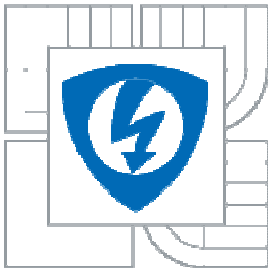
VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY



FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ
ÚSTAV TELEKOMUNIKACÍ

FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION
DEPARTMENT OF TELECOMMUNICATIONS

BEZPEČNOSTNÍ AUDIT FIREWALLU

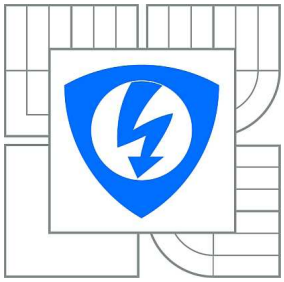
FIREWALL SECURITY AUDIT

DIPLOMOVÁ PRÁCE
MASTER´S THESIS

AUTOR PRÁCE — Bc. JIŘÍ KRAJÍČEK
AUTHOR

VEDOUCÍ PRÁCE — Ing. RADIM PUST
SUPERVISOR

BRNO 2010



VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

Fakulta elektrotechniky a komunikačních technologií

Ústav telekomunikací

Diplomová práce

magisterský navazující studijní obor
Telekomunikační a informační technika

Student: Bc. Jiří Krajíček ***ID:*** 83593
Rocník: 2 ***Akademický rok:*** 2009/2010

NÁZEV TÉMATU:

Bezpecnostní audit firewallu

POKYNY PRO VYPRACOVÁNÍ:
Cílem diplomové práce je vyhledat komerční i nekomerční systémy umožňující provádět bezpečnostní audit firewallu (nessus a další) a popsat jejich princip činnosti. Dále navrhnout metodiku pro audit firewallu. Pomocí navržené metodiky provést audit vybraných komerčních a nekomerčních firewallu v základním nastavení. V případe zjištění bezpečnostních nedostatků navrhnout řešení vedoucí k jejich odstranení.

DOPORUCENÁ LITERATURA:

[1] TOXEN, Bob. Bezpecnost v Linuxu : Prevence a odvracení napadení systému. [s.l.] : Computer
Press, 2003. 876 s. ISBN 80-7226-716-7.
[2] KABELOVÁ, Alena, DOSTÁLEK, Libor. Velký pruvodce protokoly TCP/IP a systémem DNS . [s.l.] :
Computer Press, 2008. 488 s. ISBN 978-80-251-2236-5.

Termín zadání: 29.1.2010 ***Termín odevzdání:*** 26.5.2010

Vedoucí práce: Ing. Radim Pust

prof. Ing. Kamil Vrba, CSc.
Predseda oborové rady

UPOZORNENÍ:

ANOTACE

Cílem této diplomové práce je bezpečnostní audit firewallu. Základními úkoly je seznámit s principy nástrojů umožňující audit, vytvořit metodiku auditu a poté podle vytvořené metodiky provést bezpečnostní audit vybraných firewallů.

Teoretická část dokumentu pojednává obecně o firewallech a možnostech zapojení do síťové infrastruktury. Dále o auditu a principech nástrojů k provedení auditu. Následující praktická část se pak zabývá vytvořením metodiky včetně penetračního testování. Pomocí vytvořených metodik a procedur je poté proveden audit linuxového firewallu a firewallu Microsoft ISA 2006. Součástí každého auditu je na závěr proveden návrh změn konfigurací vedoucích k zabezpečení bezpečnostních nedostatků.

Klíčová slova: audit, firewall, bezpečnost, penetrační testy, linux, ISA 2006

ABSTRACT

An aim of master´s thesis is Firewall security audit. Main tasks this work is introduce with principles of application for audit, create methodology and with this methodology make security audit of the selected firewalls.

Theoretical part of this document deal with firewalls and possibilities of integration into network infrastructure. And next with audit and principles of application for security audit. Next practical part of this document deal with creation methodology and procedures including penetration testing. With this methodology is created audit of linux firewall and ISA 2006 included tips for change configuration providing more security.

Keywords: audit, firewall, security, penetration testing, linux, ISA 2006

BIBLIOGRAFICKÁ CITACE

KRAJÍČEK, J. *Bezpečnostní audit firewallu: diplomová práce*. Brno: Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, 2010. 76 stran. Vedoucí práce Ing. Radim Pust.

PROHLÁŠENÍ

Prohlašuji, že svou diplomovou práci na téma Bezpečnostní audit firewallu jsem vypracoval samostatně pod vedením vedoucího diplomové práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou všechny citovány v práci a uvedeny v seznamu literatury na konci práce.

Jako autor uvedené diplomové práce dále prohlašuji, že v souvislosti s vytvořením této diplomové práce jsem neporušil autorská práva třetích osob, zejména jsem nezasáhl nedovoleným způsobem do cizích autorských práv osobnostních a jsem si plně vědom následků porušení ustanovení § 11 a následujících autorského zákona č. 121/2000 Sb., včetně možných trestněprávních důsledků vyplývajících z ustanovení § 152 trestního zákona č. 140/1961 Sb.

V Brně dne ....

podpis autora

Poděkování

Děkuji vedoucímu práce Ing. Radimovi Pustovi za velmi užitečnou metodickou pomoc a cenné rady při zpracování diplomové práce.

V Brně dne …….. .....

podpis autora

Obsah

1 Úvod

Cílem diplomové práce bylo vyhledat nástroje umožňující provádět bezpečnostní audit firewallu. Tyto nástroje mohly být komerční i nekomerční a mohly být voleny pro kterýkoliv operační systém. Hlavním požadavkem bylo popsat princip jejich činnosti. Součástí práce je také návrh metodiky auditu. Ta je vytvořena tak, aby splňovala požadavky pro použití při auditu malé až střední společnosti obsahující typické prvky zabezpečení. Pomocí této metodiky jsou poté auditovány vybrané firewally v základním nastavení.

První část práce popisuje jednotlivé typy firewallů [3][4] a možnosti jejich zapojení do síťové infrastruktury.

Druhá část pojednává o bezpečnostním auditu. Vysvětluje, co znamená pojem audit a způsoby jeho provedení. Též připomíná co je důvodem auditu a penetračního testování.

Poté je přistoupeno k popisu principů testů firewallů. Tyto testy zobrazují neinvazivní i invazivní metody tj. i testy, které jsou používány především pro tzv. penetrační testování. V každé kapitole je pak uveden vždy i minimálně jeden z nástrojů pracující na daném principu.

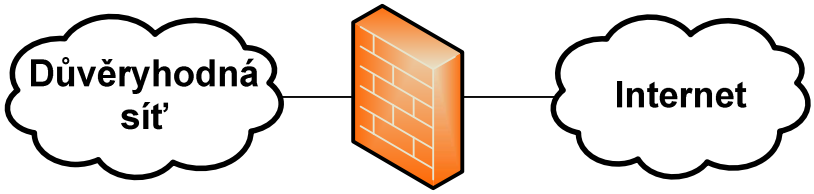
Další část obsahuje návrh auditu firewallu. Je zde vysvětlena metodika a způsob tvorby procedury pro proces auditu. Jsou zde vysvětleny jednotlivé části auditu včetně penetračního testování, ze kterých byly složeny výsledné procedury. Pro plánované aplikace, které byly následně použity pro audit, je zde stručně uvedena instalace a vysvětleny základy používání.

V závěru byly provedeny 2 audity včetně penetračního testování pro dva zvolené firewally. První byl vybrán jako zástupce nekomerčního řešení založeného na operačním systému linux. Druhý pak komerční na operačním systému Microsoft windows. Součástí je také návrh řešení k zabezpečení odhalených bezpečnostních nedostatků pomocí provedených auditů.

Poslední část tvoří závěr, seznamy obrázků, tabulek, zkratek a přílohy obsahující vytvořené procedury auditu.

2 Firewally

Firewally jsou síťová zařízení, která logicky a fyzicky oddělují dvě a více sítí s různou úrovní důvěryhodnosti viz Obr. 1. To se provádí pomocí filtrování síťového provozu podle stanovených bezpečnostních pravidel. Ty jsou zavedeny do konfigurace firewallu. V případě příchodu paketu na vstupní rozhraní zařízení, je provedena inspekce paketu a dále vyhodnocení podle vnitřních pravidel. Výsledkem je rozhodnutí, zda je paket zahozen, odmítnut nebo odeslán na výstupní rozhraní. V některých případech je firewall využíván i pro směrování datových toků.



Obr. 1: Funkce firewallu

2.1 Rozdělení firewallů

Podle toho čím je firewall tvořen, je možné rozdělení na dva typy:

- Hardwarové firewally,
- softwarové firewally.

Hardwarové firewally představují specializovaná zařízení, která často umožňují použití vedle funkce paketového filtru i jako proxy a detekčního systému IDS. Oproti softwarovým firewallům, které umožňují funkce v závislosti na instalovaném softwaru na daném PC nebo serveru, je výhoda v rychlosti a jednodušší konfiguraci. Ta se provádí převážně pomocí příkazové řádky CLI, dostupné přímo na zařízení, nebo vzdáleně přes SSH, případně pomocí grafického webového rozhraní. Příkladem hardwarového firewallu je Cisco Pix, Juniper networks netscreen a softwarového pak netfilter.

Další rozdělení je možné podle umístění na:

- Osobní firewally,
- síťové firewally.

Hlavním rozdílem je umístění firewallu v síťové architektuře a tím i rozdílné požadavky na ně kladené. Osobní firewally jsou implementovány na koncových stanicích. Slouží pro ochranu jednotlivých systémů. Kromě paketového filtru je zde využíváno kontrol, které sledují, které aplikace přistupují k prostředkům sítě, obsahují emailový spam filtr apod. Naproti tomu síťové firewally jsou využívány uvnitř síťové architektury mimo koncové stanice. Jejich úlohou je filtrovat provoz mezi více sítěmi a tím chránit i více

systémů. Dále provádět NAT a přesměrování paketů. Pro svoji funkci využívají převážně bezstavové a stavové paketové filtry. Často také obsahují podporu pro tvorbu VPN sítí. Základním požadavkem je vysoká datová propustnost a nízká poruchovost.

Podle typu filtrování lze firewally rozdělit na:

- Bezstavové paketové firewally,
- stavové paketové firewally,
- proxy.

2.2 Bezstavové paketové firewally

Jedná se o nejjednodušší paketové filtry, které se nejčastěji implementují ve směrovačích. Pro vyhodnocení analyzují z hlaviček paketů ze síťové a transportní vrstvy ISO/OSI modelu:

- Zdrojovou a cílovou IP adresu,
- zdrojový a cílový port,
- typ protokolu,
- fragmentační čísla.

Na základě těchto informací se provede porovnání s bezpečnostní politikou firewallu (příklad viz Tabulka 1), kde se rozhodne o způsobu, jak se paket dále zpracuje. Zda bude přeposlán, zahozen nebo odmítnut.

Tabulka 1: Pravidla firewallu

Pořadí	Zdrojová adresa	Zdrojový port	Cílová adresa	Cílový port	IP protokol	Akce	Poznámka
1	192.168.0.0	jakýkoli	jakýkoli	jakýkoli	jakýkoli	povolit	komunikace z LAN
2	jakýkoli	jakýkoli	192.168.0.0	>1023	jakýkoli	povolit	vyřízení komunikace pro LAN
3	jakýkoli	jakýkoli	192.168.0.10	80	TCP	povolit	webový server uvnitř LAN
4	jakýkoli	jakýkoli	jakýkoli	jakýkoli	jakýkoli	zakázat	ostatní

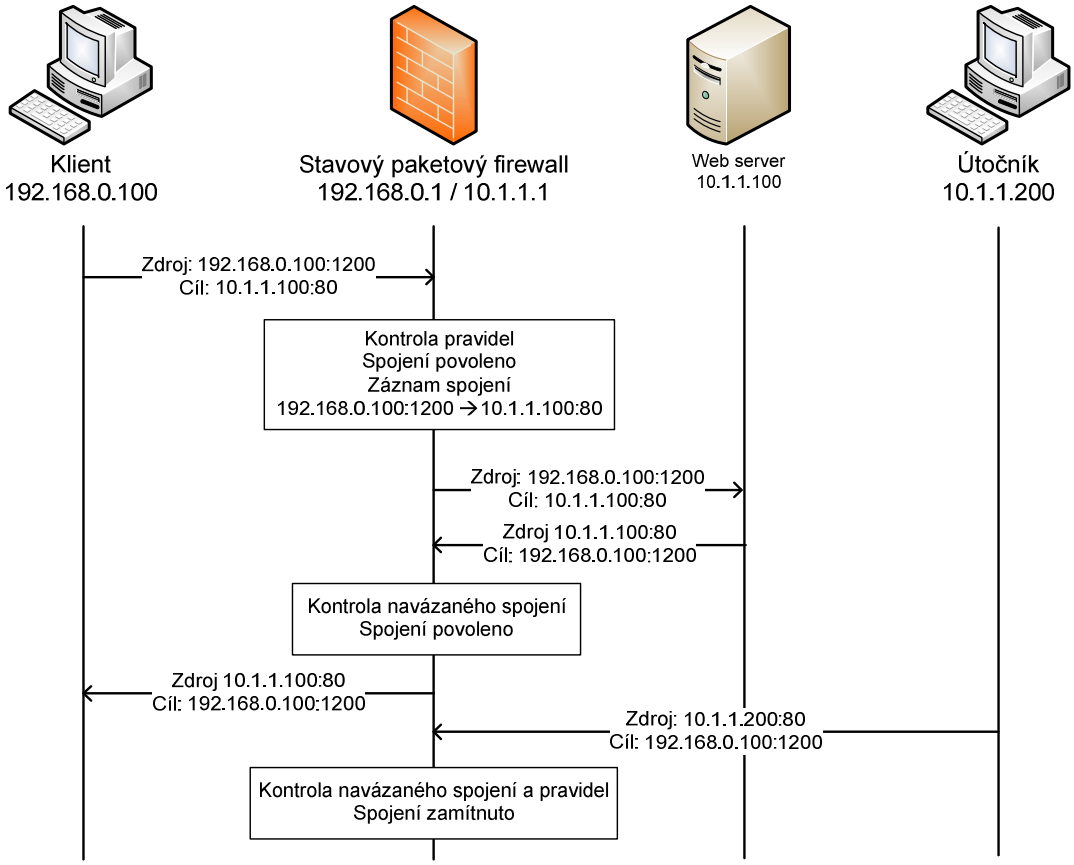
Nevýhodou bezstavových paketových filtrů je, že se musí kontrolovat všechny pakety a to i těch, které jsou součástí již navázaných spojení. Také je zde bezpečnostní problém. Ten vyplívá z požadavků na vyřizování komunikace zpět do lokální sítě LAN při spojení se vzdálenými servery, neboť je na firewallu potřeba přidat pravidlo, které do lokální sítě povolí veškerou komunikaci na vyšších portech tj. nad 1023. Ty však lze i zneužít k útokům do vnitřní sítě.

2.3 Stavové firewally

Základní nevýhody bezstavových paketových firewallů řeší firewally stavové. Ty oproti předešlým zpracovávají datové proudy a nejen jednotlivé pakety, neboť rozlišují i stavy spojení viz Obr. 2. Při navazování spojení mezi klientem a serverem je přijatý paket s příznakem SYN vyhodnocen podle pravidel firewallu a v případě povoleného spojení je zanesen do paměti záznam o navázání spojení. Tento záznam je kromě dalších paketů v daném směru využit i při posuzování spojení ze vzdálené strany ke klientovi, kde jsou zachovány patřičné IP adresy a porty. V takovém případě není potřeba prohledávat celý seznam bezpečnostních pravidel, protože pakety jsou povolovány na základě záznamu v paměti. Výhodou uvedeného řešení je mnohem vyšší rychlost firewallu.

Jestliže se přes daný firewall pokusí připojit útočník, jeho spojení bude zamítnuto. To je zapříčiněno tím, že neexistuje povolující pravidlo ani záznam o navázaném spojení pro útočníkovu IP adresu, přestože by se pokoušel spojit na port klienta, který udržuje spojení s webovým serverem.

Na závěr komunikace, při ukončování spojení klienta s webovým serverem nebo při vypršení časového limitu dochází ke smazání záznamu z paměti. Takto je zajištěno, aby nevznikaly ve firewallu tzv. díry.



Obr. 2: Stavový paketový firewall

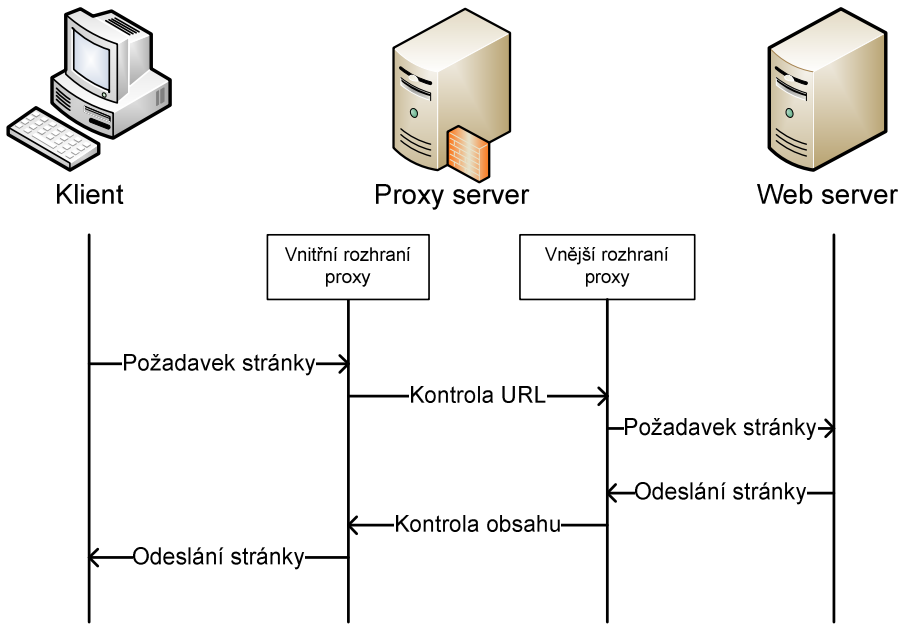
2.4 Proxy

Oproti paketovým filtrům provádějí proxy servery inspekci paketů na vyšší (aplikační) vrstvě ISO/OSI. Díky tomu umožňují kontrolovat datové toky mnohem detailněji, protože sledují veškerý obsah komunikace. Tedy i datovou část přenášející informace. Mezi funkce proxy sloužící k vyššímu zabezpečení patří:

- Skrytí IP adresy klienta pod adresu proxy,
- kontrola URL adres,
- filtrování obsahu,
- kontrolu konzistence,
- blokování směrování,
- zavedení autentizace.

Protože je však forma obsahu pro různé služby rozdílná, jsou proxy vytvořeny převážně pro konkrétní použití (protokoly). Mezi nejčastější pak patří HTTP proxy a SMTP proxy.

