realizace hrozby.[1]

1.2 Bezpečnostní funkce - řízení přístupu

Pokud se zde bude hovořit o bezpečnosti informací, nelze zde nepřipomenout pojem řízení přístupu, který se zabývá vztahem mezi aktivním objektem neboli subjektem (uživatel, aplikace, proces, atd.) a pasivním objektem (soubor, databáze, záznamové medium, atd.). Řízení přístupu je nezbytné pro zajištění důvěrnosti (Confidentiality), integrity (Integrity) a dostupnosti (Availability) objektů, tzv. CIA trojici, které představují základní bezpečnostní funkce v informační bezpečnosti [6]:

- **Důvěrnost (Confidentiality)** - je princip, že objekty nejsou vyzrazeny neautorizovaným subjektům.
- **Integrita (Integrity)** - je princip, že si objekty ponechají důvěryhodnost a mohou být úmyslně pozměněny pouze autorizovaným subjektem.
- **Dostupnost (Availability)** - je princip, že autorizovanému subjektu je garantován včasný přístup k objektům, aby mohl provádět požadovanou interakci.

Mezi další bezpečnostní funkce lze zařadit [6]:

- **Identifikace** - tvrzení subjektu o svojí totožnosti či příslušnosti.
- **Autentizace** - proces ověření identifikace.
- **Autorizace** - proces přidělení práv k vykonání určité činnosti.
- **Audit** - záznam o událostech, které ovlivňují informační bezpečnost.
- **Účtovatelnost** - garance odpovědnosti subjektů za svoji činnost.

1.3 Druhy bezpečnostních incidentů dle způsobu provedení

Bezpečnostní incidenty lze rozdělit na neúmyslné a úmyslné. Při neúmyslném někdy též nedbalostním, či náhodném bezpečnostním incidentu může vzniknout škoda na aktivech, například nezkušeným uživatelem. Úmyslný útok je označován jako využití slabého, zranitelného místa informačního systému. Útoky rozeznáváme [6]:

- **Útok přerušením** - aktivní útok na dostupnost (poškození hardware, přerušení komunikačního spoje, atd.).
- **Útok odposlechem** - útok na důvěrnost nepovoleným odposlechem, zachycení zprávy. (Detailněji popsáno v podkapitole 2. 6).
- **Útok modifikací** - útok na integritu dat, neautorizovaný subjekt pozmění data, obsah zprávy či funkčnost programu subjektu.
- **Útok přidáním hodnoty** - útok na autenticitu a integritu, neautorizovaný subjekt vloží podvržený, padělaný například záznam k souboru.

1.4 Osoby zneužívající kyberprostor - úmyslní útočníci

Tyto osoby lze rozdělit dle různých kritérií, pro tuto práci bylo zvoleno následující základní členění [1]:

- **Hackeři** - ačkoli proniká do chráněných systémů, jeho cílem není získat, poškodit nebo zničit informace či systém, ale dokázat svoje technologické znalosti a kvality získané zpravidla samostudiem.
- **Crackeři** - jejich cílem je kybernetická kriminalita za účelem finančního zisku, technologického vandalismu, teroristické aktivity či další nelegální činnosti.

Dle charakteristik nebezpečnosti útočníků lze obecně definovat[1]:

- **Script-kiddies** - skupina, která má minimální technologickou znalost. Nevytváří si vlastní škodlivé kódy, ale využívají již vytvořený nástroj, který se snaží použít.
- **Hackeři** - příležitostné zjišťování zranitelnosti systémů, nabourávání a prolamování zabezpečení, které provádí jako svůj koníček.
- **Hacktivisté** - fanaticky zaměřené skupiny aktivistů, využívající informačních technologií k šíření a prosazování politických či ideologických cílů.
- **Nespokojení zaměstnanci** - tato skupina, z nějakého důvodu pomstychtivých zaměstnanců či bývalých zaměstnanců, je velmi nebezpečná, podle pozice a informovanosti zaměstnance může vést k rozdílně závažným následkům v dané organizaci.
- **Profesionální či organizovaní hackeři** - Skupiny, které za finanční úplatu realizují napadení, prolomení ochrany systému a tím získávají určitý prospěch pro svého zadavatele. Do této kategorie lze řadit i tzv. „White hats“, kteří opět za finanční obnos vyhledávají, ovšem se souhlasem majitele firmy, bezpečnostní mezery umožňující potencionální útok.
- **Kriminální hackeři** - neboli, **Crakeři**, jejichž cílem je zisk nebo nevratná škoda. Izolované skupiny napojené na kriminální či teroristické podsvětí.

1.5 Bezpečnostní incidenty - nástroje útočníka

Útočník ke své činnosti využívá mimo svých technologických znalostí a dovedností nástroje, které lze obecně rozdělit[1]:

- **Hardwarové nástroje** - např. hledání bezpečnostních děr v hardware (čipové karty).
- **Softwarové nástroje** - výčet některých nástrojů a technik je detailněji popsán níže.
- **Sociální inženýrství** - popsáno v podkapitole 1.6.

1.5.1 Užívané programové nástroje útočníka

Exploit - program, který využívá chybu (slabinu) systému, „bezpečnostní díru“. Díky této slabině útočník může použít jiné nástroje k vniknutí do systému. Po objevení této slabiny vývojáři operačního systému či antivirového programu vytvoří „patch“ (záplatu), která po

nainstalování ošetří „bezpečnostní díru“ a daný exploit ztrácí smysl. Tento proces je nikdy nekončící cyklus.[1]

Malware - obecný název pro škodlivý software určený k vniknutí, ovládnutí či poškození systému, ve kterém se nachází. Lze sem zařadit viry, trojské koně, spyware, adware, infoware, červi i logické bomby [7]:

- **Vir** - parazitující soubor, který se připojí k programovým či systémovým oblastem, může změnit (smaže či poškodí soubory, lze dojít k zatížení procesoru apod.). Existuje nespočet druhů této „informační infekce“. Velmi často se šíří jako příloha v e-mailu či ve staženém software.
- **Trojské koně** - velmi užívaný nástroj útočníka. Jsou naimplementovány do systému bez vědomí uživatele. Po té je útočník využívá k různorodým činnostem. Např. k monitorování činnosti systému i uživatele či zneužití stanice pro DoS útok apod. Trojské koně často bývají součástí souborů stažených z internetu. Opět existuje nespočet modifikací.
- **Spyware** - jedná se o tzv. „špionážní“ program, který skrytě monitoruje, sbírá a odesílá informace o systému i uživateli.
- **Adware** - cílem tohoto programu je jakési sdělení reklamního charakteru, často bez souhlasu uživatele, které může být obtěžující.
- **Červ (Worm)** - samostatný software, který je sám schopný se vytvářet i rozesílat své kopie a tím se šířit po kyberprostoru, kde provádí předem určenou činnost. Např. vyhledává slabin systémů.
- **Logické bomby (logical bombs)** - software, který se skrytě ukládá do operačního systému či různorodých aplikací, kde následně může vykonat předem určené aktivity i destruktivního charakteru. Aktivují se např. spuštění jinou aplikací, konkrétním datem či časem (výročí určité události).
- **Keylogger** - program, který je určen ke sledování zadávaných znaků z klávesnice.
- **Hijacker** - malware, který mění, bez vědomí uživatele webovou domovskou stránku.

BackDoors - lze přeložit jako „zadní vrátka“. Pokud útočník objeví bezpečnostní slabinu, v první řadě se pokusí nainstalovat backdoors, čímž si umožní vzdáleně spravovat stanici.

DoS útok (Denial of Service - odmítnutí služby) - obecně, útočník zahltí cílový stroj tím, že vyšle větší počet požadavků než je schopen cílový stroj odbavit. Dojde k ochromení stroje či sítě, tím že je neschopný zpracování či komunikace. Tento druh útoku je v dnešní době v celosvětovém měřítku velmi rozšířený. Existuje několik technik, jako například [6]:

- **Distribuovaný DoS attack (DDoS)** - útočník využívá služeb velkého počtu „nakažených" stanic (tzv. slaves či zombie) např. trojským koněm, které vytvoří botnet (síť internetových robotů) vysílající požadavky, které jsou nekompletní, znetvořené nebo fragmentované (rozdělené) k cílovému stroji. Systém se pod náporem požadavků zhroutí. Obrana spočívá ve filtrování paketů z používaných IP adres[2], ovšem hrozí zamezení přístupu i oprávněných legitimních požadavků.
- **SYN flood attack** - útočník zneužívá principu TCP/IP[3]. Kdy klient zašle velké množství SYN datagramů serveru, server následně odpovídá SYN/ACK klientovi. Po té klient, v tomto případě útočník již neodpoví zpět serveru ACK datagramem. Server čeká na odpověď, tím se samozřejmě prodlužuje čekací dobu a legitimní požadavky nemusí být odbaveny.
- **Ping of Death attack** - útok je veden nadměrným množstvím ping[4] požadavků, což může způsobit havárii nebo restartování systému. Útoku lze předcházet pravidelnou aktualizací operačního systému či aplikací, nebo vhodným nastavením firewallu[5].
- **Stream attack** - útok je prováděn pomocí značného množství paketů[6], které jsou zasílány na různé porty systému oběti, který se snaží pakety zpracovat, čímž může dojít k jeho nefunkčnosti.
- **Teardrop attack** - útok využívá bezpečnostních chyb v operačních systémech.

Spoofing - útočník záměrně vystupuje pod jinou identitou. Například používá zfalšovanou IP adresu [6]:

- **Napodobování** - aktivní útok, kdy dochází k odchytávání přenášených dat, ze kterých se útočník snaží získat údaje, např. hesla.

[2] IP adresa (logická adresa) - číslo sloužící k jednoznačné identifikaci síťového rozhraní, používaná verze IPv4 využívající 32-bit. adresy, IPv6 využívající 128-bit. adresy.

[3] TCP/IP - rodina protokolů pro komunikaci v počítačových sítích, základní protokoly internetu.

[4] Ping - ověřuje spojení mezi dvěma síťovými rozhraními v počítačových sítích, užívá TCP/IP protokoly, odesílá IP datagramy a očekává odezvu protistrany.

[5] Firewall - hardware či software, sloužící k bezpečnému oddělení jedné počítačové sítě od druhé, např. LAN od internetu. Pomocí předem nastavených pravidel propouští data jedním směrem.

[6] Paket - blok přenášených dat.

- **Maškaráda** - pasivní útok, kdy již útočník využívá získané údaje, bez souhlasu uživatele, například přihlašovací údaje.

Hoax - neboli nevyžádaná, poplašná či podvodná zpráva uživateli např. o možných následcích škodlivého kódu, který byl na uživatelské stanici zjištěn. Největší nebezpečí spočívá v návodu pro uživatele. Pokud tyto rady důvěryhodný, nezkušený či lehkomyslný uživatel provede, hrozí poškození systému (vymazání systémových souborů) či naistalování skutečně škodlivého kódu útočníka. Některé typy hoaxů uživatele i pobaví.

Debugerry - prvotně užívané nástroje k dolaďování (odstraňování chyb) nového software. Útočník však může, zjištění chyby zneužít ke svým nekalím činnostem.

Sniffery - v některých případech se užívá název „čmuchací" software. Jedná se o odposlouchávání síťového provozu, tedy o shromažďování užitečných informací pro útočníka. Dochází k zachytávání a následnému analyzování paketu. Lze zjistit IP adresa, MAC adresa[7], typ protokolu, ale i přenášená hesla či další citlivé údaje.[1]

Skenery - tyto nástroje neslouží přímo k útoku, ale ke zjištění informací o otevřených portech na stanici. To může vést k potencionálnímu útoku, protože lze zjistit informace o slabinách systému. Tyto informace mohou být zneužity technicky znalými osobami (útočníky) ovšem, mohou být také použity ke zvýšení bezpečnosti systémů.

1.6 Sociotechniky - sociální inženýrství

Největší bezpečnostní hrozbou v kyberprostoru je lidský prvek - uživatel. Technika využívající oklamání, negativní manipulaci či přesvědčení uživatelů informačních technologií k úniku, sdělení informací, nebo k provedení některých bezpečnost ohrožujících úkonů, se nazývá sociotechnika. Též lze použít pojem sociální inženýrství.

Obrana proti sociálnímu inženýrství je velice komplikovaná, vzhledem k tomu, že zde hlavní roli hraje člověk. Umění ovládání lidí, psychologické či technologické znalosti, schopnosti útočníka oproti lehkomyslnosti, naivitě i nezkušenosti uživatele. Určité útoky jsou zachyceny v tabulce 1.

[7] MAC adresa (fyzická adresa) - dochází k přiřazení při výrobě síťové karty - jedinečný identifikátor síťového zařízení, vyjádřena pomocí hexadecimálních číslic.

