UNIVERZITA PARDUBICE
Fakulta elektrotechniky a informatiky

Využití penetračního testování pro zabezpečení počítačové sítě

Jan Dušek

Bakalářská práce
2014

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

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Jan Dušek**
Osobní číslo:	**I11507**
Studijní program:	**B2646 Informační technologie**
Studijní obor:	**Informační technologie**
Název tématu:	**Využití penetračního testování pro zabezpečení počítačové sítě**
Zadávající katedra:	**Katedra informačních technologií**

Zásady pro vypracování:

Cílem práce je odborně popsat principy využívané penetračním testováním a na jejich základě popsat postupy pro využití výsledů penetračního testování ke zvýšení zabezpečení počítačové sítě. Autor podrobně představí principy a technologie využívané k penetračnímu testování, popíše standardizované postupy pro diagnostiku sítě s využitím penetračních testů a vytvoří sadu postupů pro zlepšení bezpečnosti počítačové sítě na základě výsledků z penetračních testů. Tyto postupy autor prakticky ověří.

Rozsah grafických prací:

Rozsah pracovní zprávy:

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

Seznam odborné literatury:

SELECKÝ, Matúš, Rus HEALY a Naren MEHTA. Penetrační testy a exploitace: autorizovaný výukový průvodce. 1. vyd. Brno: Computer Press, 2012, 303 s. Samostudium. ISBN 978-80-251-3752-9.
LAMMLE, Todd, Rus HEALY a Naren MEHTA. CCNA: výukový průvodce přípravou na zkoušku 640-802. Vyd. 1. Brno: Computer Press, 2010, 928 s. Samostudium. ISBN 978-802-5123-591.
ALLEN, Lee, Rus HEALY a Naren MEHTA. Advanced penetration testing for highly-secured environments: výukový průvodce přípravou na zkoušku 640-802. Vyd. 1. Brno: Packt Publishing, 2010, 928 s. Samostudium. ISBN 978-184-9517-744.

Vedoucí bakalářské práce: **Mgr. Josef Horálek**
Katedra softwarových technologií

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

L.S.

prof. Ing. Simeon Karamazov, Dr.
děkan

Ing. Lukáš Čegan, Ph.D.
vedoucí katedry

V Pardubicích dne 31. března 2014

Prohlášení autora

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 29.04.2014 Jan Dušek

Poděkování

Rád bych tímto poděkoval vedoucímu mé bakalářské práce Mgr. Josefu Janu Horálkovi, Ph.D. za věnovaný čas a cenné rady při tvorbě této práce.

Anotace

Práce se zabývá problematikou penetračního testování počítačových sítí. Cílem je představit základní pojmy, nástroje a postupy související s penetračními testy. V poslední části práce bude provedeno penetrační testování na modelovém příkladu ukazující použití určitých nástrojů a možné přístupy penetračního testování, půjde o testování aktivních zařízení sítě od společnosti Cisco.

Klíčová slova

penetrační testování, bezpečnost počítačových sítí, Cisco IOS, Backtrack

Title

Application of penetration testing for a computer network security

Annotation

This bachelor's thesis discusses penetration testing of computer networks. The aim is to introduce the basic concepts, tools and processes associated with penetration tests. In the last part of the work penetration testing of a model example will be performed showing the use of specific tools and possible approaches of penetration testing, mostly it is going to be the testing of active network devices from Cisco company.

Keywords

penetration testing, computer network security, Cisco IOS, Backtrack

Obsah

Seznam zkratek

ACL	Access control list
AP	Access point
ARP	Address resolution protocol
CBAC	Conent-based access firewall
ČSN	Česká technická norma (dříve Československá státní norma)
DDoS	Distributed Denial of Service
DHCP	Dynamic Host Configuration Protocol
DMZ	Demilitarizovaná zóna
DoS	Denial of Service
FTP	File Transfer Protocol
FW	Firewall
HW	Hardware
ICT	Informační a komunikační technologie
IDS	Intrusion Detection System
IEC	International Electrotechnical Commission
IP	Internet protocol
IS	Informační systém
ISO	International Organization for Standardisation
LAN	Local Area Network
MAN	Metropolitan Area Network
MITM	Main-in-the-middle
NAT	Network address translation
OS	Operační systém
RFC	Request for Comments
RIP	Routing information protocol
SMB	Server Message Block
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SW	Software
TCP	Transmission Control Protocol
UPS	Uninterruptible Power Supply
VLAN	Virtuální LAN
VLSM	Variable-Length Subnet Mask
VPN	Virtual private network
WAN	Wide Area Network

Seznam obrázků

Seznam tabulek

Úvod

Informatika je nepochybně jedním z nejrychleji se rozvíjejících oborů vědy, každý den se objevují nové technologie a otevírají se nové možnosti v oblasti vývoje. Bohužel se také stejně často objevují nové bezpečnostní chyby, které mohou být zneužity k získání cenných informací. Kvůli tomu se již před vznikem internetu a sítí jako takových řešila otázka jak spolehlivě a bezpečně ochránit data, či jiná aktiva před vyzrazením či jejich znehodnocením. Každá společnost stojí před úkolem jak nejlépe svá aktiva chránit před případným zneužitím, a tím i výrazným snížením jejich důvěryhodnosti, nebo v krajních případech ohrožení celého chodu společnosti. Jedním z mnoha přístupů jak řešit tuto problematiku je využití velice efektivní metody penetračního testování. Právě touto problematikou se práce zabývá.

První kapitola je věnována problematice bezpečnosti informačních systémů, kde je popsán základ tvorby bezpečnostních přístupů a opatření, dále je představena problematika zranitelnosti, hrozeb a možných útoků na informační systémy. Další kapitola je pak přímo zaměřena na teoretické pojetí problematiky penetračního testování. Jsou zde uvedeny přístupy tvorby penetračních testů, metodologie a seznámení se základními nástroji. Poslední kapitola je praktickou částí této práce a představuje modelový příklad sítě.

Praktická část se zabývá penetračním testováním síťových prvků od společnosti Cisco, jedná se o switche typu Cisco catalyst 2960 a routery Cisco řady 2800. Cílem vytvoření modelového příkladu je ověřit bezpečnost sítě a následně ohodnotit zjištěné bezpečnostní chyby. Síť byla nasimulována v prostředí Packet Tracer a určitá část byla realizována v síťové laboratoři. Síťové prvky jsou podrobeny specifickým auditům pro danou oblast. Prováděné testování odpovídá charakteru white-box testu a testování probíhá v určitých logicky po sobě navazujících fází dle dané metodologie penetračního testování. Hlavní oblasti jsou konfigurace zařízení, poskytované služby, šifrování a síla přístupových hesel. Výstup z auditů je následně vyhodnocen dle potencionálně hrozících nebezpečí.

1 Bezpečnost informačních systémů a jejich problematika

V této kapitole je kladen důraz na seznámení s principy bezpečnosti a tvorbou infrastruktury informačních systémů k dosažení požadovaného zabezpečení. Jsou zde představeny pojmy z oblasti bezpečnostní analýzy, bezpečnostní politiky, zranitelnosti, hrozeb a útoků na IS, včetně řešení jak se proti těmto událostem bránit, případně je zcela eliminovat.

Než bude dále pojednáno o této problematice, je nutné představit základní pojmy, které s tématem práce úzce souvisí a budou zde používány:

- **Hacker** – Obecný termín, který historicky byl používán k označení zkušeného experta ICT. Dnes je tento termín spíše používán k popisu jednotlivce, který využívá své znalosti k ilegálním činnostem, například proniknutí do cizího systému, krádež dat atd. (Vachon a Graziani, 2008)

- **Etický hacking –** Postup bezpečnostního experta v oblasti ICT, který využívá stejných technik a strategií jako opravdový hacker jen s jediným rozdílem, že nalezené bezpečnostní chyby nevyužívá ke zlým úmyslům, ale naopak tyto chyby ohlašuje pro následnou nápravu. Rozdíl by se dal také jednoduše vyjádřit následující větou: Hacking je útok, naproti tomu etický hacking je obrana. (Harper et al., 2008)

- **Zranitelnost –** Pojem popisující slabiny (chyba v programu, nedostatky v konfiguraci, selhání, fyzické poškození), které umožňují útočníkovi proniknout do systému.

Použitá terminologie:

- **Router** – směrovač, zařízení provádějící směrování.

- **Switch** – přepínač, zařízení sloužící k větvení sítí.

- **Hub** – rozbočovač, zařízení sloužící k větvení sítí (nahrazováno zařízením switch).

1.1 Bezpečnostní politika a analýza

Důležitým pojmem této kapitoly je pojem **bezpečnostní politika** a pro objasnění tohoto pojmu vyjděme z článku Bezpečnostní politika v časopise COMPUTERWORLD, kde Tomáš Přibyl pojednává o bezpečnostní politice následovně: „Bezpečnostní politika by měla být vypracována na základě bezpečnostní analýzy, tedy bezpečnostní politika představuje jakési přenesení získaných informací do praxe. Představuje zkrátka interní předpis, který vymezuje základní principy bezpečnosti informačního systému. Po schválení vedením slouží jako závazné nařízení pro zaměstnance.“ (Přibyl, 2005b)

Je zde kladen důraz na nastavení pravidel bezpečnostní politiky, její aplikaci a následně porovnání se skutečnou situací v dané instituci. Myslí se tím zejména řádné

dodržování těchto pravidel. Klíčovou roli pak hraje ověřování správnosti a funkčnosti těchto mechanismů.

Hlavní cíle bezpečnostní politiky jsou:

- definovat hlavní cíle při ochraně informací,
- stanovit způsob jak bezpečnost řešit,
- určit pravomoce a zodpovědnosti.

Dalším pojmem souvisejícím s bezpečnostní politikou je **bezpečnostní analýza**. „Analýza je procesem, který konkrétní situaci podrobuje důkladnému posuzování z hlediska stavu, vazeb, příčin nebo důsledků. Bezpečnostní analýza pak představuje proces, který tuto situaci rozebírá z hlediska informační bezpečnosti.“ (Přibyl, 2005a) Bezpečnostní analýzou se zabývá spousta subjektů jak národních, tak nadnárodních. V rámci spolupráce Mezinárodní standardizační organizace ISO a IEC vznikla celá řada norem, například:

ISO/IEC 27002, směrnice pro tvorbu bezpečnostních norem a účinné postupy řízení bezpečnosti, která definuje následující oblasti:

- analýzu rizik,
- bezpečnostní politiku,
- správu uchovávání informací,
- správu aktiv,
- lidský faktor,
- provozní podmínky a fyzickou bezpečnost,
- komunikaci a řízení provozu,
- řízení přístupu,
- pořízení, vývoj a údržbu informačního systému,
- postup v případě napadení,
- řízení kontinuity podnikaní,
- plnění.

Bezpečnostní analýza zahrnuje primárně tyto aspekty:

- stanovení bezpečnostních cílů organizace,
- určení prostředků, dokumentů, které mají být chráněny,
- identifikace síťové infrastruktury (aktuální topologie včetně datových zdrojů) a kritických zdrojů, které je třeba chránit, jako je vývoj, finance a lidské zdroje.

„V souvislosti s bezpečnostní analýzou se setkáváme s pojmem **analýza rizik,** což je proces inventarizace aktiv a rizik a proces jejich ohodnocení. Jinými slovy: Analýza má za úkol stanovit aktiva instituce, jejich hodnotu i rizika, která jim hrozí, a navrhnout protiopatření. Cílem analýzy je nastavit potřebnou úroveň bezpečnosti, neboť v praxi musí existovat vztah mezi hodnotou aktiv a náklady vynaloženými na jejich ochranu.“ (Přibyl, 2005a)

Analýza rizik musí poskytnout odpovědi na tři základní otázky:

- Co nastane, když nebudou informace chráněny?
- Možnosti porušení bezpečnosti informací?
- S jakou pravděpodobností se to může stát?