Z pohledu funkčnosti tyto systémy tvoří formu prostředníka, viz Obr. 3. Při žádosti klienta o webovou stránku požadavek převezme HTTP proxy systém a pokud je vyžadováno, je následně provedena autentizace. Dále proxy provede kontrolu URL, zda nepatří mezi blokované adresy. Pokud je URL povolena, proxy server vytvoří nové spojení s webovým serverem. Ten odešle požadovanou stránku zpět na proxy, kde je provedena kontrola a filtrace obsahu. Poté je stránka přeposlána klientovi.



Obr. 3: Princip proxy

Přestože by se mohlo zdát, že proxy mohou zastávat samostatné systémy bezpečnější než předešlé firewally, není tomu tak. Jsou používány společně s některou formou paketového firewallu. Ty mimo filtraci ostatních služeb blokují komunikace, které by mohly vést k odepření služby proxy tzv. DoS útoky. Dalším požadavkem na správnou funkci proxy je udržování aktuálnosti databáze obsahující nebezpečné URL adresy a nebezpečné řetězce určené k filtraci.

Mezi výhody pak patří vyšší bezpečnost a uchovávání stránek, které prošly přes proxy tzv. proxy caching. Tím je možné vyřídit určité opakující požadavky přímo proxy serverem a odlehčit síťovým prostředkům. Aby ale nedocházelo k zobrazování neaktuálního obsahu, je doporučováno stanovit optimální dobu časovače, po jehož vypršení je daný obsah vymazán.

2.5 Překlady síťových adres NAT

Vzhledem k rozšiřujícím se požadavkům pro připojení zařízení do sítě, dochází k postupnému vyčerpávání volných jedinečných IPv4 adres. Aby se tento jev zpomalil, vznikly mechanismy překladů síťových adres NAT popisované v RFC 1631. Ty jsou konfigurovány na firewallech a směrovačích.

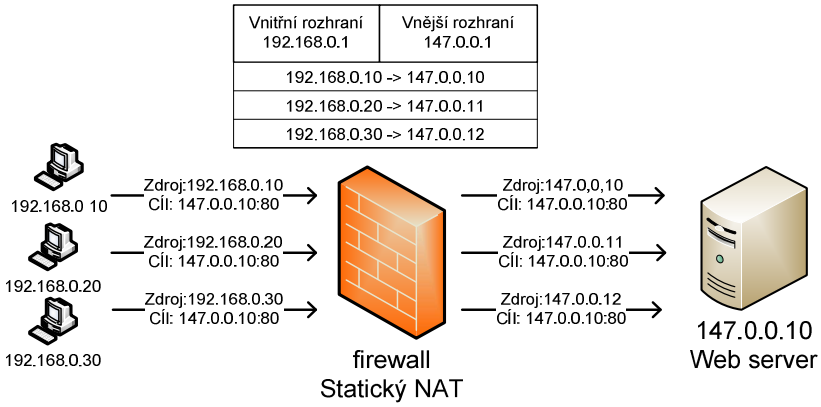
Pro svoji funkci využívají veřejných jedinečných adres, používaných na vnějších rozhraních síťových zařízení, a privátních adres jak zobrazuje Tabulka 2, používaných na vnitřních rozhraních. Tyto privátní adresy lze pak použít pro více lokálních sítí, přestože poté již nejsou jedinečné. Adresování v rámci rozlehlé sítě je zajištěno pomocí NATu, kdy je proveden překlad privátních adres na adresu vnějšího rozhraní nebo na adresy přidělené NATu.

Tabulka 2: Privátní adresy

Třída adres	Rozsah	Prefix
A	10.0.0.0-10.255.255.255	10.0.0.0/8
B	172.16.0.0 - 172.31.255.255	176.16.0.0/12
C	192.168.0.0 - 192.168.255.255	192.168.0.0/16

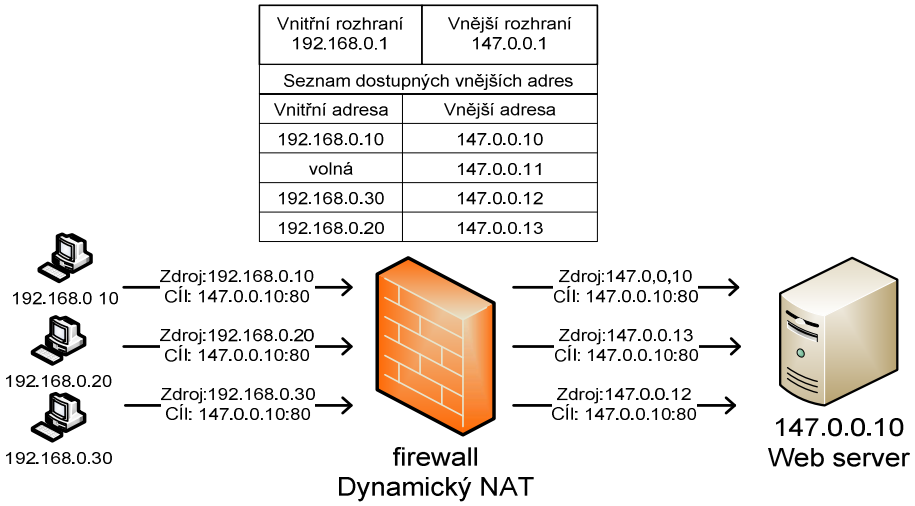
Podle způsobu jak se překlad provádí lze provést rozdělení na následující základní typy:

- Statický NAT provádí překlad jedna ku jedné, viz Obr. 4. Pro každou privátní adresu je jednoznačně definována veřejná adresa. Tento typ se používá především pro servery uvnitř lokálních sítí s privátní adresou. Takto dochází k jejich zpřístupnění z veřejných sítí pod definovanou veřejnou adresou.



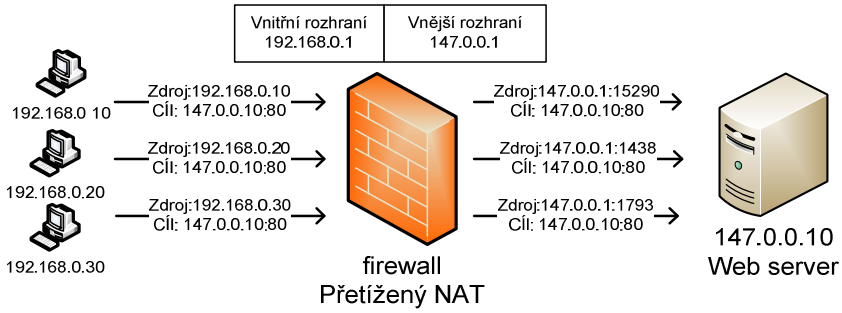
Obr. 4: Statický NAT

- Dynamický NAT provádí překlad na veřejnou adresu vybranou z přiřazeného seznamu, viz Obr. 5. Rozdílem oproti předchozímu typu je, že nemusí být pro danou privátní adresu zvolena vždy stejná veřejná adresa. Také může nastat případ, kdy jsou již veřejné adresy vyčerpány. Poté je přístup do vnější sítě odmítnut.



Obr. 5: Dynamický NAT

- Přetížený NAT představuje speciální typ. Překlad se provádí na jednu adresu vnějšího rozhraní. Pro rozlišení komunikací ze sítě vnitřního rozhraní se používá portů, viz Obr. 6. V případě potřeby zveřejnění vnitřního serveru pro vnější síť se provádí přesměrování portů. To je zajištěno rezervací konkrétního portu, kdy při příchodu komunikace na tento port dochází k přesměrování komunikace na patřičný server.



Obr. 6: Přetížený NAT

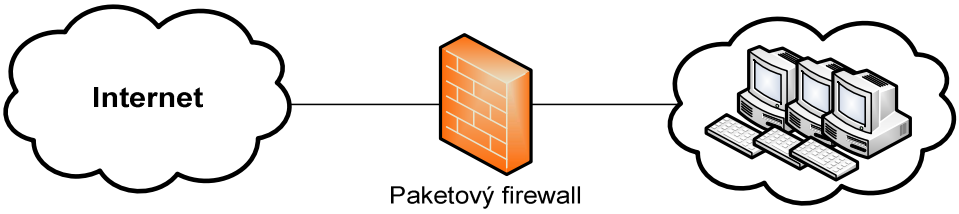
2.6 Implementace firewallů v síťové topologii

Jak již bylo popsáno, existuje několik druhů, typů, značek i možností zapojení firewallů. Orientace v dané problematice se tak může zdát obtížná. Přesto lze situaci zjednodušit faktem, že se firewallů využívá především ve funkci brány připojení do internetu. Výběr konkrétních firewallů je pak dán službami, které mají poskytnout, stupněm poskytované bezpečnosti a finančními možnostmi. V závislosti na těchto skutečnostech vzniklo několik typických implementací firewallů do síťové infrastruktury. Mezi nejzákladnější patří tyto:

- S paketovým firewallem,
- s paketovým firewallem a proxy,
- s jedním nebo dvěma paketovými firewally a demilitarizovanou zónou (DMZ).

2.6.1 Implementace s paketovým firewallem

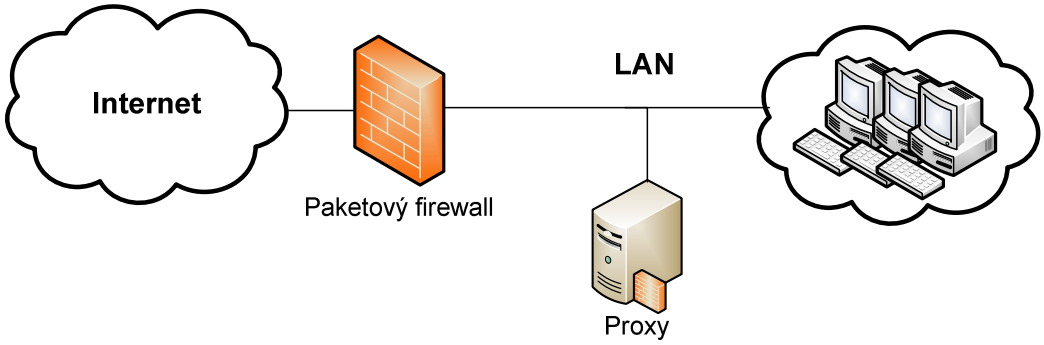
Nejzákladnější implementací je zapojení s jedním paketového firewallem, viz Obr. 7. Ten může být stavový i bezstavový v závislosti na požadavcích bezpečnosti. Realizace je tvořena směrovačem (bezstavový paketovým firewall) nebo pomocí specializovaného síťového firewallu (stavový paketový firewall). Jejich úlohou je základní filtrace paketů a případně poskytování překladu adres - NATu. Proto se dnes již stávají nedílnou součástí každé síťové infrastruktury. Výhodou tohoto řešení je výrazné navýšení bezpečnosti (oproti sítím bez síťových firewallů), možnost realizace překladu adres a tím i skrytí celých podsítí. To vše při zachování nízkých finančních nákladů a malém navýšení požadavků na údržbu.



Obr. 7: Implementace s paketovým firewallem

2.6.2 Implementace s paketovým firewallem a proxy serverem

Toto řešení představuje předešlé zapojení s tím rozdílem, že je zde navíc zahrnut proxy server, viz Obr. 8. Ten je umístěn jako služba přímo na firewallu nebo za firewallem, tedy na straně LAN sítě, aby byl chráněn před případnými útoky z vnější sítě. Na proxy jsou pak směrovány pakety podporovaných protokolů a zbývající síťový provoz prochází jen paketovým filtrem. Výhodou proxy je zavedení vyšší bezpečnosti na daných protokolech. Ta je zajištěna autentizací a filtrací na vyšších vrstvách síťového modelu. Mezi nevýhody je možné uvést omezení proxy na konkrétní podporované protokoly. Navýšení zabezpečení se tedy týká pouze vybraných protokolů.



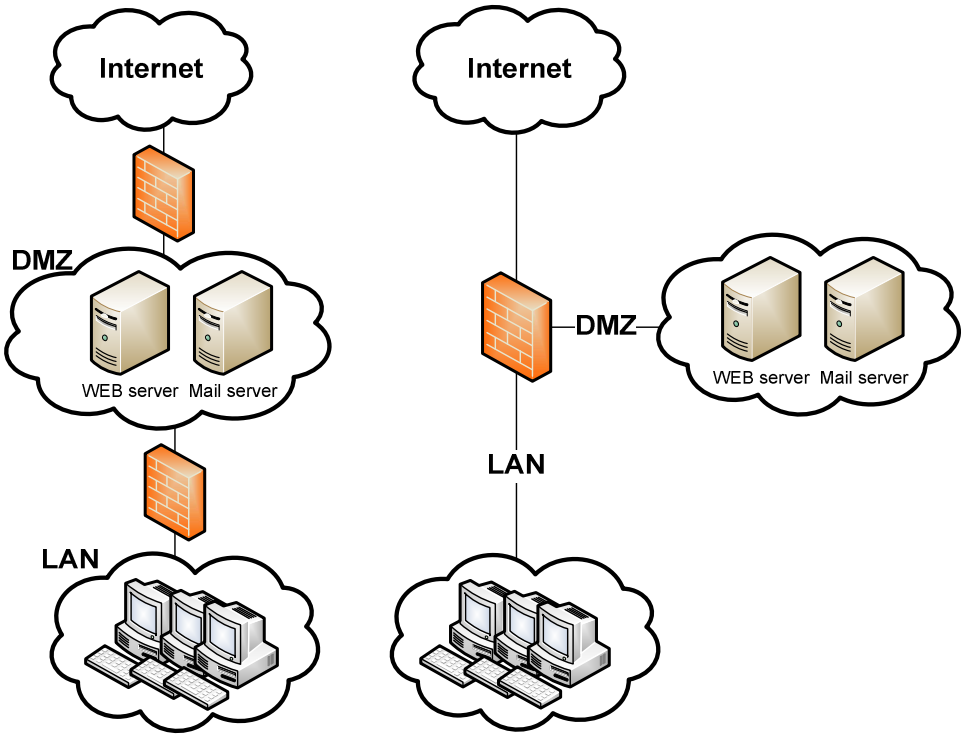
Obr. 8: Implementace s paketovým firewallem a proxy

2.6.3 Implementace s paketovým firewallem a DMZ

Tato implementace paketového firewallu do síťové topologie vytváří mimo oddělenou lokální síť ještě jednu podsíť. Tou je demilitarizovaná zóna, často nazývaná zkratkou DMZ. Je to podsíť, kde jsou zpravidla zapojovány zabezpečené systémy, jako jsou servery, které poskytují služby i pro vnější sítě. Důvodem vytváření těchto podsítí jsou rozdílné požadavky na bezpečnostní politiky firewallu a také bezpečnostní riziko, které by představovali systémy při zapojení do lokálních sítí. Případný útočník při úspěšném útoku dosáhne přístupu pouze do podsítě DMZ, která je tvořena zabezpečenými systémy a ne do celé lokální sítě.

Samotné vytvoření těchto podsítí může být zajištěno dvěma způsoby. První způsob je při použití dvou paketových filtrů, viz Obr. 9 a). Na prvním firewallu dochází k filtraci pro obě podsítě současně, avšak bezpečnostní politika firewallu musí povolit přístup ke službám provozovaných v DMZ. Tím by mohly vzniknout bezpečnostní díry nebezpečné pro LAN síť. Proto je dále zařazen druhý firewall, který je striktnější a nedostatky prvního firewallu vyfiltruje. Vzhledem k použití dvou firewallů při

přístupu z vnější sítě do LAN, přináší toto řešení vysokou míru zabezpečení. Nevýhodou je administrativní složitost, neboť při kaskádním spojení více firewallů je náročnější kontrola návaznosti pravidel tak, aby nedocházelo k filtraci požadovaných služeb. Druhý způsob je zobrazen na Obr. 9 b). Ten využívá pouze jednoho firewallu, který provádí i směrování do patřičné podsítě. Filtrace se tak pro LAN a DMZ provádí odděleně. Výhodou je jednoduchost a menší finanční náročnost.



a) b)

Obr. 9: Implementace DMZ: a) s dvěma paketovými firewally, b) s jedním paketovým firewallem

3 Audit informatiky

Auditem [1] je možné označit objektivní vyhodnocení kontroly informací a událostí s cílem zjistit soulad s dokumentovanými údaji, analyzovat rizika a informovat o současném stavu. Samotný audit představuje soubor činností prováděných nezávislými auditory pro stanovení rozdílu mezi současným stavem a kritérii stanovených před auditem. Proces těchto činností by měl být prováděn v souladu s metodickými postupy řízení kontroly a správy organizace. Výsledkem provedeného auditu by měla být podrobná závěrečná zpráva. Podle oblasti auditu informačních systémů je možné rozdělit na:

- Bezpečnostní audit - audit informačních systémů, penetrační testy, analýza rizik,
- technický audit – audit HW, audit SW, audit infrastruktury,
- legislativní audit - zákon 101/2000 Sb., zákon 365/2000 Sb., zákon 148/1998 Sb.).

3.1 Interní bezpečnostní audit

Interní audit je objektivní nezávislá činnost pro analýzu stavu bezpečnosti. Cílem je ujistit se, že ochrana systému je přiměřená k rizikům. Výsledkem je podklad pro vedení společnosti k zajištění optimalizace provozu, bezpečnosti a procesů. Prováděn je pověřenými odborně znalými zaměstnanci společnosti bez závislosti na externím subjektu.

3.2 Externí bezpečnostní audit

Externí audit je prováděn na základě objednávky externím subjektem. Jeho rozsah je dán potřebami společnosti nebo může být stanoven legislativou. Provedení je zajištěno specialisty nezávislé externí společnosti, kteří objektivně posuzují stav bezpečnosti pomocí auditu případně i penetračním testováním. To umožňuje posoudit i reakce administrátorů při reálných útocích. Výsledkem může být kromě závěrečné zprávy auditu i získání certifikovaného osvědčení o bezpečnosti systému.

3.3 Bezpečnostní audit

Z hlediska stále častějších případů narušení bezpečnosti informačních systému se stává bezpečnostní audit velice důležitou součástí práce IT oddělení. Jeho úkolem je analyzovat rizika, provádět kontrolu informačních systémů a provádět vyhodnocování v závislosti na bezpečnostních politikách společnosti. Cílem je minimalizace rizik různých typů napadení, odcizení či zničení dat. Úsilí vynaložené na bezpečnostní audit

by mělo zajistit maximální bezpečnost a zvýšit povědomí o bezpečnosti u jednotlivých pracovníků informačních technologií (správců systému) i uživatelů.

Samotný proces auditu se provádí fyzicky na zařízení. Podmínkou je plný přístup k zařízení zpravidla za asistence administrátora. Jedná se o neinvazivní metodu porovnáváním zjištěných hodnot k požadovaným nebo doporučovaným.