Tabulka 1 - Oblasti sociotechnických útoků, taktika a obrana.

Oblasti útoku	Sociotechnické taktiky	Obrana
Telefon	Předstírání identity, přesvědčování	Zaměstnanci nesmí vydávat svá hesla, důvěrné informace
Vstup do budovy	Vniknutí v převleku	Průkazy, ostraha
Kancelář	Nahlížení přes rameno	Hesla používat pouze s jistotou, že se nikdo nedívá
Kancelář	Procházení budovy a vyhledávání nezabezpečených kanceláří	Host v doprovodu kompetentní osoby
Místnost serveru	Pokus o logování, odstranění vybavení, nahrání škodlivého kódu (trojský kůň), kterým lze následně získat informace	Místnost s umístěním serveru musí být řádně zabezpečena. Vedení seznamu vybavení
Telefonní ústředna	Přesměrování linek	Kontrola hovorů
Odpadkový koš	Prohledávání odpadků	Řádná skartace důležitých dokumentů či medií, odpadkové kontejnery zabezpečené v monitorované oblasti
PC síť (intranet, internet)	Monitorování, odchytávání hesel	Sledování softwarového vybavení počítačů
Kancelář	Zcizení dokumentů	Hierarchie důvěrnosti dokumentů a adekvátní zacházení s nimi

Zdroj: upraveno podle [1]

1.7 Phishing

Jedním z druhu sociálního inženýrství je phisihg. Kdy je snaha útočníka vylákat důvěrné informace (např. čísla peněžních účtů s přihlašovacími údaji, čísla kreditních karet,…) od uživatele nejčastěji pomocí e-mailových zpráv, ve kterých je uveden klamavý obsah. Útočník se může vydávat za bankovní instituci, za použití zfalšované adresy.

1.8 Zabezpečení pomocí hesel

Zabezpečit počítač, počítačovou síť či informační systém lze mimo jiné pomocí statického hesla. Pokud mají být přihlašovací údaje bezpečné, je třeba si uvědomit několik zásad:

- Odolné tzv. silné heslo by mělo být dostatečně dlouhé. Je třeba si uvědomit, že každé heslo je prolomitelné, je to pouze otázka času.
- Znaky tvořící heslo jsou kombinací malých písmen (a-z), velkých písmen (A-Z), číslic (0-9) či speciálních znaků (např.! @#$%^&*~). Heslo by nemělo dohromady dávat slovo dávající smysl a zároveň by nemělo být odvoditelné z informací o uživateli hesla.
- Heslo by se nemělo nikomu sdělovat. Uživatel by měl zvážit, jakékoliv zaznamenávání hesla, být obezřetný při přihlašovaní z veřejných míst a heslo nikam neukládat, např. do internetových prohlížečů.
- Heslo je vhodné měnit po určitém časovém období (např. 1x za 3 měsíce).
- Pro každý systém, službu užívat jiné heslo.
- Uživatel musí mít kontrolu nad strojem, kde heslo používá.

Na paměti je dobré mít i to, že se lze k počítači přihlásit i vzdáleně.

1.8.1 Prolamování hesel - Password crackers

Pokud útočník neodhadne heslo z informací zjištěných o uživateli, nebo heslo neodpozoruje či nepřehraje, pak může využít dvě základní techniky útoku na prolomení hesel:

- **Slovní útok (Dictionary attack) -** z vlastní databáze výrazů postupně zkouší vyhledat slovo tvořící heslo. Lze použít i slovníkový útok s permutací.
- **Útok hrubou silou (Brute Force Attack) -** využívá systematického testování všech možných kombinací znaků, což je velmi časově náročné.

Každý rok, na mnoha informačních zdrojích jsou zveřejňována celosvětově nejužívanější hesla. Obecně jsou stále stejná. Tabulka 2 zobrazuje deset nejpoužívanějších hesel.

Tabulka 2 - Deset nejpoužívanějších hesel.

password	1234567
123456	monkey
12345678	111111
qwerty	654321
abc123	Své křestní jméno, či svých nejbližších

Zdroj: upraveno podle [14]

1.9 Rizikové chování v kyberprostoru

Do pojmu kyberprostoru je jistě možné zařadit informační a komunikační fenomén současnosti - internet, který využívají celosvětově miliony uživatelů. Tento virtuální svět je však v mnoha vlastnostech odlišný od skutečného světa. Například komunikace mezi jednotlivými uživateli je specifická tím, že je neosobní, je virtuální. Chybí zde nonverbální komunikace, gesta i mimika, ale především uživateli internetu je umožněno vystupovat pod virtuální identitou, která může být naprosto odlišná, než je uváděná. Jako příklad lze uvést sociální sítě[8] nebo chat[9], kde uživatelé vystupují pod nickem (přezdívkou). Velký počet lehkomyslných uživatelů si neuvědomuje možnost nebezpečí zneužití osobních důvěrných informací.[8]

Mezi rizika komunikace v kyberprostoru lze spatřovat:

1.9.1 Kybergrooming

Což je chování uživatelů internetu, které má v oběti vyvolat falešnou důvěru a přimět ji k osobní schůzce. Výsledkem této schůzky může být sexuální zneužití oběti, fyzické násilí na oběti, zneužití oběti pro dětskou prostituci, k výrobě dětské pornografie apod. Je to jistý druh psychické manipulace realizované prostřednictvím internetu, mobilních telefonů a dalších zařízení souvisejících s ICT[10].

S touto hrozbou se lze setkat na veřejném chatu, internetových „seznamkách“, instant messengery a VoIP (např. ICQ, Skype) a v posledních letech také na sociálních sítích (Facebook, Twitter a další).

Oběťmi jsou i děti a mládež nejčastěji ve věku 11 - 17 let, především dívky. Útočníci tvoří heterogenní skupinu, v které lze nalézt jak uživatele s nízkým tak i vysokým sociálním statutem (právníky, učitele, policisty). Výjimkou není ani to, že pachatel oběť zná, nebo je rodinný známý.[9]

1.9.2 Kyberstalking

Tento pojem byl odvozen od stalkingu (pronásledování), což je opakované, dlouhodobé, systematické či stupňované obtěžování. Útočník v tomto případě pronásledovatel svou oběť obtěžuje, zastrašuje SMS zprávami, e-maily či telefonáty. Pokud pronásledovatel ke své

[8] Sociální síť (Social network) - propojení lidí v tomto případě pomocí informačních a komunikačních technologií.

[9] Chat (rozhovor) - komunikace mezi účastníky sítě, kdy účastníci rozhovoru píší vzkazy na klávesnici; psané znaky se okamžitě objevují i na obrazovce druhého účastníka rozhovoru.[10]

[10] ICT - informační a komunikační technologie.

činnosti použije ICT, mluvíme o kyberstalkingu - zasílání různých zpráv pomocí instant messengerů (ICQ), chatu, prostřednictvím VoIP[11] technologií, sociálních sítí apod. Díky virtuálnímu prostředí, kyberstalker může využít výhod anonymity.

Za cíl pronásledovatele je v oběti vyvolat pocit obavy, strachu.

Útočník může být bývalý partner, pronásledovatel celebrit, sociálně neobratný nápadník, chorobně poblázněný milovník, sexuální pronásledovatel i „čistý“ kyberstalker, který se neodhodlává k fyzickým útokům.

Stalking/kyberstalking nelze podceňovat, protože může předznamenávat závažné trestné činy.[11]

1.9.3 Kyberšikana

Tímto termínem lze označit nebezpečné komunikační jevy odehrávající se pomocí ICT. Cílem či důsledkem útočníka je ponížení, ublížení nebo jiné poškození oběti.

Útočník kyberšikany opět může využít anonymity i klamavé identity, která popírá rozdíly v pohlaví, věku, sociálního postavení, fyzické či psychické dispozice. Útočníkem může být kdokoli, kdo disponuje dostatečnými technickými znalostmi i ten který nedisponuje např. fyzickou schopností na typickou šikanu.

Obětí kyberšikany se může stát jakýkoliv uživatel virtuálního prostoru. Útočník si může oběť v kyberprostoru vybrat i nahodile, např. podle nicku či věku. Vzhledem ke specifikaci virtuálního světa, oproti reálnému světu; pomluva, nadávka, diskriminující materiály, mívají často daleko rozsáhlejší a déle trvající následky pro oběti kyberšikany.[12]

1.9.4 Možnosti obrany uživatele

Pokud uživatel rozpozná výše zmíněné nebezpečí je na místě ukončit spojení - nekomunikovat byť s potencionálním útočníkem, ovšem ani neoplácet, nemstít se. Dále zamezit, blokovat útočníkovi přístup - např. přes poskytovatele komunikační, informační služby. Je vhodné si i změnit virtuální identitu. Další postup nahlášení je dosti specifický dle druhu a intenzity útoku, např. ohlásit hrozbu či útok příslušným orgánům činným v trestním řízení.[12]

[11] VoIP (Voice over Internet Protocol) - technologie umožňující přenos digitalizovaného hlasu (telefonování) prostřednictvím počítačové sítě - internetu, intranetu nebo jiného datového spojení. [13]

1.10 Další pravidla bezpečného chování v kyberprostoru

1) Pravidelná aktualizace aplikací, zejména operačního systému a bezpečnostních software (firewall, antivirový program či jiné).
2) Pravidelná kontrola funkčnosti bezpečnostních software.
3) Bez znalostí neměnit konfiguraci bezpečnostních software.
4) V nevyžádaném e-mailu nestahovat přílohy, neotvírat odkazy.
5) Přes e-mail neaktualizovat, ani se nepřihlašovat na účet.
6) Při identifikaci, zadávání přístupových jmen a hesel přes internetové stránky, ověřit, zda komunikace probíhá pomocí asymetricky šifrovaného protokolu HTTPS (Hypertext Transfer Protocol Secure).
7) Osobní, citlivé i důvěrné informace zadávat pouze přes ověřený, bezpečný prostor internetu. Například, neposílat přes e-mail čísla účtů či kreditních karet.
8) Na cizích pracovních stanicích, včetně internetových kaváren, se nepřihlašovat na účty.
9) U nezašifrovaných bezdrátových sítí mít stále na paměti skutečnost, snadné odposlouchávání komunikace.

Dále je potřebné si uvědomit, že útočník může snadno zneužít nedokonalou autentizaci či autorizaci. Stejně tak nesprávné přidělování prostředků, nedostatečnou implementaci zabezpečení, společné oprávnění pro více uživatelů či aplikací, nebo nevhodné pracovní návyky uživatelů (zaměstnanců). Výše uvedené umožní útočníkovi získat neoprávněný přístup k zásadním síťovým prostředkům.[23]

2 MODELOVÉ SITUACE UŽIVATELŮ KYBERPROSTORU

Kyberprostor je tvořen navzájem propojenými sítěmi informačních prostředků. Pro názornost si lze představit internet - propojení počítačů ve smyslu počítačových sítí.

Počítačové sítě je možné členit podle různých kritérií, například:

- **dle rozlehlosti** (WAN, MAN, LAN, PAN);
- **dle uspořádání uzlů** (client/server, peer-to-peer);
- **dle topologie fyzické/ logické** (kruh, hvězda, sběrnice).

V této práci budou nastíněny modelové situace počítačových sítí malého rozsahu typu SOHO (Small Office, Home Office) LAN (Local Area Network) a to konkrétně pro modely:

- **domácí počítačová síť;**
- **počítačová síť pro malou firmu;**
- **počítačová síť malé obce.**

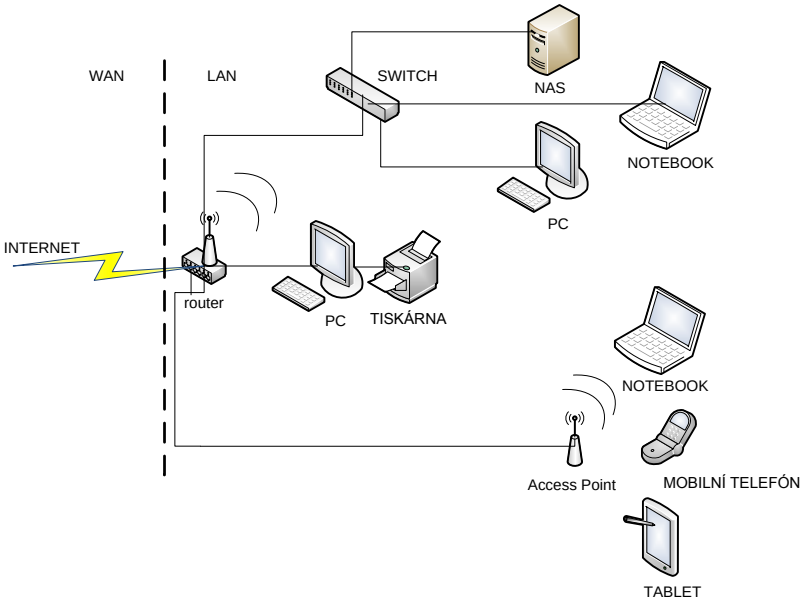
Všechny tyto modely spojuje to, že jsou svým rozsahem či připojeními prvky podobné. Ve všech výše uvedených modelových situacích je velmi často opomíjena či zanedbávána správa sítě a tedy i informační bezpečnost. Vlastníci či provozovatelé uvedených počítačových sítí, nevyhledávají či si nemohou dovolit profesionální monitorování sítě. Důvody mohou být finanční či vědomostní. Jistou možností, jak zvýšit svoji informovanost o tom, co v síti probíhá a zároveň snížit pravděpodobnost možného bezpečnostního incidentu s minimálními či nulovými náklady, je používání volně dostupného monitorovacího nástroje. Vyhledat takový monitorovací nástroj, který by obsáhl všechny potřebné funkce a mohl tak konkurovat komerčním nástrojům, je zdánlivě nemožné. Ovšem při kombinaci několika těchto nástrojů, lze docílit potřebné informovanosti.