1.1.1 Postup tvorby analýzy rizik

Již na začátku je třeba říci, jak uvádí Přibyl (2005a), že není možné vytvořit obecný model (šablonu) pro analýzu rizik. Toto plyne z odlišného charakteru a chodu věcí v každé společnosti. Analýza rizik by měla být přizpůsobena potřebám instituce (ne tedy potřebám interního nebo externího subjektu, který analýzu provádí). Proto je ve vlastní analýze rizik nesmírně důležitá přípravná fáze. Podle rozsahu analyzovaného systému, podle interních možností, podle potřeby bezpečnosti a podle dalších faktorů lze vybírat jeden ze čtyř přístupů analýzy rizik, které definuje norma ČSN 13335. Ještě před tím, než přistoupíme k výběru nejvhodnější metody, je třeba provést tzv. hrubou analýzu rizik. Ta je někdy též označována jako orientační, neboť slouží pouze k získání základního přehledu a ke zmapování terénu. Přibyl též pojednává o několika přístupech k tvorbě analýzy rizik. Pracovně je označme následovně:

1. **Základní přístup**: Jde o velmi jednoduchou metodu, v jejímž rámci se nedělá nic jiného, než že se implementují již vytvořené, prověřené a uznávané (v normách, standardech apod.) postupy. Využití této metody je vhodné ve standardních systémech, kde se nepředpokládají nějaké zvláštní odchylky a výjimky.
   - Výhody: rychlost, nízké náklady, implementace ověřených prvků.
   - Nevýhody: zanedbaní specifik společnosti – nastavení špatné úrovně zabezpečení.

2. **Neformální přístup**: Metoda podobná v mnoha ohledech výše zmíněnému základnímu přístupu, ovšem s tím rozdílem, že nedochází k nasazení strukturovaných a přesně popsaných metod. Neformální přístup je celý založen na zkušenostech a znalostech osoby (osob), která (které) analýzu provádí. Neformální přístup se doporučuje ve velmi malých a prakticky unifikovaných systémech, kde se nedají předpokládat jakékoliv odchylky od normálu.
   - Výhody: vysoká rychlost, relativně nízké náklady.
   - Nevýhody: lidský faktor – subjektivní či nepodložená rozhodnutí.

3. **Podrobná analýza rizik**: Metoda, která staví na vytvoření zcela nového modelu. Podrobná analýza rizik představuje důkladnou analýzu stavu, vztahů, chování, toku dat atd. Z toho samozřejmě vyplývají doporučení, která jsou precizně podložená fakty a která jsou vytvořená dotyčnému systému takříkajíc „na míru“. Využití této metody je vhodné v institucích s velmi složitou strukturou informačního systému a/nebo s vysokou potřebou kvalitního zabezpečení (finanční instituce, velké firmy apod.).
   - Výhody: nejpodrobnější, nejbezpečnější.
   - Nevýhody: časová náročnost, vysoké náklady na realizaci.

4. **Kombinovaný přístup**. Přístup využívající několika z výše uvedených přístupů. Kombinovaný přístup je možné provést v přesně strukturovaných systémech. Je vhodný například pro některé instituce s centrálou a množstvím typizovaných poboček. Pro ústředí se použije podrobná analýza rizik, zatímco na jednotlivé pobočky lze nasadit přístup základní, nebo dokonce jen neformální.
   - Výhody: optimalizace nákladů – časové a lidské zdroje.
   - Nevýhody: určení přístupů jednotlivým prvkům a následná provázanost.

1.2 Zranitelnost

Dalším pojmem souvisejícím s problematikou bezpečnosti je zranitelnost. V anglickém jazyce též označováno termínem „vulnerability“. Pojem zranitelnost má mnoho různých pojetí. Pro účel práce se zaměřme na technické pojetí a zejména aplikaci této problematiky v počítačových sítích. Vachon a Graziani (2008) rozdělují zranitelnost do následujících sekcí:

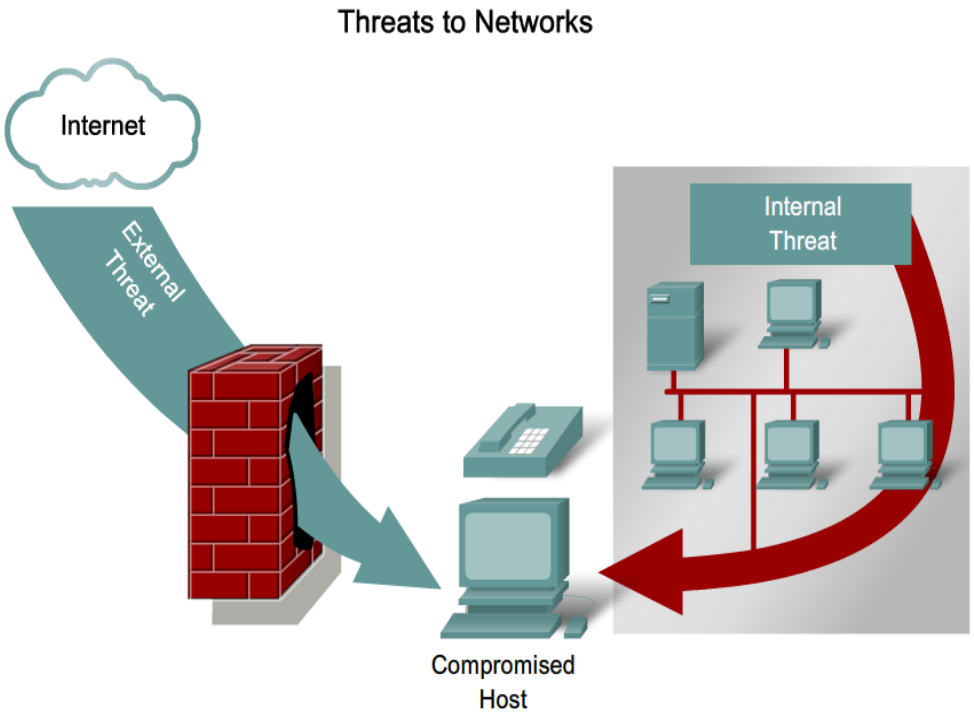
- **Technologické vlastnosti a chyby**
  - Bezpečnostní nedostatky komunikačních protokolů (například rodina TCP/IP protokolů).
  - Bezpečnostní chyby v OS (Linux, Windows, Unix, OS X).
  - Bezpečnostní chyby síťových zařízení (router, switch, hub, firewall).

- **Konfigurační slabiny**
  - Nezabezpečené uživatelské účty, nebo zabezpečené nedostatečně – krátká hesla, hesla přenášená a uložená v čitelné podobě, v tzv. prostém textu.
  - Výchozí nastavení zařízení, případná neaktuálnost.
  - Nenastaveno omezení směrování dat v síti – eliminace šíření směrovacích informací na určitých rozhraních, ACL.
  - Síťové služby – nezavedeny bezpečnostní mechanismy, například ověření zdroje při přijetí zprávy.

- **Nedostatky v bezpečnostní politice**
    - Neexistence specifikace pro vytváření hesel (délka a zastoupení určitých znaků) – náchylnost k tzv. slovníkovým útokům.
    - Nesrovnalosti v přístupu – není určen jednotný přístup pro práci se zařízeními.
    - Nezavedena dokumentace IS – dodržování konvencí pro názvy, adresace atd.
    - Není stanoveno oprávnění k instalaci, či manipulaci HW a SW vybavením – např. zaměstnanec si připojí vlastní wi-fi router, a tím může za jistých předpokladů vytvořit místo zneužitelné k proniknutí do vnitřní sítě.
    - Neexistuje plán obnovy při selhaní.

1.3 Rozdělení hrozeb sítě

Možné hrozby sítě nám ukazuje obr. 1, kde jsou hrozby členěny do dvou skupin. První skupinou jsou hrozby (threats) dle jejich zdroje (původu). Rozdělují se na **vnější** (external) a **vnitřní** (internal). Další zdroj hrozeb plyne již přímo z fyzického umístění a prostředí, kde se zařízení nachází. (Barker, Morris, 2012)



Obrázek 1: Hrozby sítě (Barker, Morris, 2012)

Barker a Morris (2012) dělí hrozby následovně:

Vnější hrozby – představují útoky na IS z vnějšího prostředí (síť internet), které mají většinou za cíl získat neoprávněný přístup do sítě, nebo se případně snaží způsobit poškození. Příkladem může být generování velkého množství požadavků, které zaplaví síť, a tím způsobí znepřístupnění poskytovaných služeb (DoS útoky – vysvětleny dále).

Vnitřní hrozby – jde o útoky, které přicházejí ze samotné napadené sítě (validní přístupové údaje). Původ těchto útoků bývá většinou od samotných zaměstnanců, kde důvodem může být průmyslová špionáž nebo pomsta.

Fyzické hrozby – jde o poškození HW (aktivní a pasivní prvky sítě) v důsledku několika faktorů, patří sem například podmínky prostředí, kdy je třeba regulovat především teplotu a vlhkost. Velkou doménou jsou také hrozby plynoucí z poškození elektrickým proudem, může jít o kolísání, napěťové špičky, rušení, případná celková ztráta el. energie. Poslední větší skupinou jsou fyzické hrozby plynoucí z údržby, zde je nutné zdůraznit neodbornou manipulaci se zařízením, neefektivně vedenou kabeláž (časté ohyby, nesprávně instalované koncovky). Posledním bodem je nutné zmínit, že je vhodné vést systém značení kabeláže. V závislosti na objektech hrozby existují různé prevence fyzických hrozeb.

- **Prevence hrozeb plynoucích z podmínek prostředí –** regulace teploty, řízení vlhkosti, proudění vzduchu atd.
- **Prevence hrozeb plynoucích z poškození elektrickým proudem –** UPS, elektrocentrály, redundantní napájecí zdroje.
- **Prevence hrozeb při manipulaci s kabeláží a zařízeními –** správně vedená kabeláž (eliminace ohýbání a namáhání kabelu), zřejmé značení kabelů, používání ochranných pomůcek proti elektrostatickému napětí (zemnící „patička“, kroužek).

1.4 Rozdělení útoků a obrana proti nim

Tato podkapitola přibližuje problematiku možných útoků, včetně obrany proti nim a dále popisuje skutečnosti, které mohou ohrozit informační systém v daných oblastech. Útoky mohou být různorodé, ať zaměřené ryze na síťové prostředky nebo na lidské zdroje. Oblast síťových útoků se dle Barkera a Morrise (2012) dělí na:

- **reconnaissance** (průzkum),
- **access** (přístup),
- **denial of service** (odmítnutí služby),
- **worms, viruses and trojan horses** (červy, viry a trojské koně).

Zvláštní oblastí útoků cílících na uživatele je tzv. sociální inženýrství. Jde o metodu, která nevyžaduje prakticky žádné technické znalosti útočníka k získání přístupu do IS. Do této kategorie patří například útok využívající podvodné elektronické zprávy – často žádající o zaslání citlivých dat (hesla, osobní údaje), tento typ útoku se nazývá phishing. Ochranu proti tomuto druhu útoku je možné zajistit školením uživatelů a filtrací

podezřelých zpráv. Případně je možné zajistit ochranu bezpečnostními aplikacemi, které chrání uživatele před podvodným obsahem, jedná se o tzv. anti-phishingovou ochranu.

Nyní bude pojednáno o jednotlivých typech útoků podrobněji, pro tento účel vycházejme z publikace od Barkera a Morrise (2012).

1.4.1 Reconnaissance

Jedná se o neoprávněné monitorování, mapování systému, síťových prvků a služeb. Průzkum se dělí na:

- **External reconnaissance** – prozkoumávání sítě, které je prováděno z vnějšku sítě, většinou prostřednictvím internetu. Postup je popsán v následujících krocích:
  - **Vyhledání dostupných informací** – v této fázi jde o získání základních informací o zkoumaném objektu, jako jsou používané technologie, využitý adresní prostor a další informace. Příkladem nástrojů využitelných k získání informací jsou databáze Whois[1], utilita nslookup[2] a další.
  - **Zjištění aktivity stanic** – k testování aktivity stanic („Kdo odpovídá“) se používá nástroj ping[3]. Pro urychlení testovaní daného adresního rozsahu, který byl zjištěn již v předchozím kroku, se používá metody „ping sweep“. Představuje systematické testování všech adres v daném rozsahu. Nástroje využívající této metody jsou fping, gping.
  - **Informace o běžících službách, otevřené porty** – po zjištění aktivních stanic, následuje získání informací o tom, které služby a porty jsou aktivní, dochází k tzv. skenování portů, kde můžeme využít nástroje jako např. Nmap, SuperScan. Díky těmto nástrojům je také možné zjistit verze běžících protokolů, včetně informací o operačních systémech.
  - **Vyhodnocení –** posledním krokem je již analýza nasbíraných informací a hledání bezpečnostních chyb.

  Prevence:

  - Zablokovaní nevyužívaných portů a deaktivace nevyužívaných služeb.
  - Zavedení pravidel pro filtraci (ACL a FW), např. zahazování ICMP paketů.