3.4 Penetrační testování

Penetrační test [1] je speciální technika při bezpečnostním auditu. Zhodnocení bezpečnosti probíhá pokusem o průnik metodami i použitými nástroji blízký reálnému útoku. Testy se provádějí na základě expertních zkušeností metodou "etického hackingu" a ve shodě s normami ČSN ISO/IEC TR 13335 a ČSN ISO/IEC 17799. Oproti klasickému auditu je testování prováděno ze vzdáleného počítače z internetu nebo z vnitřní sítě. Výsledkem je identifikování slabin a doporučení jak útokům zamezit. Též je možné touto metodou ověřit krizový plán a monitorovací systémy.

Postup při testování je následující:

- Shromažďování informací,
- pokusy o průnik do systémů,
- eskalace.

Při shromažďování informací probíhá identifikace aktivních zařízení, topologie a služeb. Důležitou součástí je také identifikace OS, výrobců síťových komponent atp. V této fázi je snaha o co nejdetailnější informace umožňující definovat slabiny vzdálené sítě. Poté pomocí získaných informací následují pokusy o průnik. Pokud se podaří proniknout na vzdálený systém, ale je získáno pouze částečné kontroly nad systémem, postupuje se do třetí fáze eskalace. Ta představuje postupné provádění pokusů vedoucích k získání co nejvyšší kontroly nad systémem. Nejčastěji pak k získání administrátorského oprávnění. Na konci se v případě reálného útoku provádí ještě promazání logů a odstranění stop z napadeného systému. Při penetračním testování se tento krok neprovádí. Případné záznamy mohou být dále použity k analýze a vyhodnocování.

4 Principy auditu firewallu

4.1 Analýza logů

Nejdůležitější částí bezpečnostního auditu je zajisté analýza logů. Logy většinou představují textové soubory, které obsahují záznamy o změnách konfigurací, zahozených nebo povolených komunikacích a incidentech. Zápis probíhá průběžně při provozu jednotlivých síťových prvků, jako jsou firewally, směrovače nebo systémy detekce narušení a průniku. Protože mohou být soubory s logy velice nepřehledné (mohou obsahovat i tisíce záznamů), vznikly programy, jež ulehčují jejich analýzu. Příkladem mohou být komerční aplikace AlgoSec Firewall Analyzer, Tufin SecureTrack nebo nekomerční Base, Acid, Fwlog atd.

V první fázi analyzátoru probíhá sběr logů podporovaných zařízení. Poté probíhá analýza parsováním logovacích souborů. Ty mohou mít různou strukturu, proto analyzátory umožňují zpracovat pouze logy konkrétních zařízení. Z firewallů jsou to nejčastěji následující:

- Check point – 1,
- Cisco PIX,
- Juniper,
- Syslog server.

Jako výstup jsou vytvořeny reporty přístupné převážně na webovém serveru. Součástí reportů může být i analýza rizik stanovující míru bezpečnosti.

4.2 Detekce bezpečnostních děr OS a služeb

Z hlediska komplexního auditu firewallu je nutné zahrnout do testování i operační systém firewallu a další poskytované služby. Pokud by nebyl OS firewallu dostatečně zabezpečen, mohlo by dojít k narušení bezpečnosti vedoucí i ke změně nastavení pravidel firewallu útočníkem. Bezpečnost OS a služeb je přitom závislá na počtu bezpečnostních děr.

Bezpečnostní díry jsou chybně napsané kódy aplikace způsobeny programátorem. Ty jsou odhalovány specialisty ze zdrojových kódů nebo pomocí reverzního inženýrství z kompilovaných aplikací. Pro danou aplikaci je poté vydána záplata, která danou chybu opravuje. Než je ale záplata vydána může dojít ke zneužití:

- Odepření služby tzv. Denial of Service,
- ovládnutí vzdáleného systému.

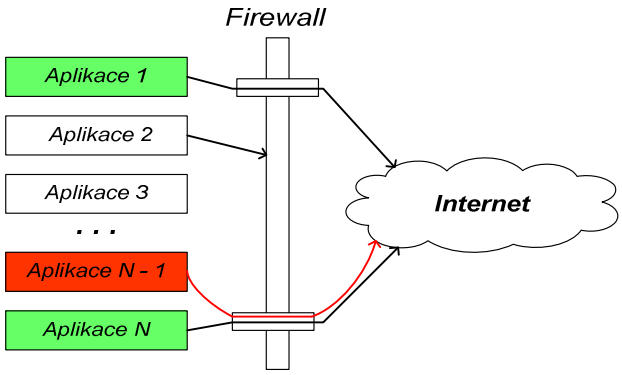
Z principu je zřejmé, že jednotlivé bezpečnostní díry jsou závislé na konkrétní verzi aplikace. Databáze obsahující verze těchto nebezpečných aplikací a signatury chyb je využívána programy pro detekci bezpečnostních děr. Ty provádějí skenování

vzdáleného systému a porovnávají spuštěný OS a služby se signaturami databáze. Z výsledků jsou vytvářeny reporty obsahující záznamy zneužitelných chyb testovaného systému.

Pro vlastní audit je možné využít programy detekující bezpečnostní chyby jako Tenable nessus, Microsoft Baseline Security Analyzer, OpenVAS. Pokud se provádí i penetrační testování, je možné otestovat zranitelnost pomocí Metasploit, milworm. Tyto nástroje je ale potřeba používat opatrně, neboť může dojít ke škodám na testovaných zařízeních.

4.3 Leak testy

Leak testy [9] představují malé nedestruktivní programy, které se pokoušejí obejít bezpečnostní politiky firewallu. Z principu činnosti vysvětleného dále se jedná především o testy firewallů personálních. Cílem těchto programů je otestování firewallu na odchozí spojení z počítače. Při správné činnosti firewallu je spojení při spuštění těchto testů blokováno. V opačném případě je možné zneužít takového chování firewallu pro funkčnost spyware programů a trojských koňů, které takto mohou odesílat data do sítě. Taková nová spojení nejsou firewallem identifikována jako nedůvěryhodná a v učícím režimu na ně neupozorní. To je způsobeno skrýváním se za jiné důvěryhodné procesy nebo zahájením spojení pomocí procesů, které mají odchozí spojení firewallem povoleno viz Obr. 10.



Obr. 10: Princip leak testů

Podle způsobu jak takového skrytí jednotlivé programy dosahují, je možné je rozdělit do následujících skupin:

- Substitution,
- launching,
- DLL injection,
- Code injection,
- Browser services,
- System services.

Příklady leak testů zobrazuje Tabulka 3. [5]

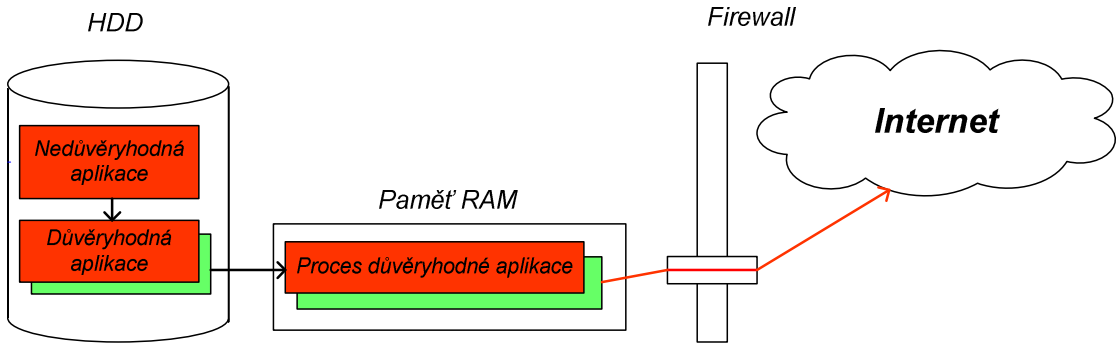
Tabulka 3: Leak testy

metoda	název testu
Subtitution	Runner LeakTest, Coat
Launching	Ghost, TooLeaky, Wallbreaker
DLL injection	FireHole, Jumper
Code injection	AWFT, CopyCat
Browser services	Breakout, OSfwbypass, PCFlank
System services	BITSTester, Breakout2, DNStester

4.3.1 Substitution leak testy

Substitution leak [9] testy využívají pro obcházení firewallu techniky substituce souborů nebo procesů. Důvěryhodné spustitelné soubory na disku nebo data důvěryhodných procesů v paměti RAM jsou zaměněny za nedůvěryhodné, viz Obr. 11.

.



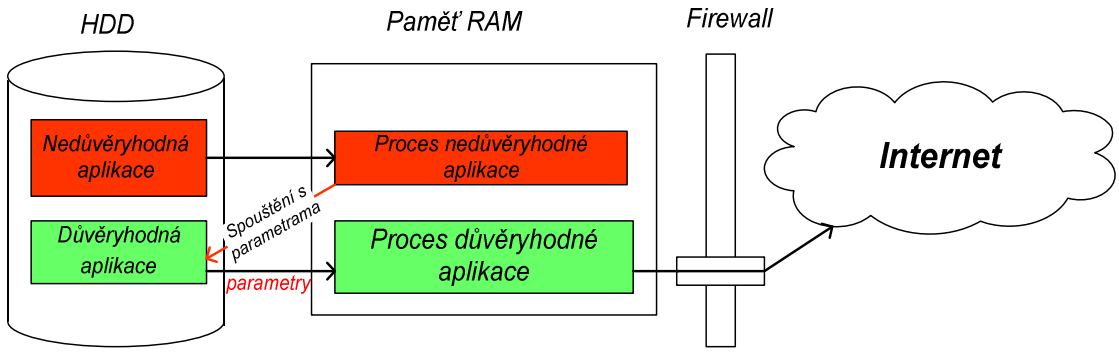
Obr. 11: Substitution Leak testy

Nevhodný firewall poté tyto programy posuzuje podle pravidel stanovených pro původní důvěryhodné programy. Metody jak dosáhnout substituce jsou následující:

- Záměna spustitelného souboru věrohodného procesu na disku,
- přejmenování nedůvěryhodného souboru jménem důvěryhodného,
- záměna dat důvěryhodného procesu zavedeného v paměti RAM za nedůvěryhodná.

3.3.2 Launching leak testy

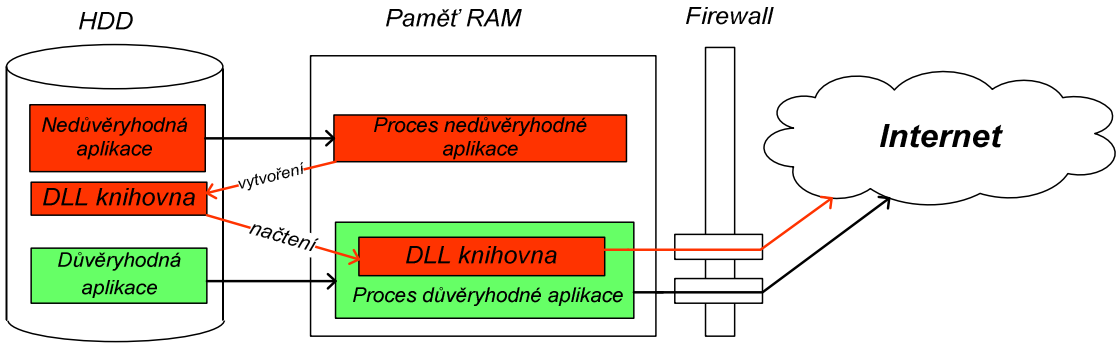
Základem této metody leak testů [9] je spouštění důvěryhodné aplikace pomocí příkazové řádky se zadáním dalších parametrů. Přes tuto spuštěnou aplikaci poté nedůvěryhodná aplikace odesílá svá data, viz Obr. 12. Nejčastějším případem je spouštění webového prohlížeče. Aby však uživatele neupozornilo podezřelé chování systému, je okno prohlížeče skryto.



Obr. 12: Launching leak testy

4.3.3 DLL injection leak testy

Metodou DLL injection [9] se injektuje nedůvěryhodná dynamická knihovna DLL do adresného prostoru důvěryhodného procesu, viz Obr. 13. To lze zajistit například modifikací systémového registru.

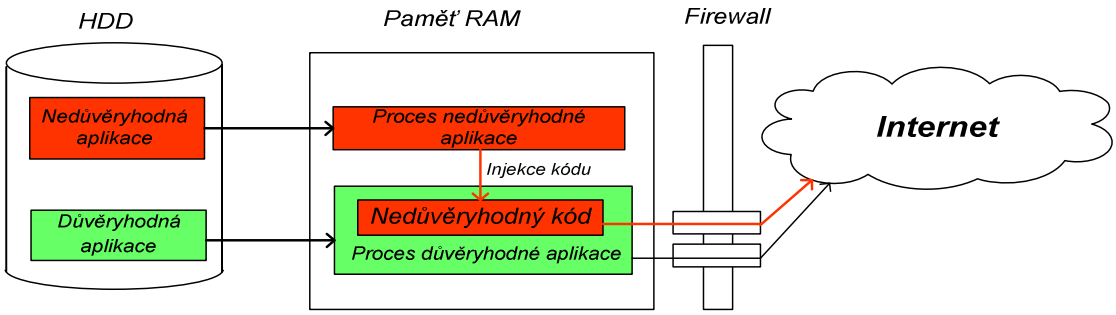


Obr. 13: DLL injection leak testy

4.3.4 Code injection leak testy

Metoda využívá injekci nevěrohodného programového kódu do adresného prostoru věrohodného procesu bez použití dynamické knihovny DLL [9]. Po zavedení kódu je inicializována síťová komunikace, na které nedůvěryhodná aplikace může odesílat data, viz Obr. 14. Pro injekci je možné využít několika způsobů:

- Nalezeni důvěryhodného procesu v paměti RAM a následně injekce kódu do tohoto procesu,
- zavedení důvěryhodného procesu do paměti RAM a v něm vytvoření nového vlákna,
- zavedení důvěryhodného procesu do paměti RAM a úprava paměti procesu.



Obr. 14: Code injection leak testy

4.4 Skenování portů

Skenování portů [7] je aktivní technika využívaná primárně pro testování koncových stanic sítě na otevřené TCP nebo UDP porty. Lze ji však použít i pro detekci pravidel personálního i síťového firewallu. Podle příznaku a portu odesílaného paketu je očekávána odezva v podobě zpět odeslaného paketu s určitým příznakem. Pomocí toho, zda daný paket je zpět odeslán a pomocí příznaku zpětně přijatého paketu, lze odvodit stav vzdáleného portu:

- Otevřený port,
- zavřený port,
- filtrovaný port,
- nefiltrovaný port.

Nejběžnějším typem skenování je za použití TCP handshake (TCP CONNECT skenování). Aby bylo možné získat co nejvíce informací a také aby skenování bylo skryto před systémy detekce narušení IDS a systémy detekce průniku IPS, vzniklo několik dalších typů skenování:

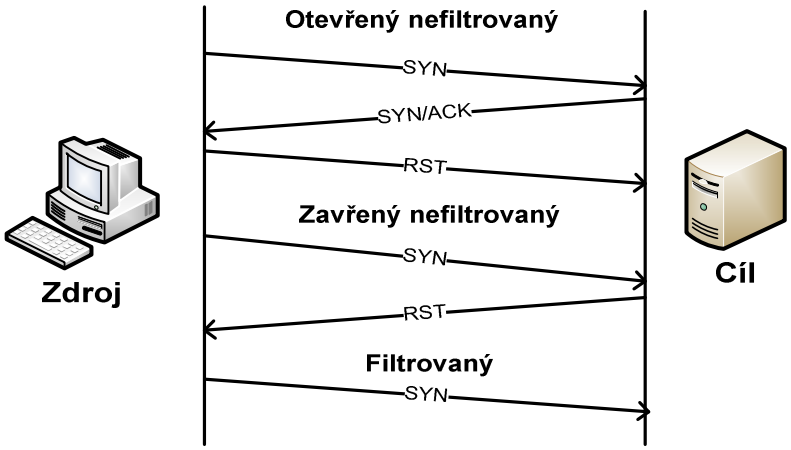
- TCP SYN skenování,
- TCP ACK skenování,
- TCP FIN skenování,
- TCP NULL skenování,
- TCP IDLE skenování,
- UDP skenování.

Nejpoužívanějším programem pro skenování portů je NMAP a Superscan. Výhodou NMAP je ale možnost stanovit typ skenování a provozovat jej na Linuxu i Windows, proto je pro testování firewallů vhodnější.

4.4.1 TCP SYN skenování

TCP SYN skenování oproti klasickému TCP CONNECT nevytváří úplné spojení na zadaný port. Z tohoto důvodu docházení k lepšímu skrytí. Pokud na vzdáleném systému probíhá logování navázaných spojení, toto skenování není zaznamenáno.

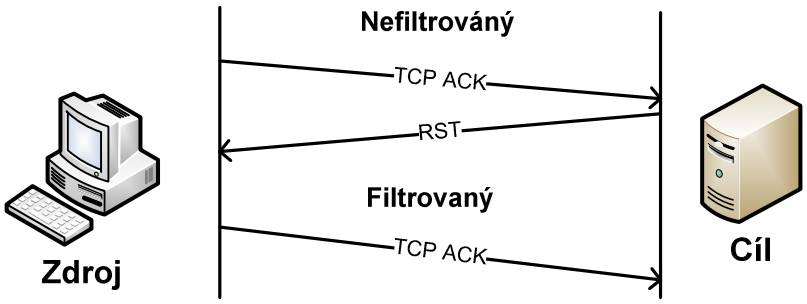
Při spuštění zašle na vzdálený systém na zadaný port paket s příznakem SYN. V případě otevřeného nefiltrovaného portu je zpět zaslán SYN/ACK, na který je reagováno paketem s příznakem RST. Pokud je zadaný vzdálený port uzavřen, nedojde k odpovědi paketem SYN/ACK avšak RST. Další možností je případ, kdy nepřijde žádná odpověď. V takovém případě je zadaný vzdálený port filtrován firewallem. Dané scénáře zobrazuje Obr. 15.



Obr. 15: SYN skenování

3.4.2 TCP ACK skenování

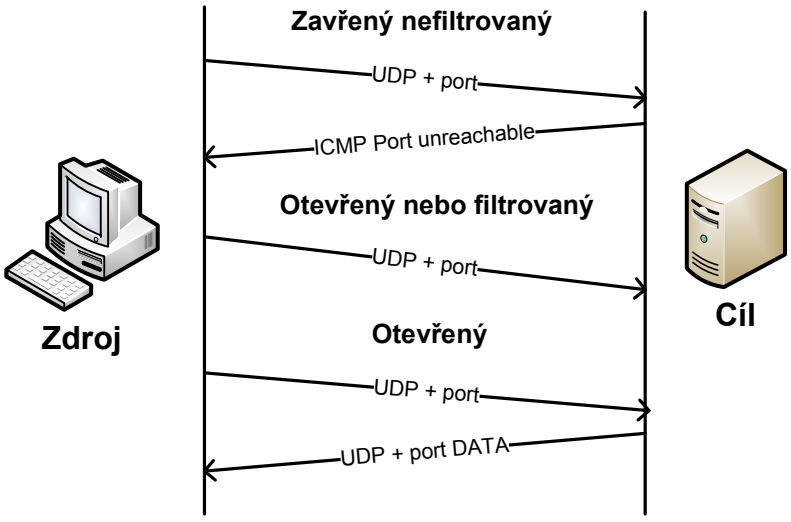
Tento typ skenování se používá převážně pro testování firewallu, protože nedetekuje jednoznačně, které porty jsou otevřené. Jeho cílem je zjistit, zda jsou dané porty filtrovány či nikoliv. Na vzdálený systém na zadaný port se odesílá paket s příznakem TCP ACK s náhodným sekvenčním a potvrzovacím číslem. V případě, že je port nefiltrovaný, vzdálený systém ho vyhodnotí jako nekorektní a zpět zašle odpověď RST. V opačném případě je port filtrovaný a odpověď nepřijde, viz Obr. 16.



