Jihočeská univerzita v Českých Budějovicích
Pedagogická fakulta
katedra informatiky

Ochrana webových serverů a penetrační test

BAKALÁŘSKÁ PRÁCE

Luděk Horák

vedoucí bakalářské práce
Ing. Ladislav Beránek, CSc., MBA

České Budějovice 2006

Anotace

Tato práce je určena zejména správcům webových serverů a také pracovníkům, kteří se zabývají bezpečností Internetu. Hlavním cílem této bakalářské práce bylo stručně popsat problematiku bezpečnosti webových serverů a v praktické části práce provést penetrační test, kterým je možno zabezpečení webového serveru otestovat. Důležitý cíl, který jsem si kladl, bylo vytvoření takového postupu, kterému by porozuměl i začínající administrátor. Tedy vytvořit jakousi šablonu, podle které by si mohl tento administrátor prověřit, zda je jím spravovaný webový server dostatečně zabezpečen.

S ohledem na rozsah tohoto dokumentu však není možné detailně popsat postupy používané hackery ani detailně popsat každý krůček potupu v provedeném penetračním testu. Provedení tohoto testu přeci jenom vyžaduje určité předběžné znalosti počítačových sítí a operačních systémů. Některé použité výrazy jsou vysvětleny na konci dokumentu.

Abstract

This dissertation work is assigned to web server administrators as well as to all engineers dealing with Internet security. The main subject of this work was to briefly describe the problem of web server security and do the penetration test which tests the web server security in practical part. An important aspect was to create such instructions so even administrator - beginner would be able to follow them. So I have created a model which would enable administrators to check if the server they are in charge of is adequately protected.

In the respect of extent of the document it is not possible to describe all the detailed procedures hackers use nor the penetration test procedures step by step. The test requires certain knowledge of computer net and operating systems. Certain specific terms are explained at the end of this document.

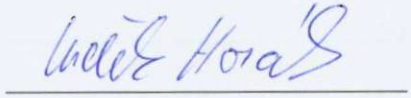
Poděkování

Rád bych touto cestou poděkoval vedoucímu bakalářské práce Ing. Ladislavu Beránkovi,CSc.,MBA za pomoc, rady a připomínky k obsahu této práce. Také bych rád věnoval poděkování sdružení Southgate, které mi dalo prostor pro mé testování.

Prohlášení

Prohlašuji, že jsem tuto bakalářskou práci vypracoval samostatně, a že jsem veškerou použitou literaturu uvedl v Seznamu použité literatury.

Luděk Horák



Obsah

OBSAH **5**

ÚVOD **7**

1. BEZPEČNOST WEBOVÝCH SERVERŮ **8**

1.1 Statistika napadání 8

1.2 Jaké informace webové servery shromažďují a jaké technologie k tomu používají 9

1.3 Jak mohou kriminální živly zneužít naše osobní údaje 13

1.4 Typy útoků používané hackery 14

1.4.1 Brutal Force Attack – útok hrubou silou *15*

1.4.2 Social Engineering *15*

1.4.3 Hardwarové útoky *17*

1.4.5 Softwarové útoky *18*

DNS spoofing 18
ICMP bombing 18
Source routing attack 19
Mitnick Attack 19
TCP splicing, hijacking 20
FTP bouncing 20
Racing attacks 21
DoS attacks 22
DDos 22
Buffer overflows 23

2. TYPY ZABEZPEČENÍ **24**

2.1 Firewall 24

2.2 Brutal Force Attack 25

2.3 Social Engineering 25

2.4 DoS 25

2.5 Obecné rady pro ochranu 27

3. PENETRAČNÍ TEST **29**

3.1 Techniky a postupy 29

3.2 Výsledek penetračního testu 31
3.3 Princip a filozofie 33
3.4 Penetrační test vs. bezpečnostní audit 34
4. PROVEDENÍ PENETRAČNÍHO TESTU 36
4.1 Technické detaily 37
4.2 Pasivní prohledávání 37
4.2.1 DNS 37
4.1.2 Hledání informací pomocí vyhledávačů 55
4.2 Aktivní prohledávání 57
4.3 Testování bezpečnosti aplikací 62
4.4 Doporučení 69
4.5 Zranitelnosti 69
4.5.1 DNS internal zone information důležitost - vysoká 69
4.5.2 DNS recursive query důležitost – středně vysoká 70
4.5.3 Nižší verze serveru Apache důležitost – střední 70
4.5.4 Nižší verze PHP důležitost – střední 71
4.5.5 Aktivní debug mód na Apache důležitost – nízká 71
4.5.6 Zjištění verze DNS důležitost – nízká 71
4.5.7 Závěr penetračního testu 71
ZÁVĚR 73
POUŽITÝ SOFTWARE 74
POUŽITÁ LITERATURA A INTERNETOVÉ ZDROJE 75
POUŽITÉ VÝRAZY 77

Úvod

Nedílnou součástí tohoto dokumentu je CD medium. Na tomto mediu jsou uloženy všechny nástroje uvedené v použitém softwaru. Také se na CD nachází 3 reporty, které vygenerovali automatizované nástroje(Nikto, N-Stealth, Nessus).

V první části tohoto dokumentu se nachází popis nejrůznějších útoků, které hackeři používají. Také se podíváme na stručnou statistiku a na to co webové servery udržují za informace a jak se dají zneužít.

Další část jsem naopak věnoval tomu jak se bránit proti vybraným technikám útoku a poohlédneme se po obecném zabezpečení webového serveru.

V třetí kapitole se podíváme blíže na definici penetračního testu. Ale nejen to. Jsou zde vysvětleny techniky a postupy testu. Také jsem zařadil do této kapitoly porovnání penetračního testu s bezpečnostním auditem.

Čtvrtá část je věnována samotnému postupu testu. Provedeme pasivní a aktivní prohledávání sítě(serveru) a otestujeme bezpečnost aplikací. V závěru penetračního testování se podíváme na výsledek a doporučení.

1. Bezpečnost webových serverů

1.1 Statistika napadání

Statistiky napadení webových serverů hovoří za vše. Následující tabulka obsahuje počet nahlášených případů napadení. Díky masovému využívání automatizovaných nástrojů k napadání strojů připojených k internetu, se staly útoky naprosto běžnou záležitostí. Počet nahlášených případů poskytuje velice málo informací týkajících se rozsahu a výsledku útoků. Vyvíjí se nová technika statistik, která snad bude schopna počet útoků důvěryhodně zjistit.

1988 1989

Rok	1988	1989
Případy	6	132

1990 – 1994

Rok	1990	1991	1992	1993	1994
Případy	252	406	773	1,334	2,34

1995 – 1999

Rok	1995	1996	1997	1998	1999
Případy	2,412	2,573	2,134	3,734	9,859

2000 – 2004

Rok	2000	2001	2002	2003
Případy	21,756	52,658	82,094	137,529

tabulka 1. Statistika případů napadení

Z této tabulky vyplívá, že napadání webových serverů má rostoucí tendenci. Dá se tedy předpokládat, že jakýkoliv stroj připojený k internetu byl či dříve nebo později bude napaden.

1.2 Jaké informace webové servery shromažďují a jaké technologie k tomu používají

Živnou půdou pro obchod jsou informace o zákaznících a potenciálních zákaznících - o tom, co kupují, co se jim líbí a nelíbí, co potřebují a po čem touží. Elektronický obchod není v tomto směru žádnou výjimkou. Webové obchodní společnosti zajímá naše adresa, zboží, které jsme již nakoupili, a další rysy našeho chování v roli zákazníka. Svůj význam má pro ně i shromažďování dat, která nejsou přímo přiřazena k našemu jménu, zejména údajů o našich zvycích při pohybu po webu.

Informace, u nichž lze předpokládat, že jich může být použito k naší identifikaci, nebo jsou přímo spojeny s naší osobou (naše jméno, adresa, telefonní číslo, e-mailová adresa, čísla účtů, různá referenční čísla a další podobná data) jsou považovány za osobní údaje a zacházení s nimi upravuje zákon na ochranu osobních údajů. Z toho vyplývá, že máme ze zákona (zákon č. 101/2000 sb. O ochraně osobních informací) určitá práva k osobním údajům, které se nás týkají, například k informacím, které o nás shromažďují webové servery.

Informace související s naším zdravotním stavem, rasovou a etnickou příslušností, členstvím v odborech, politickými postoji a světonázorem, sexuální orientací a záznamy v trestním rejstříku jsou zařazeny do kategorie citlivých údajů a jejich ochrana je přísnější. Bez našeho výslovného souhlasu nesmí být shromažďovány (s výjimkami stanovenými v jiných zákonných normách – zákon o státní správě, policii atd.).

Nejjednodušší a nejpřímější způsob shromažďování našich osobních informací legitimními webovými servery spočívá v situacích, kdy se tyto informace sami rozhodneme poskytnout, například zaregistrujeme-li se v rámci prodejní kampaně či spotřebitelské soutěže, využijeme-li nabídky zdarma

poskytovaných služeb nebo zboží, vytvoříme-li si na webovém serveru účet (například u internetové cestovní kanceláře nebo banky), nakoupíme-li přes Internet zboží nebo se zúčastníme nějakého průzkumu.

V této oblasti máme naštěstí vše pevně v rukou. Můžeme se sami rozhodnout, zda požadované informace poskytneme nebo ne.

Poznámka: Informace o našem osobním životě může každý dostatečně cílevědomý zájemce načerpat z webových adresářů nebo diskusních skupin. Pokud například přispíváme do diskusních skupin pod svým skutečným jménem nebo e-mailovou adresou, měli bychom počítat s tím, že naše příspěvky mohou na webu zůstat velmi dlouhou dobu a lze je snadno najít pomocí vyhledávacích nástrojů.

Některé informace, které weboví obchodníci shromažďují (například číslo kreditní karty, adresa a telefonní číslo) jsou nezbytné k provádění transakcí. Díky uchování některých osobních informací, například seznamu zakoupeného zboží, dodací adresy, velikosti oblečení nebo položek v seznamu přání, může obchodník přizpůsobit další komunikaci s námi našim osobním preferencím. Uložení těchto informací nám rovněž může ušetřit námahu s jejich opakovaným zadáváním při každé návštěvě webového serveru.

Webové obchodní společnosti mohou získané informace využít také při zasílání speciálních nabídek a upozorňování na související výrobky a služby jiných společností. Nabídky třetích stran nám mohou zasílat samy, mohou však také předat nebo prodat naše jméno, e-mailovou adresu a případně i další informace jiným společnostem, které nás budou kontaktovat v rámci vlastních propagačních akcí.

Společnosti, které si zakládají na své pověsti, nám umožní tyto formy využití našich osobních informací určitým způsobem ovlivňovat. V Evropské unii, USA, Kanadě a Austrálii navíc platí zákony omezující použití a sdílení osobních údajů v e-mailových obchodních kampaních.

Webové obchodní společnosti a organizace chtějí vědět, jak uživatelé utrácejí své peníze a svůj čas na jejich webových serverech. Podobně jako turnikety na fotbalovém stadiónu nebo v metru sledují také webové servery počty návštěvníků (přesněji řečeno počty připojených počítačů), zatímco totožnost návštěvníků zůstává skryta.

- Webové servery mají mnoho možností sledování našeho počítače při návštěvách webových stránek. Mohou zjišťovat, které weby jsme navštívili, data a časy návštěv, dobu jejich trvání, zobrazené webové stránky a místa na stránkách, na která jsme klepli myší, atd.

- Webové servery mohou rovněž načíst internetové nastavení našeho prohlížeče (například aplikace Internet Explorer nebo Netscape) a určit zemi nebo stát, kde je umístěn náš počítač, použitý operační systém a typ prohlížeče, přesnou adresu IP našeho počítače a adresu webového serveru, ze kterého přicházíme.