- **Internal reconnaissance** – prozkoumávání sítě, které je prováděno zevnitř sítě, většinou jde přímo o zaměstnance. K odposlechu se využívají analyzační nástroje, jako je třeba Wireshark, který umožňuje přečtení obsahů nesených v datových paketech, případně shromažďování a hledání možností zneužití. Příklad dat náchylných k odposlechu je jakýkoliv protokol, který přenáší data sítí v nešifrované podobě (prostý text), např. SNMP[4] v první verzi, telnet, CDP atd.

[1] Databáze, která slouží k evidenci údajů o majitelích internetových domén a adres IP.
[2] Utilita sloužící pro testování DNS serverů.
[3] Utilita, která testuje funkčnost spojení tzv. konektivitu.
[4] Protokol pro správu síťových zařízení, který poskytuje prostředky ke sběru informací o jejich stavu.

Prevence:

- Eliminace používání zařízení hub.
- Šifrovaní dat.
- Stanovení takových pravidel v bezpečnostní politice, aby bylo dbáno na šifrované přenosy v síti. Příkladem může být zákaz využívat protokol telnet, SNMP verze 1 atd.

1.4.2 Access

Access útok spočívá v získání přístupu k danému zařízení a případně i možnost proniknout dál do sítě. Přístupové útoky využívají známé chyby zabezpečení v autentizaci služeb, např. FTP[5], SMB[6], webové služby a dalších. Útočníci se zaměřují hlavně na přístup k webovým účtům, databázím a dalším zdrojům citlivých informací.

- **Útoky na získání hesla** – Principem těchto útoků je uhádnutí, či zjištění hesla a je několik způsobů jak toho dosáhnout. Prvním způsobem útoku na získání hesla je tzv. **brute-force** útok (hrubá síla), kde je možné využít slovník, který obsahuje soubor slov v daném jazyce, a tyto slova jsou postupně zkoušeny jako heslo. U tohoto útoku můžeme využít ještě další způsob, a to je algoritmické generování řetězců. Tento útok může být při vysoké síle hesla náročný na čas. Další možný způsob je využití **trojského koně**, který například zaznamenává veškeré vstupy z klávesnice a zasílá je útočníkovi. Poslední způsob útoku na získání hesla, který je zde zmíněn, je prosté odposlechnutí přenášeného hesla po síti v nešifrované nebo dešifrovatelné podobě za pomoci tzv. **paketového snifferu**.
  - Možná ochrana:
    - **Bezpečnostní politika** – stanovení pravidel pro vytvoření silného hesla, které budou uživatelé nuceni dodržovat.
    - **Určení maximálního počtu přihlášení.**
    - **Užívání šifrovacích mechanismů.**

- **Zneužití důvěrných zdrojů** (trust exploitation) – Tento útok je založen na napadení dostupného zařízení z vnějšího prostředí, většinou umístěného na vnější straně firewallu (DMZ[7]). Napadená stanice je pro vnitřní síť důvěryhodná, tudíž má oprávnění komunikovat s vnitřní sítí. Další útok, který je založen na zmíněném principu, se nazývá **přesměrování portu** (port redirection). Princip techniky port redirection spočívá v tom, že dokážeme z externí sítě komunikovat se stanicí na vnitřní síti, aniž by měla veřejnou adresu, právě díky specifickému portu, který je klíčem k přesměrování na požadovanou stanici. Na této metodě je zmíněný útok postaven. Napadené stanici se nainstaluje SW, který zaručí přesměrování komunikace z určitého veřejného portu na daný lokální komunikační port.

[5] Nešifrovaný protokol pro přenos souborů.
[6] Protokol, který slouží ke sdílenému přístupu k souborům, tiskárnám atd.

- Možná ochrana:
  - **Snížení úrovně „důvěry“ –** zavést omezení pro zařízení dostupná z vnější sítě. Platí i pro port redirection.
  - **Více ověřovacích mechanismů** – Možností je zavedení např. techniky VLAN a vyvarování se jedinému ověření přes adresu IP.
  - **Zavedení systému pro odhalení průniku** (IDS) – při útoku je možno ihned odhalit proniknutí a eliminovat následky průniku do IS.

- **Man-in-the-Middle** – V překladu do českého jazyka pojem znamená „muž uprostřed“, což vystihuje princip tohoto útoku. Útočník se dostane mezi dvě komunikující zařízení a odposlouchává, nebo dokonce modifikuje komunikaci mezi nimi. Lze je rozdělit do dvou větších kategorií: v první kategorii se jedná o útoky v lokálních sítích a v druhé o útoky v prostředí internetu (případně MAN nebo WAN sítích). Tento typ útoku souvisí s mnoha útoky, např. zjištění hesla, DoS.

  Příklady MITM útoků:

  ARP Cache Poisoning – technika, která využívá slabiny v ARP protokolu. Každý host na síti dynamicky aktualizuje svoji ARP Cache pomocí protokolu ARP, jde o rámce ARP-request a ARP-reply. Slabina spočívá v tom, že host je schopen zapsat do své ARP Cache změny bez předchozího vyslání příslušného ARP-request rámce. V této situaci odpovědi nazýváme gratuitous (bezdůvodné), protože si o ně příjemce neřekl. (Haller, 2006)
  - Možná ochrana:
    - **ARP inspection** – kontrola ARP-reply rámců.
    - **Port Security** – stanovení maximálního počtu adres MAC na rozhraní zařízení, omezení provozu, ošetření nepoužívaných portů atd.
    - **Statické přiřazení záznamu do ARP tabulky –** vhodné pouze pro malé sítě.

  Port Stealing – Útok je vykonáván za stejným účelem jako ARP Cache Poisoning. Útok však spočívá v „krádeži“ portů na switchi. Základním požadavkem je, aby útočník znal adresu MAC oběti, a následně musí zmást switch, resp. modifikovat záznamy v jeho CAM tabulce. Zmatení switche spočívá v posílání paketů s cílovou adresou MAC rovnou adrese MAC útočníka. Zdrojová adresa MAC bude nastavena na adresu MAC oběti. (Haller, 2006)
  - Možná ochrana:
    - Ochrana je totožná s výše uvedenou ochranou proti útoku ARP Cache Poisoning.

[7] Oblast informačního systému, která je z určitých důvodů oddělena od ostatních zařízení, příkladem může být webový server, poštovní server atd.

DHCP Spoofing – Útok využívá faktu, že na jedné síti může běžet více DHCP serverů. Další fakt, který tomuto útoku pomáhá, je, že regulérní servery nejsou „příliš“ rychlé. DHCP Spoofing je útok, kdy útočník zapojí do sítě svůj falešný DHCP server, který odpovídá na pakety DHCP-discovery stanicím a přiděluje jim podvržené adresy IP (výchozí brána, DNS server). Potom tedy bude veškerý provoz od klienta směrovaný ven ze sítě procházet přes útočníkův počítač. (Barker a Morris, 2012)

- Možná ochrana:
  - **Využití techniky DHCP Snooping** – určení věrohodných portů, které mohou posílat DHCP zprávy, z ostatních portů jsou tyto zprávy zahazovány.
  - **Port Security –** stanovení maximálního počtu adres MAC na rozhraní zařízení, omezení provozu, ošetření nepoužívaných portů atd.

Základní obrana proti MITM útokům:

- **Využití VPN tunelů** – veškerá komunikace je šifrovaná, útočník nevidí čitelný obsah dat.
- **Port Security –** stanovení maximálního počtu adres MAC na rozhraní zařízení, omezení provozu, ošetření nepoužívaných portů atd.

- **Buffer overflow** (přetečení vyrovnávací paměti) – Tento pojem představuje bezpečnostní chybu, kdy jde o naplnění bufferu (paměťové uložiště) větším množstvím dat, než pro který byl vytvořen. Důvodem zařazení této chyby do podkapitoly útoky je její možné zneužití k řízení daného programu vlastními instrukcemi, a tím případně obejít bezpečnostní mechanismy za účelem získání pravomocí, dat atd. Názorným příkladem můžou být programovací jazyky, které nehlídají integritu paměti (přesněji meze polí), jako je C/C++, kdy při přetečení dojde k přepsání dat v paměti. Nejlépe se této chyby využívá, pokud je buffer lokální v nějaké funkci. Pak se totiž jako každá lokální proměnná nachází na zásobníku a jeho přetečením můžeme přímo ovládat běh daného programu. Proti tomuto typu útoku však přímo **ochrana neexistuje**, můžeme se snažit pouze o minimalizaci chyb při vývoji daného SW vhodnými testovacími metodami, nicméně tato problematika je již nad rámec této práce.

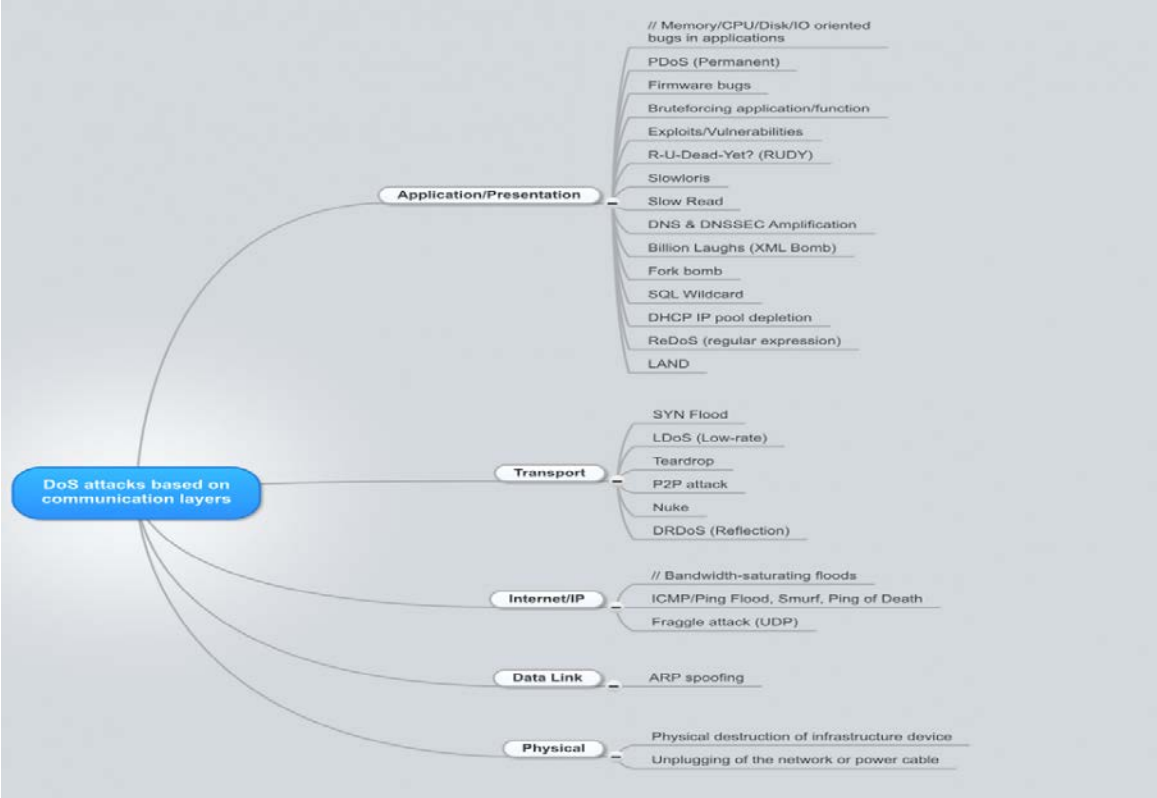
1.4.3 Denial of Service

O této problematice velmi podnětně pojednává Čmelík (2013), který pojímá Denial of Service (DoS) jako síťové útoky, které brání přístupu k službám. Tyto útoky blokují služby sítě zahlcováním spojení, zhroucením serverů nebo programů běžících na serverech, vyčerpáváním zdrojů na serveru, případně jinak brání legitimním klientům v přístupu ke službám sítě. DoS útoků však existuje nespočet forem, možností a stále další způsoby se objevují. V této sekci není cílem popsat všechny možnosti, jde pouze o základní seznámení a vytvoření si představy o dané problematice. Pro přehled je přidáno rozdělení DoS útoků dle vrstev TCP/IP modelu viz obr. 2.

DoS útoky mohou mít celou škálu podob, od útoku jednoho paketu (single packet atack), který způsobí zhroucení serveru, až po koordinované záplavy paketů od mnoha

stanic. Při útoku jednoho paketu je poslán do sítě zvláště přizpůsobený paket, který využívá známé zranitelnosti operačního systému nebo aplikace a zablokuje server nebo některé služby jím poskytované.