Jak již bylo zmíněno, uvedené modelové situace využívají SOHO LAN. V případě krátkého dosahu do 3 - 5 metrů, kdy uživatel propojuje například notebook s telefonem se jedná o PAN (Personal Area Network).

2.1 Domácí počítačová síť

Bez současných informačních a komunikačních prostředků si již dnes neumíme představit život v naší společnosti. Nyní je zcela přirozené, že se v domácnostech nachází více než jedno toto zařízení. V minulosti nebyla počítačová síť v domácnosti tak často využívána, a pokud

ano, byly do domácí sítě spíše zapojovány stolní počítače či notebooky. Dnes je dostupná velká škála zařízení, které jsou možná zapojit do domácí počítačové sítě, jako například mobilní telefony, tablety, televizory, NAS, multimediální přehrávače, síťové tiskárny či IP kamery. Na obrázku 1 je zobrazen možný model domácí počítačové sítě.[17]



Obrázek 1 - Grafické znázornění počítačové sítě SOHO - dům.

Zdroj: vlastní zpracování.

Spojování jednotlivých zařízení v sítí lze uskutečnit pomocí kabelu či bezdrátově WLAN (Wireless LAN). WLAN pracuje na principu šíření elektromagnetických vln (viz podkapitola 2. 5).

V tomto a následujících modelech počítačových sítí se používá kabel TP (Twisted Pair), neboli kroucená dvojlinka, tvořena čtyřmi páry. Odstranění šumu je zde ošetřeno tím, že dva vodiče v páru jsou zkrouceny do sebe po celé délce. Kabely jsou zakončeny u rozvodů zásuvkami nebo na panelu rozvaděče konektory RJ-45. Vybudování kabelového připojení je nákladnější než bezdrátové připojení, ale z hlediska rušení či dokonce odposlouchávání provozu sítě je použití kabelu vhodnější. (viz podkapitola 2. 6.)

Počítačovou síť je možné využít:

- ke sdílení prostředků v síti (tiskárna či NAS);
- ke sdílení dat, řešit lze pomocí NAS, kde jsou sdílená data uložena;
- ke komunikaci (například VoIP).

2.1.1 NAS - Network Attached Storage

NAS představuje datové úložiště v síti LAN. V malých sítích si tento datový prvek získává čím dál větší popularitu. NAS je díky relativně příznivé ceně, snadné konfiguraci i administraci pro uživatele SOHO sítí vhodný jak pro sdílení, ukládání, tak i pro pravidelné zálohování dat. V jeho útrobách se skrývá jeden či více pevných disků, které většinou tvoří diskové pole typu RAID[12]. NAS lze použít jako víceúčelové úložiště s různými protokoly pro přenos souborů. Na obrázku 2. je vyobrazen jeden z mnoha typů na trhu. Navíc některé modely NAS umožňují hardwarové šifrování dat.

Obrázek 2 - Příklad úložiště typu NAS.

Zdroj:[18]

2.1.2 Router - směřovač

Lokální síť se připojuje k internetu, tedy do širšího kyberprostoru, prostřednictvím routeru, který odděluje vnější síť od zařízení připojených za ním. Pomocí tohoto zařízení lze rozšířit připojení k internetu i pro další zařízení. Většina modelů umožňuje i bezdrátové připojení (Wi-Fi). Pokud by bylo potřebné připojit více zařízení kabelem, než je k dispozici portů na routeru, je nutné připojit další zařízení - switch (přepínač). Switch umožňuje další větvení sítě o další zařízení. Data, která přijdou na jeden port, se rozešlou pouze na port kterému náleží.

Některé modely routerů umožňují konfiguraci takových funkcí, které mohou zvýšit bezpečnost v síti. Například zřízení dalších bezdrátových sítí, ke kterým se mohou připojit hosté, nemusíme jim tedy sdělovat své hesla k připojení. Dále je možné zřídit účet pro hosty pouze k připojení internetu, nebo jen do vnitřní sítě v případě zaměstnanců. Případně monitoring přenesených dat včetně filtrace obsahu.

[12] RAID (Redundant Array of Independents Disks) - vícenásobné diskové pole nezávislých disků, kde dochází ukládání dat na více disků. Existují různé metody (RAID 0, RAID 1, RAID 5, RAID 6 či RAID 10).

Router používá NAT (Network Address Translation), tedy síťový překlad adres, kdy přes jednu IP adresu přidělenou od poskytovatele se k internetu připojí více zařízení. Což může zvýšit bezpečnost, protože potencionální útočník nemusí rozpoznat skutečnou IP adresu.[28]

Každé zařízení v síti musí mít jednoznačnou identifikaci pro komunikaci, což je zmiňovaná IP adresa. V lokální síti by se neměly propojit dva routery přes své konektory pro místní síť, mohl by nastat problém při přidělování IP adresy.[17]

2.1.3 Možné hrozby uživatele domácí počítačové sítě

Možné hrozby kybernality pro uživatele domácí počítačové sítě lze spatřovat především ve zneužití důvěrných informací nebo identity při lehkomyslném používání ICT. Dále sem patří:

- kybergrooming (viz podkapitola 1. 9. 1);
- kyberstalking (viz podkapitola 1. 9. 2);
- kyberšikana (viz podkapitola 1. 9. 3);
- finanční podvody - phishing (viz podkapitola 1. 7).

Přitom útočník může používat různých forem škodlivých kódů. Zde je možné zařadit i nežádoucí, obtěžující reklamu. Před těmito hrozbami ochrání uživatele především informovanost o těchto hrozbách a jejich možné následky. Dále pak racionální a zodpovědné chování v kyberprostoru:

- používat aktualizovaný antivir;
- neotvírat došlou poštu s podezřelým obsahem;
- používat monitorovací nástroj pro správu sítě;
- ostatní bezpečné chování v kyberprostoru (viz podkapitola 1. 10).

Tedy mimo jiné ověřit, kdo využívá naši počítačovou síť, zejména při používání bezdrátových technologií. Zde hrozí největší riziko možného odposlechu sítě (viz podkapitola 2. 6.). Domácí počítačová síť pravděpodobně nebude obsahovat taková data, která by byla pro útočníka natolik zajímavá, ovšem nelze zcela vyloučit možné neoprávněné vniknutí do sítě. V oblasti bezpečnosti se nevyplácí nic podceňovat. Uživatel by měl v neposlední řadě být informován o tom, pokud se s některou touto hrozbou setká, kam tento bezpečnostní incident nahlásí.

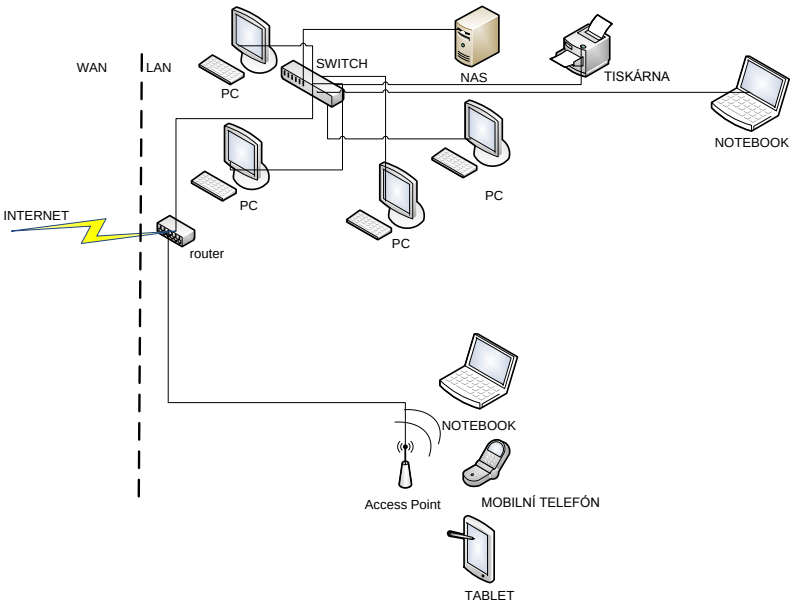
2.2 Počítačová síť pro malou firmu

Pokud větší firma, společnost využívá počítačovou síť, obvykle používá jako centrální prvek sítě systém rack. Což je standardizovaný systém určen pro montáž a propojování elektronických zařízení pomocí kabelů a to přehledně do sloupců nad sebe. Vše je umístěno v rámu ocelové konstrukce. V racku je osazení zvlášť routerem, firewallem i switchem. Pokud je k dispozici Wi-Fi, tak je poskytována v podobě centrálně řízených prvků.

Pro modelovou situaci v této kapitole je však na mysli počítačová síť typu SOHO malé firmy maximálně do 8 pracovníku. Tyto společnosti si nemohou dovolit zaměstnávat osobu výhradně odpovědnou za správu sítě. Osoba, která je pověřena "dohledem" provozuschopností sítě má většinou tuto funkci přidruženou s některou jinou funkční náplní. Obvykle je odborníkem v jiné oblasti než IT. Mírně pokročilé uživatelské znalosti by měly být dostačující pro základní monitorování sítě pomocí nástrojů, které jsou popsány ve 3 kapitole.

Jedná se zde o propojení zařízení do počítačové sítě v řádu jednotek. Tato síť, typu peer to peer, tedy rovný s rovným užívá principu rovnocennosti počítačů. Není zde žádný tzv. hlavní počítač (server), který by řídil, spravoval činnost sítě. Obdobná síť je definována v předchozí podkapitole 2.1, až na drobné odlišnosti:

- Modelová situace v počítačové síti malé firmy kterou zobrazuje obrázek 3, je od domácí sítě odlišná především použitím více pracovních stanic na platformě stolních počítačů.
- Vzhledem k tomu, že firmy mívají vybudované primárně kabelové připojení ke sdílení dat či zařízení, bezdrátové technologie se nevyužívají tak často, ale spíše k připojení s vnějšími sítěmi - internetem a to pomocí mobilních zařízení.
- Sdílení a pravidelné zálohování dat, ale i sdílení síťových zařízení, jako je například síťová tiskárna, bývají využívána častěji, než u domácí sítě. Firma při používání NAS, bude využívat toto zařízení pro sdílení a zálohování firemních dat, domácnost spíše na multimediální data.



Obrázek 3 - Grafické znázornění počítačové sítě SOHO - firma.

Zdroj: vlastní zpracování.

V dnešní době se stále více rozšiřuje používání IP kamery k zabezpečení domácnosti, obytných či komerčních prostor, tedy i kanceláří. IP kamery slouží k nepřetržitému sledování prostoru pomocí kabelové, ale i bezdrátové sítě. Z hlediska bezpečnosti je vhodnější použití síťového kabelu, bezdrátové připojení by mohl útočník či zloděj snadno vyrušit. K ukládání dat z IP kamer lze využít výše zmiňovaný NAS. Některé modely IP kamer se napájí přímo z elektrické sítě, jiné jsou napájeny přes síťový kabel funkcí PoE (Power over Ethernet). Což má výhodu v ušetření kabeláže, ale především pokud by došlo k výpadku elektrické energie, bude-li počítačová síť napájena ze záložního zdroje, je i nadále IP kamera provozuschopná.