- Některé společnosti, například sítě reklamních agentur, mohou sledovat pohyb našeho počítače mezi více webovými servery. K tomu společnost potřebuje umístit svá data (například reklamní proužek) na každou ze stránek, které chce sledovat, se souhlasem a za účasti všech webů, kde se reklama zobrazuje.

K shromažďování a uchovávání informací o nás a našich zvycích při surfování využívají webové servery především webové formuláře, soubory cookie, webové majáky a protokoly webových serverů.

Webové formuláře slouží stejně jako jejich tištěné protějšky k co nejefektivnějšímu získávání informací a k přímému přenosu těchto informací

do databází společnosti. Ať už nakupujeme letenky, účastníme se internetové aukce nebo se přihlašujeme k odběru zpráv diskusní skupiny, s nejvyšší pravděpodobností se setkáme s webovým formulářem.

Podobně jako nám stvrzenka z čistírny připomíná, že si máme jít vyzvednout čisté prádlo, soubory cookie slouží webovým serverům k připomenutí informací, které shromáždily o naší návštěvě, o tom, které stránky jsme otevřeli, o naší činnosti (se zachováním anonymity) a o osobních údajích, které jsme přitom poskytli. Soubory cookie představují nezbytnou součást efektivního využití většiny webových serverů. Mají podobu malých textových souborů, které mohou webové servery zanechat ve našem počítači a které ohlásí naši příští návštěvu.

Webové servery ukládají do souborů cookie informace o našich preferencích, využívají je k přizpůsobení zobrazovaného obsahu stránek (například místních zpráv a předpovědi počasí nebo cílených slev) a k uskutečňování transakcí (například při využití internetového bankovnictví nebo nákupech po Internetu). Soubory cookie nemohou do počítače zanést virus ani jej jinak poškodit.

Soubor cookie může obvykle načíst pouze webový server, který jej vytvořil, ačkoli společnost může umožnit jiným webovým serverům (například reklamním serverům nebo propagačním sítím) ukládat do našeho počítače soubory cookie, které se v tomto případě nazývají soubory cookie třetích stran. Propagační server tak může zaregistrovat náš počítač vždy, když se v něm zobrazí jeho reklama, a zaznamenávat údaje o tom, zda jsme na reklamu klepli myší. Tímto způsobem mohou reklamní společnosti shromažďovat informace o tom, kde již byly jejich materiály zobrazeny, a na jejich základě zefektivnit distribuci reklamy.

1.3 Jak mohou kriminální živly zneužít naše osobní údaje

Jedním ze zvláště znepokojivých trendů je zvyšování počtu případů falešných webových serverů nebo hromadných e-mailů. Tyto e-maily obsahují odkazy na podvržené webové servery požadující po uživateli zadání citlivých informací, jako je číslo bankovního účtu, rodné číslo nebo další osobní identifikační údaje. Vzhled takových e-mailů nebo webových serverů tak dokonale kopíruje webové servery legitimních a respektovaných společností, jako je například eBay, Citibank nebo Microsoft, že přiměly mnoho uživatelů odhalit citlivé osobní informace nebo spustit ve svém počítači virus.

Viry a jejich nepříjemní příbuzní, červi a trojské koně, se zaměřují především na útoky na počítače s cílem poškodit datové soubory nebo zaútočit na další počítače a webové servery. Viry a červy však lze použít také jako prostředky k neoprávněnému získání našich osobních údajů. Zvláště zákeřný virus může do napadených počítačů například instalovat program shromažďující uživatelská jména a hesla, která si autor viru může kdykoli vyzvednout.

K podvodnému softwaru patří programy, které provádějí v počítači určité operace bez předchozího upozornění a získání souhlasu uživatele. Tyto operace mohou zahrnovat sběr osobních údajů, zobrazování nevyžádaných reklam a změny nastavení prohlížeče (například aplikace Internet Explorer nebo Netscape). Kromě zjevných nepříjemností může mít jejich činnost také další následky sahající od snížení celkového výkonu počítače až ke zneužití osobních údajů.

- Příkladem podvodného softwaru je špionážní software (spyware). Může bez našeho svolení shromažďovat naše osobní údaje a informace o našem počítači. (V tom se liší od souborů cookie, které můžeme prostřednictvím svého prohlížeče kdykoli přijmout nebo odmítnout.) Cílem špionážního softwaru se můžeme stát při

stahování hudby nebo filmů z některých programů zaměřených na sdílení souborů, při hraní některých volně šiřitelných her a při práci s dalšími programy, které pocházejí z neznámého zdroje.

- Dalším druhem podvodného softwaru je neautorizovaný reklamní software (adware), který může po instalaci ze strany bezohledné reklamní společnosti generovat proud nevyžádané reklamy, jež se zobrazuje v překryvných oknech a obtěžuje nebo pobuřuje uživatele. V některých případech mohou být tyto programy tak agresivní, že se jich lze zbavit pouze vypnutím počítače. Také jejich obsah může vyvolávat znepokojení, zvláště v případech, kdy se děti dostanou na server určený pro dospělé a jsou zahrnuty záplavou nevhodných obrázků.

Někteří jednotlivci o nás mohou v extrémním případě získat tolik informací, že se za vás dokáží vydávat, a to nikoli pouze na Internetu. Tyto případy označujeme pojmem krádež identity a představují stále větší problém. Zloději identity mohou zneužít naše číslo sociálního pojištění a rodné číslo k vyzvednutí našich sociálních dávek, nakupovat na naši kreditní kartu, otevřít si pod naším jménem účet v bance, vzít si půjčku naše jméno a dokonce spáchat zločin pod naší identitou.

1.4 Typy útoků používané hackery

Bezpečnost dat je v dobách internetových snad nejvíce diskutovaným tématem. Často slyšíme o průniku hackerů do různých systému a možná už jsme se s tím setkali na vlastní kůži... Zde je krátký přehled způsobů, kterými hacker může proniknout do našeho systému.

1.4.1 Brutal Force Attack – útok hrubou silou

Jedním z nejjednodušších způsobů, jak se potencionální narušitel dostane do našeho systému je uhodnutí hesla. V současné době již existuje natolik dokonalý software, který je schopen během poměrně krátkého časového okamžiku vyzkoušet obrovské množství kombinací znaků (tzv. útok hrubou silou). Kromě toho tyto programy disponují obsáhlým slovníkem, z něhož se generují nejčastější řetězce používané jako hesla. Můžeme si být téměř jistí, že hesla typu: "heslo", "jméno_naší_přítelkyně" apod. není žádný problém odhalit. Některé systémy, například *OpenVMS*[1] se před těmito útoky brání tak, že uživateli, který opakovaně zadá chybné heslo dočasně zablokují přístup.

1.4.2 Social Engineering – sociální inženýrství

Práce s lidmi souvisí s bezpečností informačních systémů mnohem více, než se všeobecně předpokládá. Technika, anglicky zvaná social engineering, je mezi útočníky na počítačové systémy velmi oblíbená. Český ekvivalent se hledá velmi těžko, proto se budeme držet anglického označení SI. Je to totiž jeden z nejsnazších způsobů napadení cílového systému. Od útočníka vyžaduje pouze trochu bystrosti a dobré vyjadřovací schopnosti.

Cílem tohoto útoku je zpravidla získání citlivých informací či přímo průnik do systému. Útočník se bude snažit zjistit různé informace. Nyní se podíváme na to, jaké techniky a triky se při tomto druhu útoku používají:

[1] OpenVMS je operační systém. VMS je zkratka pro Virtual Memory System, Open označuje "otevřený systém" - respektuje a používá "otevřené standardy".

- struktura sítě,
- vnitřní a vnější IP adresy,
- IP adresy hraničních firewallů,
- jména osob a jejich osobní informace,
- bezpečnostní politika (bezpečnostní postupy a nastavení),
- telefonní čísla a adresy,
- programové vybavení,
- přístupová hesla.

Jaké triky útočník používá?

Zpravidla se vydává za někoho jiného. Může se například stát, že si útočník zjistí jména správců sítě a pak zavolá nic netušícímu uživateli, předstírá, že je správce, a chce po něm, aby si změnil heslo nebo změnil nastavení systému. Uživatel to v dobré víře opatření provede a bezpečnostní incident je na světě. Rovněž se útočníci mohou vydávat za zástupce poskytovatele připojení a požadovat od správce sítě přenastavení firewallů nebo změnu přístupových hesel. Základním předpokladem úspěchu u tohoto druhu útoku je dobrá znalost místních podmínek a pravidel. Rovněž je užitečná znalost osob, kterých se útok týká. Pokud útočník vzbudí důvěru a prokáže znalost situace, málokdo uživatel odmítne udělat to, co požaduje. To však od útočníka vyžaduje znalost prostředí. Získá ji z různých míst, ale nejčastěji z informací, které publikuje sama společnost. Zjistit jména správců sítě, registrátorů domén, webmasterů či pracovníků technické podpory dnes není žádný problém. Mnoho takových informací je publikováno na firemních webových stránkách či v propagačních materiálech konkrétních podniků. Ve

státní správě je situace ještě mnohem horší. K získání podobných informací však může použít útočník rovněž SI a takzvaně "vytáhnout" tyto informace z pracovníka firmy a následně je použít k dalšímu SI útoku. Může například zavolat na informační linku společnosti a představit se jako zástupce firmy, která se zabývá prodejem softwaru. Bude požadovat jména a telefonní čísla osob, na něž se může se svojí nabídkou obrátit. Triků je opravdu mnoho a záleží jen na útočníkově vynalézavosti a šikovnosti, jaké informace může zjistit. Nejsou výjimkou situace, kdy se útočníkovi podaří zjistit hesla k důležitým systémům a klíčovým serverům. Klamat však nemusí útočník jen po telefonu, ale i přes fax či e-mail.

1.4.3 Hardwarové útoky

Využívají k útoku nedokonalosti hardware. Mezi nejznámější patří tzv. sniffing, tj. na síti odposloucháváme pakety, které nám nepatří. Například na síti typu Ethernet (jeden z nejrozšířenějších typů) se data neposílají konkrétnímu počítači (není to ani možné), ale celému segmentu. Specializovaný program (tcpdump, pohodlněji sniffit) přepne ethernet kartu do "promiskuitního módu" (k tomu jsou obvykle vyžadována práva administrátora) a ta přijímá a zapisuje obsahy všech paketů s danými vlastnostmi. V těchto paketech, pokud nejsou vedeny kryptovaně, je otevřeně vypsáno uživatelské jméno a heslo, které používá uživatel při přihlašování do systému.

Další varianta hardwarového odposlouchávání vyžaduje alespoň minimální technickou zdatnost. Jedná se o "napíchnutí" drátu, např. mezi modemem a počítačem a následný odposlech dat. Pozor: Mluvíme o datech digitálních, "počítačových". Odposlech modemového spojení z telefonních drátů je záležitost technicky značně komplikovaná.

Do této skupiny „hardwarových útoků“ by se daly zařadit i krádeže hardware. Pokud bude server zabezpečen výborně po softwarové stránce i tak

to nebude nic platné, když si někdo počítač odnese či z něj odcizí pevný disk. Ochrana počítače heslem v BIOSu je naprosto nedostatečná, jednak nezabrání vyjmutí disku a navíc lze snadno zrušit resetováním paměti CMOS.

1.4.5 Softwarové útoky

Zahrnují činnost, kterou si počítačová veřejnost obvykle s hackery spojuje (tj. psaní nepochopitelných programů které dělají nepředstavitelné věci). Všechny útoky mají společný rys: Využívají chyb (přičemž za chybu považujeme i přílišnou benevolenci programu, systému či protokolu) v programech ke vlastním nekalým záměrům. Existuje nesčetné množství různých útoků; zde se pokusím vyjmenovat alespoň nejznámější:

DNS spoofing

Hacker získá rootovské práva na nameserveru dané sítě; konfigurační soubory pak upraví tak, že se prohlásí za počítač, který má oběť ve svých .rhosts. Následně se může napojit na cílový počítač bez autentifikace.