Obr. 16: ACK skenování

4.4.3 UDP skenování

Mimo TCP skenování je často potřeba otestovat i UDP porty. To lze provést UDP skenováním viz Obr. 17. Na vzdálený systém se odešle UDP paket se zadaným portem. Pokud je port uzavřen, je zpět odeslána odpověď ICMP zprávou Port unreachable. Pokud odpověď žádná nepřijde, potom nelze jednoznačně definovat, zda je port otevřený nebo filtrovaný. Je to dáno tím, že na mnoha firewallech jsou ICMP zprávy blokovány. Pokud jsou odeslána ze vzdáleného systému nějaká data, jedná se o port otevřený.

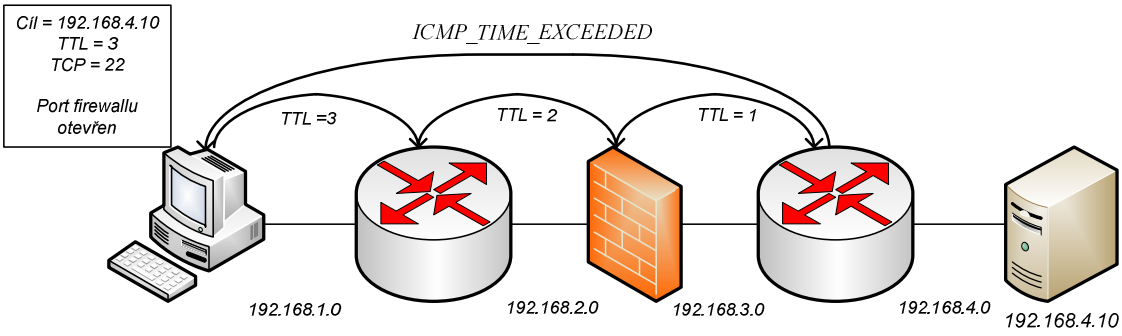


Obr. 17: UDP skenování

4.5 Detekce pravidel firewallu pomocí TTL

Detekce pravidel firewallu pomocí této metody [2] je zajištěna na principu počtů skoků. Každý paket vyslaný do sítě je limitovaný svým počtem skoků TTL, který může učinit. Skoky je tedy vyjádřen počet směrovačů či firewallů na své cestě k cíli. Průchodem přes tyto prvky se vždy toto číslo TTL o 1 sníží. Po překročení této hodnoty, tj. snížení na hodnotu 0, je paket zahozen a zpět vyslána zpráva

ICMP_TIME_EXCEEDED. V případě, že danému paketu je přiřazen i konkrétní TCP nebo UDP port, je možné tuto vlastnost použít pro detekci pravidel síťové firewallu viz Obr. 18.



Obr. 18: Detekce pravidel pomocí TTL

Vyslaný paket má zadán TCP nebo UDP port, který chceme na firewallu analyzovat, a dobu života paketu TTL. Hodnotu TTL je potřeba zvolit o 1 vyšší než je počet skoků k testovanému firewallu. Nyní mohou nastat dvě možnosti. V případě, že hodnota TTL je snížena na nulu, je vyslána chybová zpráva ICMP, což vypovídá o otevřeném portu na firewallu. Druhou možností je uzavřený port na firewallu, při kterém paket dále neprojde a je zahozen. Chybová zpráva ICMP přijata nebude. Při tomto testování jsou však potřeba splnit tyto podmínky:

- Znalost počtu skoků k firewallu,
- znalost IP adresy hosta za firewallem.

Pro testování touto metodou je možné použít programy firewalk nebo Hping2. Nevýhodou Hping2 však je možnost testování v jednom okamžiku jen jeden port. Též je nutné si uvědomit, že ani jeden z programů neumožňuje detekovat výpadky sítě a ztrátu paketů nezpůsobených filtrací firewallem nebo špatnou detekci způsobenou filtrací ICMP zpráv firewallem. Tudíž je možné v některých případech docházet ke zkreslení výsledků.

4.6 Testování hesel

Testování hesel se provádí k testování bezpečnosti samotného firewallu. Zabývá kontrolou síly hesel, použitých kryptografických algoritmů a způsobu jejich uložení. Jeho provádění je závislé na způsobu přístupu k systému. Testování lze provádět:

- Přímo v OS,
- vzdáleně přes síť.

Při přímém přístupu k operačnímu systému se provádí především kontrola hesel používaných k přístupu do OS. Posuzuje se způsob uložení hesel, typ použitého

kryptografického algoritmu a síla použitých hesel. Také se provádí kontrola na přítomnost standardních nebezpečných systémových účtů, jako jsou účty Guest nebo nobody.

V případě vzdáleného přístupu přes počítačovou síť se kontroluje síla hesel používaných pro autentizaci síťových služeb. Tento proces následuje po provedení skenování vzdáleného počítače, při kterém se detekují otevřené porty a identifikují se služby provozovaných na těchto portech. Protože je však možné, že vzdálený systém využívá některé z metod k zamezení zkoušení hesel. Tedy omezení počtu pokusů v časových intervalech, doporučuje se provádět toto testování v co největším časovém horizontu.

Metody jaké lze použít pro test síly hesel jsou následující:

- Využití slabin kryptografického algoritmu,
- Bruteforce metoda,
- test pomocí slovníku.

První metoda spočívá v dříve odhalených slabinách kryptografického algoritmu. Pokud se pro ukládání hesel používá již prolomeným bezpečnostních algoritmů, je možné získat hesla přímým dekódováním úložišť hesel.

Další metoda, též nazývaná jako metoda hrubou silou, provádí testování zkoušením všech možných kombinací. Před spuštěním se definují znaky, ze kterých bude heslo složeno, a počet znaků definující délku hesla. Poté se již provádí zakódování složených hesel patřičným algoritmem a porovnání s uloženým řetězcem, nebo častěji použití hesle tj. pokus zadáním (zkoušením) těchto hesel k přístupu.

Třetí metoda pro testování využívá vytvořeného slovníku. Ten představuje soubor s uloženými hesly, které jsou při testování zkoušeny. Hesla, která tento slovník obsahuje, jsou vybrána z obecně nejvíce používaných hesel.

5 Návrh auditu firewallu

5.1 Audit firewallu

Při kontrole bezpečnosti firewallu se mnozí administrátoři milně domnívají, že se jedná pouze o kontrolu nastavení pravidel filtrování. Kontrola pravidel je sice z hlediska funkce firewallu nejdůležitější, avšak audit firewallu představuje mnohem širší kontrolu. Nelze opomíjet i důležitost fyzické bezpečnosti, logování apod. Proto je vhodné zavést určitou metodiku postupu pro provádění auditu.

5.1.1 Metodika auditu firewallu

Jednotlivé body navrženého postupu jsou následující:

- Definice auditu a získání informací z dokumentace,
- řízení bezpečnosti a personální bezpečnost,
- kontrola firewallu,
- kontrola pravidel filtrování,
- kontrola údržby a monitorování,
- penetrační testování.

Na počátku auditu je nutné získat přehled o bezpečnostních politikách společnosti a síťové topologii. Je vhodné zjistit informace o IP adresách používaných v síti, poloze bezpečnostních prvků, SW vybavení i výrobcích síťových prvků. Tyto informace umožňují stanovit, co vše má být předmětem bezpečnostního auditu a vymezení způsobu kontroly případně penetračního testování. Informace jsou získávány z dostupné dokumentace nebo pohovorem s administrátory sítě.

V druhé části se provádí kontrola řízení bezpečností a personální bezpečnost. Ta spočívá v kontrolách nařízení a pravidel stanovených managementem. Také se kontroluje dostupnost těchto dokumentů. Součástí je také kontrola, zda jsou zaměstnanci řádně školeni a přiřazení odpovědnosti.

V další části je prováděna kontrola firewallu. Zde je kontrolována fyzická bezpečnost. Dále je posuzován logický přístup a autentizace. To je prováděno pro lokální přístup i pro vzdálený přístup k zařízením po síti. Součástí je také analýza bezpečnosti operačního systému, na kterém je firewall provozován.

Kontrola pravidel firewallu představuje samostatnou část auditu. Každé pravidlo je posuzováno individuálně. Jeho použití musí být odůvodnitelné a vyhovovat bezpečnostním politikám zavedených ve společnosti. Pro budoucí monitorování je kontrolováno používání pravidel s logováním.

Poslední fáze obsahuje kontroly údržby a monitorování. Zde jsou obsaženy kontroly zálohování, způsoby kontrol logů.

Volitelná nebo také samostatná fáze stanovuje testování a skenování technikou penetračního testování ze vzdálené sítě či lokální sítě. Probíhá za použití nástrojů umožňující aktivní kontrolu a testování blízké reálnému útoku. Jsou použity techniky skenování, detekce bezpečnostních děr operačního systému a způsoby průniku do systému.

5.1.2 Návrh procedury

Po stanovení metodiky testování je nyní potřeba vytvořit proceduru auditu. Ta má definovat jednotlivé kroky provádění auditu. Jejich účelem je přesně stanovit doporučený postup pro kontrolu bezpečnosti. Takto je možné zamezit opomenutí některé části kontroly, která by mohla negativně ovlivnit výsledky auditu. Vzniklé procedury budou sloužit auditorům jako průvodce procesem kontroly. Pro vytvoření procedury auditu byla vytvořena následující struktura.

Cíl kontroly: V systému nejsou spuštěny nepotřebné síťové služby.
Provedení kontroly: Na testovaném systému pomocí příkazu netstat -an.
Nálezy: Chyba - Je spuštěna nebezpečná aplikace telnet na portu 23.

Struktura obsahuje definici co je předmětem testování a pokud je to možné, definuje se i doporučený způsob provedení kontroly nebo přibližná podoba konfigurace, která by měla být použita. Ta však nemusí být v reálném provozu totožná, avšak měla by mít stejné typické znaky. Vytvářen je pro použití na OS linux. Přesto je nápomocný i pro ostatní systémy, neboť odborně znalému auditorovi lépe definuje co přesně je cílem kontroly a také danou kontrolu umí převést pro požadovaný systém. Výsledkem je zápis nálezů provedený auditorem. Ty slouží pro vyhodnocení auditu tak i jako podklady k zajištění změn vedoucích k lepšímu zabezpečení.

5.2 Postup penetračního testování firewallu

Proces penetračního testování je volitelná speciální metoda auditu, kterou je možné použít i samostatně. Jeho základní postup byl již popsán v kapitole 3.4. Další vymezení podrobnějšího postupu je pak závislé na definici cílů a typu penetračního testování. V našem případě se jedná o nejčastější typ testování z vnější sítě a kontroly, kde je cílem prověřit síťový stavový firewall s demilitarizovanou zónou využívající NAT. Proto byly vytvořeny následující moduly testů:

- Průzkum vzdálené sítě,
- testování firewallu,

- skenování, identifikace operačního systému a služeb firewallu,
- testování hesel,
- testování bezpečnostních děr.

Bližší popis je uveden v následujících podkapitolách shrnující metodiku testů vycházejících z OSSTMM 2.2 [6].

5.2.1 Průzkum vzdálené sítě

Na počátku penetračního testování jsou definovány sítě a systémy určené k testování. Ty jsou dány smlouvou (externí audit) nebo interními předpisy (interní audit), avšak obsahují pouze základní informace, jako jsou IP adresy nebo jejich rozsahy. Pro získání více informací o síti včetně možných slabin i hesel se využívá techniky průzkumu sítě. Ta lze nejlépe definovat jako kombinace sběru dat, informací a politik řízení bezpečnosti ve společnosti. Využívá veřejně přístupných informací, které lze získat z internetových diskuzí, webů, sociálních sítí, internetových systémů apod. Získané informace pak slouží k lepšímu přehledu o vzdálené síti a napomáhá při dalším postupu penetračního testování. Mezi základní úkoly této části patří:

- Identifikace tras ke vzdálené síti,
- kontrola registrací rozsahů IP adres,
- analýza záznamů DNS serverů,
- získaní informací z internetu – např. google-hacking.

5.2.2 Testování firewallu

Je cílený test na systémy zajišťující funkci síťového firewallu. Zabývá se identifikací pravidel řízení komunikace mezi lokální sítí, DMZ sítí a internetem. Tento test tedy mimo jiné identifikuje systémy dostupné a napadnutelné z vnější sítě. Součástí je i kontrola nežádoucí propustnosti firewallu při různých technikách skenování a odolnost vůči technikám DoS útoku. Úkoly testování firewallu jsou:

- Identifikace typu firewallu podle specifických znaků,
- kontrola poskytování NATu,
- detekce pravidel firewallu pomocí TTL,
- kontrola nežádoucí propustnosti paketů skenováním s různými příznaky,
- kontrola odolnosti na DoS útok.

5.2.3 Skenování, identifikace OS a služeb firewallu

Tento modul je zařazen z důvodu kontroly bezpečnosti samotného firewallu a možností jeho zkompromitování. Účelem testů je zajištění základních informací, identifikace OS a služeb systému pro další testování za použití techniky skenování. Skenování firewallu probíhá na síťové a transportní vrstvě pro identifikaci otevřených portů. Jejich srovnáním se standardními porty lze identifikovat služby provozované na tomto systému. Po připojení na tyto služby lze dále v některých případech získat přehled o verzi programu zajišťující službu, instalovaných záplatách nebo také podle specifických portů a odezvy na daných portech identifikovat provozovaný operační systém. Jednotlivé úkoly jsou:

- Skenování portů firewallu,
- porovnání otevřených portů se standardními službami na daných portech a identifikace služeb,
- identifikace aplikace zajišťující službu včetně označení verze a instalovaných záplat,
- identifikace typu OS, verze OS a instalovaných záplat.

5.2.4 Testování hesel

Tato část se zabývá kontrolou hesel a použitých kryptografických algoritmů. Protože v našem případě se provádí kontrola firewallu z vnější sítě, omezuje se testování na kontrolu síly hesel síťových služeb. Kontrola kryptografických algoritmů a louskání hesel ze souborů, jako je typická kontrola hesel operačního systému, by byla možná až v případě hloubkové kontroly již při narušení bezpečnosti a získání přístupu do systému. Kontrola testování hesel spočívá v použití metody louskání hesel. To může být pomocí slovníkového útoku nebo metodou hrubé síly, kdy se zkoušejí všechny možnosti z daného rozsahu znaků. Další možností je také kontrola výchozích hesel síťových zařízení využívající vzdálené řízení. Ty jsou zaváděny výrobci těchto zařízení pro prvotní konfiguraci. Úkoly tohoto modulu jsou:

- Kontrola použití výchozích hesel,
- louskání hesel slovníkovou metodou,
- louskání hesel hrubou silou.

5.2.5 Testování bezpečnostních děr

Přestože kontrolovaná hesla v předešlém testu mohou být dostatečně bezpečná, provozování dané síťové služby může být nebezpečné. Příčinami jsou případné

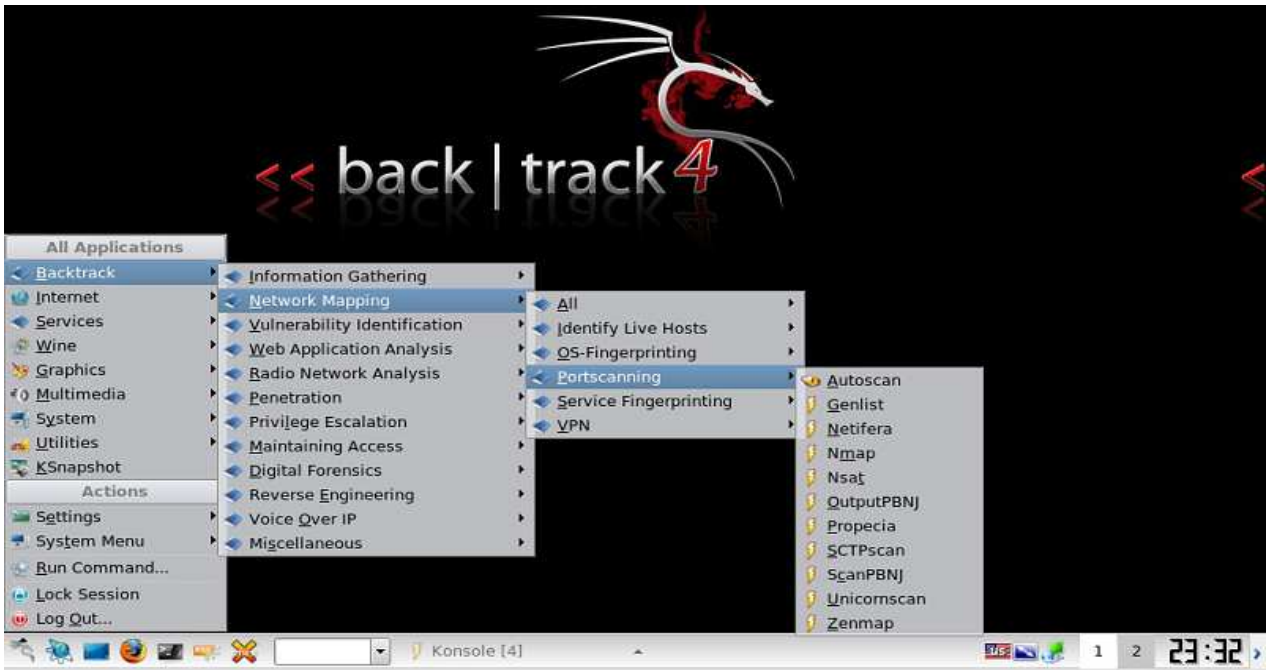
bezpečnostní díry dané verze aplikace poskytující službu. Ty jsou způsobeny chybným zápisem programového kódu. Pro jejich odhalení se používají skenery obsahující databázi s typickými signaturami a seznam postihnutelných verzí. Úkoly tohoto modulu jsou:

- Kontrola bezpečnostních děr OS,
- kontrola bezpečnostních děr aplikací poskytujících síťové služby.

5.3 Programy pro penetrační testování

5.3.1 Backtrack 4

Za operační systém pro proces auditu, který umožňuje i penetrační testování byl zvolen **Backtrack 4** viz Obr. 19. Tento OS je dostupný z www.remote-exploit.org.