Při záplavovém útoku jsou zdroje na serveru nebo na síti narušeny nebo vyčerpány záplavou paketů. Při napadení jednoho místa může být záplava celkem snadno identifikována a izolována. Mnohem sofistikovanější přístup, zvaný Distributed DoS (DDoS) útok, je nástroj pro mnoho záplavových útoků. Při DDoS útoku používá útočník k zasažení cíle množství počítačů. (Čmelík, 2013)



Obrázek 2: Rozdělení DoS útoků dle komunikačních vrstev TCP/IP modelu (Čmelík, 2013)

Blíže k některým útokům:

Ping of Death – jedná se o chybu starších OS (Windows 98, 2000). Podstatou je více dat v paketu, než by tam mělo být, definované dle norem RFC. Následkem přijmutí neakceptované velikosti ICMP Echo paketu došlo ke zhroucení OS (přetečení vstupní vyrovnávací paměti). V dnešní době prakticky nevyužitelný.

- Možná ochrana:
  - **Update systému –** záplaty systému, případná inovace.
  - **Vlastní testovací mechanismus.**

- **SYN flood** (Záplava paketu Syn) – Zneužití trojcestného potvrzovacího mechanismu TCP. Kdy je zasláno více SYN požadavků (1000 a více) na cílový server. Server odpovídá SYN-ACK paket, ale hostitel nikdy nepotvrdí komunikaci posledním ACK, tudíž server čeká na potvrzení, kdy po určité době dojde k vyčerpání všech zdrojů.

- Možná ochrana:
  - **SYN cookies** – SYN záznam je ihned odstraněn, nedokončená spojení „nijak“ nevytěžují zdroje zařízení.
  - **Stanovení limitů** – omezení přenosového pásma.

- **Smurf útok** – K útoku je využit ICMP protokol, útočník generuje ICMP Echo Request pakety, kde v záhlaví paketu je změněna adresa zdroje na adresu oběti a cílovou adresou je všesměrová adresa podsítě, v které se nachází cíl útoku. Všechny stanice v dané podsíti tedy přijmou zmíněný paket a odpovídají ICMP Echo Reply paketem na adresu oběti, tj. adresa zdroje v ICMP Request paketu.
  - Možná ochrana:
    - **ACL** – přidání pravidla zamezující posílání broadcastu (vstup do sítě).
    - **Zakázání všesměrových zpráv na určitém rozhraní** – u zařízení Cisco řešeno příkazem: no ip directed-broadcast.
    - **Omezení množství ICMP paketů.**

Základní ochrana proti DoS útokům:

- Používání anti-spoof a anti-dos filtrů.
- Limity pro rychlost a přenos dat, uměle přidané prodlevy mezi požadavky.

1.4.4 Worms, Viruses and Trojan Horses

Primárním cílem těchto útoků jsou koncové stanice sítě. Jde především o škodlivý software k infiltraci sítě, omezení služeb, či částečné ovládnutí stanic útočníkem.

- **Virus** (virus) – škodlivý software, který se váže na jiný program nebo soubor k provedení konkrétní nežádoucí funkce na počítači. Virus je šířen jak přes externí paměťová média (flash disk, CD, paměťová karta), tak i velice využívanou variantou je kanál elektronické komunikace, jako je např. email. Viry mohou poškodit software, hardware i data.

- **Worm** (červ) – zvláštní typ počítačového viru. Šíří se v podobě infikovaných souborů nebo paketů počítačové sítě. Díky automatickému šíření vzniká tzv. dominový efekt, který může mít za následek zahlcení počítačové sítě. Červi na rozdíl od virů nepotřebují k šíření interakci uživatele – šíří se sami.

- **Trojan Horse** (trojský kůň) – Stejně jako byl mytologický Trojský kůň zdánlivým darem, z něhož později vyskočili řečtí vojáci, kteří se zmocnili Tróji, jsou dnešní trojské koně počítačové programy, které vypadají užitečně, nicméně mají navíc škodlivou „funkci“ (malware).

2 Penetrační testování

Penetrační testování patří mezi techniky etického hackingu. Jde v podstatě o napodobení útoku hackera, což je nejlepší metoda jak ověřit bezpečnost a jak postupovat přesně jako útočník. Proto je tato metoda hojně využívána právě k ověření úrovně zabezpečení ve společnosti, ale i dalších problematik bezpečnosti. Penetrační testy mohou sloužit také pro stanovení priorit v rámci řešení problémů v IT infrastruktuře. Dále také mohou určit efektivnost ochrany sítě – určení zařízení, která nevyhovují bezpečnostním požadavkům atp. Výsledky testů mohou složit jako záruka důvěryhodnosti a stability podniku pro potenciální investory, obchodní partnery, akvizice, certifikáty atd. Selecký (2012) se vyjadřuje k této problematice následovně: Nicméně jako většina má to své „ale“, a to spočívá v prostém faktu, že není možné otestovat všechny prostředky, a tudíž není garantováno odhalení všech zranitelných míst. Možnosti jsou totiž značně limitovány přidělenými prostředky (finance, čas, personál).

2.1 Metodologie testování

Teoretická část této kapitoly, kde je definováno rozdělení, přístupy a zaměření, vychází z již navrhnutých a ověřených metod. Publikace, které lze považovat za relevantní k této problematice, jsou:

- Penetrační testy a exploitace (Matúš Selecký, 2012).
- A penetration Testing Model (Federal Office for Information Security, 2004).
- Penetration Testing and Cisco Network Defense (Cisco Press, 2005).

Nicméně v této části bude převážně čerpáno z publikace *Penetrační testy a exploitace*. Publikace byla vybrána z důvodu aktuálnosti a také díky tomu, že nejlépe odpovídá charakteru a rozsahu této práce.

Nyní přistupme k samotné problematice. Selecký (2012) dělí metodiku do čtyř fází:

A. Fáze 1: **Cíl a rozsah penetračního testu**

Úvodem je třeba říci, že je obtížné splnit očekávání klienta bez důkladné přípravy, jako je dohoda o stanovení cílů a objektech testování. Tudíž tato fáze slouží ke stanovení konkrétních cílů a časového plánu na základě obecných zadání a cílů. Cíle projektu navozují otázky, které mají být během testování zodpovězeny. Hlavní je vymezit cíle prioritní. Také se zde řeší zabezpečení citlivých dat – zamezení porušení právních norem společnosti, případně seznámení se všemi riziky, které mohou nastat, atd. Doporučuje se veškeré detaily ohledně těchto věcí řešit písemnou smlouvou.

B. Fáze 2: **Sběr dat**

Na základě výstupu z fáze 1 je potřeba zjistit o konkrétních systémech co nejvíce informací. Způsoby, jakými získáváme data, jsou určeny dle typu zvoleného testu (black-box, white-box, grey-box). Zmiňované typy testů budou popsány dále, kdy samozřejmě

každý typ obnáší určité výhody a nevýhody. Tato fáze představuje vytvoření obrazu o tom, jak a kde hledat informace o testovaném systému. Tyto informace jsou následně využity pro vstup do další fáze.

C. Fáze 3: **Skenování a exploitace**

Třetí fáze obnáší proces skenování testovaného systému, testovaní zabezpečení a možné pokusy o prolomení bezpečnostních mechanismů. Ze získaných informací z fáze 2 jde tedy o informace instalovaných systémů, včetně nechráněných prvků sítě s cílem najít bezpečnostní chyby, tzv. exploity[8]. Příkladem hledaní bezpečnostních děr v procesu skenování je např. umístění stanice za firewallem, které musí být důkladně testováno, jde třeba o kompletní skenování portů, což v případě ručního testování může trvat dlouho (řekněme několik hodin či dnů v závislosti na počtu testovaných stanic), obvykle se to provádí automaticky – to vše záleží na nastavení. Je třeba zmínit, že potřebný čas je třeba vzít v úvahu již při první fázi.

D. Fáze 4: **Report**

Tato fáze již vychází ze všech poznatků celého procesu penetračního testování a dělá souhrnné závěry. Penetrační testy pozbývají smyslu, pokud neposkytnou nějaký „hmatatelný“ výsledek, který bude mít smysl a přínos pro zabezpečení systému zákazníka. Výstupní zpráva z testování by měla popisovat míru rizika v daném odvětví, případně také doporučení, jak by se mohla minimalizovat, či zcela eliminovat. Obecně se report skládá z následujících částí:

- výstupní zpráva pro vedení – obecné pojetí, uvedení míry rizik,
- rozsah projektu (zaměření),
- analýza výsledků,
- podrobné shrnutí – obsahuje kompletní informace, včetně technických poznatků (používané protokoly, detailní informace o pracovních stanicích atd.).

2.2 Rozdělení penetračních testů

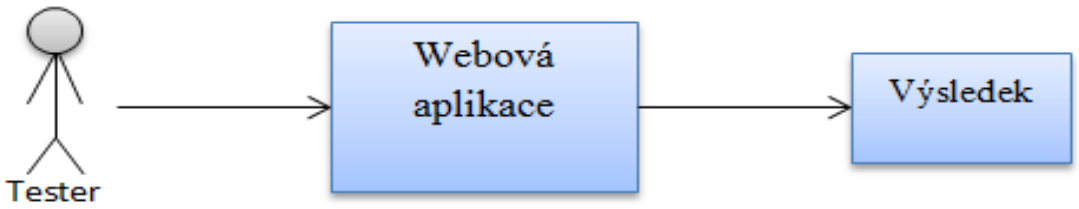
V oblasti informačních technologií lze testy rozdělit do několika základních kategorií, např. podle úrovně znalostí o testovaném systému a další. V teorii se setkáme s různými koncepcemi rozdělení, ale pro účel této práce se zaměřme na základní rozdělení, které vychází z publikace Seleckého (2012).

[8] Programy, či postupy, které využívají bezpečnostní chyby.

A. Dělení podle úrovně znalostí o testovaném sytému

Black-box testy

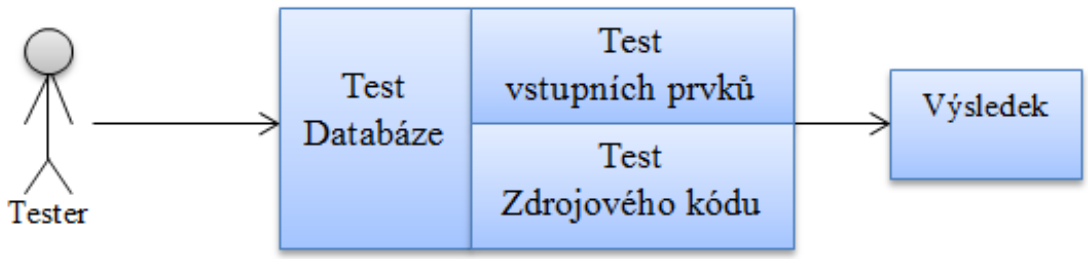
Tento typ testu je nejpoužívanějším, a to právě díky svému pojetí, které je nejčastějším útokem na daný systém. Obr. 3 nám ukazuje pohled testera na daný testovaný systém – vidí pouze aplikaci jako „černou skříňku“, která očekává vstup, a na základě toho generuje výstup. Black-box testy simulují vnější přístup útočníka, který má vstupní informace získané pouze z veřejně dostupných zdrojů, případně vlastních dotazů.



Obrázek 3: Black-box test z pohledu testera

White-box testy

Na rozdíl od předchozího typu testů white-box testy počítají s plnou vstupní znalostí testovaného systému. Pro testování aplikace tester zná její architekturu a zdrojové kódy. V případě testování počítačové sítě zná architekturu, přístupové údaje, počet zařízení atd. Na obr. 4 je znázorněn pohled testera, jak je vidět, tak oproti předchozímu přístupu je zde možnost důkladného, komplexnějšího testování. S tím také souvisí větší časová náročnost, požadavky na testera a z toho plynoucí větší celkové náklady.



Obrázek 4: White-box test z pohledu testera

Grey-box testy

Posledním způsobem je kombinace obou předcházejících typů testů, kde se snaží maximálně využít jejich výhody a přínosy. Tester zná v případě testované aplikace (systému) vnitřní logiku, ale testy provádí z hlediska uživatele. Grey-box testy mohou také

zahrnovat metody reverzního inženýrství pro určení prahových hodnot vstupních dat nebo chybových hlášení.

B. Dělení podle způsobu provádění testování

Manuální testy

Testy vytvořené testerem nevyužívají žádné nástroje, které by testovaly něco dle svých vlastních testovacích procedur.