Pokud se zde hovoří o sdílení dat pomocí NAS v rámci lokální sítě, je nutné poznamenat, že lze při splnění určitých podmínek nakonfigurovat sdílení i přístupu z vnějších sítí, přes internet.[21]

2.2.1 Možné hrozby uživatele malé firemní sítě

Uživatele této modelové sítě si lze představit jako malý podnik, firmu ale i neziskovou organizace využívající ICT pro svoji činnost či zisk. Možné hrozby jsou podobné jako v podkapitole 2. 1. 3, kde navíc hrozí:

- ztráta duševního vlastnictví;
- jiná průmyslová špionáž, například odposlechem.

Proto je nutné mít přehled o provozu sítě. Použití monitorovacího nástroje, který nedisponuje všemi funkcemi je stále lepší než nepoužití žádného nástroje.

Neoprávněný uživatel, tedy útočník, by se pravděpodobně pokusil získat, mimo jiné, tyto informace:

- know-how firmy;
- údaje o smlouvách;
- údaje o zaměstnancích;
- údaje o dodavatelích;
- údaje o odběratelích.

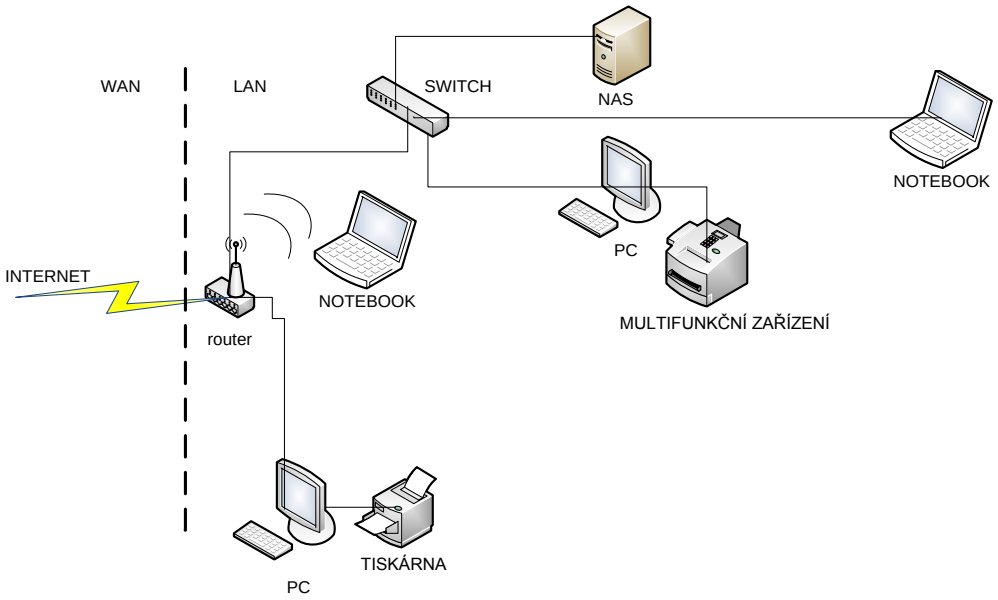
Je zde potřebné zmínit nutnost opakovaného školení a informovanosti zaměstnanců o aktuálních hrozbách sociálního inženýrství. (viz podkapitola 1. 6). Zdatný sociotechnik může získat požadované informace s menším úsilím a nižšími náklady než sofistikovaný útočník ICT. **Člověk, v tomto případě uživatel je vždy nejzranitelnější místem v systému.**

V rámci bezpečnosti v SOHO LAN zejména ve firemních či obecních sítích nelze nepřipomenout důležitý prvek, záložní zdroj energie, který zvýší bezpečnost v počítačové síti.

2.3 Počítačová síť obecního úřadu

Modelová situace počítačové sítě v této podkapitole vychází z malé obce, kde není třeba provozovat tak náročnou datovou síť s rozsáhlou agendou, jakou provozují obce s rozšířenou pravomocí. Obec s počtem do 1200 obyvatel, zpracovává základní agendu, používá počítačovou síť srovnatelnou se sítěmi SOHO uvedenými v modelech v předcházejících podkapitolách. Počet pracovníků na úřadu a tedy i počet pracovních stanic je podobný jako u domácí počítačové sítě. Možný model sítě zobrazuje obrázek 4. Pro tuto síť je typické propojování prvků pomocí kabelů. Sdílení a zejména zálohu dat lze opět řešit pomocí NAS.

Malé obce většinou nevynakládají finanční prostředky z obecního rozpočtu ke správě počítačové sítě obecního úřadu formou outsourcingu. Lidé, kteří na těchto obecních úřadech pracují, disponují ve většině případů uživatelskými znalostmi s používáním informačních technologií. Jejich odbornost spíše směřuje ke kvalitnímu chodu obce. Ale i v této síti je vhodné mít přehled o dění a tedy i o informační bezpečnosti. Jednou z možností je používání jednoho či kombinaci monitorovacích nástrojů popisovaných v kapitole 3.



Obrázek 4 - Grafické znázornění počítačové sítě SOHO - obec.

Zdroj: vlastní zpracování.

2.3.1 Možné hrozby uživatele sítě obecního úřadu

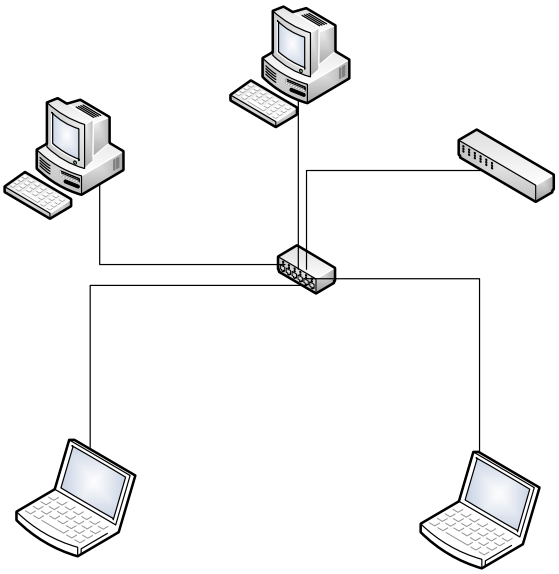
I malé obce pracují s takovými daty, o které by mohl mít potencionální útočník zájem. Především se jedná:

- údaje o obyvatelích;
- údaje spojené s chodem.

Možné hrozby jsou podobné jako v předešlých podkapitolách. Vážnou hrozbou je i zde použití sociálního inženýrství či odposlechu sítě.

2.4 Topologie modelových sítí

Všechny uvedené modelové situace počítačových sítí vycházejí z fyzické topologie ve tvaru hvězdy (star). Topologie představuje způsob propojení jednotlivých prvků v síti. Tento typ zapojení graficky znázorňuje obrázek 5.



Obrázek 5 - Grafické znázornění topologie - hvězda.

Zdroj: vlastní zpracování.

Pro tuto topologii je nutný centrální prvek, ke kterému jsou připojeny jednotlivé prvky (uzly) pomocí kabelu. Toto zapojení je vhodné pro menší počítačové sítě. Výhoda spočívá především při poruše uzlu, kdy není ohrožena provozuschopnost sítě. Nevýhodu lze spatřovat při poruše centrálního prvku.

2.5 Bezdrátové sítě

Označovány jako WLAN. Jsou typem počítačových sítí, využívajících ke spojení mezi jednotlivými prvky šíření elektromagnetických vln. Wi-Fi je standard WLAN, který vychází ze specifikace IEEE 802.11. Existuje celá řada norem IEEE 802.11 (a, b, g, n), které se liší v maximální přenosové rychlosti, propustnosti a frekvenci (2,4 nebo 5 GHz).

Komunikaci uzlů ve WLAN lze rozdělit:

- na přímou komunikaci - síť **Ad-hoc**, bezdrátové stanice komunikují mezi sebou přímo;
- na komunikaci pomocí přístupových bodů AP (Access Point) - **infrastrukturní.**

V obou případech se využívá identifikace stanic přes SSID (Service Set Identifier).[19]

U WLAN je zcela zásadní otázkou zabezpečení přenášených dat, které může ztížit možnost odposlechu či zachytávání citlivých údajů. Bezpečnost lze zabezpečit několika způsoby. Například filtrováním MAC adres, nebo pomocí šifrovacího protokolu WPA/WPA2. Často je používán i protokol WEP, který je ale díky snadnému prolomení značně nevhodný. Ovšem

ani používání WPA2 nezaručuje ochranu před sofistikovaným útokem a proto je vhodné zvýšit obranu:

- skrytím SSID identifikátoru;
- použitím silného hesla;
- kombinaci WPA2 s kontrolou MAC adresy.

2.6 Odposlech sítě

Odposlech a analýza paketů v síti, je též nazýván jako sniffing. Je to proces, kdy se zachytávají data v síťovém provozu a provádí se jejich detailní rozbor, z důvodu informovanosti o tom, co probíhá v síti. K tomuto se používá program, obecně nazývaný Sniffer. Tento nástroj může při používání neoprávněné osoby představovat jistou hrozbu pro bezpečnost sítě, byť pasivní formou. Útočník může zachytávat:

- uživatelská jména, hesla;
- důvěrné informace;
- komunikaci, která probíhá prostřednictvím VoIP;
- mapovat topologii sítě.

Sniffery lze využít i naopak, k monitorování bezpečnosti sítě či síťové administraci.[22]

Existuje několik metod k odhalení snifferu v síti, ovšem žádná nedává stoprocentní záruku. Zde jsou uvedeny některé z nich [22]:

- kontrola změn latence odezvy hostitele v síti, pomocí příkazu ping;
- sledování velkého počtu DNS[13] dotazů, bez jiného datového provozu;

Ve výše zmíněných modelových sítí typu SOHO LAN se pracuje s drátovými sítěmi, ale komunikace mezi prvky probíhá i na principu bezdrátových sítí. Při hrozbě odposlechu bezdrátové sítě neoprávněným uživatelem (útočníkem) je třeba mít na mysli, že její dosah se může pohybovat o mnoho dále než je obvodové zdivo kanceláře, pokoje či budovy. Útočník může na základě síly signálu odposlouchávat provoz sítě:

- ze sousední budovy;
- vedlejší místnosti;
- venkovního - veřejného prostranství.

[13] DNS (Domain Name System) - systém, který především překládá doménová jména na IP adresy. [10]

Odposlech drátové sítě je o něco komplikovanější. Útočník potřebuje získat fyzický přístup ke komunikačním vodičům. Pro oba přenosy však platí, většina provozu v síti není šifrována, tím pádem je velice jednoduché odposlouchávat pakety a tím získat značné množství informací.[22][23]

V rámci zjišťování slabých míst zabezpečení sítě se používají tzv. penetrační testy, neboli simulované útoky, které mohou být považované za nezákonné (etický hacking). Často používaným souborem nástrojů penetračních testů a bezpečnostních auditů je BackTrack (Linuxová Live CD distribuce) nyní verze 5R3, případně, BackTrack 6 - Kali Linux 1.0.1 (od 13. 3. 2013). Tyto nástroje jsou však využívány i útočníky.

Při správě, monitorování počítačové sítě, je nutné si uvědomit, že neoprávněné odposlouchávání dat vykazuje znaky trestné činnosti. Dle ustanovení § 182 Trestního zákoníku, kdo úmyslně poruší tajemství dopravovaných zpráv a dle ustanovení § 183 téhož zákona, kdo neoprávněně poruší tajemství listin a jiných dokumentů uchovávaných v soukromí, včetně počítačových dat. Dle ustanovení § 84 zákona č. 151/2000 Sb. o telekomunikacích, kde je definováno telekomunikační tajemství. Pokud je monitorování počítačové sítě prováděno v rámci zákonných a interních předpisů, ke správě či zajištění bezpečnosti, nejedná se o protiprávní činnost.[25][26]

2.7 Ethernet

Všechny tři modelové situace počítačových sítí využívají síťový standard, Ethernet. Ten se od sedmdesátých let minulého století neustále vyvíjel a mimo jiné neustále zvyšoval svoji přenosovou rychlost. Nyní jsou v lokálních sítích používané normy Fast Ethernet, s přenosovou rychlostí 100 Mb/s. a Gigabit Ethernet s přenosovou rychlostí až 1000 Mb/s (1 Gb/s). Aby byl Gigabit Ethernet efektivně využit, musí ho podporovat všechny prvky sítě, včetně rozvodů. Gigabit Ethernet je vhodný použít při užití NAS.[19] [20]

Při monitorování sítě je důležité zmínit pojem, promiskuitní mód síťové karty v sítích typu Ethernet. Tento mód je aktivován při spuštění snifferu na počítači, který vidí veškerý síťový provoz, včetně toho, který není pro něho určen. Musí být podporován i hardwarově, tedy síťovou kartou. Administrátor či správce sítě provádí monitorování v rámci zabezpečení bezpečnosti sítě, proto ostatním uživatelům je vhodné promiskuitní režim zakázat a to autorizací, tedy přidělením uživatelských práv. Nemělo by se dále zapomínat na možnost, jiného zavedení operačního systému a proto použít vstupní heslo do BIOSu[14].[22]

[14] BIOS (Basic Input Output System) - základní vstupní/výstupní systém, zákl. program. vybavení PC.[10]

3 MONITOROVÁNÍ SÍTĚ

3.1 Co je monitoring

Monitoring počítačové sítě je v dnešní době nepostradatelným pomocníkem ke správě sítě. K získání znalosti o činnosti v síti je možno použít monitorovací nástroj. Pomocí tohoto nástroje lze zjistit:

- dostupnost jednotlivých prvků sítě;
- kontrolu dostupnosti jednotlivých služeb;
- ověřit provozní parametry jednotlivých prvků sítě;
- měřit přenos dat;
- ověřit chybovost jednotlivých tras, či další informace.