Obr. 19: Backtrack 4

Je to linuxový operační systém postavený na distribuci **ubuntu** vytvořený speciálně pro audit a penetrační testování. Jedná se o velice uznávaný systém v řadách systémových administrátorů a etických hackerů. Oproti jiným operačním systémům obsahuje celou řadu aplikací pro skenování, testování hesel, odchytávání paketů, detekci bezpečnostních děr apod. Systém je vytvořen na **kernelu 2.6.29.4** s upravenými ovladači, díky kterým je možné použít například i packet injection ve wifi sítích. Jako grafické rozhraní používá stabilní **KDE 3.5.10.** Přestože v základním nastavení je spouštěn na úroveň 3, tj. bez grafického rozhraní s přístupem na síť, po spuštění systému a zadání uživatelského jména a hesla jej lze spustit příkazem **startx**. Poté je

doporučeno připojit se k síti, aktualizovat databázi balíčků a následně provést aktualizaci systému.

ifup eth0
apt-get update
apt-get upgrade

5.3.3 NMAP

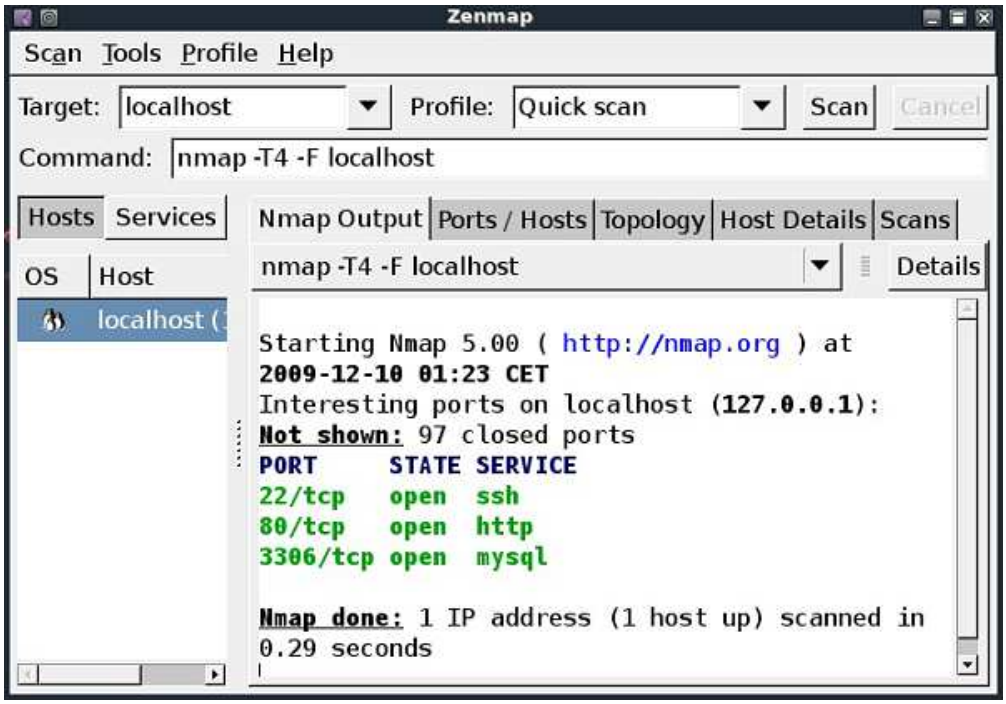
SYNTAXE:
nmap [<Scan Type> ...] [<Options>] { <target specification> }

NMAP - Network Mapper [6] dostupný z www.nmap.org je jedna z nejznámějších a nejuznávanějších open-source aplikací pro skenování v OS Linux i Windows. Byla vytvořena pro testování rozsáhlých sítí i jednotlivých hostů. Jeho předností je jednoduché použití a velké možností nastavení. Umožňuje vytvářet pakety s obsahem definovaným uživatelem jako je například definování příznaků nebo velikost paketů.

Instalace se provádí pomocí příkazu **apt-get**.

apt-get install nmap

Systém sám vyhledá nejnovější verzi (v současné době v repositářích **backtrack 4** verze **NMAP** 5.00) a tu nainstaluje včetně závislostí. Pokud je aplikace již instalována, avšak ve starší verzi než je v repositáři, dojde k jeho aktualizaci. Instalovaný balíček již obsahuje konzolovou aplikaci i grafické rozhraní nazvané **Zenmap** viz Obr. 20.



Obr. 20: Zenmap

Možnosti ovládání přes grafické rozhraní je identické jak v konzolové aplikaci, avšak vyniká svou přehledností výstupů skenování.

Zenmap je možné využívat hned po instalaci, neboť již obsahuje profily skenování. Ty obsahují, jakým způsobem se bude skenovat. Přesto je vhodnější vytvořit vlastní profily, které budou více vyhovovat potřebám auditora. To je možné provést v položce menu **Profile – New profile or command.** Nově vytvořený profil je poté možné vybrat v rolovací nabídce **Profile.** Definování cílů skenování se provádí do rolovací nabídky **Target.** Výsledný příkaz, jak by jej bylo potřeba zapsat v konzolové aplikaci pro dané nastavení je zobrazeno v editačním poli **Command**. Skenování je nyní možné spustit se tlačítkem **Scan** a výsledky se zobrazí ve spodní části programu.

5.3.4 Firewalk

Syntax:
firewalk -p [protocol] -d [destination_port] -s [source_port] [internal_IP] [gateway_IP]

Firewalk je aplikace umožňující kontrolu pravidel síťového firewallu. Funguje na principu uvedeném v kapitole 4.5 Detekce pravidel firewallu pomocí TTL. Protože tato aplikace není součástí distribuce Backtrack, je potřeba jej doinstalovat. Současná verze dostupná z openwall.net je **firewalk 5.0**. Aplikace nemá binární balíček, proto je

nutné instalovat ze zdrojových kódů. Před jeho instalací je zapotřebí splnit závislosti instalací **libnet**, **lipcap**, **libdnet**. To lze provést instalací binárních balíčků dostupných z repositářů.

apt-get install libpcap0.8-dev libnet1-dev libdnet-dev libdumbnet1-dev

Stažené zdrojové kódy následně rozbalíme a přepneme se do rozbaleného adresáře.

tar –zxf firewalk.tar.gz
cd Firewalk

Kompilace aplikace se provádí známými příkazy, které jsou postupně zadávány.

./configure
make
make install

Tímto je aplikace nainstalována. Aplikace se používá v konzoli s definováním parametrů podle potřeb testování. Součástí aplikace je i nápověda, kterou je možné zobrazit příkazem **man firewalk**.

5.3.5 Nessus

Tenable nessus 4.2 je komerční aplikace pro hledání bezpečnostních děr založená na principu klient-server. Je vytvořena pro použití na operačním systému Linux i Windows. V našem případě, kdy je využíváno pro audit operačního systému Linux je instalace prováděna pomocí balíčku Nessus-4.2.0-ubuntu804_i386.deb dostupného z www.nessus.org.

dpkg –i Nessus-4.2.0-ubuntu804_i386.deb

Po instalaci je nutné na webových stránkách Tenable souhlasit s licenčními podmínkami a nechat si vygenerovat aktivační kód. Ten je potřeba vložit do systému, aby aplikace nessus mohla stahovat testovací moduly.

/opt/nessus/bin/nessus-fetch –register <Aktivační kód>

Dále před spuštěním serverové části programu vytvoříme uživatele, který bude mít umožněno vytvářet testovací profily, definovat PC k testování a spouštět testy.

Po zadání příkazu zvolíme uživatelské jméno, heslo a odsouhlasíme přidělení administrátorských práv.

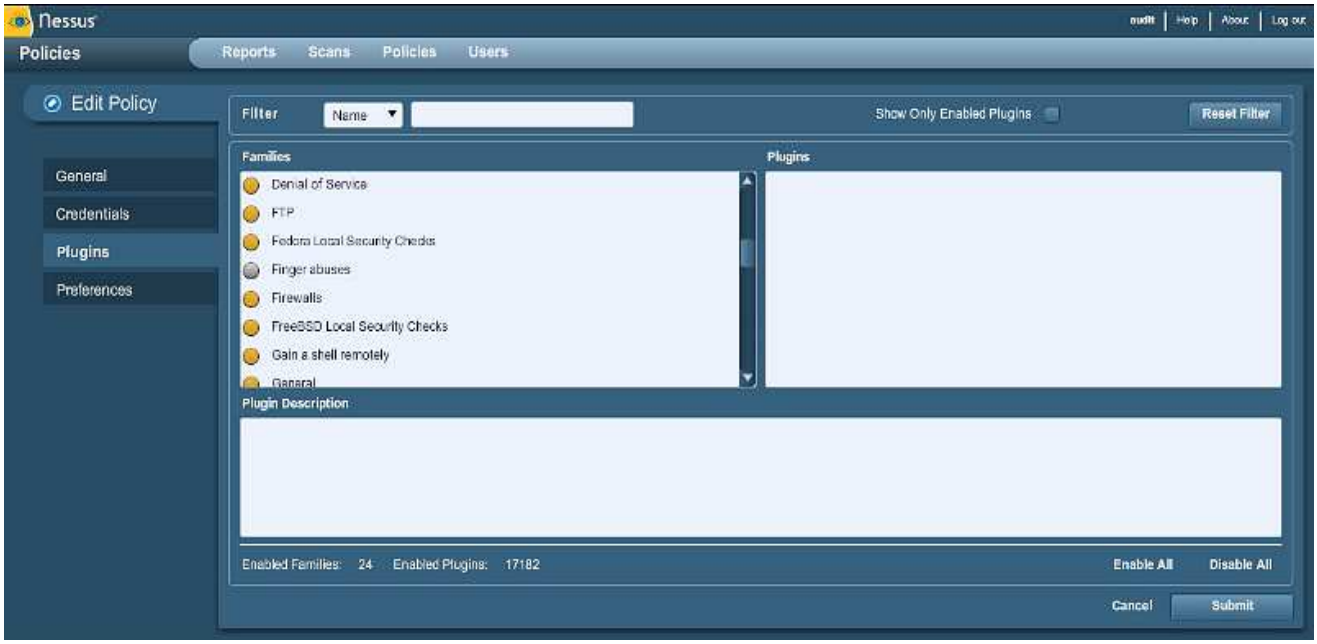
/opt/nessus/sbin/nessus-adduser

Poté aktualizujeme testovací moduly a spustíme serverovou část aplikace nessus.

/opt/nessus/sbin/nessus-update-plugins
/opt/nessus/sbin/nessusd

Tímto je serverová část připravena.

Nyní je možné přistoupit k testování. K serveru je možné připojit se pomocí konzolové aplikace nebo použít komfortnější přístup přes webové rozhraní na adrese serveru na portu 8834 viz Obr. 21.



Obr. 21: Webové rozhraní nessus

Bezpečnost webového rozhraní je řešena přístupem přes HTTPS a identifikací uživatele vytvořeným uživatelským jménem a heslem. Přes něj je možné kompletně spravovat aplikaci nessus. Položky správy jsou:

- Users – správa uživatelů nessus,
- Policies – nastavení testovací profilů,
- Scans – definice testů,
- Reports – výsledky testů.

Nejdříve je nutné vytvořit testovací profil v položce **Policies**. Zde se vybere název, způsob testování a testovací moduly podle typu zařízení, operačních systémů a služeb. Dále v položce **Scans** stanovit rozsah IP adres počítačových systémů a sítí, které mají být testovány. Zde je také přidělen testovací profil. Takto připravený test je možné již spustit. Zobrazení výsledků je možné v položce **Reports**.

5.3.6 Metasploit

Metasploit je open-source bezpečnostní aplikace pro OS Linux i Windows, kterou lze použít pro penetrační testování. Umožňuje získat kontrolu nad vzdáleným počítačem metodou exploitace. Tj. metodou zneužívající bezpečnostních děr v OS a službách. Instalační balíčky jsou dostupné na webových stránkách projektu http://www.metasploit.com/. Lze instalovat balíček framework-3.3.2-linux-i686.run, který má obsaženy i veškeré závislé balíčky. V našem případě je **metasploit** zahrnut i v repositářích, proto je možné instalovat pomocí **apt-get**.

apt-get install framework3

Poté lze již aplikaci spustit. Framework obsahuje několik typů rozhraní. Je možné si vybrat mezi:

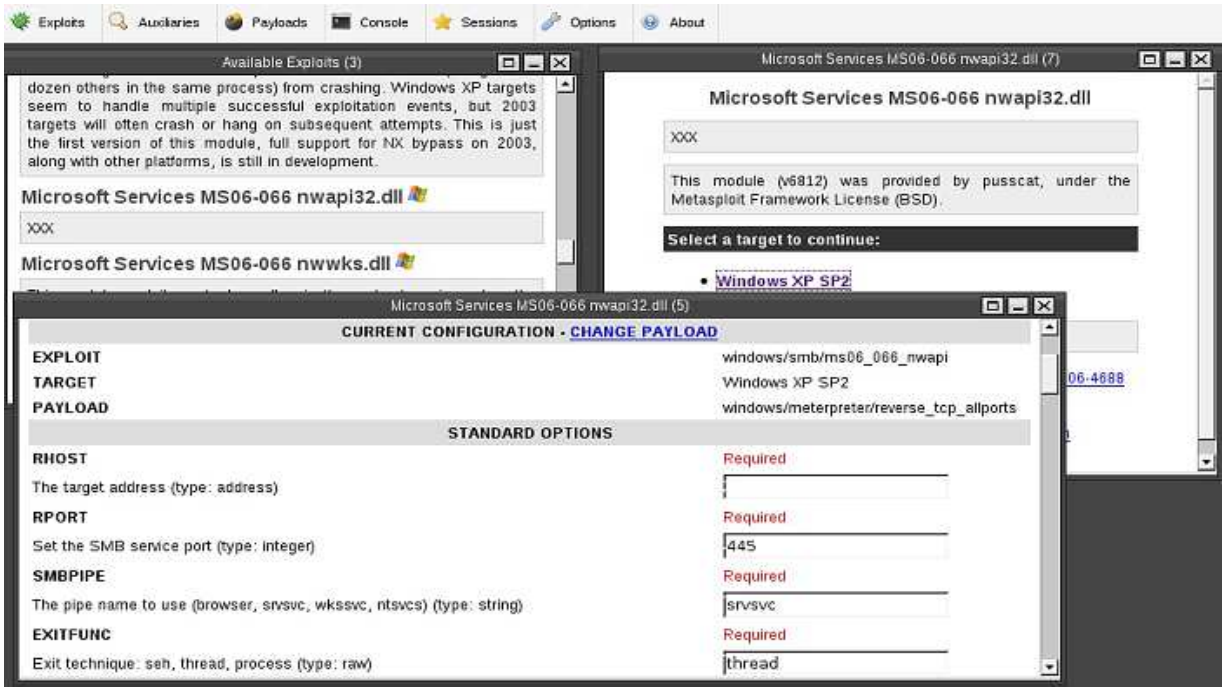
- Msfcli – příkazový interpret,
- msfconsole – konzolová aplikace,
- msfgui –grafické rozhraní,
- msfweb – webové rozhraní.

Pro snadnější používání a přehlednost je nejvhodnější použít grafické nebo webové rozhraní. Protože je ale grafické rozhraní méně stabilní, bylo vybráno webové. Po spuštění je vytvořen webový server naslouchající na portu 55555 na lokálním síťovém rozhraní loopback. K přístupu se používá webový prohlížeč se zadanou adresou **localhost:55555**.

cd /pentest/exploits/framework3
./msfweb

Webové rozhraní viz Obr. 22 obsahuje ve svém menu několik položek. **Exploits** slouží pro nastavení a spouštění exploitů. To se provádí vyhledáním konkrétního modulu. Ten je dále nutné nastavit podle cíle útoku a je mu přiřazen určitý zapouzdřený program payload. Po spuštění proběhne pokus o zneužití. Jestliže proběhne útok úspěšně, je výsledek s odkazem na vytvořený komunikační kanál daný payloadem zobrazen v menu **Session**. V **Auxiliares** jsou moduly, které slouží pro skenování, Denial of

Service apod. Další položka **Payloads** obsahuje jednotlivé kódy, které je možné zapouzdřit do exploitů. Ty slouží jako komunikační kanál mezi obětí a útočníkem. Pod položkou **Console** je možné vyvolat konzoli **metasploit**. Jedná se o konzoli jak je známo v případě spuštění **msfconsole** .



Obr. 22: Metasploit – webové rozhraní

5.3.7 Ostatní programy

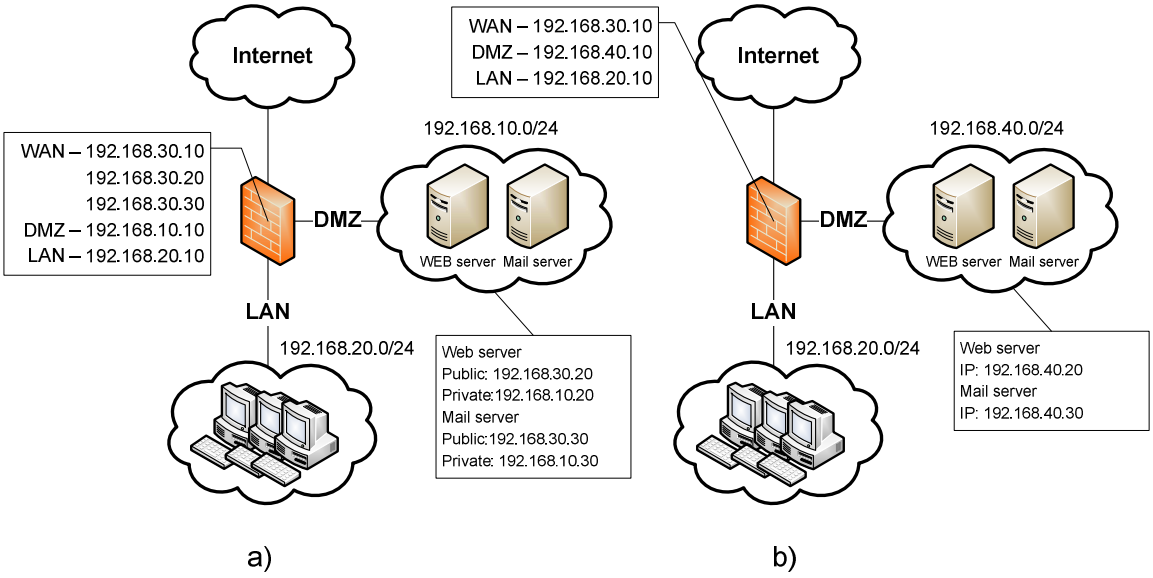
Pro penetrační testování se mimo uvedené používá mnoho dalších různých programů. Mnoho z nich je již v operačním systému backtrack nainstalováno a připraveno k použití. Jejich užití je především prostřednictvím příkazové řádky. Protože je jejich použití velice jednoduché a závislé pouze na patřičné syntaxi programu, nejsou v této práci popisovány. Z těchto programů, některých použitých i v následujícím penetračním testu, je možné jmenovat například:

- Whois, traceroute,ping, dnsenum – pro zjištění informací o vzdálené síti,
- Hping, Nemessis – pro skenování,
- Hydra, John, Medusa – pro testování hesel,
- OpenVas – pro identifikaci bezpečnostních děr.