- **Výhody:**
  - Procedury a testy přizpůsobeny specifickým požadavkům – řešení na míru.
  - Tester zná přesnou implementaci svého testu – zřejmá interpretace výstupu.
- **Nevýhody:**
  - Časová a znalostní náročnost (nutná znalost různých programovacích jazyků a systémů).

Automatizované testy

Testy jsou vykonávány pomocí nástrojů, které již mají napsané své testovací procedury. Tester již pouze ladí parametry testování a analyzuje výstup.

- **Výhody:**
  - Rychlost provádění, menší časové i znalostní nároky na testera.
  - Testy ověřeny profesionály – určitá záruka spolehlivosti testu.
- **Nevýhody:**
  - Komplexní výstup programu (složité interpretovat všechny stavové informace).
  - Neflexibilita testování – zaměření programu na daná místa zranitelnosti.

Semiautomatické testy

Testy, které využívají kombinaci automatických a manuálních testů. Jsou kompromisem mezi oběma formami s cílem o maximální využití výhod obou forem.

Kromě typů testů hovoříme o **metodice** penetračního testování. Existuje několik standardizovaných metodologií, které zaručují **systematický přístup** k testování. Zde jsou uvedené některé z nich (BackTrack 4: Security with Penetration Testing Methodology, 2011):

- Open Source Security Testing Methodology Manual (OSSTMM),
- Open Web Application Security Project (OWASP),
- Web Application Security Consortium Threat Classification (WASC-TC),
- Information Systems Security Assessment Framework (ISSAF).

2.3 Nástroje zaměřené na penetrační testování

V této podkapitole budou představeny některé nástroje, které lze pro penetrační testování využít. Nejvíce prostoru však bude věnováno nástrojům, které budou využity v modelovém příkladu této práce. Půjde jak o sofistikované distribuce, tak pouze o utility se specifickou funkcí.

Distribucí v této oblasti existuje mnoho, většinou jsou založené na jádru Linuxu. Jednou ze známých linuxových distribucí je **BackTrack**, která obsahuje nástroje pro bezpečnostní audit a penetrační testování. Tato distribuce je založena na známé distribuci Ubuntu s grafickým prostředím Gnome Classic. Poslední verzí je BackTrack 5 R3 a další její pokračovaní je již v nové distribuci nazvané **Kali Linux**, která je postavena na distribuci Debianu, avšak pro tuto práci je volena poslední verze distribuce BackTrack. Vývojem této distribuce se zabývá společnost Offensive Security. V distribuci najdeme stovky programů na různé oblasti penetračního testování, nicméně zde bude představeno jen několik z nich. K distribuci bude ještě odkazováno z důvodu jejího využití pro testování modelového příkladu sítě v praktické části. Dalšími známějšími distribucemi jsou:

- Fedora Security Spin,
- KATANA,
- Pentoo,
- BlackBuntu,
- Matriux,
- OWASP Web Testing Environment (WTE),
- Live Hacking CD,
- Samurai Web testing Framework,
- The Open Web Application Security Project (OWASP),
- Organizational System Wireless Auditor Asistent (OSWA).

Nástroje pro penetrační testování je možno rozdělit do následujících kategorií:

A. Nástroje pro sběr dat

Nástroje pro sběr dat jsou spíše informační zdroje, kde je možno zjistit rozsah adres IP, DNS servery a jména kontaktních osob. Jde hlavně o procházení volně dostupných zdrojů, jako jsou webové stránky, výroční zprávy a další, ze kterých je možné vyčíst věci jako používané softwarové technologie a další užitečné informace. Nástroje usnadňující zjištění zmíněných údajů jsou:

- Whois,
- archiv internetu,
- nslookup ,
- ping, tracert/traceroute – zjištění aktivních stanic, počet směrovačů k danému cíli,

- Nmap – komplexní nástroj, možné využití jak pro zjištění aktivních zařízení, tak i otevřených komunikačních portů atd.

B. Nástroje pro skenování a exploitace

V této části budou představeny nástroje, které lze využít při hledání a testování zranitelných míst v síti a síťových zařízení. Jak již bylo zmíněno, nejvíce prostoru je věnováno nástrojům, které následně budou využity v praktické části této práce.

Nipper

Pro tuto fázi testování byl vybrán nástroj Nipper, který je schopný provádět bezpečnostní audit převážně Cisco zařízení. Kompletní přehled podporovaných zařízení je možné najít v tabulce 1. Aplikaci není třeba již stahovat, protože je již obsažena v použité distribuci Backtrack 5 R3.

Parametr	Název zařízení
--ios-switch	Cisco IOS-based Switch
--ios-router	Cisco IOS-based Router (výchozí)
--ios-catalyst	Cisco IOS-based Catalyst
--pix	Cisco PIX-based Firewall
--asa	Cisco ASA-based Firewall
--fwsm	Cisco FWSM-based Router
--catos	Cisco CatOS-based Catalyst
--nmp	Cisco NMP-based Catalyst
--css	Cisco Content Services Switch
--screenos	Juniper NetScreen Firewall
--passport	Nortel Passport Device
--sonicos	SonicWall SonicOS Firewall
--fw1	CheckPoint Firewall-1 Firewall

Tabulka 1: Podporovaná zařízení utilitou Nipper

Provedení testu:

1. Získání konfigurace zařízení, v ukázkovém příkladu půjde o router společnosti Cisco, kde pro výpis konfigurace slouží následující příkaz:

```
Router# show runnning-config
```

2. Získanou konfiguraci překopírovat do textového souboru, následně spustit utilitu Nipper a provést příkaz:

```
nipper --input=router_konfigurace.txt --output=report.html
```

Výstupem programu je report, který je rozdělen do čtyř částí (Selecký, 2012):

- **Informace o reportu** – najdeme zde legendu, základní informace o zařízení, obsah reportu a datum provedení testu.
- **Bezpečnostní audit** – základní informace o testované oblasti, včetně předpokládaného dopadu plynoucího z chybného nastavení, dále snadnost využití zmíněné chyby a doporučení.
- **Konfigurace zařízení** – detailní výpis konfigurace testovaného zařízení.
- **Přílohy** – seznam zkratek, závažnost jednotlivých chyb a porty jednotlivých služeb.

Dsniff

Jde o balíček nástrojů pro komplexní síťový audit a penetrační testování. Obsahuje množství nástrojů jak pro pasivní, tak pro aktivní odposlech počítačové sítě. Jde například o nástroje:

- arpspoof – slouží k přesměrování provozu mezi dvěma stanicemi na přepínané síti,
- webmitm – používá se k MITM útoku na HTTPS spojení (získané například výše uvedeným arpspoof),
- sshmitm – používá se k MITM útoku na SSH (pouze pro protokol verze 1).

Ettercap

V současnosti sniffer, který implementuje všechny popsané MITM útoky a množství užitečných zásuvných modulů. Existuje varianta v grafickém rozhraní, která v reálném čase zobrazuje všechna síťová spojení, podrobné statistiky a aktivní klienty v síti.

Další časté nástroje, které patří do této kategorie, pak jsou:

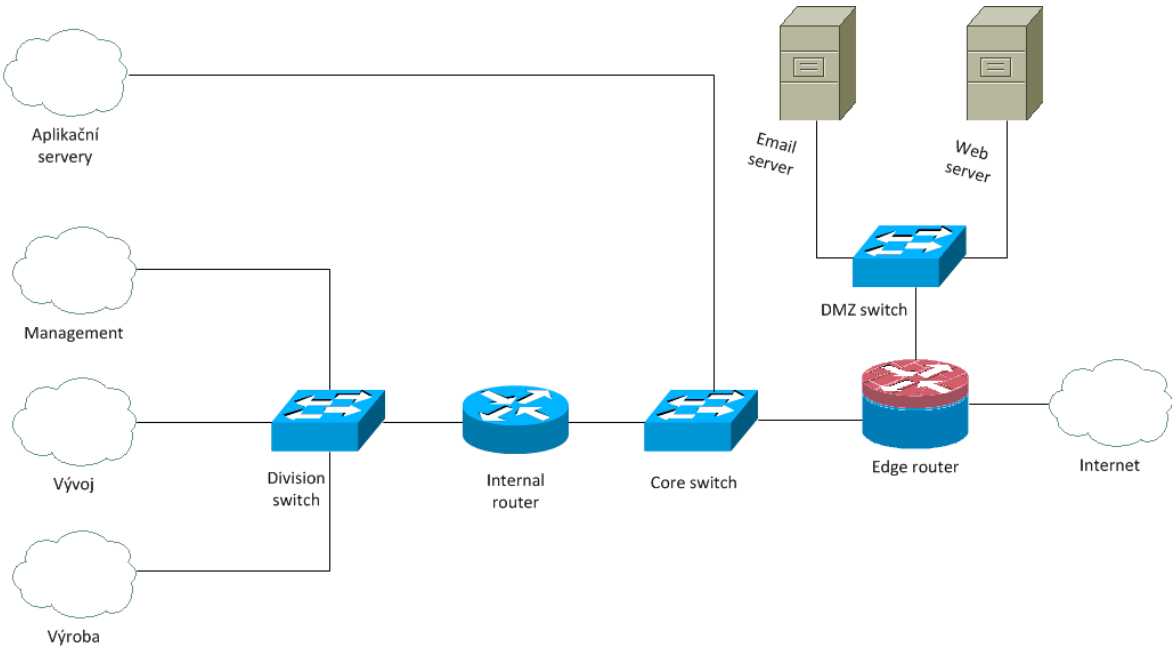
- Pytbull
- OpenVAS
- Metasploit Framework
- Nmap

3 Aplikace penetračního testování k ověření bezpečnosti počítačové sítě

Tato praktická část se zabývá ověřením bezpečnosti počítačové sítě v praxi za použití penetračního testování. K tomuto účelu je navržena laboratorní topologie, která svým rozsahem odpovídá středně velké společnosti okolo 50 zaměstnanců. Síť je navržena pro potřeby společnosti zaměřující se na vytváření webových aplikací, a tedy budou i vhodně pojmenována daná oddělení, dle charakteru společnosti. Hlavními prvky topologie, které z pohledu zabezpečení vyžadují největší pozornost, jsou: hraniční router a DMZ. Aktivní prvky sítě jsou od firmy Cisco, jde o model routeru 2811 a model switche 2960. Penetrační testování bude prováděno převážně ručně, nicméně pro audit Cisco zařízení bude použit nástroj Nipper. Metoda ručního testování byla zvolena z důvodu cílení na problematiku zranitelnosti aktivních síťových zařízení (router, switch) a jejich konfiguračních slabin. Cílem je ověřit bezpečnost a odhalit bezpečnostní rizika na simulované topologie sítě a následně poskytnout možné návrhy pro praxi.

3.1 Představení topologie

Obr. 5 ukazuje jádro počítačové sítě a vazby mezi zařízeními.



Obrázek 5: Topologie počítačové sítě

Síť je pro účel analýzy rozdělena do tzv. bezpečnostních pásem (bezpečnostní riziko), kdy první pásmo (červené – nejrizikovější) je představováno zařízením Edge router směrem k vnější síti. Druhé pásmo (žluté – méně rizikové) je představováno DMZ a posledním pásmem je pak (zelená zóna – nejméně riziková) vnitřní část sítě. Síť využívá

ke směrování protokol RIP [9] verze 2. Dále „oblak“ aplikačních serverů představuje množinu serverů s různými službami. Můžeme zde najít FTP, DHCP[10], databázový server a další. Nicméně pro tuto aplikaci bude důležitý pouze DHCP server, který poskytuje adresy oddělením managementu, vývoje a výroby. Adresní rozsah pro páteřní síť včetně aplikačních serverů je představován adresou 192.168.99.0/27.

3.1.1 Adresace topologie

Síť využívá mechanismu VLSM[11], což je efektivní z hlediska šetření adresami. Adresní rozsahy podsítí mají však dostatečné rezervy (volné adresy) pro případ rozšíření. Pro účel praktické části je použita pouze jedna podsíť, nicméně další rozšíření, či dělení je možné, ale v souladu s touto prací to není podstatné. Příkladem může být, že bychom chtěli rozdělit oddělení výroby na grafiky, kodéry atd.