Pozn.: metoda zvaná "cache poisoning" umožňuje (umožňovala, BIND 4.9.5 – unixová varianta DNS systému) podobný trik provést, i pokud hacker nemá práva superuživatele na nameserveru. Útočník zašle nameserveru chybná data, která mu naplní cache chybnými údaji, na jejichž základě nameserver rozesílá nesprávné odpovědi.

ICMP bombing

ICMP (Internet Control Message Protocol) je protokol pro zasílání zpráv o stavu sítě (např. ping využívá zpráv ICMP echo request -- echo reply ke zjištění doby odezvy). Mezi ICMP zprávy patří i informace o nedosažitelnosti cíle, využívané routery v případě, že se některý uzel ocitne mimo provoz. Útočník zašle napadenému systému blok falešných zpráv o

nedostupnosti cíle (programy k tomuto účelu sestavené se vyznačují hrozivými jmény jako "nuke" nebo "ICMPbomb"), čímž tento cíl pro napadený systém "zmizí". Tento krok se využívá v následující technice zvané:

Source routing attack

Source routing je zvláštní druh směrování, ve kterém se místo cílové adresy vyplní konkrétní "cesta" paketů přes konkrétní routery. Specifikace TCP/IP pak udává, že provoz směrovaný pomocí source-routingu se má zpět vracet pomocí reverzního směrování. Útočník si tedy vybere počítač, který je uveden v některém souboru .rlogin cílového stroje a tento počítač pomocí výše uvedené techniky ICMP bombingu "zneviditelní". Potom se prohlásí za tento počítač a díky reverznímu směrování source-routovaných paketů naváže spojení jako prověřený počítač (pokud by nebyl použit source routing, byly by pakety routovány na vnitřní síť).

Pozn.: O slabinách source-routingu se obecně ví a v běžném provozu proto obvykle není povolen.

Mitnick Attack

Také známo jako "hádání TCP sekvencí": TCP spojení závisí na číslování paketů (index během spojení roste). Při vzniku konexe je vygenerováno pseudonáhodné číslo, od kterého se pakety indexují. Pokud si útočník dokáže toto číslo zjistit, je schopen posílat korektně vypadající pakety a obejít tak autentifikaci (nebude však vidět přicházející pakety; navíc musí zajistit aby tyto nedosáhly svého adresáta a ten nezamíchal vysláním "pravých" paketů indexy zfalšovaného TCP spojení).

Příklad: Cílový počítač je oddělen od internetu firewallem, který odřezává veškerá TCP spojení z IP adres mimo lokální síť. Na lokální síti se

nachází "důvěryhodný" počítač, na který je možno otevřít TCP spojení. Na cílový počítač je povolen protokol ICMP zvnějšku.

"Důvěryhodný" počítač vyřadí útočník z provozu pomocí množství částečných TCP spojení; tak ho odřízne od sítě (DoS attack, viz níže). Dále pak útočník naváže řadu ICMP spojení a poznamená si sekvenční čísla paketů. Z těchto hodnot spočítá další číslo sekvence a pošle paket s nastavenou zdrojovou adresou "důvěryhodného" počítače. Paket projde routerem a protože má správné TCP indexy, bude přijat cílovým počítačem jako paket z "důvěryhodného" počítače.

Pozn.:Dobře nakonfigurovaný firewall by ovšem měl být schopný odhalit pakety, které přicházejí zvnějšku a přitom mají zdrojovou adresu vnitřní sítě.

TCP splicing, hijacking

Je založen na "kradení" konexe: Útočník (který se fyzicky nachází mezi dvěma komunikujícími počítači) monitoruje spojení mezi počítačem A a B. Počká si, až skončí autentifikační proces, poznamená si TCP indexy paketů a potom vyřadí z provozu počítač A. Útočník vypočítá následné TCP indexy, pokračuje v generování falešných paketů pro B a ze sítě odezírá pakety určené pro A.

Pozn. Tento útok je poměrně specifický a ve větší míře zatím nebyl pozorován. Rovněž není použitelný, pokud celé spojení probíhá kryptovaně na aplikační úrovni.

FTP bouncing

Zvláštní druh útoku, který (v omezené míře) může proniknout i přes některé firewally:

- Na lokální síti (od internetu stíněné firewallem) se nachází anonymní FTP server, přístupný zvnějšku, a je na něm veřejný adresář pro zápis(upload).

- Do tohoto adresáře nahraje připravený soubor (např. jako SMTP skript pro zaslání mailu)

- Útočník se přihlásí na FTP server a provede příkaz PORT s IP číslem cílového počítače a daným portem (v našem příkladu port SMTP - 25)

- příkazem RETR <soubor> pošle soubor na předem připravený port - výsledkem je (v našem případě) mail s falešnou adresou FTP serveru; jindy se může jednat o pokus o remote buffer overflow (např. na imap). Celá transakce bude navíc jen obtížně identifikovatelná v logách.

Racing attacks

O tento název se dělí dva druhy útoků: První spočívá v "závodu" dvou konexí, kdy se útočník snaží uhádnout zbývající znaky (znak) uživatelova hesla a konexi převzít na sebe. Je účinnou metodou u systémů s jednostrannou autentifikací; naopak neúčinkuje tam, kde se používá metodiky výzva/odpověď. Některé servery zakazují, aby autentifikační proces jednoho uživatele probíhá na dvou konexích najednou, čímž teto útok také znemožní.

Druhý typ útoků je záležitost lokální: Přichází ke slovu ve chvíli, kdy nějaký SUID(po spuštění SUID programu běží proces pod právy vlastníka) program zapisuje do world-writable adresáře (typicky /tmp). Často k takové situaci dochází u nedbale napsaných CGI skriptů běžících pod právy uživatele:

- Útočník zjistí, že SUID program ukládá svá data do world-writable adresáře.

- V tomto adresáři vytvoří odkaz na soubor, který chce změnit (to může v případě, že dočasný soubor má jméno založené na čísle aktuálního procesu, zahrnovat vytvoření několika desítek takových odkazů s pravděpodobnými čísly)
- V opravdu špatném případě dokáže útočník zmást exploitovaný program natolik, že do dočasného souboru zapíše data, která mu útočník podstrčí - například řádku souboru .rhosts
- Program zapíše do dočasného souboru svá data a tím přepíše soubor, na který odkaz ukazuje (přidá řádku do .rhosts).

DoS attacks

Útoky typu "odepření služby" (Denial of Service) - sem patří například výše uvedený ICMP bombing. Těchto útoků je ale v podstatě tolik, kolik je síťových služeb. Samy o sobě nezaručí hackerovi práva superuživatele, jsou však hojně využívány jako součást rozsáhlejších útoků, kdy je potřeba určitý počítač odstavit od sítě nebo zcela vyřadit z provozu. Škála je opravdu široká - od ARP cache poisoningu (rozesíláním falešných ARP zpráv), kdysi slavného Ping of Death (ping o velkém datovém objemu, který počítač zahltí), SYN flood útoku (zaslání TCP paketů s žádostí o navázání spojení z nedostupného počítače), přetížení mailserveru rozesláním velkého množství mailů atd. V mnoha případech se nejedná ani o využití chyb v programu, ale spíše slabiny návrhu daného protokolu. Před takovým útokem je ovšem obtížné se bránit.

DDos

Zkratka DDoS znamená "Distributed Denial of Service" a označuje variantu DoS útoku vedeného ne z jednoho počítače, ale souběžně z velkého

množství stanic. Slovo velké množství znamená v této souvislosti desítky, stovky a dokonce i tisíce stanic. Co se týká praktické realizace takového útoku, neznamená to, že v danou chvíli sedí u těchto stanic hackeři, nýbrž že na těchto stanicích je nainstalován hackerem nějaký program (tzv. zombie), který se na pokyn hackera aktivuje a zasype oběť přívalem dat.

Buffer overflows

Přetečení bufferu (buffer-overflow) je poměrně častou technikou, jak se nabourat do systému. Jednotlivé buffer-overflows se dají rozdělit podle toho, v které části paměti k nim došlo. Nejčastější z nich vznikají na zásobníku. Buffer-overflow je multiplatformní útok a dá se využít v podstatě na jakémkoliv systému.

Samotný princip přetečení bufferu je poměrně jednoduchý. V podstatě jde o to, že špatně napsaný program donutíme načíst do paměti více dat, než na kolik je stavěn. Veškeré útoky tohoto stylu využívají nějaké chyby v programu a také ze skutečnosti, že počítač udělá přesně to, co mu řekneme, ať už je to cokoliv.

Zpracovávané údaje se obvykle načítají do nějakého bufferu, čili pole bajtů, intů, charů apod. Pokud má program vstupy špatně ošetřené, můžeme mu předat více dat, než se do jeho bufferu vejde, a přepsat tak paměť těsně za tímto bufferem. Toho se dá různými způsoby zneužít k napadení systému. Pokud budeme mít štěstí, oblast paměti za přetečeným bufferem bude patřit proměnné uchovávající heslo nebo název nějakého souboru. Tuto proměnou pak přepíšeme na nějakou jinou "naši" hodnotu.

Celá věc se ovšem musí provést opatrně, abychom se nepokusili zapisovat do paměti, ke které nemáme přístup (tedy za hranice zásobníku).

2. Typy zabezpečení

Bezpečnost je dnes samostatné odvětví IT. Skládá se z řady technologií a produktů. Jedním ze základů řešení bezpečnosti počítačové sítě je firewall.

2.1 Firewall

Ten původně chránil síť před nechtěným provozem. Například umožní přístup k webovému a poštovnímu serveru, veškerý další provoz je blokován. Postupně byly do firewallu integrovány mnohé další funkce. V prvé řade autentizace, to je ověření uživatele. Předtím než může uživatel přistupovat k síťovým zdrojům musí se přihlásit a ověřit, ať už vůči interní databázi uživatelů ve firewallu nebo externím autentizačním serveru - LDAP, RADIUS atd. Z důvodu snadné integrace do sítě firewally dnes plnohodnotně podporují směrování (RIP, OSPF, BGP atd.). Samozřejmostí je integrace VPN (IPSec, PPTP, L2TP) do firewallu. Má to řadu praktických důvodů. Nejdůležitější je ten, že provoz z/do VPN tunelu může být současně prověřen firewallem. VPN provoz je šifrován a pokud by byl VPN koncentrátor za firewallem, mohl by se do sítě dostat nežádoucí provoz bez možnosti jeho ověření a blokování. V každém případě integrované řešení velice usnadňuje implementaci a zvyšuje bezpečnost. Neméně důležité je dodržování určitých přenosových parametrů, což se označuje jako kvality služby (QoS) V dnešní době je stále populárnější VoIP. Telefonovat mezi pobočkami, ať už přes pevné linky nebo VPN bez dodržení QoS prakticky není možné. Nesprávná volba firewallu může implementaci a provozování podobných aplikací znemožnit.

Firewally se začaly implementovat v 90. letech minulého století a postupem času dosáhly téměř dokonalosti při ochraně před nebezpečím typickým v té době, tj. proti neoprávněnému přístupu do sítě. Samozřejmě tyto techniky a možnosti se využívají stále, ale v dnešní době se čím dál více útoků

odehrává na sedmé tj. aplikační vrstvě. Využívá se bezpečnostních nedostatků konkrétních aplikací - IIS nebo Apache web serverů. Tento typ útoků je na síťové vrstvě nedetekovatelný a ani aplikační brána nemůže vědět například o riziku přetečení zásobníku (buffer overflow) v konkrétní aplikaci.