6 Audit a penetrační testování firewallu experimentální sítě

6.1 Topologie experimentální sítě

Sestavení experimentální sítě a firewallu pro testování vychází ze zadání práce. Jedná se tedy o síť s typickými požadavky malých až středních společností. Ty zahrnují zapojení jednoho síťového stavového firewallu ve funkci brány poskytující připojení lokální sítě, veřejně dostupných serverů a překlad adres NAT. Typické topologie takové sítě jsou zobrazeny na Obr. 23.



Obr. 23:Experimentální síť a) s privátními adresami b) s veřejnými adresami v DMZ

Rozdílem těchto dvou topologií je použití typu adres v DMZ zóně. V prvním případě, viz Obr. 23 a), je použito privátních adres 192.168.10.0/24. Proto se na výstupu provádí statický NAT s překladem na definovanou veřejnou adresu[1]. Naproti tomu v druhém případě, Obr. 23 b), je využíváno veřejných adres 192.168.40.0/24[1]. Z tohoto důvodu je prováděno přímo přesměrování z vnější sítě do DMZ. V sestavované experimentální síti jsou užity obě řešení v závislosti na použitém konfiguračním nástroji pro nastavení firewallu, viz kapitola 6.2.1 a kapitola 6.3.1. V lokální síti je použito jednotně privátních adres s překladem adres NAT.

Z pohledu přístupu a poskytování služeb pro nastavené sítě je vyžadováno, aby bylo možné z lokální sítě přistupovat k webovým službám a provádět update operačního systému. Ostatní služby pro lokální síť z vnější sítě nejsou vyžadovány, neboť

[1] Ve skutečnosti se jedná o privátní adresy, avšak pro naši experimentální síť budou zastupovat adresy veřejné.

standardně vyžadovaná služba email je dostupná z DMZ zóny a zbývající komunikace není většinou pro běžnou práci zapotřebí. Aby bylo možné k firemní poště přistupovat i z internetu, je tato služba zpřístupněna do vnější sítě. Pro komunikaci mezi mailovými severy je povolena odchozí komunikace ze serveru do internetu. Dále je ještě zpřístupněn pro lokální síť i vnější síť firemní webový server. Ostatní servery jako LDAP, DHCP, adresářové servery apod. jsou umístěny uvnitř lokální sítě. Proto se na firewallu vzhledem k těmto službám nic nenastavuje. V některých případech se pro lepší administraci a řízení sítě povolují do DMZ a z jednotlivých sítí ještě některé icmp pakety. Nejčastěji potom ping nebo traceroute. Jejich použití, kromě vybraných typů, jako je icmp-redirect, se nepovažuje za vážné bezpečnostní riziko. Přesto je dobré zvážit jejich použití vzhledem k možnostem mapování sítě. Pro administraci se povoluje port 22 pro ssh nebo 3389 pro terminal services, případně jiný v závislosti na použitém operačním systému firewallu nebo možnostech administrace. Výsledné minimální požadavky na nastavení firewallu shrnuje Tabulka 4.

Tabulka 4: Požadavky na nastavení firewallu

Zdroj	Cíl	Typ	Port	Poznámka
Any	Firewall	tcp	22	ssh
Any	Firewall	icmp	echo-request	ping
Firewall	Any	any	any	Established, Related
Lan	Wan	tcp	80, 443	HTTP, HTTPS, OS update
Lan	Wan	udp	53	DNS
Lan	Wan	icmp	echo-request	ping
Wan	Lan	any	any	Established, Related
Lan	mail_server_dmz	tcp	25, 465, 110, 143, 993, 995	SMTP, SMTPS, POP, IMAP, POPS, IMAPS
Lan	mail_server_dmz	tcp	80, 443	webové rozhraní
Lan	web_server_dmz	tcp	80, 443	HTTP, HTTPS
Lan	Dmz	icmp	echo-request	ping
Dmz	Lan	any	any	Established, Related
Wan	mail_server_dmz	tcp	25, 465, 110, 993, 143, 995	SMTP, SMTPS , POP, POPS, IMAP, IMAPS
Wan	mail_server_dmz	tcp	80, 443	webové rozhraní
Wan	web_server_dmz	tcp	80, 443	HTTP, HTTPS
Wan	Dmz	icmp	echo-request	ping
Dmz	Wan	any	any	Established, Related
mail_server_dmz	Wan	tcp	25, 456	SMTP, SMTPS - mail to mail
Wan	Dmz	tcp	25, 456	SMTP, SMTPS Established, Related

6.2 Bezpečnostní audit linuxového firewallu

6.2.1 Konfigurace linuxového firewallu

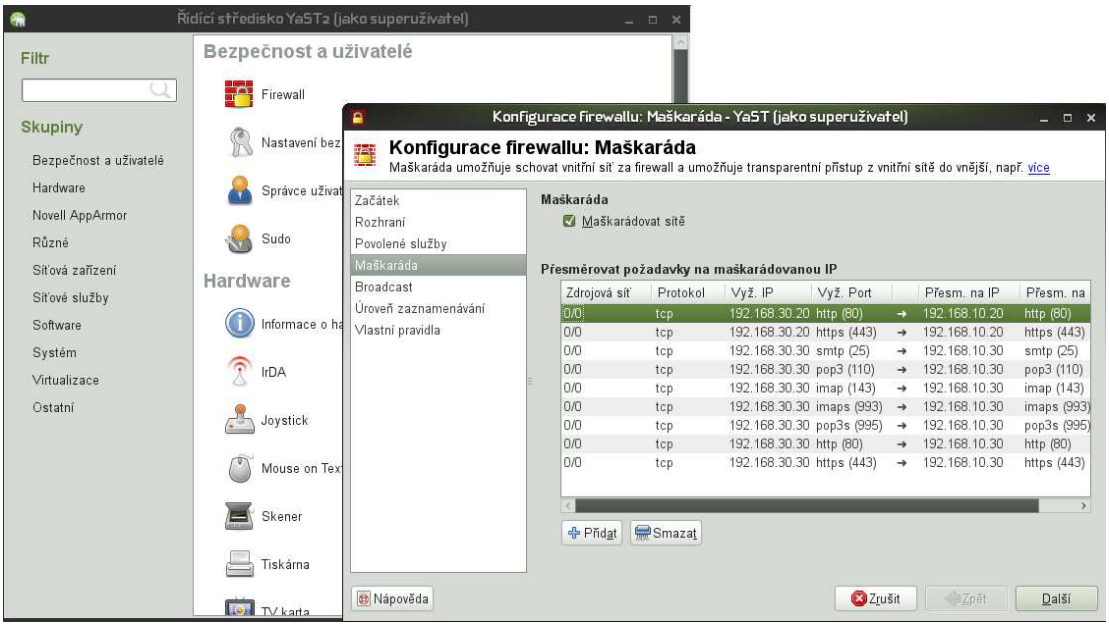
Jako zástupce nekomerčního firewallu byl vybrán iptables firewall provozovaný na linuxové distribuci opensuse 11.2 x64 v základní instalaci. Při té byl nainstalován i ssh server nastavený pro automatické spouštění naslouchající na všech rozhraních. Kromě nastavení síťových rozhraní a brány tento systém nebyl žádným dalším způsobem upravován ani zabezpečován.

ifconfig eth0 192.168.30.10 netmask 255.255.255.0
ifconfig eth0:web 192.168.30.20 netmask 255.255.255.0
ifconfig eth0:mail 192.168.30.30 netmask 255.255.255.0
ifconfig eth1 192.168.10.10 netmask 255.255.255.0
ifconfig eth2 192.168.20.10 netmask 255.255.255.0
route add default gw 192.168.30.2

Tím je zajištěno, že je operační systém v základním nastavení a je totožný případům, kdy je takový firewall nasazen v reálném provozu při čisté instalaci. Samotná konfigurace firewallu je možná několika způsoby:

- Pomocí příkazové řádky – *iptables, iptables-save, iptables-restore,*
- editací konfiguračních souborů – *SuSEfirewall2, SuSEfirewall2-custom,*
- nebo pomocí konfiguračního nástroje – Yast modul firewall.

Pro naše řešení byl použit modul firewall konfiguračního nástroje Yastu, viz Obr. 24, kdy byla provedena konfigurace pro použití privátních adres v DMZ (z důvodu omezených možností konfiguračního nástroje) a tak, aby byla zajištěna co největší shoda s požadavky na povolené služby, viz kapitola 6.1.



Obr. 24: Yast – modul firewall

Důvodem využití tohoto nástroje je časté použití tohoto nástroje při nasazování firewallu v této distribuci. Protože se však jedná o grafickou aplikaci, usnadňující úpravu konfiguračních souboru SuSEfirewall2, tak neobsahuje veškeré možnosti konfigurace, které jsou možné pomocí ostatních způsobů. Lze konfigurovat pouze:

- Způsob spouštění (při startu systému, manuálně),
- přiřazení síťových rozhrání do jednotlivých zón s možností vytvořit nové zóny,
- pravidla filtrování pro TCP nebo UDP služby dostupné na firewallu,
- možnost zapnutí NATu a konfiguraci statického NATu nebo směrování portů,
- pravidla pro broadcast vysílání,
- výběr přednastavených způsobů logování.

Také není přímo viditelné jaké konkrétní nastavení firewallu provádí. Proto je tento firewall podroben vytvořenému auditu, jehož úkolem je základní nedostatky tohoto řešení odhalit a následně dopomoci k úpravám vedoucích k lepšímu zabezpečení. Z důvodu délky je výsledný konfigurační soubor SuSEfirewall2 se skriptem uloženým pomocí *iptables-save* uložen pouze na přiloženém CD.

iptables-save > iptables.config

6.2.2 Audit linuxového firewallu a výsledky

K provedení auditu bylo využito vytvořené procedury pro testování. Proto je zachován postup udávaný tímto dokumentem. Přesto nebylo možné udělat audit kompletní. To je zapříčiněno tím, že audit byl proveden na experimentální sítí, kde nebylo možné některé části analyzovat. Mezi nevyplněné resp. neanalyzované části patří:

- Hlavička dokumentu,
- řízení bezpečnosti a personální bezpečnost,
- fyzická bezpečnost (virtualizované prostředí),
- kontrola údržby - záznamy, procedury,
- podpisy v závěru dokumentu (není tištěná verze).

Pro nedostupné části nebo pro případy, kdy je použito jiné možnosti nastavení, je nález tvořen zápisem *není dostupné*. Pro zbývající části jsou zapsány nálezy a případně vytvořeno zvýraznění žlutou nebo červenou barvou podle závažnosti s ohledem na bezpečnost nebo na nevyhovující konfiguraci požadavkům stanovených na firewall. Na závěr je dopsáno doporučení vzhledem k důležitým nálezům provedeného auditu.

Sestavení auditu by bylo standardně prováděno přímo na pracovišti na firewallu s dohledem IT pracovníka společnosti. S jeho pomocí by byly řešeny i otázky o dostupných procedurách, záznamech a jiných administrativních otázkách auditu. Také by umožnil plný přístup do systému firewallu. Protože nebyl auditován reálný firewall, ale pouze firewall ve vytvořené experimentální síti, byly auditovány až následující otázky zabývající se bezpečností přístupu do systému, jako je *zaheslovaný BIOS*, možnost *bootování z vyměnitelných médií* a *přístup do systému pomocí nezaheslovaných účtů*. Dále pak *zabezpečení souborů s hesly* a *provádění aktualizací atd.* Tyto možnosti byly kontrolovány pokusem (např. pokus o bootování z vyměnitelných médií) nebo pomocí administrativních nástrojů (např. YAST modul správce uživatelů a skupin). Pouze *zjištění spuštěných služeb* se provádí pomocí *příkazové řádky* příkazem *netstat* a zjištění povolení *SYN-cookies* zobrazením obsahu patřičného souboru *cat /proc/sys/net/ipv4/tcp-syncookies*. Další částí byla kontrola pravidel firewallu. Ta byla provedena z uložených pravidel pomocí příkazu *iptables-save > iptables.config*. Poté editací vzniklého souboru byla kontrolována jednotlivá pravidla podle přibližného vzoru v proceduře a vyhodnoceny vzhledem k požadavkům na firewall.

Z provedeného auditu bylo zjištěno několik bezpečnostních nedostatků:

- Jsou zapnuty pouze upozornění na nové aktualizace. Ty mohou vést k neaktuálnosti systému a služeb a tím k možnostem exploitace. Jako doporučení je zvážit automatické aktualizace (může docházet

k restartům) nebo zavést procedury pravidelných aktualizací s patřičnými záznamy.

- Je možné změnit bootování v zavaděči GRUB při startu systému. Doporučuje se zabezpečit GRUB heslem.
- Je zapnuto automatické přihlašování. Může tedy dojít ke zneužití při restartu, neboť dojde k zalogování do systému. Doporučuje se zakázat automatické přihlašování.
- V systému jsou spuštěny síťové služby (porty), které nejsou v souladu s požadavky na firewall. Doporučuje se dané služby vypnout.
- Byla zjištěna možnost přihlašování root přes ssh. Doporučuje se tuto možnost vypnout a zavést vyžadované příkazy do sudoers.
- Byla zjištěna možnost přistupovat z DMZ a LAN do vnější sítě bez omezení. Doporučuje se povolit pouze vyžadované služby.
- Překlad adres pro servery v DMZ je vytvořen pouze pro zadané porty. To vede k případům, kdy na ostatních portech se přistupuje k firewallu a ne k DMZ serveru. Doporučuje se vytvořit překlad adres pro servery v dmz pro všechny porty resp. bez omezení portů. Blokování řešit v chainu FORWARD.
- Není povolen ping na DMZ servery, jak je vyžadováno v zadání (způsobeno omezením grafického programu, který neumožňuje nastavit ICMP). Doporučuje se povolit ping pro DMZ servery.
- Byla zjištěna kolizní a nadbytečná pravidla. Doporučuje se odstranit tato pravidla.

Doporučení jsou též zapsány v dokumentu provedeného auditu, kde lze také dohledat konkrétní informace o nebezpečných nálezech pod daným úkolem procedury. Mezi nimi jsou například konkrétní služby, pravidla firewallu atp. Celý dokument provedeného auditu je možné shlédnout na CD.

6.2.3 Penetrační testování linuxového firewallu a výsledky

Stejně jako při auditu bylo při penetračním testování postupováno pomocí stanovené procedury. Ta však obsahuje i prvky, které nebylo možné pro experimentální síť zapsat. Byly to především:

- Hlavička procedury (penetrační testování se netýkalo společnosti),
- úkoly spojené s DNS záznamy,
- podpisy v závěru dokumentu (není tištěná verze).

Pro ostatní úkoly byly zapsány nálezy resp. dokladování pomocí výstupů použitých programů. Ty umožňují jednoznačně a s důkazem doložit informace jak je možné síť

prozkoumat a případně napadnout z vnější sítě. Na závěr jsou stručně vypsány nálezy napadnutelných slabých míst v zabezpečení firewallu.

V první části byl proveden průzkum vzdálené sítě. Jeho cílem bylo především identifikovat cestu k firewallu a detekovat servery ležící v DMZ. To se provádělo pomocí *traceroute* dvěma metodami. Klasickou metodou *traceroute*, kdy se používají UDP pakety a poté ICMP pakety, kdyby byly zakázány zprávy icmp 11.

traceroute –n $IP_server
traceroute –I –n $IP_server

Pokud cesta k testovaným serverům, předpokládaných v DMZ za firewallem, byla stejná (překlad adres nebo směrování portů) nebo delší, ale procházela přes firewall, byly shledány jako chráněné testovaným firewallem. Proto byly použity v další části testů pro kontrolu pravidel. Dále byl proveden test, zda se jedná o firewall stavový nebo bezstavový. Přitom se vycházelo ze známého faktu, že na bezstavovém se povoluje zpětná komunikace na všech vyšších portech.

nmap –sA -p1024-2000 $ip_firewall
nmap –sA -p1024-2000 $ip_server

Test probíhal jak pro firewall, tak i pro jeden vybraný server s předpokládaným umístěním v DMZ.

Poté bylo přistoupeno k testování, jehož cílem bylo zjistit povolená pravidla pro jednotlivé servery v DMZ. Testování probíhalo pro prvních 1024 portů TCP i UDP s různými příznaky.

nmap –sT -p 1-1024 $ip_serveru
nmap –sS -p 1-1024 $ip_serveru
nmap –sF -p 1-1024 $ip_serveru
nmap –sA -p 1-1024 $ip_serveru
nmap –sU -p 1-1024 $ip_serveru

Pokud by mělo být testování kompletní, muselo by být zvoleno všech 65535 portů, pro běžné testování ale postačí menší rozsah nebo zvolit konkrétní porty pro testování. Součástí kontroly pravidel pro DMZ byly také icmp pakety. Ty byly testovány pomocí programu *sing*.

sing -$icmp-type –c 1 $ip_serveru

Poslední částí testů pro DMZ zónu byla provedena identifikace povolených pravidel pomocí programu firewalk umožňující testování metodou TTL.

firewalk –s $source_port –d$destination_port –p$packet_type $ip_firewall $ip_server_dmz

Další částí bylo otestování samotného firewallu. Nejprve byl detekován operační systém podle specifických znaků a otevřených portů.

nmap –O $ip_firewall

Dále testovány otevřené porty a icmp zprávy pomocí *nmap* a *sing* způsobem jako při testování DMZ. Navíc bylo identifikováno, zda na otevřeném standardním portu běží standardní aplikace pro tento port a případně získat informace o této aplikaci (např. banner). Poté již následoval test odolnosti firewallu na určité typy útoku jako je odolnost proti fragmentaci paketů, SYN flood nebo Land attack.

Samostatná část testování hesel byla provedena, když byl dostupný nástroj pro test hesel síťových služeb s podporovaným protokolem, který byl spuštěn na firewallu. Pro ssh protokol byl použit program *xHydra* s definovaným slovníkem, který obsahoval všechny kombinace znaků abecedy do délky pěti znaků.

Na závěr testování bylo provedeno skenování na bezpečnostní díry pomocí nessus. Pokud by se vyskytla zneužitelná chyba, byl by proveden pokus o zneužití pomocí metasploit.

Výsledkem provedeného testu na firewallu provozovaném na OS opensuse, byly zjištěny tyto nálezy:

- Neblokované skenování. Umožňuje mapovat firewall a prostředí sítě.
- Povolený ping. Umožňuje zjišťovat dostupnost serverů v adresném rozsahu.
- Umožněna detekce operačního systému.
- Umožněna detekce verze ssh (banner).

Testovaný firewall byl odolný na provedené útoky a skenováním na výskyt bezpečnostních děr byly zjištěny pouze 2 lehce závažné. Ty dovolují pouze detekovat výrobce síťové karty a identifikovat informace, že stroj běží ve virtualizovaném prostředí.