- Adresace zařízení

Název zařízení	Rozhraní	Adresa IP	Maska podsítě
ISP	S0/0/0	209.165.200.226	255.255.255.252
Edge router	S0/0/0	209.165.200.225	255.255.255.252
Edge router	Fa0/0	192.168.99.1	255.255.255.224
Edge router	Fa0/1	10.1.1.1	255.255.255.240
Internal router	Fa0/0	192.168.99.2	255.255.255.224
Internal router	Fa0/1	viz tabulka subrozhraní	

Tabulka 2: Adresace rozhraní v páteřní síti

Rozhraní	Přiřazení	Adresa IP	Maska podsítě
Fa0/1.10	VLAN 10	192.168.10.1	255.255.255.240
Fa0/1.20	VLAN 20	192.168.20.1	255.255.255.224
Fa0/1.30	VLAN 30	192.168.30.1	255.255.255.224

Tabulka 3: Přidělené adresy subrozhraní

- Podsíť DMZ
  - 10.1.1.0/27
- Podsíť Management
  - VLAN 10 – 192.168.10.0/28
- Podsíť Vývoj
  - VLAN 20 – 192.168.20.0/27
- Podsíť Výroba
  - VLAN 30 – 192.168.30.0/27

[9] Dynamický směrovací protokol určený spíše pro malé a střední sítě.
[10] Protokol, který automaticky distribuuje adresy IP a konfigurace klientským stanicím (výchozí brána, DNS servery).
[11] Technika, která povoluje proměnnou délku síťové masky, tedy odstraňuje závislost na třídě adresy IP.

3.2 Fáze testování

V souladu se současnou teorií penetračního testování a charakterem této práce byly použity testovací fáze, které navrhuje Selecký (viz podkapitola 2.1).

3.2.1 Cíl a rozsah penetračního testování

Penetrační testování bude zaměřeno na testování všech připojených aktivních prvků sítě (router, switch), včetně jejich poskytovaných služeb. Jedná se o zabezpečení přístupu (síla hesla a práva), audit běžících služeb a jejich bezpečnostních děr. Laboratorní síť je testována jako celek, což představuje vnitřní síť, DMZ a hraniční router (Edge router). Prioritou v této síti bude zabezpečit hraniční router, který je jediným potencionálním rizikem pro vnější napadení sítě, zbytek sítě je schován – zaručeno technologií NAT. Dále je zaměřeno na demilitarizovanou zónu, která představuje lákavý cíl pro útok. Testy budou spíše white-box charakteru z důvodu důkladného zaměření na konfiguraci zařízení a běžících služeb, kde je tento přístup přínosný.

3.2.2 Mapování a sběr dat

Jak již bylo zmíněno, půjde převážně o penetrační testy typu white-box, tudíž většina informací je známá, tj. adresní rozsahy, jména zařízení, běžící služby a autentizační údaje. Z toho plyne, že v tomto případě bude vše známé, čerpá se zde tedy z dokumentace topologie (viz výše). Pro další informace je možné přistoupit přímo k zařízením a nahlédnout do konfiguračních souborů.

3.2.3 Skenování a exploitace

Z předchozí fáze již známe potřebné údaje k nalezení zranitelných míst. Nyní přikročíme k analýze bezpečnosti zařízení a jejich možných zneužití. Prvním analyzovaným zařízením je hraniční router (Edge router). Byl analyzován nástrojem Nipper a také testerem. Výstup z nástroje Nipper bude popsán až v poslední fázi penetračního testování. Nyní se budeme zaměřovat na testování prováděné testerem.

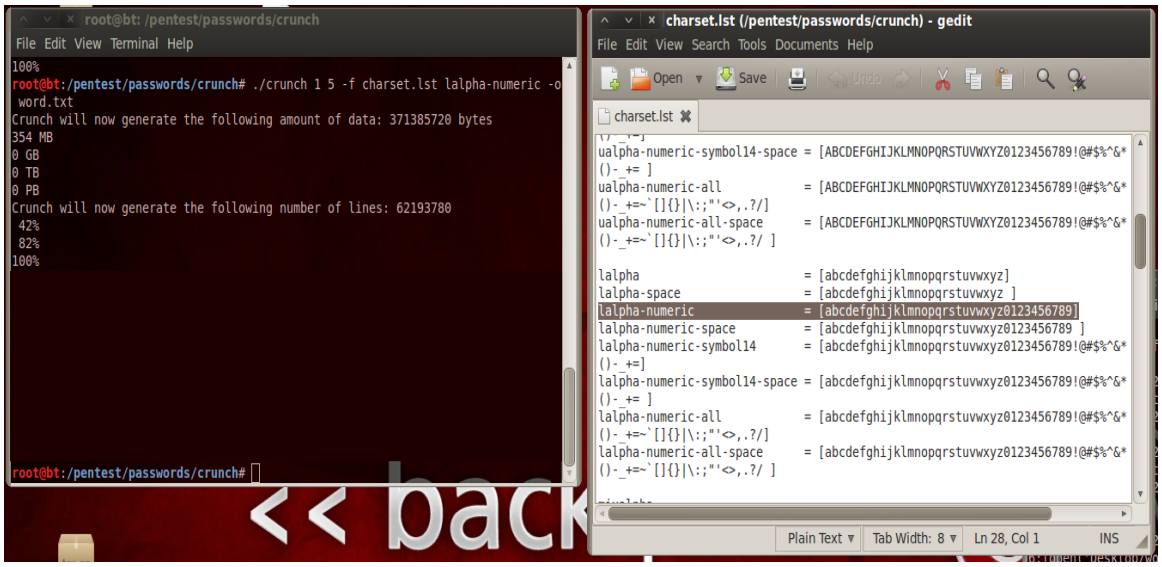
Na základě provedených testů, byly vytvořeny okruhy testování dle specifické oblasti a tyto oblasti jsou následující: síla hesla a šifrování, datový provoz a poskytované služby.

A. Testované zařízení: **Edge router**

- **Síla hesla, šifrování** – V této části půjde o zjištění síly hesel, proběhne zde tzv. audit bezpečnosti hesel. Z konfigurace zařízení bylo zjištěno, že je zde přítomno heslo k přechodu z user módu do privileged. Heslo je zašifrováno šifrovacím mechanismem MD5, který není dešifrovatelný, tedy z hash řetězce nezískáme původní podobu, tj. jak ho zadal uživatel. Nicméně je zde možnost uhádnutí hesla, půjde tedy o brute-force útok. Heslo má tuto podobu: „1mERr$pHFJEr11cgXfU.BnAHrP2.“. Ze zápisu je možné vyčíst typ řetězce hash, tj. číslo 1, které značí MD5, dále salt (sůl) „mERr“ a poslední už je kompletní hash , který se skládá ze salt a hesla. K vytvoření slovníku byl využit program

crunch, kde byly vygenerovány řetězce v rozsahu 1 až 5 znaků v kombinaci malých písmen a čísel, viz obr. 6. Základní popis parametrů zápisu vystihuje následující řádek:

```
crunch <min-délka> <max-délka> [znaky nebo  -f  /cesta/charset.lst
označení znakové sady] [-o slovnik.txt]
```



Obrázek 6: Tvorba slovníku dle parametrů

Dále pro generování specifického řetězce hash byl použit nástroj OpenSSL. Obecný zápis příkazu, včetně vysvětlivek:

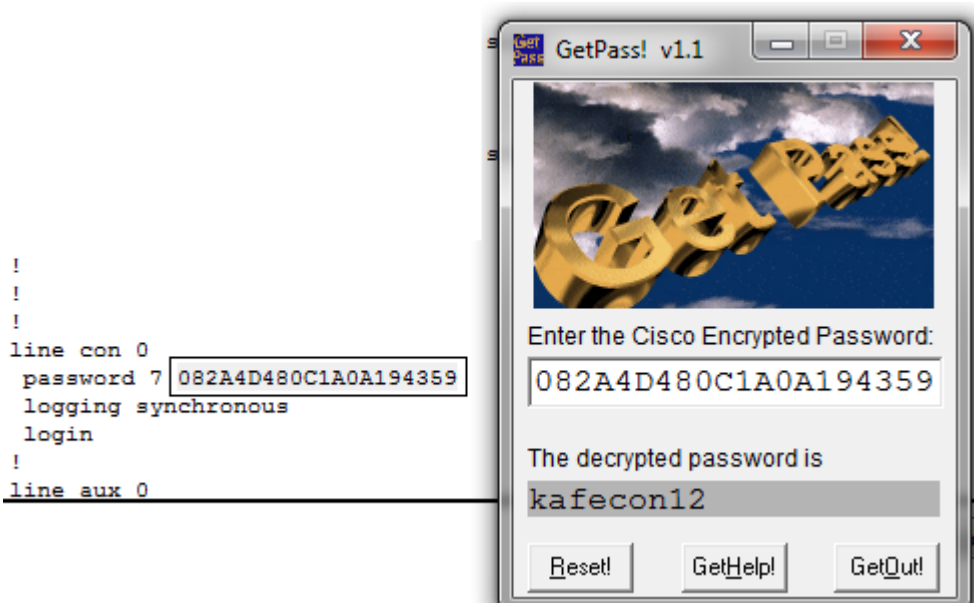
```
openssl passwd [-1] [-salt řetězec] [-table] [-in soubor]
//vysvětlivky:

[-1] – Použití MD5 šifrovacího mechanismu.
[-salt řetězec] – Přidání specifického salt.
[-in soubor] – Načítaní hesel ze souboru.
[-table] – Určuje formát výstupu „tabulka", sloupec hesla a hashe.
```

Dosazený zápis ukazuje obrázek 7, kde je možné vidět i filtraci dle odpovídajícího řetězce hash, tj. ten, který byl nalezen v konfiguračním souboru Edge routeru. Jak je dále možno vidět, tak heslo bylo nalezeno, a to za pouhých 76 minut.

Obrázek 7: Tvorba hash řetězců, včetně následné specifické filtrace

Po testu hesla k přechodu mezi módy jsou zde další hesla, a to heslo na připojení k administraci přes konzolový port a heslo k zabezpečení virtuálních spojení, jako je například telnet. Hesla byla zašifrována příkazem service password-encryption, kde dojde k zašifrování všech hesel, které jsou v prosté čitelné podobě. Společnost

Cisco tento druh šifrování označuje číslem 7 a jde o celkem slabý šifrovací algoritmus, který jde snadno dešifrovat, tento fakt byl ověřen nástrojem GetPass!, viz obr. 8. Dešifrování proběhlo téměř okamžitě po vložení zašifrovaného hesla.



Obrázek 8: Ukázka aplikace GetPass!, dešifrování

- **Datový provoz** – Testy tohoto druhu mají za cíl objevit potencionální možnosti odposlechu přenášených dat v síti. Jde především o MITM útoky. Pro analýzu síťového provozu byl využit nástroj Wireshark. Test byl zaměřen na ověření bezpečnosti a ochranu směrovacích informací protokolu RIPv2 pomocí nástroje NEMESIS-RIP. Veškeré další zjištěné informace je možné nalézt v části report.
- **Poskytované služby –** NAT, CBAC

B. Testované zařízení: **Internal router**

- **Síla hesla, šifrování** – Tato část je totožná s výše uvedenou oblastí zařízení Edge router, pouze jsou zde odlišná hesla, bude zhodnoceno ve výsledné zprávě (reportu).
- **Datový provoz** – Taktéž zde byl proveden test stejným způsobem a stejnými nástroji jako u výše uvedeného Edge routeru.
- **Poskytované služby –** DHCP Relay Agent.

C. Testované zařízení: **Division switch**

- **Síla hesla, šifrování** – Tato část je totožně testována, jak již bylo představeno výše, a vyhodnocení je možno nalézt v části report.

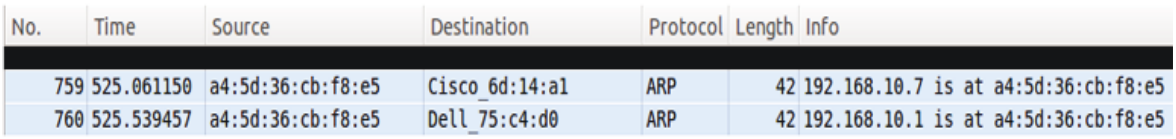
- **Datový provoz** – K otestování switche proti MITM útokům převážně na 2. vrstvě ISO/OSI modelu byl využit balíček dsniff a nástroj Ettercap. Z balíčku dsniff byl využit nástroj arpspoof, který dokáže přesměrovat provoz mezi dvěma koncovými stanicemi připojenými na daném zařízení, jde tedy o útok ARP Cache Poisoning. Útok byl simulován ze stanice, která je zařazená do VLAN 10, s adresou IP 192.168.10.6 a cílem této stanice bylo odklonit provoz v síti od stanice 192.168.10.7 do výchozí brány s adresou 192.168.10.1 a opačně přes stanici s IP adresou 192.168.10.6. Odklon síťového provozu od výchozí brány s adresou IP 192.168.10.1 do stanice s adresou IP 192.168.10.7. Šlo tedy o modifikaci ARP Cache stanice s adresou IP 192.168.10.1 pro záznam s adresou IP 192.168.10.7. Modifikace byla provedena následovně:

  ```
  arpspoof -i eth02 –t 192.168.10.1 192.168.10.7
  ```

  Odklon síťového provozu v opačném směru, bylo provedeno příkazem:

  ```
  arpspoof -i eth02 –t 192.168.10.7 192.168.10.1
  ```

  Nástrojem Wireshark je možné odchytit pakety ARP-reply, které mají za příčinu právě přesměrování provozu. Obr. 9 ukazuje poslané ARP-reply pakety na dané stanice, které způsobí změnu ARP Cache daným stanicím.