2.2 Brutal Force Attack

U tohoto druhu napadení záleží na instalovaném systému. Útok je veden na specifický účet (login a heslo). Ochrana tedy spočívá v zablokování účtu nebo zablokování IP adresy(ze které se útok provádí), po několika neplatných pokusech. Veškeré pokusy o přihlášení jsou ukládány do log souboru, ze kterého se dá viník vypátrat.

2.3 Social Engineering

Základním pravidlem by mělo být utajování informací souvisejících s bezpečností. Měl by být stanoven okruh informací a lidí, kteří k nim mají přístup. Je zbytečné, aby manažeři znali přístupová hesla k hlavním systémům, i když to často vyžadují, spíše kvůli své pozici než ze skutečné nutnosti. Toto riziko lze eliminovat zavedením falešného administrátorského účtu s nízkým oprávněním. Funguje opravdu spolehlivě. Další nutnou věcí je důkladné proškolení všech uživatelů o tom, jaké informace a komu smějí předávat. Není na škodu občas prověřit dodržování takových opatření a směrnic. Rovněž je důležité neposkytovat více informací než je opravdu nutné a všechny informace, které nejsou nezbytně potřebné, vyhledat a stáhnout z veřejných zdrojů.

2.4 DoS

Ochrana proti DoS útokům patří mezi netriviální problémy i v dnešní době. Slabých míst, která může potenciální útočník využít, je totiž mnoho.

Ochrana na úrovni síťové vrstvy

Na síťové vrstvě je možné využít jednak přímo ochranných prvků jednotlivých operačních systémů(OS) a jednak specializovaných přídavných zařízení nebo modulů.

V oblasti ochranných prvků v rámci OS je typickou volbou použití vestavěného packetového filtru (umožňujícího mimo jiné omezit maximální počet spojení z konkrétní IP adresy nebo podsítě) a například povolení tzv. „SYN-cookies". Tato technika upravuje reakci OS na žádost o vytvoření spojení – příjem SYN packetu. Namísto vyhrazení místa v tabulce spojení je jako odpověď odeslán SYN/ACK packet, který má iniciální sekvenční číslo Initial Squence Number, dále jen „ISN") nastavené na výsledek jednocestné (hash) funkce aplikované na zdrojovou a cílovou adresu, zdrojový a cílový port a časově omezenou tajnou informaci. Při přijetí ACK packetu je potom ověřena shoda vráceného ISN pomocí stejného výpočtu. V případě shody je spojení přijato, v opačném případě odmítnuto. Tato metoda tedy efektivně znemožňuje provedení SYN-flood útoku, neboť nelze vyčerpat tabulku spojení pomocí pouhého zahlcení cílového systému proudem SYN packetů.

Komerčně nabízených ochranných prvků existuje nepřeberné množství, jedním z příkladů může být DefensePro, což je aktivní síťový prvek(switch), který zároveň funguje jako aplikační firewall chránící připojené systémy proti DoS/DDoS útokům, virovým útokům, útokům na aplikace (protokoly), pokusům o průnik atd.

Ochrana na úrovni http protokolu

V oblasti ochrany proti DoS útokům na úrovni protokolu http lze obecně nalézt softwarové produkty, které se snaží buď omezovat využití prostředků serveru podle přednastavených limitů a nebo se snaží útok rozpoznat dle průvodních příznaků a následně jej neutralizovat.

Typickým zástupcem omezování je modul mod_dosevasive pro Apache, který umožňuje nastavit limit na počet požadavků se stejným URL za jednotku času na konkrétního potomka (obslužný proces). Pokud některá IP adresa překročí daný limit, je na administrátorem definovanou dobu umístěna

na černou listinu (tedy na požadavky je odpovězeno chybovým kódem bez jakékoliv snahy o jejich uspokojení). V případě, že přicházejí další požadavky během doby, kdy je IP adresa na černé listině, je „trestný čas" počítán znovu od začátku. Modul je též schopen upozornit administrátora emailem na tuto situaci nebo spustit definovaný příkaz (program) – například pro umístění IP adresu na černou listinu na firewallu.

Oproti tomu Zeus Webserever, jenž je velmi podobný Apache, poskytuje nejen možnost nastavení limitů na jednotlivé IP adresy nebo skupiny IP adres, ale zároveň obsahuje i mechanismy, které se snaží rozpoznat probíhající útok. Tyto informace jsou navíc sdíleny všemi servery uvnitř clusteru, takže je ochrana více provázaných serverů jednodušší.

2.5 Obecné rady pro ochranu

- Aktualizace - Sledovat a aktualizovat firmware ve směrovačích, případně dalších síťových prvcích. Operační systémy a další SW vyžadují aktualizace pro řešení případných chyb a často přinášejí i nové funkce.

- Kvalitní a dobře zkonfigurované směrovače - Mnoho firem má účinné nástroje proti útokům zabudované ve směrovačích nebo v systémech. Problémem je, že o tom většinou ani nevědí a navíc je neumějí zkonfigurovat. Směrovač by měl splňovat požadavky a doporučení dle RFC 2827 a 2644, samozřejmostí je nastavení filtrování pro privátní sítě (RFC 1918).

- Ingress Filtering (RFC 2827) - Funkce směrovače, kdy po aktivaci je kontrolován každý paket, který má být směrován. Podmínkou je kontrola dostupnosti zdrojové adresy přes interface, z kterého jde ven. Pakety ze zfalšovanou zdrojovou IP adresou jsou odmítnuty. Filtrování má zamezit útokům, kdy příchozí paket má podvrženou

zdrojovou adresu používanou v interních podsítích nebo privátních sítích.

- Egress Filtering - Funkce směrovače, kdy je kontrolován každý paket odcházející přes směrovač nebo router z naší sítě. V případě, že zdrojová adresa není z rozsahu vnitřní sítě, jsou pakety ignorovány. Filtr má omezit nebezpečí zneužití sítě pro útok. Filtr nelze použít ke kontrole podvržených vnitřních adres a spíše je používán pouze Ingress Filtering.

- Firewall - Povolení jen používaných portů a omezení nebo zakázání paketů ICMP.

- Antivirové programy - ochrana proti virům a instalaci neoprávněných programů.

- Odpojení systému ze sítě - Někdy nezbývá jiná možnost, než dočasně odpojit systém od vnější sítě. Urychleně je však nutné provést opatření k omezení útoku a opětovnému připojení do sítě.

- Použití systému IDS (intrusion detection system) - Sleduje jednotlivé pakety a zjišťuje, zda nejsou používány k útoku nebo jiné neoprávněné činnosti. Někdy je zaměňován s firewallem, ale IDS má jinou funkci. Samotný firewall obvykle pouze povoluje nebo zakazuje přístup na základě určitých pravidel. V závislosti na nastavení a vlastnostech IDS jsme upozorněni při podezřele velkém počtu paketů SYN na síti, resp. počítači, případně velkém počtu paketů SYN používajících velké množství portů. Obojí totiž může znamenat útok, případně provádění skenování systému. Samotný princip IDS je podobný spíše antivirovému programu, je založen na detekci abnormálních (nezvyklých) činností (tím může

být nezvykle velký provoz, velké zatížení systémových prostředků,..) nebo detekcí nejznámějších útoků. V závislosti na konfiguraci pravidel je při útoku odesláno varování a může být zároveň překonfigurován firewall, aby blokoval útok.

3. Penetrační test

PENETRACE – míra odolnosti měřená hloubkou vniknutí zkušebního tělesa do zkoušeného materiálu
(Akademický slovník cizích slov)

Penetrační test je obvykle definován jako simulace hackera pokoušejícího se o průnik z internetu na veřejně přístupné servery a služby. Vyjdeme-li z definice slova „penetrace" uvedené na začátku tohoto oddílu, je vnímání „penetrační test = průnikový test" naprosto správné, nicméně jak bude ukázáno v následujících několika odstavcích, náplň penetračních testů je resp. může být podstatně širší než pouhé otestování odolnosti firemních WWW stránek.

3.1 Techniky a postupy

používané při penetračních testech lze velmi stručně charakterizovat následovně:

- *TCP/IP hacking* – prvním krokem testu je tzv. portscan (např. nástrojem NMAP), následuje použití automatických nástrojů pro testování slabin (např. ISS, CyberCop, Nessus), na základě výsledků automatizovaných testů je provedeno manuální testování a hlubší prozkoumání „podezřelých" nálezů (např. hledání slabin podobných některým veřejně publikovaným – nejčastěji používané

databáze slabin: BUGTRAQ, CVE) a některé specifické testy (např. útoky na heslo, útoky protokolem NETBIOS).

- *Dialup hacking* – použité techniky a metody jsou téměř totožné jako v předchozím případě, zadáním ovšem není seznam IP adres nýbrž seznam telefonních čísel (případně rozsah telefonních čísel, u kterých je metodou tzv. wardialingu testována přítomnost modemu), konkrétní provedení je velmi závislé na způsobu provozu testovaného modemového připojení.

- *„social" hacking* – při tomto testu je jednak testována účinnost antivirové ochrany vůči virům přicházejícím z internetu (elektronickou poštou nebo stažením zavirovaného souboru internetovým prohlížečem – tj. protokolem FTP, HTTP nebo HTTPS), dále lze použitím testovacího trojského koně změřit, jaké procento uživatelů spustí podezřelou přílohu e-mailové zprávy a zároveň lze v praxi demonstrovat hrozby, které ze strany skutečných trojských koní vyplývají (např. vyzrazení prakticky libovolného dokumentu, ke kterému má uživatel přístup).

Vnější test je možno provádět v několika variantách:

- *se znalostí vs. bez znalosti* – test „bez znalosti" předpokládá omezenou, případně žádnou znalost konzultanta o prostředí podniku a tím je velmi blízký reálnému útoku, test „se znalostí" se naopak opírá o detailní informace o testovaném prostředí (např. síťová topologie, detaily o provozovaných aplikacích, popis bezpečnostních mechanizmů apod.),

- *skrytý vs. kooperativní* – o skrytém testu nejsou informováni řadoví pracovníci systémové podpory podniku, čímž se prováděný test blíží reálnému pokusu o průnik a prověří reakční mechanizmy

při skutečném útoku, zatímco kooperativní penetrační test staví na plné informovanosti a spolupráci zainteresovaných pracovníků systémové podpory.

Interní test se pochopitelně vždy provádí ve spolupráci s pracovníky systémové podpory podniku a s plnou znalostí o jeho prostředí. U vnitřního testu, vzhledem k poměrně velkému počtu zařízení ve vnitřní síti a vysoké pracnosti manuálního testování, se obvykle v prvním kroku provádí automatizovaný test všech zařízení, ale důkladným manuálním testů jsou podrobena pouze vybraná zařízení (obvykle klíčové servery příp. vybrané pracovní stanice).

3.2 Výsledek penetračního testu

Výsledek penetračního testu nám poskytne obrázek o tom, čeho by při současné úrovni znalostí mohl dosáhnout útočník při reálném útoku. Vzhledem k tomu, že konzultant provádějící penetrační test používá velmi podobné nástroje, techniky a postupy jako reální útočníci, je hlavním přínosem penetračního testu praktické prověření bezpečnostních mechanizmů. Výsledkem testu je poměrně přesný obrázek o tom, čeho by mohl dosáhnout v případě skutečného útoku reálný útočník při aktuální úrovni znalostí o bezpečnostních slabinách a úrovni v současnosti dostupných technických prostředků.