6.2.4 Návrh pro zvýšení bezpečnosti auditovaného firewallu

Provedeným auditem a penetračním testováním bylo zjištěno několik nedostatků, které tvoří bezpečnostní riziko. Pro zvýšení zabezpečení je nutné tyto nedostatky odstranit. Proto byl vytvořen návrh řešení vedoucí k jejich odstranění.

Prvním bodem je zvážení možnosti automatických aktualizací, které jsou nejčastěji ponechány na manuálních instalacích, aby nedocházelo k výpadkům firewallu z důvodu aktualizací vyžadujících restart. Poté je možné přistoupit ke konfiguraci zabezpečení zavaděče *GRUB* pomocí ovládacího panelu *Zavaděč*

v konfiguračních panelech *YASTu*. Zde se doporučuje smazat možnost bootování z disket a v záložce *instalace zavaděče – volby zavaděče* nastavit heslo pro přístup do GRUBu. Dalším bodem zabezpečení je vypnutí automatického přihlašování v modulu *YASTu správce uživatelů a skupin* a vypnutí nepotřebných služeb. Pro spuštěné nepotřebné služby je vhodné přímé smazání programů poskytujících tyto služby. To je možné provést pomocí modulu *správce programů* odstraněním balíčků *postfix, CUPS a RPCBind.* Dále se doporučuje zakázání přihlašování uživatele *root* pro vzdálenou správu pomocí ssh, jenž lze provést patřičným nastavením v modulu *Konfigurace sshd*. Dále lze provést změnu konfigurace pravidel firewallu. Původně použitý modul *Firewall* v konfiguračních panelech *YASTu* není možné použít, protože ten pro své omezené možnosti nedovoluje provést potřebné změny. Stejně tak není možné použít skripty *SuSEfirewall2*. Provede se tedy nastavení umožňující konfiguraci firewallu pomocí příkazu *iptables*. Musejí se tedy vytvořit nové spouštěcí skripty z předlohy */etc/init.d/skeleton,* aby bylo možné nastavit firewall automaticky při každém spouštění systému. Registrace do patřičných úrovní běhu systému se provede příkazem *chkconfig* a původní spouštěné skripty firewallu *SuSEfirewall2-init a SuSEfirewall2-setup* musejí být tímto příkazem zastaveny. Nově vytvořený skript se nastaví pro spouštění příkazu *iptables-restore,* který načítá konfiguraci *iptables,* například ze souboru */etc/init.d/iptables.config.* Poté je možné provést potřebné změny v konfiguraci pravidel firewallu příkazem *iptables*. Během tohoto procesu se odstraní nadbytečná a kolizní pravidla, povolí se ping do DMZ, omezí se připojení z LAN a DMZ do vnější sítě a provede se změna NATování pro DMZ jak ukládá doporučení auditu. Uvedené nastavení se poté uloží příkazem iptables-save do vytvořeného souboru pro automatické spouštění (iptables.config).

Z penetračního testování byly zjištěny další nálezy. Protože ping je pro síť vyžadován a detekce operačního systému je podložena vyžadovanou službou ssh, jedinou možností vedoucí k vyššímu zabezpečení je odstranění banneru ssh. Ten by umožňoval detekovat jeho verzi a tím umožnil vyhledávání konkrétních exploitů. Jeho odebrání resp. změnu lze provést editací konfiguračního souboru sshd_config a přidáním cesty na nový v položce *Banner*. Ten je možný vytvořit i prázdný.

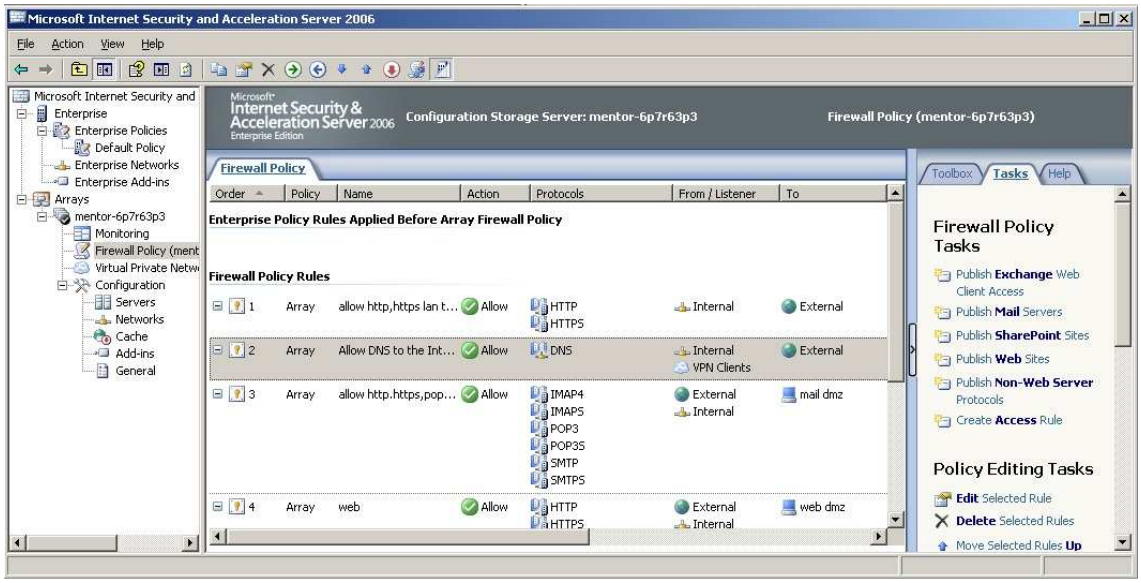
6.3 Kontrola Microsoft ISA serveru

6.3.1 Konfigurace Microsoft ISA 2006

Jako zástupce komerčního firewallu byl vybrán Microsoft ISA server 2006. Ten je popisován jako integrovaná brána zabezpečení na hranici sítě, která pomáhá chránit

prostředí IT před ohroženími z Internetu. Výhodou je integrace stavového firewallu, proxy serveru, VPN koncentrátoru, logování i základního IDS v jednom řešení.

Ve své podstatě je tento firewall nadstavbou pro 32 bitový operační systém windows server 2003, v našem případě ve verzi R2. Při splnění všech požadavků se provádí instalace ISA serveru standardním způsobem z instalačního balíčku msi nebo spuštěním exe souboru. Po instalaci se vytvoří nová administrační konsole ISA server management, viz Obr. 25, kde je již možné provádět konfiguraci firewallu.



Obr. 25: ISA console

Pomocí té lze kompletně konfigurovat veškeré možné nastavení firewallu. Administrace je velice jednoduchá a přehledná.

Pro nastavení firewallu pro experimentální síť se nejdříve provedl výběr typu sítě ze šablony *3 –Leg Perimeter*, kde se definují rozsahy adres pro jednotlivé zóny. Definice NATu je provedena automaticky. Nastavení předpokládá veřejné IP adresy v DMZ zóně, kde se provádí pouze směrování. NAT se provádí pouze při přístupu z lokální sítě do veřejné nebo DMZ. Pravidla filtrování byla nastavena ve *Firewall policy* v závislosti na konfiguračních možnostech s důrazem na shodu s požadavky experimentální sítě. Výsledné nastavení politik firewallu je vyexportováno a z důvodu délky uložen pouze na přiloženém cd.

6.3.2 Audit ISA 2006 a výsledky

Omezení auditu a jeho provádění v prvních částech bylo téměř totožné, jak je popsáno při auditu linuxového firewallu v kapitole 6.2.2. Pouze v některých bodech bylo využito specifických ovládacích panelů podle možností operačního systému.

Rozdílný postup nastal v případě kontroly pravidel firewallu. Ta byla provedena přímo v konsoli pro konfiguraci *ISA server management*, přesněji položka *firewall policy*.

Z provedeného auditu byly zjištěny následující nedostatky:

- Jsou zapnuty pouze upozornění na nové aktualizace. Ty mohou vést k neaktuálnosti systému a služeb a tím k možnostem exploitace. Jako doporučení je zvážit automatické aktualizace (může docházet k restartům) nebo zavést procedury pravidelné aktualizace se záznamy o provedených aktualizacích.
- Není zapnuto automatické odhlášení při nečinnosti v operačním systému. Při opomenutí odhlášení zůstane uživatel (administrátor) zalogován a útočník může mít přímý přístup do systému. Doporučuje se zapnout automatické odhlášení při nečinnosti v systému.
- V systému jsou spuštěny síťové služby (porty), které nejsou v souladu s požadavky na firewall. Doporučuje se dané služby vypnout.
- Bylo zjištěno logování všech komunikací přes firewall. Vyhledávání v logovacích souborech pak může být komplikované. Doporučuje se omezit míru logování.

Doporučení jsou též zapsány v dokumentu provedeného auditu, kde lze případně také dohledat konkrétní informace o nebezpečných nálezech pod daným úkolem procedury. Mezi nimi jsou například konkrétní služby, pravidla firewallu atp.

6.3.3 Penetrační testování ISA 2006 a výsledky

Stejným postupem jako v kapitole 6.2.3 bylo postupováno při penetračním testování firewallu ISA 2006. Také omezení testování bylo totožné. Jediným rozdílem bylo, že nemohlo být provedeno testování hesel síťových služeb. Příčinou byl nepodporovaný protokol RDP pro dostupné aplikace umožňující zkoušení hesel. Z výsledků penetračního testování byly zjištěny tyto nálezy:

- Neblokované skenování. Umožňuje mapovat firewall a prostředí sítě.
- Povolený ping. Umožňuje zjišťovat dostupnost serverů v adresním rozsahu.
- SYN flood způsobuje zhoršení odezvy firewallu. V kritickém případě by mohlo dojít k Denial of service?
- Umožněna detekce operačního systému.

6.3.4 Návrh pro zvýšení bezpečnosti auditovaného firewallu

Provedeným auditem a penetračním testováním bylo zjištěno několik bezpečnostních nedostatků. Ty je potřeba pro zvýšení bezpečnosti firewallu a přidružených podsítí odstranit. Proto byly jednotlivé doporučení a nálezy vyhodnoceny pro danou síť a vytvořen návrh pro vedoucí jejich odstranění.

Z doporučení auditu o aktualizacích je vhodné zvážit možnost zavedení jejich automatických instalací, přestože většinou jsou ponechány na manuálních z důvodu aktualizací vyvolávající restart systému. Při takovém nastavení je ale vhodné zavést alespoň procedury stanovující jejich pravidelné provádění a vytvářet záznamy o těchto instalacích. Další změna nastavení firewallu se doporučuje zapnutím automatického odhlášení. To je možné provést pomocí ovládacího panelu *Display properties* v záložce screen saver. Zde se nastaví prázdný šetřič obrazovky po uplynutí např. 5 minut a povolí se možnost *vyžadovat heslo při obnovení*. Dalším krokem je vypnutí služby podporující *NetBIOS over TCP/IP* pracující na nepotřebných portech 135 a 139. To lze provést v ovládacím panelu *services* vypnutím automatického spouštění a vypnutím služby *TCP/IP NetBIOS Helper*. Také je vhodné vypnout podporu na všech síťových adaptérech v rozšířeném nastavení Internet protokolu síťových rozhraní v položce *wins* (Local Area Connection – Properties – Internet Protocol – Properties – Advanced - WINS), kde je položka *NetBIOS settings*. Dalším bodem je omezení logování firewallu, tak, aby se usnadnilo vyhledávání a byla poskytnuta větší přehlednost logů. Toto nastavení se provede v nastavení v konfigurační konzoli firewallu. Omezení je vhodné provést především pro spojení, které bylo firewallem povoleno, neboť tyto logy neposkytují příliš užitečných informací. Nastavení lze provést úpravou daných povolovacích pravidel v záložce Action, kde se provede odtržení volby logování.

Vzhledem k nálezům penetračního testování není potřeba provést žádné radikální změny. Pouze je vhodné povolit detekci skenování portů firewallu, která je standardně vypnuta v části *General - Enable Intrusion Detection and DNS Attack Detection.* Pro nebezpečí SYN flood se provede kontrola nastavení v *Configure Flood Mitigation Setting*, kde je možné nastavit blokování spojení po přijetí většího množství paketů než je dovolená mez. Toto nastavení je již v základním nastavení zapnuta. Je ale možné zpřísnit dovolenou mez. Detekci operačního systému z posledního bodu penetračního testování zabránit nejde. Je vyžadována povolená služba RDP pro vzdálenou správu. Pomocí té lze ale určit OS, neboť se jedná o službu, která je provozována pouze na Microsoft Windows.

7 Závěr

V diplomové práci byly popsány firewally a možnosti integrace do síťové infrastruktury, obecně vysvětlen pojem audit informatiky a typy auditu. Dále pak základní principy aplikací pro bezpečnostní audit firewallu.

V praktické části byl proveden návrh metodiky pro bezpečnostní audit firewallu a penetračního testování. Jedná se tedy o řešení klasickou formou kontroly i metodou blízké reálnému útoku. Podle zvolené metodiky byly také vypracovány procedury procesu auditu. Ty umožňují audit malé až střední společnosti předpokládající jeden síťový stavový firewall ve funkci brány s LAN sítí a DMZ sítí pro veřejně dostupné servery. Vytvořené procedury pak byly použity pro audit vybraných firewallů. Z nekomerčních byl vybrán linuxový firewall distribuce OpenSuse 11.2 x64 a z komerčních ISA 2006. Jejich konfigurace představovala pouze základní změny nastavení pomocí grafických rozhraní tak, aby nastavení odpovídalo typickým požadavkům malých až středních společností. Výsledkem kontroly byl zápis doporučení změn firewallu (audit) a zápis nálezů (penetrační testování). Tyto výsledky byly dále vyhodnoceny a následně proveden stručný návrh řešení pro odstranění bezpečnostních nedostatků.

Přínosem diplomové práce je vytvoření metodiky a procedur pro provádění bezpečnostního auditu firewallu. Ty jistě v obdobné podobě již existují a jsou využívány společnostmi poskytující auditorské služby. Nevýhodou je ale jejich nedostupnost, neboť představují KNOW-HOW těchto společností. Závěrem je také důležité uvědomit si a respektovat fakt, že i vytvořená metodika a procedury pro audit podléhají životnímu cyklu. Je tedy důležité provádět jejich pravidelné kontroly, aktualizace a revize.

Seznam použitých zkratek

ACK	Acknowledgment; Příznak potvrzujících paketů o správném doručení.
DLL	dynamic link library. Část programového kódu, která je spouštěnou aplikací načtena do paměti a používána.
DoS	Denial of Service; Síťový útok vedoucí k odepření služby.
DMZ	Demilitarized zone. Demilitarizovaná zóna firewallu.
FIN	Finish; Příznak TCP paketů zajišťující konec komunikace.
HTTP	Hypertext transport protokol; Internetový protokol pro přenos hypertextových dokumentů.
ICMP	Internet Control Message Protocol; Jeden z rodiny síťových protokolů IP k přenosu chybových a řídicích zpráv.
IP	Internet protocol; Síťový protokol ze sady protokolů TCP/IP.
IPv4	Internet protocol version 4; Internetový protokol verze 4.
ISO/OSI	International organization for standardization/Open systems interconnection; Standardizovaný abstraktní referenční model síťové architektury.
LAN	Local area network: Lokální síť
PSH	Push; Příznak TCP paketů.
OS	Operating system; Operační systém.
RAM	Random acces memory; Označení operační paměti počítače.
SMTP	Simple mail transfer protocol; Protokol zajišťující přenos elektronické pošty.
RST	Reset; Příznak TCP paketů pro reset spojení.
SYN	Synchronize; Příznak paketů navazujících spojení. Obsahují sekvenční čísla.
TCP	Transmission Control Protocol; Spojovaný transportní přenosový protokol.
TTL	Time to live; Doba života paketu.
UDP	User datagram protocol; Protokol přenosové vrstvy bez navazování spojeni.

Seznam obrázků a tabulek

Literatura

[1] NĚMEC, PETR. *Audit informačních systémů nebo penetrační testy?.* Praha : Proceedings of the 16th International Conference on Systems Integration, June 10 - 11, 2008. ISBN 978-80-245-1373-7.

[2] GOLDSMITH, DAVID a SCHIFFMAN, MICHAEL. *Firewalking* [online].1998, [Cit.2009.11.30].
URL:< www.packetstormsecurity.org/UNIX/audit/firewalk/firewalk-final.pdf>

[3] STREBE, MATTHEW a PERKINS, CHARLES. Firewalls *24Seven, Second Edition* Sybex,2002. ISBN: 0−7821−4054−8

[4] KOMAR, BRIAN a EEKELAAR, RONALD a WETTERN, JOERN. *Firewalls for dummies, 2nd edition.* Willey publishing, 2003. ISBN: 0-7645-4048-3

[5] MATOUŠEK, DAVID a FISCHER, CARSTEN. *Introduction-firewall-leak-testing* [online]. 2006, [Cit. 2009.10.18]. URL:<www.matousec.com/Introduction-firewall-leak-testing .pdf>

[6] HERZOG PETE. *OSSTM 2.2* [online]. 2006. [Cit. 2010.05.01].
URL:<www.isecom.org/mirror/ osstmm.en.2.2 .pdf>

[7] CHRISTOPHER, ROGER. *Port Scanning Techniques and the Defense Against Them*. SANS Institute, 2001.

[8] FYODOR. *The Art of Port Scanning* [Online]. 2009. [Cit. 2009.10.10]
URL:< http://nmap.org/book/toc.html >

[9] GREBENNIKOV, NIKOLAY. *Using leak tests to evaluate firewall effectiveness* [online]. 2007, [Cit. 2009.10.20].
URL:<www.securelist.com/en/analysis?pubid=204791977 >

Seznam příloh

A Obsah CD

/Microsoft_ISA_2006/

Bezpecnostni_audit_firewallu_ISA_2006.pdf
isa_2006_config.xml
nessus_report_ISA2006.html
pentest_ISA2006.pdf

/OpenSuse_11.2_x64/

Bezpecnostni_audit_firewallu_OpenSuse_11.2_x64.pdf
iptables.config
nessus_report_OpenSuse.html
pentest_OpenSuse_11.2_x64_firewall.pdf

/DP_bezpecnostni_audit_firewallu.pdf

B Audit firewallu

Bezpečnostní audit firewallu

Číslo auditu:..... Datum:.....

Adresa:.....
.....
.....

Kontaktní osoba:.....

Telefon:.....

Doporučení:

1 Řízení bezpečnosti a personální bezpečnost

1.1 Řízení bezpečnosti - bezpečnostní politiky

1.1.1 Jsou dokumentované bezpečnostní politiky schválené managementem?

1.1.2 Obsahují bezpečnostní politiky jména, kdo navrhl bezpečnostní dokument a kdo jej schválil?

1.1.3 Jsou zavedeny prokazatelné seznámení zaměstnanců s bezpečnostními politikami?

1.1.4 Jsou bezpečnostní politiky a nařízení společnosti dostupné zaměstnancům?

1.1.5 Jsou zavedeny nařízení ukládající bezpečnostní kontroly a audity?

1.1.6 Jsou zavedeny nařízení stanovující pravidelné bezpečnostní reporty? (zprávy o bezpečnostních incidentech, risk management)

1.2 Personální bezpečnost

1.2.1 Je zodpovědnost o bezpečnosti pro jednotlivé pracovní funkce definována v popisu práce a v bezpečnostních politikách?