No.	Time	Source	Destination	Protocol	Length	Info
759	525.061150	a4:5d:36:cb:f8:e5	Cisco_6d:14:a1	ARP	42	192.168.10.7 is at a4:5d:36:cb:f8:e5
760	525.539457	a4:5d:36:cb:f8:e5	Dell_75:c4:d0	ARP	42	192.168.10.1 is at a4:5d:36:cb:f8:e5

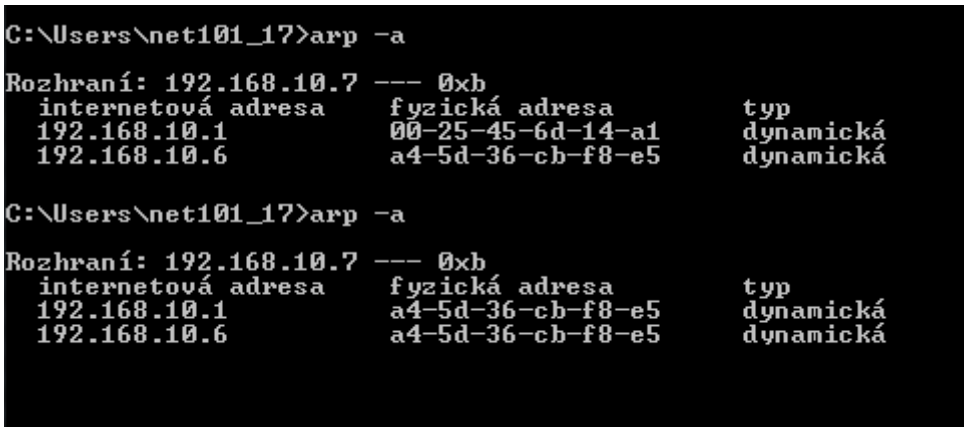
Obrázek 9: Zachycené ARP-reply pakety v programu Wireshark

Pro orientaci výše zobrazených údajů je přiložena tabulka ukazující adresaci a role v tomto simulovaném útoku.

Role	Adresa IP	Adresa MAC
Výchozí brána	192.168.10.1	Cisco_:6d:14:a1
Útočník	192.168.10.6	a4:5d:36:cb:f8:e5
Oběť	192.168.10.7	Dell_:75:c4:d0

Tabulka 4: Popis stanic pro útok ARP Cache Poisoning

Výsledek tohoto útoku je možné vidět na obrázku 10, kde je zobrazen výpis ARP Cache oběti před útokem a po něm.



Obrázek 10: ARP Cache oběti (před a po útoku ARP Cache Poisoning)

- **Poskytované služby –** VLAN.

3.3 Report

Audit byl prováděn ručně testerem a také pomocí auditovacího nástroje Nipper. Výsledky budou dále zkompletovány dle testovaných zařízení. Obecně můžeme říci, že v sítí běží několik nevyužívaných a potencionálně zneužitelných služeb, jde i o služby, které by bylo vhodné nahradit bezpečnějšími, například Telnet pro vzdálenou správu zařízení. Z toho plynou velká rizika, kdy útočník může získat plný přístup k primárním prvkům sítě, a tím také modifikovat datový provoz v sítí. Díky auditu hesel byla zjištěna nedostatečná úroveň používaných hesel, bylo by vhodné volit hesla nad 15 znaků, včetně využití i speciálních znaků a velice vhodnou praktikou je mít hesla odlišná v tom smyslu, aby nebylo možné hesla čistě odvozovat na základě nějakého principu (například inkrementace čísla o daný počet). Síť je náchylná na jakýkoliv výpadek spojení, neexistuje žádná redundance, dále to může také vést k zahlcování určitých oblastí sítě a následnému odstavení poskytovaných služeb. Detaily k daným konfiguracím jsou uvedeny v tabulkách níže a kompletní report z nástroje Nipper je možné nalézt v příloze na CD. Konfigurace některých zařízení je možné nalézt v příloze A a ostatní konfigurace je možné nalézt na CD.

Nyní budou zhodnocena jednotlivá zařízení, která jsou z pohledu bezpečnosti nejdůležitější.

A. Testované zařízení: **Edge router**

Zařízení je hranicí mezi vnější a vnitřní sítí. Provoz je filtrován CBAC ve spolupráci s ACL. Konfiguraci je možné nalézt v příloze A, včetně kompletní konfigurace zařízení. Edge routeru byla přiřazena největší priorita, důvodem byl fakt, že toto zařízení je jediným možným bodem pro útok z vnější sítě. Nejvíce bezpečnostních chyb bylo zaznamenáno v konfiguraci. Zařízení bylo v podstatě konfigurováno jen pro používané služby, zbytek byl ponechán ve výchozím nastavení. Největším rizikem se jeví služba Telnet. Dále zde není nastaven žádný monitorovací mechanismus, nelze tedy reagovat na

případné útoky v jejich „zárodcích“, jde například o zaznamenání brute-force útoků, DoS a dalších.

Audit konfigurace zařízení

Bezpečnostní chyba	Riziko	Popisek
TCP keep alive messages	Vysoké	Při deaktivaci této služby je možné zařízení zahlcovat požadavky TCP spojení, a tím zařízení zahltit, jde tedy o možnost DoS útoku.
Nenastaven exec-timeout	Střední	Nekorektní ukončení, či zapomenutí odhlášení administrátora nevede k ukončení relace po daném čase, spojení bude stále aktivní – může vést k zneužití přístupu.
Neošetřeny nepoužívané porty (Auxilirary port)	Nízké	Nevyužívané porty mohou vést k cílům útoku. Útok může být představován uživatelem, který se přepojuje port po portu a hledá nezabezpečený port (nutný fyzický přístup k zařízení). Proto se doporučuje převést tyto porty do neaktivního stavu (shutdown).
IP source routing	Střední	Velice vhodné je tuto techniku vypnout z důvodu zpřístupnění informací o síti útočníkovi, útočník si určuje „trasu“ provozu paketů v síti.
Telnet	Vysoké	Provozování tohoto protokolu může vést k odposlechu komunikace a dále k získání přístupu k danému zařízení. Doporučuje se nahradit tento protokol šifrovanou variantou SSH.
ICMP redirect	Střední	Zprávy redirect protokolu ICMP mohou být zneužity. Vzdálený útočník zasílá upravené ICMP-redirect zprávy, které se začnou hromadit na zařízení, kdy dojde po určitém čase k vyčerpání veškeré paměti zařízení, a tím k odstavení poskytovaných funkcí zařízení.
CDP	Střední	Používání protokolu na tomto zařízení není nijak přínosné, naopak přináší rizika. Útočník z paketů získá informace o zařízení (verze IOS, platforma, název zařízení).
Logging	Vysoké	Bez monitorování je velice problematické zaznamenat nelegitimní přístup do systému, případné pokusy o prolomení přístupu. Souvisí s tím také veškerá detekce (DoS útoky).
Proxy ARP	Střední	V tomto případě je tato vlastnost spíše rizikem, jeví se zde náchylnost k ARP spoofing a DoS útokům.
Minimum Password Length	Nízké	Definovat minimální délku hesla je dobrou praktikou, nicméně volba silného hesla by

		neměla souviset s tímto příkazem, ale měla by být samozřejmostí, případně tvorbu hesla ošetřit v bezpečnostní politice.
BOOTP	Vysoké	Vzhledem k nevyužívání tohoto protokolu je velice vhodné tuto službu zakázat. Útočník může díky této službě stáhnout kopii operačního systému na daném zařízení.
IP Unreachables	Střední	Povolením těchto zpráv umožňujeme rychlejší a efektivnější mapování sítě útočníkovi (běžící služby, aktivní zařízení).
Login banner	Nízké	Jde o nastavení varovné zprávy při přihlášení před neoprávněnými přístupy.
Domain lookups	Střední	V případě nevyužívání DNS je vhodné tuto službu vypnout (jedná se pouze o DNS na tomto zařízení v rámci OS). V případě využívání náchylnost k MITM útokům.
PAD	Nízké	Další běžící nevyužívaná služba, zvyšuje pouze riziko útoku.
MOP	Nízké	Nevyužívaný běžící protokol, který zvyšuje riziko útoku.

Audit hesel

Hesla	Síla hesla	Prolomení	Riziko
Přechod do konf. módu	Slabé	Brute-force	Vysoké *
Správa konzole	Střední	Brute-force	Vysoké *
Virtuální spojení (Telnet)	Střední	Brute-force, odposlech	Vysoké

* K prolomení hesla je nutné mít fyzický přístup k zařízení.

Audit provozovaných služeb

Služba	Zranitelnost	Zneužitelnost	Riziko
RIPv2	Zabezpečení směr. informací	Modifikace směrovacích tabulek	Kritické
CBAC	Nezjištěno	X	X
NAT	Nezjištěno	X	X

B. Testované zařízení: **Internal router**

Internal router slouží k interní správě počítačové sítě v daných odděleních, jde především o komunikaci mezi VLAN, tedy tento router vystupuje v tzv. Router-on-a-Stick pozici. Dále také zde dochází ke směrování DHCP požadavků na DHCP server. Jako v minulém případě se zde objevují většinou chyby, které plynou z neošetření výchozího nastavení zařízení, nicméně je nutné se zaměřit i na tvorbu silných hesel a využívání šifrovaní v komunikaci. Jako v předchozím testovaném zařízení je největším rizikem používání služby Telnet.

Audit základní konfigurace

Bezpečnostní chyba	Riziko	Popisek
TCP keep alive messages	Vysoké	Při deaktivaci této služby je možné zařízení zahlcovat požadavky TCP spojení, a tím zařízení zahltit, jde tedy o možnost DoS útoku.
Nenastaven exec-timeout	Střední	Nekorektní ukončení, či zapomenutí odhlášení administrátora nevede k ukončení relace po daném čase, spojení bude stále aktivní – může vést k zneužití přístupu.
Neošetřeny nepoužívané porty (Auxilirary port)	Nízké	Nevyužívané porty mohou vést k cílům útoku. Útok může být představován uživatelem, který se přepojuje port po portu a hledá nezabezpečený port (nutný fyzický přístup k zařízení). Proto se doporučuje převést tyto porty do neaktivního stavu (shutdown).
IP source routing	Střední	Velice vhodné je tuto techniku vypnout z důvodu zpřístupnění informací o síti útočníkovi, útočník si určuje „trasu“ provozu paketů v síti.
Telnet	Vysoké	Provozování tohoto protokolu může vést k odposlechu komunikace a dále k získání přístupu k danému zařízení. Doporučuje se nahradit tento protokol šifrovanou variantou SSH.
ICMP redirect	Střední	Zprávy redirect protokolu ICMP mohou být zneužity. Vzdálený útočník zasílá upravené ICMP redirect zprávy, které se začnou hromadit na zařízení, kdy dojde po určitém čase k vyčerpání veškeré paměti zařízení, a tím k odstavení poskytovaných funkcí zařízení.
CDP	Střední	Používání protokolu na tomto zařízení není nijak přínosné, naopak přináší rizika. Útočník z paketů získá informace o zařízení (verze IOS, platforma, název zařízení).

Logging	Vysoké	Bez monitorování je velice problematické zaznamenat nelegitimní přístup do systému, případné pokusy o prolomení přístupu. Souvisí s tím také veškerá detekce (DoS útoky).
Proxy ARP	Střední	V tomto případě je tato vlastnost spíše rizikem, jeví se zde náchylnost k ARP spoofing a DoS útokům.
BOOTP	Vysoké	Vzhledem k nevyužívání tohoto protokolu je velice vhodné tuto službu zakázat. Útočník může díky této službě stáhnout kopii operačního systému na daném zařízení.
IP Unreachables	Střední	Povolením těchto zpráv umožňujeme rychlejší a efektivnější mapování sítě útočníkovi (běžící služby, aktivní zařízení).
Login banner	Nízké	Jde o nastavení varovné zprávy při přihlášení před neoprávněnými přístupy.
Domain lookups	Střední	V případě nevyužívání DNS je vhodné tuto službu vypnout (jedná se pouze o DNS na tomto zařízení v rámci OS). V případě využívání náchylnost k MITM útokům.
PAD	Nízké	Další běžící nevyužívaná služba, zvyšuje pouze riziko útoku.
MOP	Nízké	Nevyužívaný běžící protokol, který zvyšuje riziko útoku.