V následujících bodech jsou další velmi podstatné skutečnosti týkající se výsledků penetračních testů:

- Problematickým bodem penetračních testů je faktor času. Pokud budeme srovnávat konzultanta provádějícího penetrační test a reálného útočníka, je možné předpokládat zhruba stejnou úroveň znalostí, přibližně stejné nástroje, techniky a použité postupy, ovšem zcela zjevnou nevýhodou konzultanta je časové omezení (u

externích testů obvykle několik dní). V porovnání s konzultantem může reálný útočník přípravě i vlastnímu provedení pokusu o průnik věnovat podstatně více času a tím výrazně zvýšit své šance na „úspěch".

- Je třeba si uvědomit, že zjištění učiněná v rámci penetračního testu vypovídají o účinnosti bezpečnostních opatření při úrovni znalostí (publikované bezpečnostní slabiny apod.) a úrovni dostupných technických prostředků v době provádění testu, z čehož logicky vyplývá, že vypovídací hodnota výsledku penetračního testu, a to ať mluvíme o externím nebo interním, s postupem času klesá (jsou publikovány nové bezpečnostní slabiny, jsou zveřejněny nové techniky průniků apod.).

- Ani negativní výsledek penetračního testu neznamená odhalení absolutně všech bezpečnostních slabin testovaných komponent (operačních systémů, aplikací apod.) – dosavadní zkušenosti jednoznačně ukazují, že četnost odhalování nových bezpečnostních slabin v běžně provozovaných aplikacích a systémech s postupem času rozhodně neklesá, ba naopak díky snaze výrobců předehnat konkurenci jsou často uváděny na trh produkty, u nichž bezpečnost jejich provozu rozhodně nebyla prioritou jejich autorů.

- V rámci penetračního testu nejsou ovšem podrobena testování pouze technická opatření, v případě skrytého testu to jsou rovněž opatření organizační (zejména kontrolní a monitorovací mechanizmy související s dozorem testovaných zařízení a systémů). Ačkoli nám to může připadat jako okrajová záležitost, ale praktické zkušenosti jsou velmi alarmující – např. je naprosto běžné, že v případě „úspěšné" penetrace systémoví administrátoři

tento incident vůbec nezaregistrují (příklad z praxe: penetrován firewall a na něm následně založen nový uživatel nebo kompromitován WWW server a následně instalován backdoor – v obou případech se administrátoři o průniku dozvěděli až na prezentaci výsledků penetračního testu). Pochopitelně pokud jde o životně důležité služby, jejichž nefunkčnost je „očividná" (např. elektronická pošta), jsou problémy identifikovány poměrně rychle, většinou ovšem není zjišťována příčina, ale pouze řešeny následky.

3.3 Princip a filozofie

Penetrační testy spolu například s bezpečnostními audity patří do skupiny služeb, které by se daly označit jako „kontrolní". To znamená, že cílem penetračního testu není vyřešit bezpečnostní problémy testovaných zařízení, systémů nebo aplikací, ale jistým způsobem (v případě penetračního testu simulací pokusu o průnik) prověřit a zhodnotit úroveň zabezpečení, a to jak na úrovni technických, tak i organizačních opatření.

Obsahem závěrečné zprávy o průběhu a výsledcích penetračního testu jsou pochopitelně také konkrétní návrhy opatření, která nějakým způsobem eliminují nalezené slabiny, tato opatření ovšem rozhodně nelze vnímat tak, že jejich implementací vyřešíme všechny otázky zabezpečení testovaných zařízení. Vzhledem k tomu, že základní filozofií penetračního testu je simulace pokusu o průnik prostřednictvím sítě (ať už z internetu nebo z vnitřní LAN) – zjednodušeně řečeno „z dálky", existuje celá řada slabin, které obvykle nejsou, a ani z principu nemohou být v rámci penetračního testu odhaleny.

Mezi příklady toho, co penetrační test rozhodně neodhalí patří jakékoli slabiny související s fyzickou bezpečností, chybně nastavená přístupová práva, logování nebo systémový audit, nedostatečná pravidla řízení přístupu (např. triviální hesla, která se čistě náhodou nepodařilo „uhádnout"),

penetrační test není schopen detekovat dřívější napadení systému, na základě testu nelze např. posoudit celkovou koncepci bezpečnosti apod.

Na druhou stranu je penetrační test prakticky jediným způsobem jak například odhalit, že se systém nebo aplikace chová jinak než deklaruje její výrobce resp. dodavatel – např. za jistých okolností dojde k jejímu zhroucení, zahlcení, je možno obejít formálně velmi přísné bezpečnostní mechanizmy, nalezenou slabinu lze zneužít např. k získání neoprávněného přístupu k datům v systému apod.

3.4 Penetrační test vs. bezpečnostní audit

Bezpečnostní audit i penetrační test patří společně do skupiny kontrolních služeb souvisejících s informační bezpečností. Z toho vyplývá, že obě tyto služby mají za cíl posoudit úroveň zabezpečení aplikací, systémů nebo zařízení, která jsou předmětem testu resp. auditu. Mezi odborníky se můžeme setkat s různými pohledy na vztah mezi penetračním testem a bezpečnostním auditem, někteří tvrdí, že penetrační test je nejvyšší možný stupeň jistoty zabezpečení, naopak jiní považují penetrační test za nahodilý, nesystematický způsob posouzení bezpečnosti, jehož negativní výsledek spíše vytváří iluzi o úrovni bezpečnostních opatření. Jak už to tak obvykle chodí, pravda je někde uprostřed mezi těmito extrémními názory. Pro lepší názornost následuje charakterizování služeb na analogii s domem a záměrem zjistit jeho odolnost proti vloupání.

- **Penetrační test** – v tomto případě si najmeme odborníka, kterého postavíme před zamčený dům a aniž by jsme mu sdělili jakékoli další informace požádáme ho, aby se pokusil proniknout dovnitř (analogie: najmeme si konzultanta, který se snaží kompromitovat např. naši kritickou WWW aplikaci).

- **Bezpečnostní audit** – zde si opět povoláme odborníka, kterému předáme plán domu a klíče a požádáme ho, aby posoudil, jak je dům odolný proti zlodějům (analogie: při auditu WWW serveru se auditor přihlásí k serveru s oprávněním správce a při posuzování má k dispozici kompletní informaci o nastavení operačního systému, jednotlivých aplikací apod.).

Již v předchozí části příspěvku byly uvedeny příklady bezpečnostních slabin, které nelze (nebo jen velmi obtížně) v rámci penetračního testu odhalit a naopak příklady slabin, které lze odhalit de facto pouze penetračním testem. Podíváme-li se na zmíněné příklady slabin z pohledu bezpečnostního auditu, zjistíme, že to, co penetrační test neodhalí (nedostatečná fyzická bezpečnost, nastavení přístupových práv, pravidla řízení přístupu, zakládání/rušení uživatelů apod.) je téměř vždy předmětem šetření v rámci bezpečnostního auditu, který případné slabiny odhalí.

Penetrační test a bezpečnostní audit nelze považovat za konkurenční, vzájemně nahraditelné služby, ale za služby, které se velmi vhodně doplňují. Z tohoto důvodu je v praxi velmi často nabízen bezpečnostní audit společně s penetračním testem, neboť kombinace obou těchto produktů poskytuje velmi komplexní obrázek o úrovni zabezpečení prověřovaného zařízení, systému nebo aplikace.

4. Provedení penetračního testu

Tato kapitola obsahuje výsledky penetračního testu, který byl prováděn pro sdružení Southgate.

Cílem tohoto testu bylo zjištění bezpečnosti webových serverů provozovaných sdružením Southgate z pohledu Internetu.

Test zahrnuje :

Passive mapping of client environment – pasivní prohledání klientského prostředí znamená, získání co možná největšího počtu informací o cílové síti a to tak, aby nebyly patrné nějaké neobvyklé aktivity, které by varovali administrátory. Toto zahrnuje použití všech možných standardních nástrojů, jako je dig, host, atd. Také sem patří získávání informací z cílové stránky, e-mailových zpráv atd.

Active mapping of client environment – zahrnuje aktivity, které jsou zaměřovány na cílové stroje. Chceme porozumět, jaké další služby stroje nabízejí. Jak je síť chráněna(jestliže je) a jak je nastaven firewall(pokud nějaký je). K aktivnímu mapování se používají speciální utility, které mohou zanechat stopy v nějakém logu.

Application testing – použití speciálních scannerů, které jsou schopné prohledat určitý počet aplikací, jejich nastavení, verze, konfigurace a porovnat jej podle databáze již známých bezpečnostních děr.

Test nezahrnuje :

Zjišťování a odhalování (ne)zabezpečených bezdrátových sítí

Speciální softwarové programování(viry/červy)

Rozsáhlé aplikační testování

DoS nebo DDoS útoky

Využití aplikačních exploitů

4.1 Technické detaily

Penetrační test probíhal od 18.04.06 – 25.04.06. K testování byl použit počítač AMD Barton 2500+ s operačním systémem Windows XP professional. Počítal byl připojen do sítě CZFreeCB. Veškerý provoz byl povolen(žádný firewall na routerech nebyl použit). Na počítači byl nainstalován firewall z důvodů povolení pouze důležitého provozu. Počítač vystupoval pod IP adresou 10.108.20.108. Část testů musela být provedena na linuxové platformě, pro kterou jsou vybral jednu z nejstarších nekomerčních distribucí - Slackware ve verzi 2.6.11.7

4.2 Pasivní prohledávání

4.2.1 DNS

Na samém začátku je potřeba zjistit veškeré informace dostupné na internetu o daném subjektu, bez použití takových úkonů, které by mohli vést k našemu odhalení.

Prvně vyzkoušíme příkaz whois(whois je služba, která zjišťuje informace o doméně v centrálním registru):

```
c:\dig\Win>whois southgate.cz
% This whois looks up records in off-line generated
% database maintained by the CZ.NIC. Results needn't
% contain all available information, see also on-line full
% information search service at the web-site http://www.nic.cz/
%
% Rights restricted by copyright.
% See http://www.nic.cz/en/copyright.php
% WHOISD server version: 2.2.3 build: Oct 14 2005 11:45:00
% Server id: #whois-2/p
```

```
% Timestamp: 22.04.2006 (dd.mm.yyyy) 09:02 (hh:mm) CEST

domain:         southgate.cz
descr:          SouthGate CZFreeCB
admin-c:        SOUTHGATE
tech-c:         WEB4U
reg-c:          REG-WEB4U
nserver:        ns.southgate.cz ns2.southgate.cz
glue:           ns.southgate.cz 88.146.126.2
glue:           ns2.southgate.cz 88.146.126.3
created:        20050216
changed:        20060324
expire:         20070216


role:           SouthGate CZFreeCB
address:        Doubravice 65
address:        Ceske Budejovice
address:        37006
address:        The Czech Republic
admin-c:        SOUTHGATE_ADMIN
tech-c:         SOUTHGATE_ADMIN
nic-hdl:        SOUTHGATE
e-mail:         info@southgate.cz
created:        20050215
changed:        20050215

role:           Web4U s.r.o.
address:        Tyrsova 551
address:        Jindrichuv Hradec II
address:        377 01
address:        The Czech Republic
admin-c:        CUCKOO
admin-c:        LUKU
nic-hdl:        WEB4U
e-mail:         info@web4u.cz
created:        20010810
changed:        20030911

person:         Radovan Moser
address:        Doubravice 65
```

```
address:        Ceske Budejovice
address:        37006
address:        The Czech Republic
phone:          +420.775304554
nic-hdl:        SOUTHGATE_ADMIN
e-mail:         moser@patrokolos.cz
created:        20050215
changed:        20050215

person:         Martin Kukacka
address:        Tyrsova 551
address:        Jindrichuv Hradec II
address:        377 01
address:        The Czech Republic
phone:          +420.777838738
fax-no:         +420.543254384
nic-hdl:        CUCKOO
e-mail:         domeny@web4u.cz
created:        20010810
changed:        20031021

person:         Lukas Kunovsky
address:        Straznicka 1
address:        Brno - Slatina
address:        627 00
address:        The Czech Republic
phone:          +420.543254362
fax-no:         +420.543254384
nic-hdl:        LUKU
e-mail:         domeny@web4u.cz
created:        20020309
changed:        20040227

Total 6 records
```