1.2.2 Jsou zaměstnanci prokazatelně proškoleni a trénováni?

1.2.3 Jsou definovány disciplinární zaměstnanců porušující bezpečnostní nařízení?

2 Kontrola firewallu - Fyzická bezpečnost, logický přístup

2.1 Fyzická bezpečnost

2.2.1 Je firewall umístěn v oddělené uzamykatelné místnosti? (např. serverovna)

2.2.2 Je zavedena forma autentifikace při přístupu k firewallu?

2.2.3 Je firewall umístěn v uzamykatelné skříni? (racková skříň)

2.2.4 Je zabezpečena kabeláž proti přímému přístupu? (volně dostupná x chráněná)

2.2.5 Je zavedena forma dohledu nad zařízením? (kamerový systém apod.)

2.2.6 Je využívána záloha napájení? (UPS, generátory)

2.2.7 Je prostředí klimatizováno?

2.2.8 Je veden prokazatelný záznam přístupů k zařízení?

2.2.9 Je přístup k veškeré dokumentaci o firewallu zabezpečen? (uzamykatelná skříň, trezor)

2.2 Logický přístup

2.2.1 Je zavedena politika řízení oprávnění pro definování přístupu ke specifickým zařízením a službám?

2.2.2 Je zavedena politika vytváření a mazání uživatelských účtů?

2.2.3 Je zavedena politika hesel? (změna hesel, síla hesel apod.)

2.2.4 Jsou zavedeny automatické aktualizace?

2.2.5 Je zaheslován přístup do BIOSu?

2.2.6 Je zakázáno startování systému z vyměnitelných médií?

2.2.7 Je zaheslován přístup do operačního systému?

2.2.8 Jsou zakázány nezaheslované účty Guest apod.?

2.2.9 Je zakázáno automatické přihlášení?

2.2.10 Je při nečinnosti po časovém limitu vyžadováno heslo pro přístup do systému?

2.2.11 Jsou datové soubory s hesly zabezpečeny, šifrovány?

2.2.12 Jsou spuštěny jen vyžadované služby?

netstat -an

2.2.13 Pokud je spuštěna vzdálená správa, je použito šifrování? (ssh, HTTPS atd.)

2.2.14 Je při vzdáleném přístupu zakázáno přímé přihlašování administrátorského účtu?

2.2.15 Je vyžadována autentizace pro vzdálenou správu?

2.2.16
Nejsou využívána defaultní hesla zařízení?

3 Kontrola pravidel filtrování

Doporučení auditu: Audit pro jeden stavový paketový firewall filtrující provoz pro lokální sítí a DMZ využívající IPv.4.

3.1 Jaký firewall je použit? (HW X SW)

3.2 Na jakém operačním systému firewall běží?

3.3 Jaké rozsahy IP adres firewall používá a jak jsou přiděleny síťovým rozhraním a do zón?

3.4 Jaké servery poskytují služby vnější síti? (IP adresy, služby)

3.5 Jsou veškeré veřejně dostupné servery v DMZ síti?

3.6 Jsou ostatní PC řádně přiděleny do LAN sítě (sítí)?

3.7 Je spouštění firewallu automatické?

3.8 Je zavedeno správné pořadí pravidel?

- *Anti-spoofing filtr (blokované privátní adresy, interní adresy z vnější sítě),*
- *logování a blokování útoků,*
- *zakazující pravidla,*
- *povolovací pravidla – uživatelská (např. veřejný web server),*
- *povolovací pravidla – správa (např. SNMP),*
- *logování (odladění filtrování, informace o filtrované komunikaci na síti).*

3.9 Je zakázán tzv. source routing?

3.10 Je logování dostatečně omezováno? (počet záznamů za jednotku času)
-m --limit $Nr/$TIME -j LOG

3.11 Jsou defaultní politiky nastaveny na zahazování paketů?
iptables -P INPUT DROP
iptables -P FORWARD DROP
iptables -P OUTPUT DROP

3.12 Jsou zakázány příchozí pakety z vnější sítě se zdrojovou adresou vnějšího rozhraní?

3.13 Jsou zakázány příchozí pakety z vnější sítě s privátní zdrojovou adresou (RFC 1918), neroutovatelnou adresou nebo adresou APIPA?

3.14 Je zakázáno broadcast vysílání na jednotlivých rozhraních? Je-li vyžadováno, je blokováno alespoň icmp broadcast vysílání (RFC 2644)?
iptables -A INPUT -i $ANY_IF -m pkttype --pkt-type broadcast -j drop
iptables -A FORWARD -i $ANY_IF -m pkttype --pkt-type broadcast -j drop

3.15 Je zakázáno multicastové vysílání?
iptables -A INPUT -i $ANY_IF -m pkttype --pkt-type multicast -j drop
iptables -A FORWARD -i $ANY_IF -m pkttype --pkt-type multicast -j drop

3.16 Je logován a blokován tzv. SYN-flood na všech rozhraních na vstupu a v tabulce FORWARD? Je zapnut SYN-cookies?

3.17 Jsou logovány a blokovány tzv. Bogus (falešné) pakety na všech rozhraních na vstupu a v tabulce FORWARD?
--tcp-flags SYN, FIN SYN, FIN

3.18 Je logováno a blokováno FIN/URG/PSH skenování na všech rozhraních na vstupu a v tabulce FORWARD?
--tcp-flags ALL FIN, URG, PSH

3.19 Je logováno a blokováno SYN/RST skenování na všech rozhraních na vstupu a v tabulce FORWARD?
--tcp-flags SYN, RST SYN, RST

3.20 Je logováno a blokováno FIN skenování na všech rozhraních na vstupu a v tabulce FORWARD?
--tcp-flags FIN, ACK FIN

3.21 Je logováno a blokováno FIN Stealth skenování na všech rozhraních na vstupu a v tabulce FORWARD?
--tcp-flags ALL FIN

3.22 Je logováno a blokováno Null skenování na všech rozhraních na vstupu a v tabulce FORWARD?
--tcp-flags ALL NONE

3.23 Je logováno a blokováno XMAS skenování na všech rozhraních na vstupu a v tabulce FORWARD?
--tcp-flags FIN, URG, PSH

3.24 Je blokováno UDP skenování na všech rozhraních na vstupu a v tabulce FORWARD?

3.25 Je povolena komunikace na rozhraní loopback?
iptables -A INPUT -i lo -j ACCEPT
iptables -A OUTPUT -i lo -j ACCEPT

3.26 a) V případě veřejných adres v DMZ je prováděn NAT pro LAN na externím rozhraní firewallu i na rozhraní DMZ?
iptables -t nat -s $LAN -o $EXT_IF -A POSTROUTING -j MASQUERADE
iptables -t nat -s $LAN -o $DMZ_IF -A POSTROUTING -j MASQUERADE

3.26 b) V případě privátních adres v DMZ je prováděn NAT na externím rozhraní firewallu pro obě sítě?
iptables -t nat -o $EXT_IF -A POSTROUTING -j MASQUERADE

3.27 Je povolena zpětná komunikace, tj. povolení navázaných spojení?
iptables -A FORWARD -i $EXT_IF -o $LAN_IF -m state --state ESTABLISHED, RELATED
iptables -A FORWARD -i $DMZ_IF -o $LAN_IF -m state --state ESTABLISHED, RELATED
iptables -A INPUT -m state --state ESTABLISHED, RELATED

3.28 Které služby jsou při přístupu na firewall blokovány?
iptables -A INPUT -i $ANY_IF -p $PACKET_TYPE --dport $PORT -j DROP
iptables -A INPUT -p icmp -m icmp --icmp-type $Nr -j DROP

3.29 Na vstupu jednotlivých rozhraní je povolena komunikace pouze pro požadované služby poskytované firewallem?

iptables -A INPUT -i $ANY_IF -p $PACKET_TYPE --dport $PORT -j ACCEPT

iptables -A INPUT -p icmp -m icmp --icmp-type $Nr -j ACCEPT

3.30 Které služby jsou zakázány z Lan do vnější sítě?

iptables -A FORWARD -i $LAN_IF -o $EXT_IF -p $PACKET_TYPE --dport $port -j DROP

iptables -A FORWARD -i $LAN_IF -o $EXT_IF -p icmp -m icmp --icmp-type $Nr -j DROP

3.31 Jsou povoleny pouze specifické služby (porty) vnější sítě pro LAN? (připojení na internet)

iptables -A FORWARD -i $LAN_IF -o $EXT_IF -p $PACKET_TYPE --dport $port -j ACCEPT

iptables -A FORWARD -i $LAN_IF -o $EXT_IF -p icmp -m icmp --icmp-type $Nr -j ACCEPT

3.32 Které služby jsou zakázány z Lan do DMZ?

iptables -A FORWARD -i $LAN_IF -o $DMZ_IF -p $PACKET_TYPE --dport $port -j DROP

iptables -A FORWARD -i $LAN_IF -o $DMZ_IF -p icmp -m icmp --icmp-type $Nr -j DROP

3.33 Jsou povoleny pouze požadované služby (porty) poskytované servery v DMZ síti pro LAN?

iptables -A FORWARD -i $LAN_IF -o $DMZ_IF -p $PACKET_TYPE -- dport $port -j ACCEPT

iptables -A FORWARD -i $LAN_IF -o $DMZ_IF -p icmp -m icmp --icmp-type $Nr -j ACCEPT

3.34 Které služby jsou zakázány z DMZ do Wan?

iptables -A FORWARD -i $DMZ_IF -o $WAN_IF -p $PACKET_TYPE --dport $port -j DROP

iptables -A FORWARD -i $DMZ_IF -o $WAN_IF -p icmp -m icmp --icmp-type $Nr -j DROP

3.35 Jsou povoleny pouze požadované služby (porty) poskytované servery v DMZ síti pro LAN?

iptables -A FORWARD -i $DMZ_IF -o $WAN_IF -p $PACKET_TYPE -- dport $port -j ACCEPT

iptables -A FORWARD -i $DMZ_IF -o $WAN_IF -p icmp -m icmp --icmp-type $Nr -j ACCEPT

3.36 a) V případě veřejných adres v DMZ je prováděn forward pro poskytované služby.

iptables -A FORWARD -i $EXT_IF -d $IP_SERVER -p $PACKET_TYPE --dport $PORT -j ACCEPT

iptables -A FORWARD -i $EXT_IF -d $IP_SERVER -p icmp -m icmp --icmp-type $Nr -j ACCEPT

3.36 b) V případě privátních adres v DMZ je prováděn překlad adres a forward pro poskytované služby?

iptables -A PREROUTING -d $PUBLIC_IP_DMZSERVER -i $EXT_IF -j DNAT --to-destination $PRIVATE_IP_DMZSERVER

iptables -A FORWARD -i $EXT_IF -d $PRIVATE_IP_DMZSERVER -p $PACKET_TYPE --dport $PORT -j ACCEPT

iptables -A FORWARD -i $EXT_IF -d $PRIVATE_IP_DMZSERVER -p icmp -m icmp --icmp-type $Nr -j ACCEPT

3.37 Je povolena zpětná komunikace pro daný server v DMZ poskytující služby?

iptables -A FORWARD -s $IP_SERVER -p $PACKET_TYPE -m state --state ESTABLISHED, RELATED -j ACCEPT

3.38 Je prováděno logování paketů před konečným zahozením v INPUT, OUTPUT i FORWARD tabulce?

3.39 Dochází ke vzájemné kolizi pravidel?

3.40 Jsou některá pravidla nadbytečná?

4 Kontrola údržby a monitorování

4.1 Kontrola údržby - záznamy, procedury

4.1.1 Jsou vedeny záznamy o haváriích HW a výpadcích firewallu?

4.1.2 Jsou vedeny záznamy o reinstalacích, restartech a obnovách ze záloh?

4.1.3 Jsou vedeny záznamy o provedených zálohách?

4.1.4 Jsou zálohy správně vytvořeny? (zda jsou skutečně vytvořeny při automatických zálohách)

4.1.5 Jsou zálohy pravidelně kontrolovány?

4.1.6 Jsou vytvořeny procedury schvalování pro změny konfigurací firewallu?

4.1.7 Jsou vedeny záznamy změn konfigurací firewallu?

4.1.8 Jsou vedeny záznamy o bezpečnostních incidentech?

4.1.9 Jsou vytvořeny procedury reakcí na bezpečnostní incidenty?

4.2 Monitorování, logování

4.2.1 Je zavedeno monitorování firewallu? (status, bezpečnostní incidenty, zasílání upozornění apod.)

4.2.2 Je prováděno logování firewallu?

4.2.3 Jsou logovány veškeré útoky a užitečné informace firewallu?

4.2.4 Je míra logování přiměřená?

4.2.5 Jsou logovací soubory zálohovány?

4.2.6 Je prováděna pravidelná kontrola logů?

Jméno auditora:..... Datum:.....

Převzal:..... Datum:.....

C Penetrační testování firewallu

Penetrační testování firewallu

Číslo testu:..... Datum:.....

Adresa:.....
.....
.....

Kontaktní osoba:.....

Telefon:.....

Úvod

Tento dokument je vytvořen jako procedura, jak postupovat při externím síťovém penetračním testování. Současně jej lze použít jako report penetračního testování. Cílem je otestovat dostupnost a bezpečnost hraničního firewallu. Při testu se předpokládá použití paketového firewallu s demilitarizovanou zónou. Proxy systémy nejsou cílem testování. Jednotlivé části testů jsou následující:

- Průzkum vzdálené sítě,
- testování firewallu,
- skenování, identifikace operačního systému a služeb firewallu,
- testování hesel,
- testování bezpečnostních děr.

1 Známé údaje

1.1 Informace o společnosti (název, adresa, kontakty, zaměstnanci).

1.2 Informace o firewallu (IP adresa, typ zapojení firewallu).

1.3 Ostatní informace.

2 Průzkum vzdálené sítě

2.1 Identifikace doménového jména nebo ip adresy firewallu.
nslookup $IP
nslookup $domain

2.2 Informace o registracích domény a přidělených rozsazích ip adres.
whois $domain
whois $ip

2.2 Informace o doméně. Zjistit případné servery umístěné za firewallem v dmz podle IP adres (adresy podobné firewallu, adresy přiděleného rozsahu).

dig $domain

./dnsenum.pl $domain

2.3 Zjistit cestu k firewallu.

Pro TCP traceroute je nutné znát otevřený port na firewallu. Pokud není znám, je potřeba provést nejprve skenování firewallu.

UDP traceroute

traceroute -n $IP_firewall

ICMP traceroute

traceroute -I -n $IP_firewall

Způsob: Výsledek:

2.4 Identifikovat, zda servery společnosti leží za testovaným firewallem.

Testují se známé servery společnosti a získané záznamy z bodu 2.2. Použití ip adres nebo doménového jména. Servery ležící za firewallem je možné považovat v případě identické cesty nebo delší se stejnou trasou jako u firewallu.

traceroute –n $IP_server

ICMP traceroute

traceroute –I –n $IP_server

Způsob: Výsledek:

2.5 Získat veřejně dostupné informace. Využití tzv. google-hacking.

Zkoušení vyhledat na internetu pomocí známých údajů informace o konfiguracích, technických dotazech, bezpečnostních dírách apod.

3 Testování firewallu

3.1 Identifikace typu firewallu.

Test otevřených vyšších portů >1024. Pokud je nefiltrováno jedná se o nestavový. V opačném případě je stavový. Identifikace vychází z pravidla, kdy na bezstavovém firewallu musí být povoleny vyšší porty pro zpětná navázaná spojení.

nmap –sA -p1024-2000 $ip_firewall
nmap –sA -p1024-2000 $ip_serverl

3.2 Identifikace NATu.
Pokud jsou ip adresy veřejných serverů stejné jako firewall, jedná se pravděpodobně o směrování portů. Pokud jsou adresy odlišné, jedná se pravděpodobně o NAT 1:1.

3.3 Zjistit povolené porty pro servery v dmz.
Servery z bodu 2.4 otestovat na povolené porty pomocí různých typů skenování.
nmap –sT -p 1-1024 $ip_serveru
nmap –sS -p 1-1024 $ip_serveru
nmap –sF -p 1-1024 $ip_serveru
nmap –sA -p 1-1024 $ip_serveru
nmap –sU -p 1-1024 $ip_serveru

3.3 Zjistit povolené icmp zprávy pro servery v DMZ.
Servery z bodu 2.4 otestovat na povolené icmp zprávy.
sing -$icmp-type –c 1 $ip_serveru

3.4 Zjistit povolené porty pomocí TTL
firewalk –s $source_port –d$destination_port –p$packet_type $ip_firewall $ip_server_dmz

4 Skenování, identifikace operačního systému a služeb firewallu

4.1 Identifikovat operační systém.
nmap –O $ip_firewall

4.2 Zjistit povolené porty pro firewall.
Povolené porty pomocí různých typů skenování.

nmap –sT -p 1-1024 $ip_serveru
nmap –sS -p 1-1024 $ip_serveru
nmap –sA -p 1-1024 $ip_serveru
nmap –sF -p 1-1024 $ip_serveru
nmap –sU -p 1-1024 $ip_serveru
nmap –sN -p 1-1024 $ip_serveru

4.3 Zjistit povolené icmp zprávy pro firewall.
Otestovat firewall na povolené icmp zprávy.
sing -$icmp-type –c 1 $ip_serveru

4.4 Zjistit typ služby na portu.
Některé porty mohou být obsaženy i jinými službami než standardními nebo lze získat více informací o verzi apod.
nc $ip_firewall $port
připojení webovým prohlížečem

4.5 Otestovat odolnost proti fragmentovému útoku.
Použít metodu skenování s možností fragmentace.
nmap –sS -f -p 1-1024 $ip_serveru

4.6 Otestovat odolnost na SYN flood.
hping3 –S $ip_firewall --flood

4.6 Otestovat odolnost na Land attack.
hping3 –S –a $ip_firewall –p $port $ip_firewall

5 Testování hesel

5.1 Otestovat defaultní hesla administrace.

Otestovat služby poskytující možnost administrace na defaultní hesla. Tyto služby jsou identifikovány v bodě 4.2 a 4.4.

5.2 Otestovat sílu hesel.
Použít aplikaci umožňující brute-force metodu louskání hesel na podporovaný port.

6 Testování bezpečnostních děr

6.1 Identifikovat bezpečnostní díry v aplikacích a operačním systému.
Spustit aplikaci umožňující vyhledávání bezpečnostních děr.
nessus

6.2 Případné otestování zneužití bezpečnostních děr.
Spouštění expploitů pomocí metasploit.

Nálezy:

Jméno auditora:..... Datum:.....

Převzal:..... Datum:.....