Toto vyhodnocování lze provádět on-line či off-line, tedy v reálném čase sledovat okamžitý stav, nebo z uložených hodnot historických informací, které se mění v čase. Všechny tyto údaje síťového provozu lze mimo jiné využít k detekci bezpečnostních incidentů i ke zvýšení celkové bezpečnosti systému.[16]

Při definování monitorování počítačových sítí, je potřebné zmínit primární úkol monitoringu, což je zajištění účtovatelnosti aktivit subjektů a zároveň vyhledávání nestandardních, zlomyslných či nemorálních aktivit vedoucích k selhání, narušení nebo omezení činnosti systémů. Tuto činnost lze evidovat pomocí záznamů, reportů a následně ji analyzovat.[6]

V dnešní době existují specializované firmy zabývající se monitorováním počítačových sítí, které využívají profesionálních aplikací. Monitorovacích nástrojů je k dispozici nepřeberné množství. Existují však i kvalitní produkty, které nejsou na komerční bázi, ale jsou volně dostupné, tedy bezplatné.

Před vlastním monitorováním sítě je nutné si stanovit, co je přesně potřebné sledovat, případně co má vyšší prioritu. Na základě těchto určených kritérií je možné si zvolit adekvátní nástroj či kombinaci více produktů. Dále je nezbytné, naplánovat a následně nastavit přehledný výstup z monitoringu. Zde stojí za zvážení, jaký zjištěný stav je nutný bezprostředně nahlásit z důvodu okamžité reakce bezpečnostní funkce a jaké zjištěné informace jsou dostačující až po následné analýze.

Následně budou popisovány monitorovací nástroje, které jsou volně dostupné, uživatelsky nenáročné a použitelné pro počítačové sítě malého rozsahu, dle modelů popisovaných

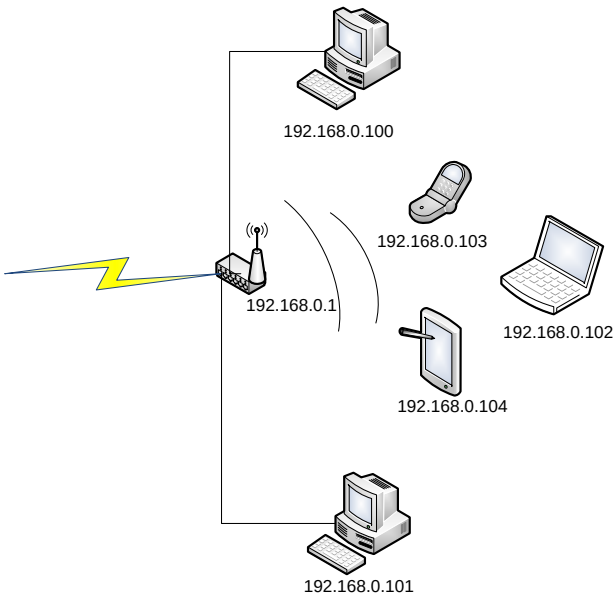
v kapitole 2. Pro všechny tyto modely počítačových sítí platí, že monitorovací nástroj bude spravovat osoba s mírně pokročilými uživatelskými vědomostmi.

Většina popisovaných zdarma dostupných programů (vyjma open-source licencí), jsou označovány jako freeware, což je program, za který se nevyžadují poplatky. Ovšem, autor si může stanovit vlastní licenční podmínky, například, že program nesmí být nijak pozměňován či si může omezit způsob použití, tedy rozdílné podmínky pro domácí použití a pro firmu. Před instalací je vždy nutné se seznámit s licenčními podmínkami.

3.2 Testovaná domácí počítačová síť

Níže popsané nástroje byly testovány na domácí počítačové síti, kterou zobrazuje obrázek 6. Síť byla složena z následujících zařízení:

- router Tenda W311R (IP 192.168.0.1) připojený k internetu;
- stolní PC (IP 192.168.0.100);
- stolní PC (IP 192.168.0.101);
- notebook (IP 192.168.0.102);
- tablet (IP 192.168.0.104);
- mobilní telefon (IP 192.168.0.103).



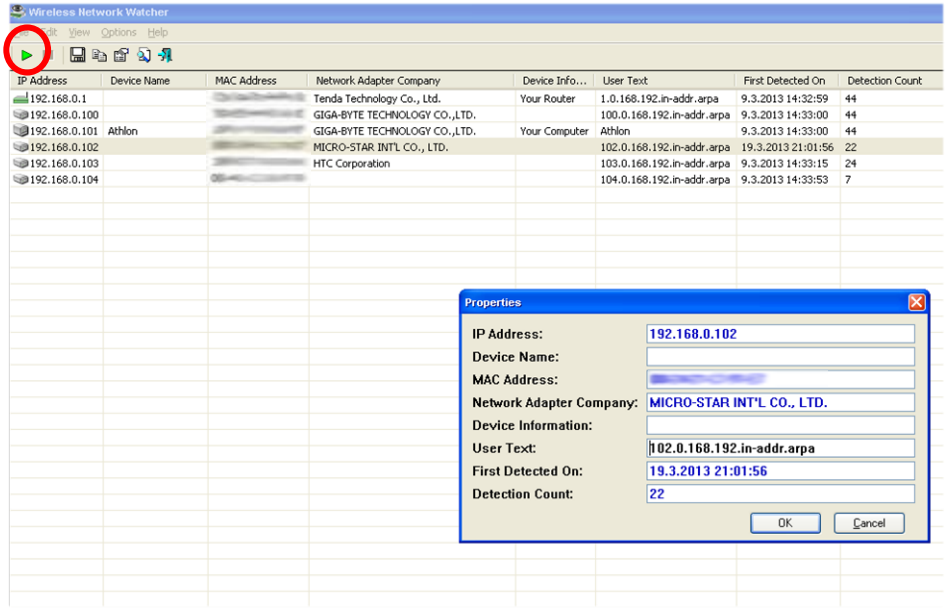
Obrázek 6 - Grafické znázornění testované počítačové sítě.

Zdroj: vlastní zpracování.

Na následujících obrázcích, které zobrazují popisované monitorovací nástroje, budou částečně vymazány MAC adresy prvků v síti.

3.3 NirSoft Wireless Network Watcher

V rámci monitorování sítě je zásadní být informován o připojených zařízeních do sítě. Toto lze zjistit z administračního rozhraní routeru, ale také z nástroje Wireless Network Watcher od společnosti Nirsoft. Po spuštění aplikace se zobrazí dialogové okno, obrázek 7, které po kliknutí na ikonu zelené šipky vyhledá připojené zařízení.



Obrázek 7 - Grafické znázornění dialogového okna Wireless Network Watcher.

Zdroj: vlastní zpracování.

U jednotlivých zařízení se zobrazí IP adresa, název, MAC adresa, výrobce a další informace. Po dvojkliku na zařízení se zobrazí technické podrobnosti (properties). Výsledky lze uložit do souboru. Zajímavou funkcí je opakované skenování sítě (Option/Background Scan) a nastavení zvukového signálu (Option/Beep On New Device), pokud dojde k připojení nového zařízení. Toto lze využít k monitorování připojení zařízení k bezdrátové síti, například neoprávněného uživatele.

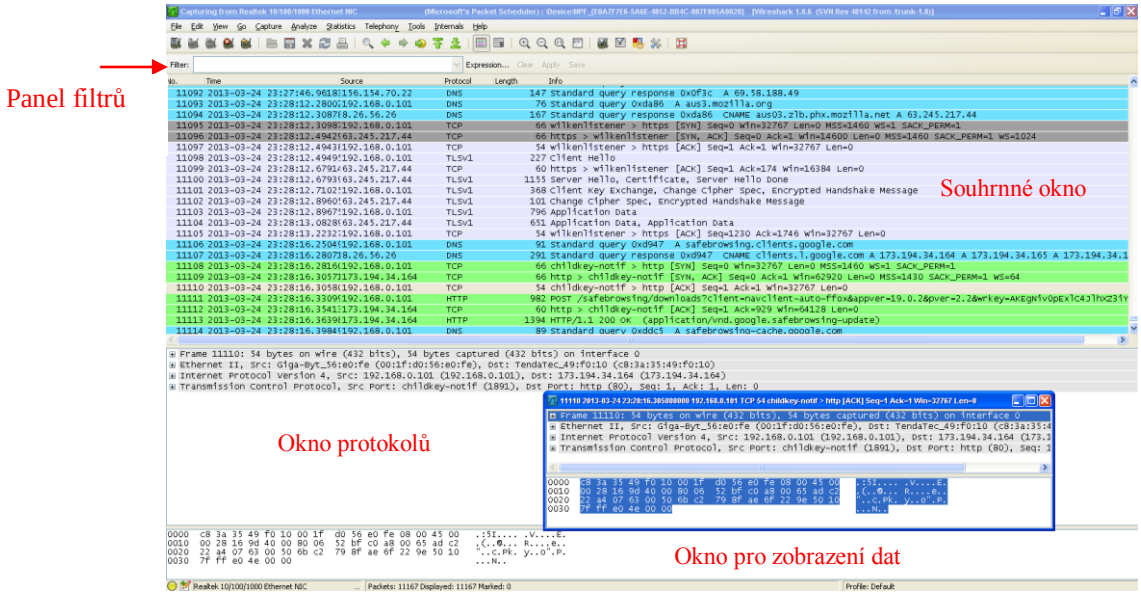
Zde jsou uvedeny další informace o tomto uživatelsky přívětivém nástroji, který má v názvu bezdrátové sítě, ale lze skenovat i sítě LAN malého rozsahu:

- instalace: ano (existuje verze i bez instalace);
- jazyk: angličtina (čeština lze doinstalovat, viz domovská stránka);
- pro operační systém: Microsoft Windows 2000/Vista/XP/7/8, Server 2003/2008;
- aktuální verze: 1.58;
- domovská stránka: http://www.nirsoft.net/utils/wireless_network_watcher.html.

3.4 Wireshark

Wireshark je zdarma šiřitelný, jako open-source licence GNU General Public Licence, tedy jako "svobodný software". Předchůdce Wiresharku je software Ethereal. Wireshark patří mezi tzv. síťové analyzátory. Provádí čtení paketů v počítačové síti, které následně dekóduje a zobrazuje je do srozumitelného formátu. Wireshark dokáže pracovat se 750 typů protokolů, včetně hlavních protokolů internetu (IP, TCP, UDP[15], ICMP[16]). Zachytávat je lze z několika typů sítí, včetně Ethernet či IEEE 802.11. Umožňuje bohaté nastavení filtrace paketů. Data umí vykreslovat i v grafech. Pracuje jak v promiskuitním, tak i nepromiskuitním módu.[22]

Při instalaci Wiresharku je třeba naistalovat WinPcap, což je soubor knihoven a ovladačů umožňující zachytávání paketů a síťovou analýzu u síťových adaptérů.



Obrázek 8 - Grafické znázornění dialogového okna Wireshark.

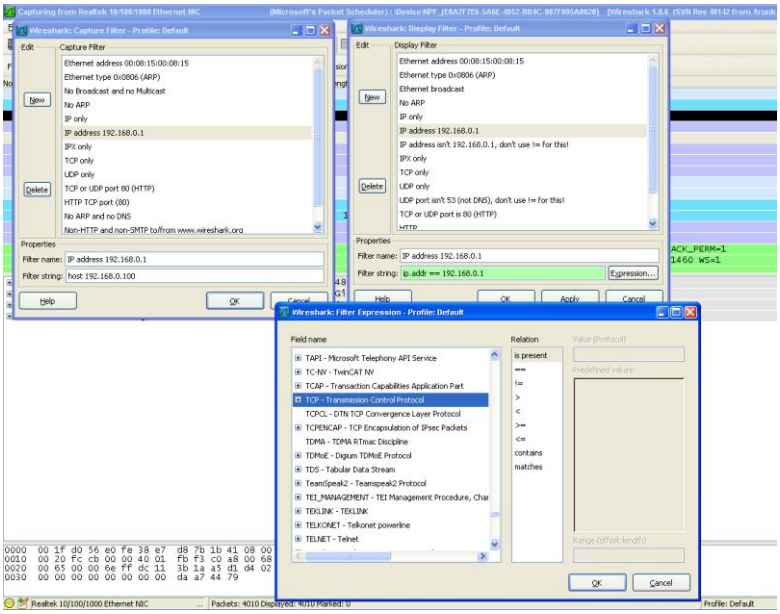
Zdroj: vlastní zpracování.