Nic zajímavého jsme nezjistili. Pouze jméno osoby, na kterou je doména registrována(adresu,e-mail,telefon) a přítomnost name serveru.

```
c:\dig\Win>dig southgate.cz any

; <<>> DiG 9.3.2 <<>> southgate.cz any
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 598
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 8, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;southgate.cz.                  IN      ANY

;; ANSWER SECTION:
southgate.cz.                  86400     IN          SOA        ns.southgate.cz.
dns.southgate.cz. 2006040308 3600 1800 604800 900

southgate.cz.            86400    IN       TXT      "CZFree http://www.czfree.net
(NonComercial NETwork Czech Republic)"

southgate.cz.                       86400      IN           TXT          "CZFreeCB
http://www.czfreecb.net (NonComercial NETwork Ceske Budejovice)"

southgate.cz.                86400     IN         TXT        "SouthGate CZFreeCB
http://www.southgate.cz (Civil Corporation - Internet connection)"

southgate.cz.            86400    IN       NS       ns.southgate.cz.

southgate.cz.            86400    IN       NS       ns2.southgate.cz.

southgate.cz.            86400    IN       MX       10 mail.southgate.cz.

southgate.cz.             86400    IN        LOC      48 56 0.000 N 14 31 0.000 E
520.00m 1m 10000m 10m


;; Query time: 125 msec
;; SERVER: 10.108.15.1#53(10.108.15.1)
;; WHEN: Sat Apr 22 12:36:01 2006
;; MSG SIZE  rcvd: 415
```

Nyní již víme, že jmenné servery pro doménu jsou ns.southgate.cz a ns2.southgate.cz(jako sekundární). Také již víme, že poštovní službu zajišťuje stroj mail.southgate.cz. Z výpisu je také jasné, že se jedná o nekomerční síť v České republice a že se nachází v Českých Budějovicích.

Je celkem zvláštní používat pouze jeden stroj na poštovní služby. Pokud by stroj na obstarávání poštovních služeb selhal, bylo by doručování pošty na doménu v nesnázích. Raději se tedy ještě jednou ujistíme příkazem

dig s parametrem „MX“, který nám vypíše pouze informace o poštovních serverech.

```
C:\dig\Win>dig southgate.cz mx

; <<>> DiG 9.3.2 <<>> southgate.cz mx
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 1931
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 0

;; QUESTION SECTION:
;southgate.cz.                  IN      MX

;; ANSWER SECTION:
southgate.cz.           86400   IN      MX      10 mail.southgate.cz.

;; AUTHORITY SECTION:
southgate.cz.           86400   IN      NS      ns2.southgate.cz.
southgate.cz.           86400   IN      NS      ns.southgate.cz.

;; Query time: 125 msec
;; SERVER: 10.108.15.1#53(10.108.15.1)
;; WHEN: Sat Apr 22 16:38:44 2006
;; MSG SIZE  rcvd: 86
```

I po dalším testu jsme objevili jen jeden poštovní server. Vyzkoušel jsem ještě další jiné testy, ani ty však neprokázaly výskyt dalšího poštovního serveru.

Teď vyzkoušíme nslookup. V podstatě dostaneme ty samé informace, ale v jiném formátu. Je lepší používat více nástrojů, abychom měli více pohledů na danou věc. Zapneme také debug mód. Může být dobrý pro testovací(a naše) účely, protože nám může dát spoustu důležitých informací.

```
C:\Documents and Settings\Taker>nslookup
Výchozí server:   server.southgate.cz
Address:  10.108.15.1

> set db2
> set q=any
> set debug
```

```
> southgate.cz
Server:  server.southgate.cz
Address:  10.108.15.1

------------
Got answer:
    HEADER:
        opcode = QUERY, id = 2, rcode = NOERROR
        header flags:  response, auth. answer, want recursion, recursion avail.
        questions = 1,  answers = 8,  authority records = 0,  additional = 0

    QUESTIONS:
        southgate.cz, type = ANY, class = IN
    ANSWERS:
    ->  southgate.cz
        ttl = 86400 (1 day)
        primary name server = ns.southgate.cz
        responsible mail addr = dns.southgate.cz
        serial  = 2006040308
        refresh = 3600 (1 hour)
        retry   = 1800 (30 mins)
        expire  = 604800 (7 days)
        default TTL = 900 (15 mins)
    ->  southgate.cz
        text =
        "CZFreeCB    http://www.czfreecb.net    (NonComercial    NETwork    Ceske
Budejovice)"
        ttl = 86400 (1 day)
    ->  southgate.cz
        text =
        "SouthGate   CZFreeCB   http://www.southgate.cz   (Civil   Corporation   -
Internet connection)"
        ttl = 86400 (1 day)
    ->  southgate.cz
        text =
        "CZFree http://www.czfree.net (NonComercial NETwork Czech Republic)"
        ttl = 86400 (1 day)
    ->  southgate.cz
        nameserver = ns.southgate.cz
        ttl = 86400 (1 day)
    ->  southgate.cz
```

```
        nameserver = ns2.southgate.cz
        ttl = 86400 (1 day)
    -> southgate.cz
        MX preference = 10, mail exchanger = mail.southgate.cz
        ttl = 86400 (1 day)
    -> southgate.cz
        ??? unknown type 29 ???
        ttl = 86400 (1 day)

------------
southgate.cz
        ttl = 86400 (1 day)
        primary name server = ns.southgate.cz
        responsible mail addr = dns.southgate.cz
        serial  = 2006040308
        refresh = 3600 (1 hour)
        retry   = 1800 (30 mins)
        expire  = 604800 (7 days)
        default TTL = 900 (15 mins)
southgate.cz
        text =
        "CZFreeCB  http://www.czfreecb.net  (NonComercial  NETwork  Ceske
Budejovice)"
        ttl = 86400 (1 day)
southgate.cz
        text =
        "SouthGate  CZFreeCB  http://www.southgate.cz  (Civil  Corporation  -
Internet connection)"
        ttl = 86400 (1 day)
southgate.cz
        text =
        "CZFree http://www.czfree.net (NonComercial NETwork Czech Republic)"
        ttl = 86400 (1 day)
southgate.cz
        nameserver = ns.southgate.cz
        ttl = 86400 (1 day)
southgate.cz
        nameserver = ns2.southgate.cz
        ttl = 86400 (1 day)
southgate.cz
        MX preference = 10, mail exchanger = mail.southgate.cz
```

```
        ttl = 86400 (1 day)
```

Před tím než budeme pokračovat, stručně se podíváme na výsledek. Žádné nové informace v IP adresách/jménech nejsou. Avšak hned na začátku můžeme vidět:

header flags: ..... want recursion, recursion avail.

Tzn., že server server podporuje rekusivní dotazy. K tomu co to znamená se dostaneme později.

Nyní pro dotaz použijeme jeden z jmenných serverů southgate.cz.

```
> server ns.southgate.cz
------------
Got answer:
    HEADER:
        opcode = QUERY, id = 3, rcode = NOERROR
        header flags:  response, auth. answer, want recursion, recursion avail.
        questions = 1,  answers = 2,  authority records = 2,  additional = 0

    QUESTIONS:
        ns.southgate.cz, type = A, class = IN
    ANSWERS:
    ->  ns.southgate.cz
        canonical name = server.southgate.cz
        ttl = 86400 (1 day)
    ->  server.southgate.cz
        internet address = 10.108.15.1
        ttl = 86400 (1 day)
    AUTHORITY RECORDS:
    ->  southgate.cz
        nameserver = ns.southgate.cz
        ttl = 86400 (1 day)
    ->  southgate.cz
        nameserver = ns2.southgate.cz
        ttl = 86400 (1 day)

------------
Výchozí server:   server.southgate.cz
Address:  10.108.15.1
Aliases:  ns.southgate.cz
```

```
> southgate.cz
Server:  server.southgate.cz
Address:  10.108.15.1
Aliases:  ns.southgate.cz

------------
Got answer:
    HEADER:
        opcode = QUERY, id = 4, rcode = NOERROR
        header flags:  response, auth. answer, want recursion, recursion avail.
        questions = 1,  answers = 8,  authority records = 0,  additional = 0

    QUESTIONS:
        southgate.cz, type = ANY, class = IN
    ANSWERS:
    ->  southgate.cz
        ttl = 86400 (1 day)
        primary name server = ns.southgate.cz
        responsible mail addr = dns.southgate.cz
        serial  = 2006040308
        refresh = 3600 (1 hour)
        retry   = 1800 (30 mins)
        expire  = 604800 (7 days)
        default TTL = 900 (15 mins)
    ->  southgate.cz
        text =
        "CZFree http://www.czfree.net (NonComercial NETwork Czech Republic)"
        ttl = 86400 (1 day)
    ->  southgate.cz
        text =
        "CZFreeCB   http://www.czfreecb.net   (NonComercial   NETwork   Ceske
Budejovice)"
        ttl = 86400 (1 day)
    ->  southgate.cz
        text =
        "SouthGate  CZFreeCB  http://www.southgate.cz  (Civil  Corporation  -
Internet connection)"
        ttl = 86400 (1 day)
    ->  southgate.cz
        nameserver = ns2.southgate.cz
        ttl = 86400 (1 day)
```

```
    -> southgate.cz
       nameserver = ns.southgate.cz
       ttl = 86400 (1 day)
    -> southgate.cz
       MX preference = 10, mail exchanger = mail.southgate.cz
       ttl = 86400 (1 day)
    -> southgate.cz
       ??? unknown type 29 ???
       ttl = 86400 (1 day)

------------
southgate.cz
       ttl = 86400 (1 day)
       primary name server = ns.southgate.cz
       responsible mail addr = dns.southgate.cz
       serial  = 2006040308
       refresh = 3600 (1 hour)
       retry   = 1800 (30 mins)
       expire  = 604800 (7 days)
       default TTL = 900 (15 mins)
southgate.cz
       text =
       "CZFree http://www.czfree.net (NonComercial NETwork Czech Republic)"
       ttl = 86400 (1 day)
southgate.cz
       text =
       "CZFreeCB   http://www.czfreecb.net   (NonComercial   NETwork   Ceske
Budejovice)"
       ttl = 86400 (1 day)
southgate.cz
       text =
       "SouthGate  CZFreeCB  http://www.southgate.cz  (Civil  Corporation  -
Internet connection)"
       ttl = 86400 (1 day)
southgate.cz
       nameserver = ns2.southgate.cz
       ttl = 86400 (1 day)
southgate.cz
       nameserver = ns.southgate.cz
       ttl = 86400 (1 day)
southgate.cz
```

```
        MX preference = 10, mail exchanger = mail.southgate.cz
        ttl = 86400 (1 day)
```

Zde je nejdůležitější úsek:

```
southgate.cz
        ttl = 86400 (1 day)
        primary name server = ns.southgate.cz
        responsible mail addr = dns.southgate.cz
        serial  = 2006040308
        refresh = 3600 (1 hour)
        retry   = 1800 (30 mins)
        expire  = 604800 (7 days)
        default TTL = 900 (15 mins)
```

Ze sériového čísla(které je v doporučeném formátu YYYMMDDxx), zjistíme, že poslední změna byla provedena (30.04.2006). Je to pouze kousek informace, která však může odhalit chování administrátora.