Audit hesel

Hesla	Síla hesla	Prolomení	Riziko
Přechod do konf. módu	Slabé	Brute-force	Vysoké *
Správa konzole	Střední	Brute-force	Vysoké *
Virtuální spojení (Telnet)	Střední	Brute-force, odposlech	Vysoké

* K prolomení hesla je nutné mít fyzický přístup k zařízení.

Audit provozovaných služeb

Služba	Zranitelnost	Zneužitelnost	Riziko
RIPv2	Zabezpečení směr. informací	Modifikace směrovacích tabulek	Vysoké
DHCP relay agent	Nezjištěno	X	X

C. Testované zařízení: **Division switch**

Tento switch slouží k propojení daných oddělení v rámci VLAN. Obecně lze říci, že switch je nezabezpečený proti útokům na druhé vrstvě ISO/OSI modelu, jde tedy především o útoky s působností v lokálním segmentu počítačové sítě. Z výše uvedených bezpečnostních slabin plyne, že zařízení je náchylné k MITM útokům, jako je například ARP Cache Poisoning, MAC Flooding, Port Stealing a další.

Audit základní konfigurace

Bezpečnostní chyba	Riziko	Popisek
TCP keep alive messages	Vysoké	Při deaktivaci této služby je možné zařízení zahlcovat požadavky TCP spojení, a tím zařízení zahltit, jde tedy o možnost DoS útoku.
Nenastaven exec-timeout	Střední	Nekorektní ukončení, či zapomenutí odhlášení administrátora nevede k ukončení relace po daném čase, spojení bude stále aktivní – může vést k zneužití přístupu.
IP source routing	Střední	Velice vhodné je tuto techniku vypnout z důvodu zpřístupnění informací o síti útočníkovi, útočník si určuje „trasu“ provozu paketů v síti.
CDP	Střední	Používání protokolu na tomto zařízení není nijak přínosné, naopak přináší rizika. Útočník z paketů získá informace o zařízení (verze IOS, platforma, název zařízení).
Logging	Vysoké	Bez monitorování je velice problematické zaznamenat nelegitimní přístup do systému, případné pokusy o prolomení přístupu. Souvisí s tím také veškerá detekce (DoS útoky).
BOOTP	Vysoké	Vzhledem k nevyužívání tohoto protokolu je velice vhodné tuto službu zakázat. Útočník může díky této službě stáhnout kopii operačního systému na daném zařízení.
Login banner	Nízké	Jde o nastavení varovné zprávy při přihlášení před neoprávněnými přístupy.

Audit hesel

Hesla	Síla hesla	Prolomení	Riziko
Přechod do konf. módu	Střední	Brute-force	Vysoké *
Správa konzole	Střední	Brute-force	Vysoké *

* K prolomení hesla je nutné mít fyzický přístup k zařízení.

Z důvodu většinou totožných problémů další zařízení zde detailněji probírány nebudou. Nicméně audity zařízení a konfigurace je možné nalézt na CD zařízení.

Závěr

Tato bakalářská práce se zabývala problematikou bezpečnosti informačních systémů a testováním IS pomocí penetračních testů. Práce nejprve představila problematiku penetračního testování počítačových sítí. Hlavním cílem práce pak bylo aplikovat tuto metodu na modelovou síť, ověřit míru bezpečnosti a ohodnotit možná rizika.

V první kapitole byly představeny základní pojmy z oblasti bezpečnosti a zranitelnost IS. Šlo především o představení možných útoků a hrozeb na IS, včetně ochrany a obrany daných oblastí. Tato kapitola představovala určitou přípravu k zavedení optimálních bezpečnostních opatření ve společnosti a měla uvést specifické přístupy k řešení bezpečnostních rizik IS.

V druhé kapitole byla popsána problematika penetračního testování z teoretického hlediska. Především šlo o představení podstaty penetračního testování, možnosti přístupu testera k provádění, členění a stručné představení základních metodik testování, kde v souladu s charakterem práce byly vybrány nejznámější metodiky, které ale nebyly zapojeny do praktické části. Pro praktickou část byla zvolena pak vlastní specifická metodika, a to z důvodu specifického zaměření práce na penetrační testování aktivních prvků sítě.

V třetí kapitole práce byl již předveden praktický modelový příklad, který byl podroben penetračnímu testování. K provádění penetračního testování byla využita linuxová distribuce Backtrack ve verzi 5 R3, která je velice vhodnou volbou právě k těmto potřebám a nalezneme zde spoustu nástrojů nejenom k vedení útoků, ale také k tvorbě bezpečnostních auditů, kde byl využit nástroj Nipper. Postup penetračního testování byl proveden dle kroků odpovídajících již zmiňované metodologii v druhé kapitole.

Z této práce vyplývá, že problematika bezpečnosti je velice důležitou doménou každého IS a penetrační testování je účinnou metodou k odhalení velkého množství zranitelných míst.

Žádoucím rozšířením této práce by bylo porovnání a využití bezpečnostních metodik penetračního testování jako OSSTMM a dalších, včetně možného rozšíření oblasti testování i na koncové stanice.

Literatura

ALI, Shakeel a HERIYANTO. BackTrack 4: Security with Penetration Testing Methodology. *Packt Publishing* [online]. 2011 [cit. 2014-03-01]. Dostupné z WWW: <http://www.packtpub.com/article/backtrack4-security-penetration-testing-methodology>.

BARKER, Keith a Scott MORRIS. *CCNA security 640-554 official cert guide.* Indianapolis: Cisco Press, 2012, 700 s. ISBN 978-1-58720-446-3.

ČMELÍK, Martin. DoS a DDoS útoky. *Security-Portal.cz* [online]. 2013 [cit. 2014-03-01]. Dostupné z WWW: <http://www.security-portal.cz/clanky/seznamte-se-%E2%80%93-dos-ddos-%C3%BAtoky>.

HALLER, Martin. Seriál Odposloucháváme data na přepínaném Ethernetu. *Lupa.cz* [online]. 2006 [cit. 2014-04-09]. ISSN 1213-0702. Dostupné z WWW: <http://www.lupa.cz/serialy/odposlouchavame-data-na-prepinanem-ethernetu>.

HARPER, Allen et al. *Hacking: manuál hackera*. 1. vyd. Praha: Grada, 2008, 399 s. ISBN 978-80-247-1346-5.

PŘIBYL, Tomáš. Bezpečnostní analýza. *Computerworld: Ucelený informační zdroj pro IT profesionály* [online]. 2005a [cit. 2014-03-01]. Dostupné z WWW: <http://computerworld.cz/archiv/bezpecnostni-analyza-22926>.

PŘIBYL, Tomáš. Bezpečnostní politika. *Computerworld: Ucelený informační zdroj pro IT profesionály* [online]. 2005b [cit. 2014-03-01]. Dostupné z WWW: <http://computerworld.cz/archiv/bezpecnostni-politika-22927>.

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

VACHON, Bob a Rick GRAZIANI**.** *Accessing the WAN: CCNA exploration companion guide.* Indianapolis: Cisco Press, 2008, xxiv, 668 s. ISBN 1-58713-205-2.

WEBER, Filip. DoS a DDoS útoky a ochrana proti nim. *Svět sítí: Informace ze světa počítačových sítí* [online]. 2008 [cit. 2014-03-01]. Dostupné z WWW: <http://www.svetsiti.cz/clanek.asp?cid=DoS-a-DDoS-utoky-a-ochrana-proti-nim-1-742008>.

WHITAKER, Andrew a Daniel P. NEWMAN**.** *Penetration testing and network defense*. Indianapolis: Cisco Press, 2006. ISBN 15-870-5208-3.

Příloha A – Konfigurace zařízení

Edge router

```
version 12.4
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname Edge_Router
!
enable secret 5 $1$mERr$pHFJEr11cgXfU.BnAHrP2.
!
ip inspect name out_inside udp
ip inspect name out_inside icmp
ip inspect name out_inside tcp
ip inspect name http_dmz http
spanning-tree mode pvst
!
interface FastEthernet0/0
 ip address 192.168.99.1 255.255.255.224
 ip access-group LAN_OUT in
 ip nat inside
 duplex auto
 speed auto
!
interface FastEthernet0/1
 ip address 10.1.1.1 255.255.255.240
 ip access-group DMZ_OUT in
 ip nat inside
 ip inspect http_dmz out
 duplex auto
 speed auto
!
interface Serial0/0/0
 ip address 209.165.200.225 255.255.255.252
 ip access-group LAN_DMZ_UN_IN in
 ip nat outside
 ip inspect out_inside out
 clock rate 64000
!
interface Serial0/0/1
 no ip address
!
interface Vlan1
 no ip address
 shutdown
!
router rip
 version 2
 redistribute static
 passive-interface FastEthernet0/1
 network 10.0.0.0
 network 192.168.99.0
 no auto-summary
!
ip nat inside source list NAT_OVERLOAD interface Serial0/0/0 overload
ip classless
ip route 0.0.0.0 0.0.0.0 Serial0/0/0
```

```
!
!
ip access-list standard NAT_OVERLOAD
 remark Management
 permit 192.168.10.0 0.0.0.15
 remark Vyvoj
 permit 192.168.20.0 0.0.0.31
 remark DMZ
 permit 10.1.1.0 0.0.0.15
ip access-list extended LAN_OUT
 remark RIP
 permit udp any any eq 520
 remark Management
 permit ip 192.168.10.0 0.0.0.15 any
 remark Vyvoj
 permit ip 192.168.20.0 0.0.0.31 any
 deny ip any any
ip access-list extended LAN_DMZ_UN_IN
 remark WWW server
 permit tcp any host 10.1.1.14 eq www
 remark smtp server
 permit tcp any host 10.1.1.15 eq smtp
 deny ip any any
ip access-list extended DMZ_OUT
 remark smtp server to any
 permit tcp host 10.1.1.15 any eq smtp
 deny ip any any
!
line con 0
 password 7 082A4D480C1A0A194359
 logging synchronous
 login
!
line aux 0
!
line vty 0 4
 exec-timeout 5 0
 password 7 082A4D480C150C19175A5E
 login
!
!
end
```

Internal router

```
version 12.4
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname Internal_Router
!
!
enable secret 5 $1$mERr$oqS9mx9Yn4Jm/ZjTWNB9O0
!
!
!
spanning-tree mode pvst
```

```
!
interface FastEthernet0/0
 ip address 192.168.99.2 255.255.255.224
 duplex auto
 speed auto
!
interface FastEthernet0/1
 no ip address
 duplex auto
 speed auto
!
interface FastEthernet0/1.10
 encapsulation dot1Q 10
 ip address 192.168.10.1 255.255.255.240
 ip helper-address 192.168.99.3
!
interface FastEthernet0/1.20
 encapsulation dot1Q 20
 ip address 192.168.20.1 255.255.255.224
 ip helper-address 192.168.99.3
!
interface FastEthernet0/1.30
 encapsulation dot1Q 30
 ip address 192.168.30.1 255.255.255.224
 ip helper-address 192.168.99.3
!
interface Vlan1
 no ip address
 shutdown
!
router rip
 version 2
 passive-interface FastEthernet0/1
 network 192.168.10.0
 network 192.168.20.0
 network 192.168.30.0
 network 192.168.99.0
 no auto-summary
!
ip classless
!
line con 0
 password 7 082A4D480C1A0A194059
 login
!
line aux 0
!
line vty 0 4
 password 7 082A4D480C150C1917595E
 login
!
end
```

Division switch

```
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
```

```
service password-encryption
!
hostname Division_Switch
!
enable secret 5 $1$mERr$XmnamXkdSsljSqhlSSaef1
!
!
!
no ip domain-lookup
!
spanning-tree mode pvst
!
interface FastEthernet0/1
 switchport mode trunk
!
interface FastEthernet0/2
 switchport access vlan 10
!
interface FastEthernet0/3
 switchport access vlan 20
!
interface FastEthernet0/4
 switchport access vlan 30
!
interface Vlan1
 no ip address
 shutdown
!
!
line con 0
 password 7 082259451B100E141D055C5578
 login
!
line vty 0 4
login
line vty 5 15
login
!
!
end
```