Grafické uživatelské rozhranní verze 1.8.6 zobrazuje obrázek 8. Pod panelem nástrojů se nachází panel filtrů. V souhrnném okně se zobrazují zachycené pakety s dalšími údaji, sloupce zleva: číslo rámce, čas, adresa zdroje, protokol, další informace například o navazování spojení - SYN, ACK, FIN. O paketu označeném v souhrnném okně jsou vypsány podrobné údaje v okně protokolů a skutečná data v okně pro zobrazení dat.[22]

[15] UDP (User Datagram Protocol) - transportní protokol poskytující nespojovanou, nespolehlivou datagramovou službu.[10]

[16] ICMP (Internet Control Message Protocol) - slouží k signalizaci mimořádných událostí v sítích na IP protokolech.[19]

Ve Wiresharku lze nastavit filtry pro zobrazení (D*isplay Filter*) či filtry pro zachytávání dat (C*apture Filter*). Obrázek 9 zobrazuje nastavení těchto filtrů s možností přidání dalších výrazů pomocí tlačítka Expression. Pro uživatele může být toto definování náročnější.[22]



Obrázek 9 - Dialogová okna nastavování filtrů ve Wireshark.

Zdroj: vlastní zpracování.

Wireshark jde použít mimo jiné k rekonstrukci paketů či k odhalení chatování (aktivita IRC - Internet Relay Chat protokolu), některého z uživatelů sítě. Výstup lze uložit nebo vytisknout. Vyhodnocující data mohou být načtena ze souboru.

Tento mocný nástroj je sice uživatelsky náročnější, ovšem svými možnostmi, kdy dokáže zobrazit značné množství podrobných informací o komunikaci na síti, může konkurovat komerčním nástrojům.

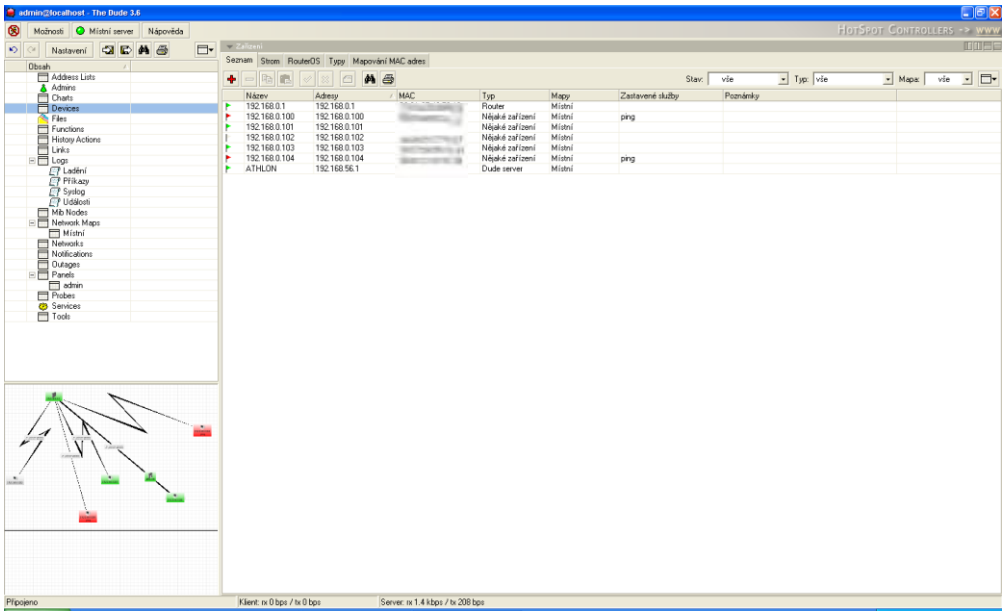
K tomuto nástroji, jednomu z mála monitorovacích nástrojů, byl vydán podrobný průvodce v češtině, kniha z vydavatelství CPRESS - *Wireshark a Ethereal: kompletní průvodce analýzou a diagnostikou sítí* viz [22]. Tato kniha může být nápomocí pro uživatelé modelových situací popsaných v kapitole 2.

Další informace o nástroji Wiresharku:

- instalace: ano;
- jazyk: angličtina;
- pro operační systém: Microsoft Windows, Linux, Solaris, BSD a Mac OS X;
- aktuální verze: 1.8.6;
- domovská stránka: http://www.wireshark.org.

3.5 The Dude

Tento uživatelsky přívětivý síťový monitor od firmy MicroTik, umožňuje spravování sítě tím, že dokáže automaticky prozkoumávat síť, kreslit schémata sítě, monitorovat služby či oznamovat případné problémy.



Obrázek 10 - Grafické rozhranní nástroje The Dude.

Zdroj: vlastní zpracování.

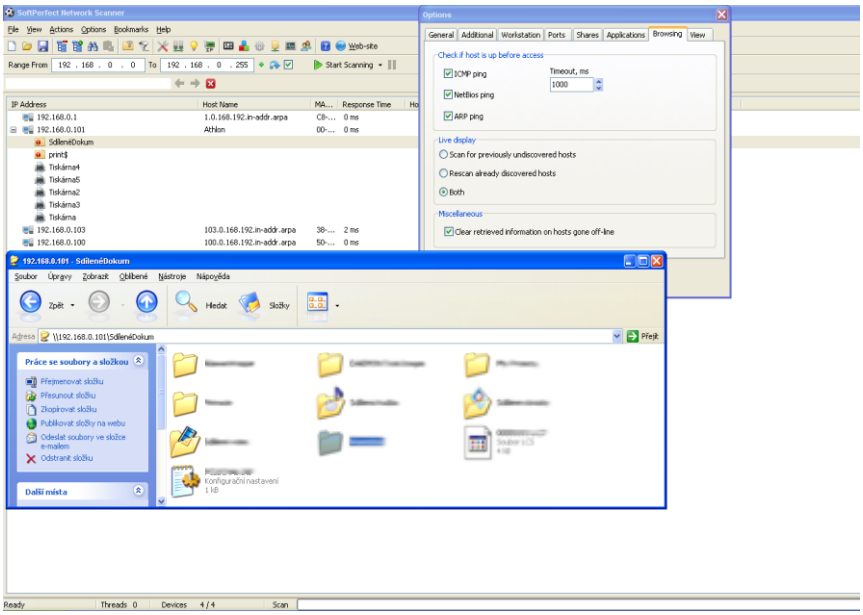
Instalace nástroje je snadná, mnohé uživatele potěší částečné počeštění aplikace. The Dude umožňuje kreslení vlastních map a přidávání vlastních zařízení. Vytvořená jednoduchá mapa testované sítě je zobrazena v levém spodním rohu na obrázku 10. Nad mapou sítě, v levé části obrázku 10, je zobrazen list nastavení The Dude, vpravo lze vidět informace o sledovaném zařízení. Jednotlivé zařízení lze monitorovat individuálně včetně využití grafů. Monitorování zařízení probíhá pomocí protokolů SNMP[17], ICMP, DNS a TCP. The Dude umožňuje přímý přístup k nástrojům vzdálené správy zařízení. Níže jsou uvedeny další informace sloužící potencionálním uživatelům produktu The Dude:

- instalace: ano;
- jazyk: angličtina /čeština;
- pro operační systém: Linux, Mac OS, Microsoft Windows 2000/XP/2003/Vista/7/8;
- aktuální verze: 3.6/4.0 beta 3;
- domovská stránka: http://www.mikrotik.com.

[17] SNMP (Simple Network Management Protocol) - řídící protokol, určen pro správu sítě.[10]

3.6 SoftPerfect Network Scanner

Tento monitorovací, uživatelsky snadný, pokročilými funkcemi vybavený nástroj pracující v grafickém prostředí nevyžaduje instalaci. Při monitorování sítě je základní informace o připojených zařízeních v síti. Nastavením rozsahu IP adres "Range From", "To" lze vyhledat zařízení v síti i zjistit jejich MAC adresu. Dále lze detekovat a zobrazit skryté sdílené složky. Umožňuje skenovat síťové jednotky, umí připojit sdílené zařízení či vyhledat otevřené TCP/UDP porty. Nástroj využívá program ping. Na obrázku 11 jsou zobrazeny vyhledané zařízení v síti, otevřené sdílené složky i soubory. Otevřené okno Options, ukazuje na možné nastavení programu ping.



Obrázek 11 - Grafické rozhranní nástroje SoftPerfect Network Scanner.

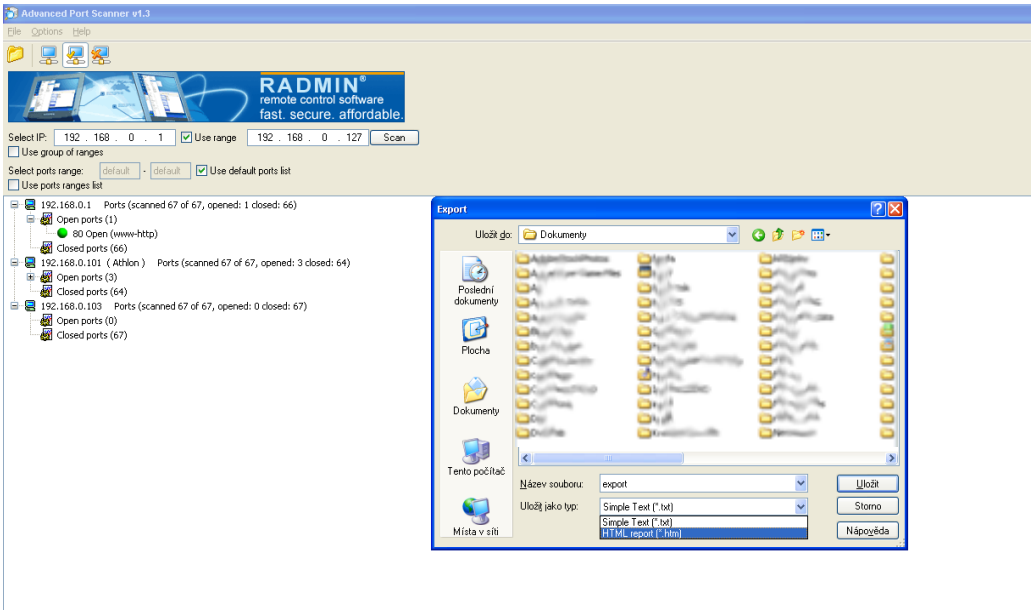
Zdroj: vlastní zpracování.

SoftPerfect Network Scanner disponuje i jinými funkcemi, mimo jiné podporuje Wake-On-LAN, tedy vypínání zařízení přes počítačovou síť. Výsledky skenování lze uložit do HTML, XML, CSV či TXT souborů.

- instalace: ne;
- jazyk: angličtina;
- pro operační systém: Windows 2000/XP/2003/Vista/7/8, Server 2003/2008;
- aktuální verze: 5. 4. 10;
- domovská stránka: http://www.softperfect.com.

3.7 Advance Port Scanner

Advanced Port Scanner je přehledný, rychlý, snadno ovladatelný port skener. Nástroj pracující v grafickém rozhraní umí vyhledat zařízení v síti. Pomocí nastavení rozsahu lze skenovat požadované IP adresy. Dále program na vyhledaných strojích skenuje porty. Skenováním portů lze identifikovat druh služby běžící na monitorovaném stroji, případně stav portů (open, close). Na otevřené porty se lze připojit, na zavřené nikoliv. Port, neboli číslo síťového portu, je speciální adresa (0 až 65535), která slouží v počítačových sítích k identifikaci odesílajících a přijímajících aplikací. Například port 80 představuje webovou službu, přenos WWW stránek i jiných dat s protokolem HTTP.[19]



Obrázek 12 - Grafické rozhraní nástroje Advanced Port Scanner.

Zdroj: vlastní zpracování.