Podíváme se dále na rekurzivní dotazy na ns.southgate.cz. Zeptáme se jmenného serveru southgate.cz na informaci o doméně centrum.cz. Jestliže budou fungovat rekurzivní dotazy, může je potenciální útočník využít k různým účelům.

```
> centrum.cz
Server:  server.southgate.cz
Address:  10.108.15.1
Aliases:  ns.southgate.cz


------------
Got answer:
    HEADER:
        opcode = QUERY, id = 5, rcode = NOERROR
        header flags:  response, want recursion, recursion avail.
        questions = 1,  answers = 8,  authority records = 2,  additional = 4

    QUESTIONS:
        centrum.cz, type = ANY, class = IN
    ANSWERS:
    ->  centrum.cz
        nameserver = host1.netcentrum.cz
```

```
        ttl = 2115 (35 mins 15 secs)
    -> centrum.cz
        nameserver = host2.netcentrum.cz
        ttl = 2115 (35 mins 15 secs)
    -> centrum.cz
        MX preference = 10, mail exchanger = mail8.centrum.cz
        ttl = 600 (10 mins)
    -> centrum.cz
        MX preference = 10, mail exchanger = mail1.centrum.cz
        ttl = 600 (10 mins)
    -> centrum.cz
        MX preference = 10, mail exchanger = mail2.centrum.cz
        ttl = 600 (10 mins)
    -> centrum.cz
        MX preference = 10, mail exchanger = mail5.centrum.cz
        ttl = 600 (10 mins)
    -> centrum.cz
        MX preference = 10, mail exchanger = mail6.centrum.cz
        ttl = 600 (10 mins)
    -> centrum.cz
        MX preference = 10, mail exchanger = mail7.centrum.cz
        ttl = 600 (10 mins)
    AUTHORITY RECORDS:
    -> centrum.cz
        nameserver = host2.netcentrum.cz
        ttl = 2115 (35 mins 15 secs)
    -> centrum.cz
        nameserver = host1.netcentrum.cz
        ttl = 2115 (35 mins 15 secs)
    ADDITIONAL RECORDS:
    -> host1.netcentrum.cz
        internet address = 213.29.7.239
        ttl = 1370 (22 mins 50 secs)
    -> host2.netcentrum.cz
        internet address = 81.0.254.36
        ttl = 2352 (39 mins 12 secs)
    -> mail1.centrum.cz
        internet address = 213.29.7.233
        ttl = 1436 (23 mins 56 secs)
    -> mail6.centrum.cz
        internet address = 213.29.7.198
```

```
        ttl = 411 (6 mins 51 secs)

------------
centrum.cz
        nameserver = host1.netcentrum.cz
        ttl = 2115 (35 mins 15 secs)
centrum.cz
        nameserver = host2.netcentrum.cz
        ttl = 2115 (35 mins 15 secs)
centrum.cz
        MX preference = 10, mail exchanger = mail8.centrum.cz
        ttl = 600 (10 mins)
centrum.cz
        MX preference = 10, mail exchanger = mail1.centrum.cz
        ttl = 600 (10 mins)
centrum.cz
        MX preference = 10, mail exchanger = mail2.centrum.cz
        ttl = 600 (10 mins)
centrum.cz
        MX preference = 10, mail exchanger = mail5.centrum.cz
        ttl = 600 (10 mins)
centrum.cz
        MX preference = 10, mail exchanger = mail6.centrum.cz
        ttl = 600 (10 mins)
centrum.cz
        MX preference = 10, mail exchanger = mail7.centrum.cz
        ttl = 600 (10 mins)

centrum.cz
        nameserver = host2.netcentrum.cz
        ttl = 2115 (35 mins 15 secs)
centrum.cz
        nameserver = host1.netcentrum.cz
        ttl = 2115 (35 mins 15 secs)
host1.netcentrum.cz
        internet address = 213.29.7.239
        ttl = 1370 (22 mins 50 secs)
host2.netcentrum.cz
        internet address = 81.0.254.36
        ttl = 2352 (39 mins 12 secs)
mail1.centrum.cz
```

```
        internet address = 213.29.7.233
        ttl = 1436 (23 mins 56 secs)
mail6.centrum.cz
        internet address = 213.29.7.198
        ttl = 411 (6 mins 51 secs)
```

Rekurzivní dotazy jsou aktivní. Měly by sloužit pouze pro naše účely a v našem prostředí.

Využívání našeho DNS k dalšímu rekurzivním dotazům by mohlo způsobit:

- Zatížení našeho serveru – ostatní uživatelé internetu mohou náš DNS server využít pro jejich rekurzivní dotazy.

- Schování něčí identity – Někdo může využít DNS server pro rekurzivní dotazy na potenciální cíl útoku. Jeho identita zůstane v tomto případě schována. Veškeré dotazy budou provedeny naším DNS serverem.

- Stát se součástí DDoS útoku – protože rekurzivní dotazy v sobě nesou mnohem více informací než normální dotazy, mohly by být použity ke generování provozu.Vytvořením UDP DNS paketů ve kterých útočník změní odchozí adresu(jeho cíl), může vytvořit rekurzivní dotazy. Jejich odpovědi budou doručeny danému cíli. Podle jeho vytvořených paketů to vypadá, že daný cíl je chce. Avšak tisíce takovýchto paketů z různých DNS serverů mohou být nasměrovány v jeden čas na jeden cíl. To může potenciálně vést k zahlcení cílové síťové linky. Zlomyslný útočník tak zůstane perfektně ukrytý i v tomto případě.

- DNS cache poisoning – Útočníkův DNS server s odpovědí na požadavek, pošle také „otrávený" záznam o jiné doméně, který dns server zařadí do svojí dns-cache. DNS servery tuto informaci

začnou používat. Avšak nebudou kontrolovat, jestli je informace pravdivá nebo nepravdivá.

- Existují další možné útoky, jejich popis však nebylo možné zařadit z důvodu rozsahu práce.

Zopakujme si tedy nyní vše, co již víme doméně southgate.cz. K potvrzení dosavadních informací použijeme http://www.geektools.com:


```
Final results obtained from whois.ripe.net.
Results:
% This is the RIPE Whois query server #1.
% The objects are in RPSL format.
%
% Note: the default output of the RIPE Whois server
% is changed. Your tools may need to be adjusted. See
% http://www.ripe.net/db/news/abuse-proposal-20050331.html
% for more details.
%
% Rights restricted by copyright.
% See http://www.ripe.net/db/copyright.html

% Note: This output has been filtered.
% To receive output for a database update, use the "-B" flag.

% Information related to '88.146.126.0 - 88.146.126.255'

inetnum: 88.146.126.0 - 88.146.126.255
netname: SOUTHGATECB
```

```
descr: SouthGate CZFreeCB
country: CZ
admin-c: SC5628-RIPE
tech-c: SC5628-RIPE
status: ASSIGNED PA
mnt-by: VIDEOONLINE-MNT
mnt-lower: VIDEOONLINE-MNT
source: RIPE # Filtered
person: SouthGate CZFreeCB
address: SouthGate CZFreeCB
Doubravice 65
Ceske Budejovice
370 06
Czech Republic
phone: +420 775 304 554
phone: +420 606 767 463
nic-hdl: SC5628-RIPE
abuse-mailbox: southgate_czfreecb@paleo.cz
source: RIPE # Filtered
% Information related to '88.146.0.0/17AS6706'
route: 88.146.0.0/17
descr: Czech On Line a.s. Praha
origin: AS6706
mnt-by: VIDEOONLINE-MNT
source: RIPE # Filtered
```

Southgate.cz využívá celou třídu C IP adres '88.146.126.0 - 88.146.126.255'.

```
; <<>> DiG 9.3.2 <<>> southgate.cz axfr
;; global options:  printcmd
southgate.cz.                   86400     IN          SOA         ns.southgate.cz.
dns.southgate.c
z. 2006040308 3600 1800 604800 900
southgate.cz.             86400    IN       TXT      "CZFree http://www.czfree.net
(NonComercial NETwork Czech Republic)"
southgate.cz.                       86400      IN            TXT          "CZFreeCB
http://www.czfreecb.ne
t (NonComercial NETwork Ceske Budejovice)"
southgate.cz.                 86400     IN          TXT        "SouthGate CZFreeCB
http://www.southgate.cz (Civil Corporation - Internet connection)"
```

```
southgate.cz.            86400   IN      NS      ns.southgate.cz.
southgate.cz.            86400   IN      NS      ns2.southgate.cz.
southgate.cz.            86400   IN      MX      10 mail.southgate.cz.
southgate.cz.            86400   IN      LOC     48 56 0.000 N 14 31 0.000 E
520.
00m 1m 10000m 10m
daath.southgate.cz.      86400   IN      CNAME   services.southgate.cz.
pc.davidos.southgate.cz. 86400   IN      A       10.108.18.108
dchub.southgate.cz.      86400   IN      CNAME   services.southgate.cz.
dns.southgate.cz.        86400   IN      CNAME   server.southgate.cz.
dns2.southgate.cz.       86400   IN      CNAME   services.southgate.cz.
dude.southgate.cz.       86400   IN      A       10.108.15.7
firewall.southgate.cz.   86400   IN      A       10.108.15.3
forum.southgate.cz.      86400   IN      CNAME   services.southgate.cz.
ftp.southgate.cz.        86400   IN      CNAME   services.southgate.cz.
irc.southgate.cz.        86400   IN      CNAME   services.southgate.cz.
mail.southgate.cz.       86400   IN      CNAME   server.southgate.cz.
mysql.southgate.cz.      86400   IN      CNAME   services.southgate.cz.
nat1.southgate.cz.       86400   IN      CNAME   firewall.southgate.cz.
nat2.southgate.cz.       86400   IN      CNAME   firewall.southgate.cz.
nat3.southgate.cz.       86400   IN      CNAME   firewall.southgate.cz.
nat4.southgate.cz.       86400   IN      CNAME   firewall.southgate.cz.
nat5.southgate.cz.       86400   IN      CNAME   firewall.southgate.cz.
nat6.southgate.cz.       86400   IN      CNAME   firewall.southgate.cz.
nat7.southgate.cz.       86400   IN      CNAME   firewall.southgate.cz.
nat8.southgate.cz.       86400   IN      CNAME   firewall.southgate.cz.
nat9.southgate.cz.       86400   IN      CNAME   firewall.southgate.cz.
ns.southgate.cz.         86400   IN      CNAME   server.southgate.cz.
ns2.southgate.cz.        86400   IN      CNAME   services.southgate.cz.
ntp.southgate.cz.        86400   IN      CNAME   services.southgate.cz.
pc.pambroz.southgate.cz. 86400   IN      A       10.108.17.117
pop3.southgate.cz.       86400   IN      CNAME   server.southgate.cz.
pc.pupik.southgate.cz.   86400   IN      A       10.108.15.15
server.southgate.cz.     86400   IN      A       10.108.15.1
services.southgate.cz.   86400   IN      A       10.108.15.4
smtp.southgate.cz.       86400   IN      CNAME   server.southgate.cz.
pc.taker.southgate.cz.   86400   IN      A       10.108.18.8
*.tcp.southgate.cz.      86400   IN      SRV     0 0 0 .
finger.tcp.southgate.cz. 86400   IN      SRV     0 0 79 .
ftp.tcp.southgate.cz.        86400       IN              SRV         10  10  21
ftp.southgate.cz.southg
```

```
ate.cz.
http.tcp.southgate.cz.      86400       IN              SRV             0  0  80
www.southgate.cz.southgat
e.cz.
http.tcp.southgate.cz.      86400       IN              SRV             10  0  80
www2.southgate.cz.southg
ate.cz.
ssh.tcp.southgate.cz.       86400       IN              SRV             10  10  22
ssh.southgate.cz.southg
ate.cz.
*.udp.southgate.cz.     86400   IN      SRV     0 0 0 .
vampir.southgate.cz.    86400   IN      CNAME   services.southgate.cz.
ventrilo.southgate.cz.  86400   IN      CNAME   services.southgate.cz.
verliadmin.southgate.cz. 86400  IN      CNAME   services.southgate.cz.
pc.vittorio.southgate.cz. 86400 IN      A       10.108.18.101
www.southgate.cz.       86400   IN      CNAME   services.southgate.cz.
http.tcp.www.southgate.cz.   86400   IN              SRV             0  0  80
www.southgate.cz.southgate.cz.
http.tcp.www.southgate.cz.   86400   IN              SRV             10  0  80
www2.southgate.cz.southgate.cz.
southgate.cz.                   86400       IN          SOA         ns.southgate.cz.
dns.southgate.c
z. 2006040308 3600 1800 604800 900
;; Query time: 390 msec
;; SERVER: 10.108.15.1#53(10.108.15.1)
;; WHEN: Sun Apr 23 18:52:28 2006
;; XFR size: 54 records (messages 1)
```

Zde jsme získali velice cennou informaci o struktuře sítě, včetně lokálních adres. Nejen to. Již dokonce víme, jaké služby na jaké adrese běží. Také vidíme jisté uživatele a přímo jejich lokální IP adresy. Toto není rozhodně dobré. Takovéto informace by neměli být rozhodně přístupné komukoliv na Internetu.