Na obrázku 12 jsou zobrazena vyhledaná zařízení v rozsahu IP 192.169.0.1 až 192.168.0.127. Advanced Port Scanner vyhledal tři zařízení. U zařízení s IP adresou 192.169.0.1 je zeleně označen otevřený port 80. U portů lze před skenováním předdefinovat rozmezí. Výstup lze uložit, jak zobrazuje obrázek 12., do souboru TXT i HTM. Nástroj je volně šiřitelný, což je vykoupeno reklamou firmy (banner), která skener vytvořila.

- instalace: ano;
- jazyk: angličtina;
- pro operační systém: Microsoft Windows 2000/XP/2003/Vista/7/8;
- aktuální verze: 1.3;
- domovská stránka: http:// www.radmin.com.

3.8 InSSIDer

Při správě a monitorování bezdrátové sítě je mnohdy potřebná informovanost. Jeden z mnoha užitečných nástrojů se nazývá InSSIDER, který je poskytován v rámci Open Source licence. Přehledné grafické rozhraní při spuštění nabídne pohled, který zobrazuje obrázek 13. Nástroj vyhledá dostupné Wi-Fi sítě. Dále, jak zobrazuje obrázek 13 z leva, poskytne informace o SSID (název sítě), Channel - číslo kanálu vysílače, RSSI (kvalita signálu), zabezpečení bezdrátové sítě, MAC adresu routeru sítě, Max Rate - teoretická max. rychlost přenosu (Mbps[18]), Vendor - název přístupového bodu, typ sítě (infrastrukturní, ad-hoc) a čas prvního záznamu o připojení. V dolní části obrázku 13 je viditelný graf vyhledaných sítí, konkrétně pro pásmo 2,4 GHz, který může napomoci při řešení kolizí. Na vodorovné ose jsou zobrazeny obsazené kanály 1 až 14 a vertikální osa ukazuje sílu signálu v jednotkách dBm.

Obrázek 13 - Pohled na dialogové okno nástroje inSSIDer 2.1.

Zdroj: vlastní zpracování.

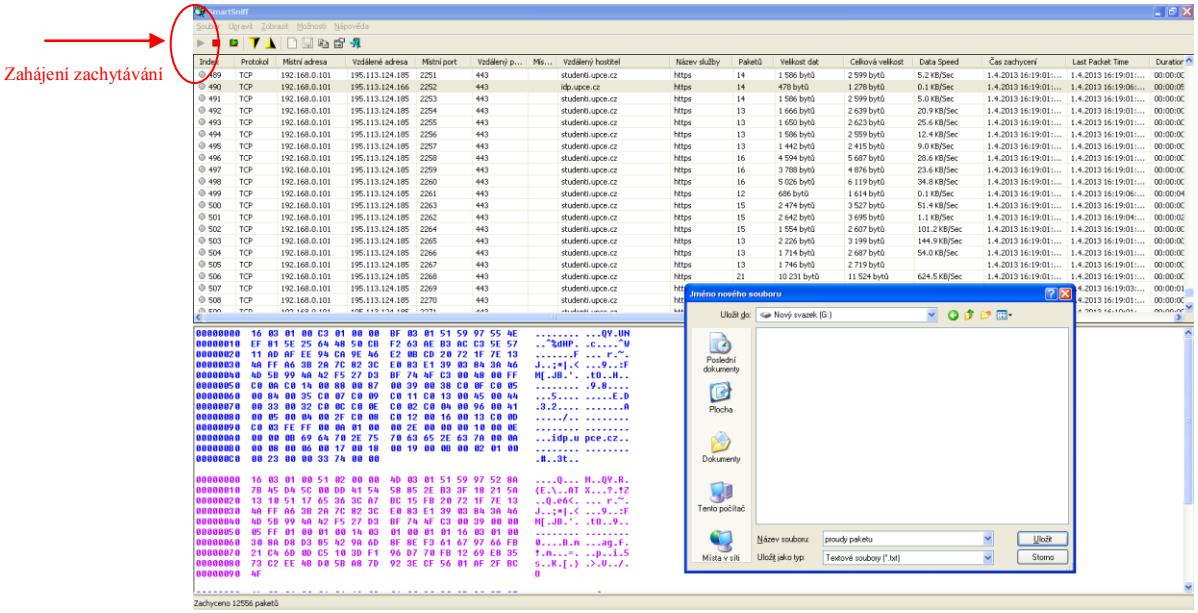
InSSIDer podporuje filtraci vyhledaných informací a použití GPS s exportem polohy.

- instalace: ano;
- jazyk: angličtina;
- pro operační systém: Microsoft Windows 2000/XP/2003/Vista/7/8;
- aktuální verze: 2.1.6;
- domovská stránka: http://www.metageek.net.

[18] Mbps - jednotka přenosové rychlosti udávající megabity za sekundu.

3.9 SmartSniff

SmartSniff od společnosti Nirsoft po snadné instalaci nabízí grafické uživatelské rozhraní monitorovacího nástroje, kterým lze zachytávat TCP/IP pakety procházející místní síti. Pro monitorování je potřeba mít nainstalovaný WinPcap a síťovou kartu v promiskuitním módu. Před prvním zapnutím, je třeba vybrat metodu snímání síťové karty. Obrázek 14 zobrazuje dialogové okno nástroje. Kde lze vyčíst mimo jiné druh protokolu (TCP, UDP, ICMP), IP adresy, čísla portů, hostitelské www stránky, název služby, velikost dat, rychlost připojení či čas zachycení. Podrobnější informace lze zobrazit po označení řádku. Jednotlivé proudy paketů lze uložit do TXT.



Obrázek 14 - Grafické rozhraní nástroje SmartSniff 2.00.

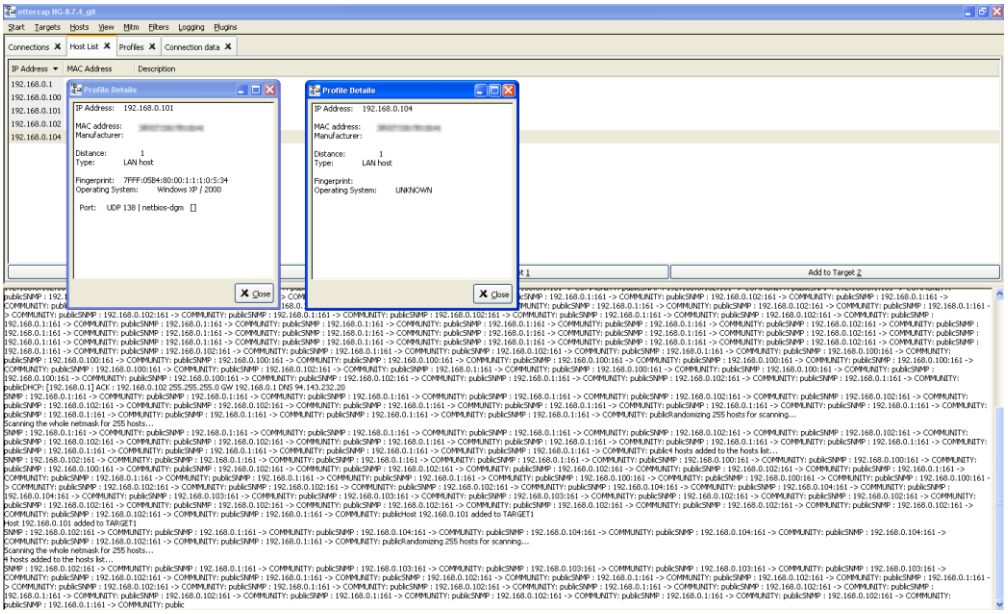
Zdroj: vlastní zpracování.

SmartSniff lze přímo spustit i z přenosného média. Zachytávání je možné nastavit řetězcem filtrů Captrure i Display Filters. Obecně lze konstatovat, SmartSniff je uživatelsky snadnější a přehlednější než Wireshark.

- instalace: ano/smsniff.exe lze zkopírovat do libovolné složky-instalace není nutná;
- jazyk: angličtina/existuje čeština, soubor smsniff.ini nakopírovat do složky SmartSniff a spustit program;
- pro operační systém: Microsoft Windows 2000/XP/2003/Vista/7/8;
- aktuální verze: 2.05;
- domovská stránka: http://www.nirsoft.net/utils/smsniff.html.

3.10 Ettercat

Původně byl tento GNU GPL nástroj vyvinut k zachytávání hesel a testování bezpečnosti sítě. Po spuštění v menu Options je třeba zkontrolovat Promisc mode. Monitorování se zahájí v nabídce Sniff/Unifield sniffing, následně se nastaví síťové rozhraní a poté v nabídce Start/Sart sniffing. V nabídce Hosts/Scan for hosts lze vyhledat stanice v síti. Na obrázku 15 jsou zobrazena vyhledaná zařízení v síti, s podrobnými informacemi o zařízení (IP adresa, MAC adresa, či operační systém). Operační systém tabletu - Android 4.0, však Ettercat nevyhledal, zařízení nekomunikovalo. I tento nástroj umožňuje monitorovat komunikaci v síti, v podobě informací o protokolech, portech, či velikosti objemu dat.



Obrázek 15 - Grafické rozhraní nástroje Ettercat 0.7.4.

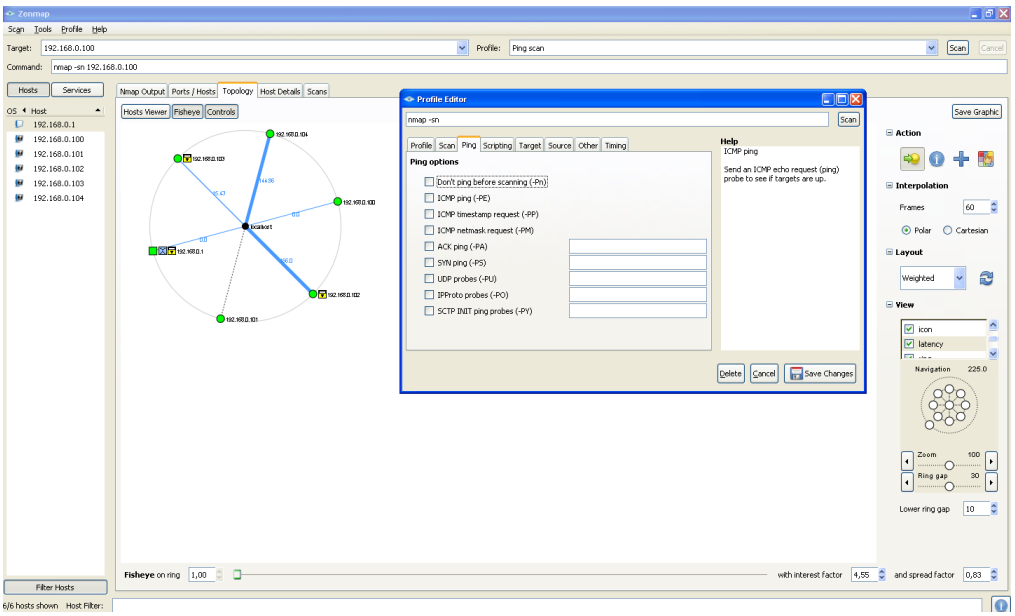
Zdroj: vlastní zpracování.

Ettercat umožňuje různé druhy filtrování. Obsahuje velké množství nástrojů k odhalování, testování, zabezpečení hesel, umožňuje i rozbor šifrovaných protokolů. Složitější uživatelské grafické rozhraní může způsobovat začínajícím uživatelům problémy. Po osvojení nástroje však uživatelům poskytne kompletní informace při monitorování sítě. Ettercat je však často využíván i útočníky.

- instalace: ano;
- jazyk: angličtina;
- pro operační systém: Linux, Microsoft Windows 2000/XP/2003/Vista/7/8;
- aktuální verze: 0.7.6;
- domovská stránka: http://ettercap.sourceforge.net.

3.11 NMAP

Tento často používaný nástroj slouží k bezpečnostnímu a diagnostickému prozkoumávání sítě. Podporuje široké možnosti skenování, včetně skenování portů a jejich služeb. Původní NMap (Network Mapper) se používal v příkazové řádce. Nyní existuje grafické rozhraní Zenmam. Je distribuován jako GPL. Při instalaci je možné výběr komponent (WinPcap, Zenmap - GUI Nmapu, Ncat - scanner portů a Telnet, Ndiff - práce s XML, Nping).



Obrázek 16 - Grafické rozhraní nástroje Zenmap 6.01.

Zdroj: vlastní zpracování.

Na obrázku 16 je zobrazena grafická topologie testované sítě, sestavená po skenování Zenmapu, který dokáže identifikovat jednotlivé zařízení v síti, včetně používaného operačního systému. Lze využít i značné množství ping testů (obrázek 16). Dále je možné využít různorodé skenování sítě. Např. TCP connect či SYN scan. Nástroj lze použít i ke skenování rozlehlých sítí. Uživatelsky nepatří mezi nejsnadnější, ale existují podrobné návody na domovské stránce, zejména v sestavování příkazů skenování.

- instalace: ano;
- jazyk: angličtina;
- pro operační systém: Linux, Solaris, BSD, Mac OS X, Microsoft Windows;
- aktuální verze: 6.25;
- domovská stránka: http://nmap.org.

3.12 Integrované programy v operačních systémech

K základnímu analyzování či monitorování počítačové sítě, lze využít nástroje integrované v operačních systémech Microsoft Windows nebo Linux. Uvedené programy se zadávají pomocí uživatelského rozhraní příkazové řádky.

3.12.1 Ipconfig/Ifconfig

Ipconfig se používá v operačních systémech Microsoft Windows a ifconfig pro Linux. Po zadání příkazu se zobrazí IP adresa, maska podsítě a výchozí brána pro síťový adaptér. Lze použít přepínač "all" (příklad pro Windows*: ipconfig/all*), následně dojde k zobrazení podrobných informací o konfiguraci.[27]

3.12.2 Ping

Příkaz, který vysílá žádost ICMP na cílovou stanici, ta vyšle zpět zprávu ICMP s odpovědí. Lze tedy zkontrolovat dostupnost cílové adresy IP, test latence či chybovost trasy. Zjištěný výsledek se vypíše. Zadávat je možné IP adresu (například: ping 192.168.0.101), nebo doménu (například: *ping seznam.cz*). Zadávání je stejné jak ve Windows, tak i v Linuxu.[27]

3.12.3 Tracert/Traceroute

Tracert se používá v operačních systémech Microsoft Windows a Traceroute pro Linux. Příkaz slouží ke kontrole cesty zadané cílové IP adresy. Vypíší se uzly od zdroje k cíli. (příklad pro Windows*: tracert 192.168.0.101*). Využívá se ke kontrole chybného směrování, či při diagnostice problému v počítačové síti.[27]

4 DOPORUČUJÍCÍ SHRNUTÍ UŽIVATELŮM

Každá z modelových situací, uvedených v kapitole 2, je něčím specifická. Stejně jako nástroje uvedené v kapitole 3. Před použitím monitorovacího nástroje je vhodné si stanovit účel použití a k tomu vybrat vhodný nástroj. Například:

- k rychlému vyhledání připojených, či nově připojených zařízení, použít NirSoft Wireless Network Watcher;
- k analýze paketů, využít síťový analyzátor Wireshark, či uživatelsky méně náročný SmartSniff;
- ke skenování portů Advanced Port Scanner, či SoftPerfect Network Scanner;
- k zobrazení schématu sítě The Dude;
- pro bezdrátové sítě lze využít InSSIDER;
- ke kompletnímu monitoringu využít Ettercat, či NMap;
- v některých případech může být dostačující použití některého z integrovaných nástrojů v operačních systémech, například ping, k ověření dostupnosti zařízení.

Každý z výše uvedených nástrojů umožňuje více funkcí, než zde bylo stručně uvedeno. Pro zvýšení bezpečnosti v počítačové síti použitím některého nástrojů uvedeného v kapitole 3, je však nutné zdůraznit:

- **před používáním výše uvedených nástrojů, je vždy se třeba pečlivě seznámit se směrnicemi či zásadami používání pracovních stanic i počítačové sítě.**

Pro monitorování soukromé domácí počítačové sítě tento bod odpadá, nicméně osoba, která bude jakýkoliv nástroj používat, by se měla předem seznámit s tím, co nástroj umožňuje, k čemu slouží a případně co může neodborným užíváním způsobit. Toto platí pro všechny modelové situace. Předpokládá se, že v těchto modelových situacích bude nástroj používat uživatel s mírně pokročilými znalostmi v oboru IT. Kapitola 3 může těmto uživatelům přinést základní představu o používání některého z uvedených nástrojů.

Uživatel by se však měl řídit doporučeními uživatelům kyberprostoru, jak preventivně eliminovat hrozící nebezpečí popsaných v kapitole 1, aby snížil riziko bezpečnostního incidentu a zároveň tím zvýšil informační bezpečnost. Je však stále mít na paměti:

- **sebelepší technické zabezpečení počítačové sítě je k ničemu, pokud se nebude uživatel chovat zodpovědně a ukázněně.**

ZÁVĚR

Cílem této práce bylo vytvoření přehledu základních skupin bezpečnostních incidentů v prostředí počítačové sítě, dostupných nástrojů pro monitoring a odhalovaní nežádoucích činností uživatelů sítě.

Bezpečnost v počítačové síti je velmi rozsáhlé téma. Vzhledem k předepsanému rozsahu, byla první část práce věnována obecnému popisu možných bezpečnostních incidentů v rámci kyberprostoru, tedy hrozeb v počítačových sítích, včetně popisu některých pravidel a zásad, které rizikového chování, či úspěšné dokončení úmyslného bezpečnostního incidentu útočníkovy ztíží. Druhá část je věnována modelovým situacím počítačových sítí malého rozsahu. Provozovatelé či uživatelé těchto sítí k odhalování nežádoucích, neoprávněných činností mohou využít některého z monitorovacích nástrojů popsaných ve třetí části. Poslední část obecně shrnuje používání nástrojů popisovaných ve třetí části.

Modelové situace vychází z počítačových sítí typu SOHO LAN pro domácnost, malou firmu a obecní úřad malé obce. V těchto modelových situacích často není prováděn monitoring sítě a tedy i dohled nad informační bezpečností. Pomocí nástrojů uvedených ve třetí části, lze monitorování sítě z pohledu bezpečnosti provádět s minimálními náklady a se znalostmi mírně pokročilého uživatele IT. Pro potencionálního útočníka sítě tohoto typu nepředstavují významný cíl, vzhledem k důležitosti dat, nicméně útočník může sázet na nízký stupeň zabezpečení a podniknout útok.

SEZNAM ZDROJŮ A POUŽITÉ LITERATURY

[1] JIROVSKÝ, Václav. Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství. Praha: Grada, 2007. ISBN 978-80-247-1561-2.

[2] Kyberhrozby a kyberterorismus. In: Kyber - CESES [online]. 2011 [cit. 2012-04-20]. Dostupné z: http://ceses.cuni.cz/CESES-70-version1-Kyber.pdf.

[3] Analýza současného stavu a trendů vývoje trestné činnosti na úseku informačních technologií a internetu včetně návrhu řešení. In: Koncepce boje proti trestné činnosti v oblasti informačních technologií včetně Harmonogramu opatření [online]. 2008 [cit. 2012-04-20].
Dostupné z: http://aplikace.mvcr.cz/archiv2008/dokument/2006/informacni.pdf.

[4] JIROVSKÝ, Václav, HNÍK, Václav a KRULÍK, Oldřich. Kybernetické hrozby: Výzva pro moderní společnost. In: Kybernetické hrozby: Výzva pro moderní společnost [online]. 2006 [cit. 2012-04-21].
Dostupné z: http://aplikace.mvcr.cz/archiv2008/bezpecnost/informacni.html.

[5] Česká televize [online]. 29. února 2012 [cit. 2012-04-21]. Studio 6, Ondřej FILIP, výkonný ředitel cz.nic. Dostupné z: http://www.ceskatelevize.cz/ivysilani/1096902795-studio-6/212411010100229/obsah/192369-kyberneticka-bezpecnost.

[6] STEWART, James Michael, TITTEL, Ed, a CHAPPLE, Mike. *CISSP: Certified Information Systems Security Professional study guide*. 3rd ed. San Francisco: SYBEX, c2005, 759 p. ISBN 07-821-4443-8.

[7] Cyber_vyzkum_studie_pojmy.pdf. In: Základní definice, vztahující se k tématu kybernetické bezpecnosti [online]. 2009 [cit. 2012-04-22]. Dostupné z: http://www.mvcr.cz/clanek/o-NAS-bezpecnost-a-prevence-dokumenty-bezpecnost-a-prevence-dokumenty-kyberneticke-hrozby.aspx.

[8] Vyhráváme včerejší bitvy. Vyhráváme včerejší bitvy. 2009, č. 55. [cit. 2012-04-22]. Dostupné z: http://hn.ihned.cz/c1-35773180-vyhravame-vcerejsi-bitvy.

[9] KOPECKÝ, Kamil. Kybergrooming: Nebezpečí kyberprostoru. In: Kybergrooming: Nebezpečí kyberprostoru [online]. Olomouc, 2010 [cit. 2012-04-23]. ISBN 978-80-254-7573-7. Dostupné z: http://vzdelavani.e-bezpeci.cz/clanek.php?id=oprojektu.

[10] HLAVENKA, Jiří. Výkladový slovník výpočetní techniky a komunikací. 3. vyd. Praha: Computer Press, 1997, 452 s. ISBN 80-722-6023-5.

[11] KOPECKÝ, Kamil. Stalking a kyberstalking: Nebezpečné pronásledování. In: Stalking a kyberstalking: Nebezpečné pronásledování [online]. Olomouc, 2010 [cit. 2012-04-24]. ISBN 978-80-254-7737-3.
Dostupné z: http://vzdelavani.e-bezpeci.cz/clanek.php?id=oprojektu.

[12] KOPECKÝ, Kamil a KREJČÍ, Veronika. Rizika virtuální komunikace: (příručka pro učitele a rodiče). In: Rizika internetové komunikace [online]. Olomouc, 2010 [cit. 2012-04-23]. ISBN 978-80-254-7866-O.
Dostupné z: http://vzdelavani.e-bezpeci.cz/clanek.php?id=oprojektu.

[13] Co je VoIP?. In: JOYCE ČR, s.r.o.: 1-2-3 Spojeno [online]. 2012 [cit. 2012-04-24]. Dostupné z: http://www.joyce.cz/co-je-voip.

[14] 25 nejhorších hesel používaných v roce 2011. *Zive.cz* [online]. 2011 [cit. 2012-04-25]. Dostupné z: http://www.zive.cz/bleskovky/25-nejhorsich-hesel-pouzivanych-v-roce-2011/sc-4-a-159606/default.aspx.

[15] Internet. *SFH Blog* [online]. 2013 [cit. 2013-03-07]. Dostupné z: http://sfh.naasat.in/2013/01/metaphors-analogies-narrative-and-smac.html.

[16] Internet. PŘIBYL, Tomáš. Monitoring sítě – jaké jsou základní kameny?. [online]. [cit. 2013-02-28]. Dostupné z: http://ictsecurity.cz/09/06/2-monitoring-site/monitoring-site-jake-jsou-zakladni-kameny.html.

[17] *Computer: život s počítači*. Brno: Computer Press Media, 2011, roč. 18, 21/2011. ISSN 1210-8790.

[18] Internet. *RNDX4250-100NAS* [online]. 2013 [cit. 2013-03-10]. Dostupné z: http://www.officefirewalls.com/readyNAS/nvx/readyNAS-nvx-dual-gigabit-desktop-storage-1tb-w-2x500gb.html.

[19] KABELOVÁ, Alena a DOSTÁLEK, Libor. *Velký průvodce protokoly TCP/IP a systémem DNS*. 5., aktualiz. vyd. Brno: Computer Press, 2008, 488 s. ISBN 978-80-251-2236-5.

[20] ODOM, Wendell. *Počítačové sítě bez předchozích znalostí*. Vyd. 1. Brno: CP Books, 2005, 383 s. ISBN 80-251-0538-5.

[21] *Computer: život s počítači*. Brno: Computer Press Media, 2012, roč. 19, 18/2012. ISSN 1210-8790.

[22] OREBAUGH, Angela. *Wireshark a Ethereal: kompletní průvodce analýzou a diagnostikou sítí*. Vyd. 1. Brno: Computer Press, 2008, 444 s. ISBN 978-80-251-2048-4.

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

[24] Internet. CSIRT [online]. 2011 [cit. 2013-03-28]. Dostupné z: http://www.csirt.cz.

[25] Zákon č. 40/2009 Sb., Trestní zákoník.

[26] Zákon č. 151/2000 Sb., o telekomunikacích.

[27] SHINDER, Debra Littlejohn. *Počítačové sítě: nepostradatelná příručka k pochopení síťové teorie, implementace a vnitřních funkcí*. Praha: SoftPress, 2003, 752 s. ISBN 80-864-9755-0.

[28] BIGELOW, Stephen J. *Mistrovství v počítačových sítích: správa, konfigurace, diagnostika a řešení problémů*. Vyd. 1. Překlad Petr Matějů. Brno: Computer Press, 2004, 990 s. ISBN 80-251-0178-9.