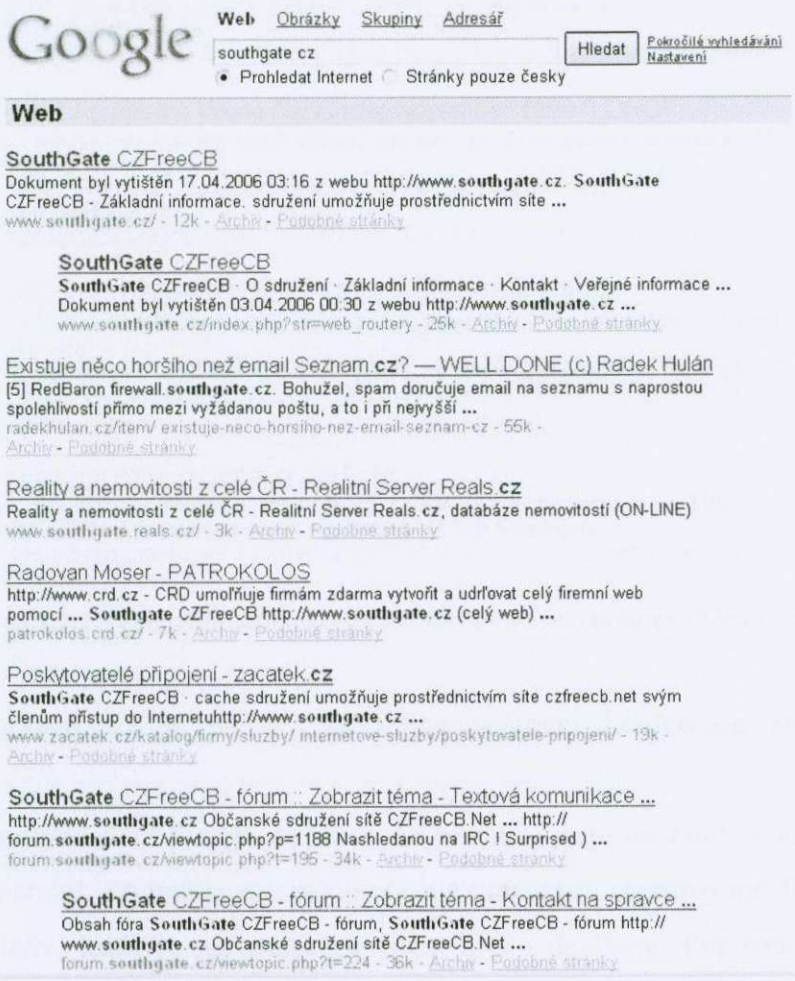
```
C:\Tools\dig\Win>host www.southgate.cz
www.southgate.cz is an alias for services.southgate.cz.
services.southgate.cz has address 10.108.15.4
www.southgate.cz is an alias for services.southgate.cz.
www.southgate.cz is an alias for services.southgate.cz.
```

Synonymum pro www.southgate.cz je services.southgate.cz.

4.1.2 Hledání informací pomocí vyhledávačů

Podíváme se co by jsme mohli najít o sdružení Southgate na Internetu. Začneme každodenním vyhledávačem http://www.google.com. Podíváme se také na mailové konference(jestli nějaké existují). Nezajímají nás v tomto momentě informace běžně dostupné. Pokusíme se najít informace(v poštovní konferenci či webu) typu – otázky ohledně bezpečnosti, problémů apod. spjaty se southgate.cz. To nám poskytne informace o prostředí, administrátorech, použité technologii apod.

Toto je výsledek vyhledávání.



Obrázek č.1 – Vyhledání informací o southgate.cz


Web Obrázky **Skupiny** Adresář

southgate cz Hledat Rozšířené prohledávání skupin Nastavení

Vyhledávání ve všech skupinách

MITY WEGETARIANIZMU cz. 1 - przypisy
... Wine, alcohol, platelets, and the French paradox for heart disease. Lancet, 1992, 339:1523-6.; (b) TLV Ulbright and DAT **Southgate**. ...
alt.pl.dieta.optymalna - 26 Lis 2003 13:39 od Krystyna*Opty* - 5 zpráv - 1 autor

Fans Across the World Newsletter 99. June 2000
Fans Across the World June 2000 Newsletter 99 B. Wilkinson, c/o 15 Manor Drive, **Southgate**, London, N14 5JH, Great ... (http://doris.sumperk-net.cz/Parcon/ homepage ...
rec.arts.sf.fandom - 5 Čen 2000 02:10 od B.J. Wilkinson - 1 zpráva - 1 autor

Fans Across the World Newsletter, November 1999
... Please note that my postal address has switched to my parents' address at: 15 Manor
Drive, **Southgate**, London, N14 5JH ... (email: pavelm@brainsys.cz; pmikulastik@usa ...
maus.freizeit.f+sf - 5 Lis 1999 00:17 od Thomas Recktenwald - 1 zpráva - 1 autor

Fans Across the World Newsletter November 1999 *LONG*
... Please note that my postal address has switched to my parents' address at: 15 Manor
Drive, **Southgate**, London, N14 5JH ... (email: pavelm@brainsys.cz; pmikulastik@usa ...
rec.arts.sf.fandom - 5 Lis 1999 07:34 od B.J. Wilkinson - 1 zpráva - 1 autor

NET-HAPPENINGS Digest - 23 Jul 1998 (#1998-495)
... MISC> **Southgate** College - Uk 12. ... Subject: MISC> on-line directory - Czech Republic
Sent: Thursday, July 23, 1998 10:01 AM From: resou...@mbox.vol.cz http://www ...
schl.news.nethappen - 25 Čec 1998 06:26 od Automatic digest processor - 1 zpráva - 1 autor

Nine Pound Bird Strike on an F-22
... I'm surprised Denyav hasn't surfaced to show that the birdstrike is proof that the F22 can't meet its maneuvering criteria. :-)) Bob **Southgate**
rec.aviation.military - 13 Říj 2002 02:07 od Mike Dennis - 13 zpráv - 9 autorů

Obrázek č.2 - Vyhledání informací o southgate.cz pomocí poštovních konferencí

Z Obrázku č.2 je patrné, že žádné poštovní konference nejsou k dispozici.

Při prohledávání fóra(je založeno na phpbb2) jsem na žádné důležité informace nenarazil. Zřejmě jsou k dispozici, ale pouze pro registrované členy. Zkusil jsem tedy, jestli je registrace povolena i pro ne-členy. Registrace je povolena, ale je schvalována správcem. Takže jsme nic zajímavého nenašli.

Pravděpodobně by se zde dal využít social engineering, ale tuto metodu jsem po úvaze zavrhl. Jedná se o malou organizaci, kde se všichni dobře znají.

4.2 Aktivní prohledávání

Nyní se budeme snažit najít všechny „žijící" stroje na straně southgate.cz. Budeme vystupovat jako někdo, kdo se snaží z nějakého důvodu dostat na různé servery southgate.cz různými nástroji. Nejspíše budu odhalen, ale to už je otázka jiná.

Standardní nástroj na takovéto testování je ping a tracert(traceroute). ICMP bude nejspíš zakázáno(snad mimo ICMP chyb).

```
PING services.southgate.cz (88.146.126.9): 56 data bytes
64 bytes from 88.146.126.9: icmp_seq=0 ttl=47 time=120.510 ms
64 bytes from 88.146.126.9: icmp_seq=1 ttl=47 time=120.097 ms
64 bytes from 88.146.126.9: icmp_seq=2 ttl=47 time=121.891 ms
64 bytes from 88.146.126.9: icmp_seq=3 ttl=47 time=123.716 ms
64 bytes from 88.146.126.9: icmp_seq=4 ttl=47 time=120.950 ms
```

ICMP není zakázáno. Bylo by dobré na tomto místě posoudit, jestli je potřeba mít icmp protokol povolený. Pomocí ping flood(DoS) by bylo možné stroj zahltit a tím pádem by mohlo dojít k zastavení dostupných služeb.

Nyní se podíváme, jaký webový server je nainstalován na našem serveru southgate.cz. To zjistíme velice jednoduše. Použijeme velice mocný nástroj netcat (také přezdívaný armádní švýcarský nůž).

```
C:\Tools\netcat\Win\netcat>nc www.southgate.cz 80
get html1/1
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<HTML><HEAD>
<TITLE>400 Bad Request</TITLE>
</HEAD><BODY>
<H1>Bad Request</H1>
Your browser sent a request that this server could not understand.<P>
```

```
Invalid URI in request get html1/1<P>
<HR>
<ADDRESS>Apache/1.3.34 Server at www.southgate.cz Port 80</ADDRESS>
</BODY></HTML>
C:\Tools\netcat\Win\netcat>
```

Jak vidíme je použit webový server Apache ve verzi 1.3.34.

Další kroky nás povedou ke zjišťování „živých" strojů v celé třídě C, tedy 88.146.126.0-255.

```
This file was generated by Angry IP Scanner
Visit http://www.angryziber.com/ for the latest version

Scanned 88.146.126.1 - 88.146.126.254
20.4.2006 10:52:27

IP                      Ping            Hostname

88.146.126.2            60 ms           N/A
88.146.126.3            47 ms           N/A
88.146.126.4            53 ms           N/A
88.146.126.5            46 ms           N/A
88.146.126.6            46 ms           N/A
88.146.126.7            68 ms           N/A
88.146.126.9            84 ms           N/A
88.146.126.100          113 ms          N/A
88.146.126.101          122 ms          N/A
88.146.126.106          90 ms           N/A
```

Zde je výpis „živých" strojů. Na těchto strojích bude dále zkoumal vybrané porty, pomocí nástroje nmap.

```
# Nmap 4.03 scan initiated Tue Apr 25 01:22:54 2006 as: nmap -P0 -sS -sU -
TSneaky -vv -oA southgate_126.1 -p T:80,25,53,23,22,110,U:53,67,68,69
88.146.126.2,3,4,5,6,7,9,100,101,106
Interesting ports on 88.146.126.2:
PORT    STATE         SERVICE
22/tcp  filtered      ssh
23/tcp  filtered      telnet
25/tcp  filtered      smtp
```

```
53/tcp  closed          domain
53/udp  open|filtered domain
67/udp  open|filtered dhcps
68/udp  open|filtered dhcpc
69/udp  open|filtered tftp
80/tcp  filtered        http
110/tcp filtered        pop3

Interesting ports on 88.146.126.3:
PORT    STATE           SERVICE
22/tcp  filtered        ssh
23/tcp  filtered        telnet
25/tcp  filtered        smtp
53/tcp  closed          domain
53/udp  open|filtered domain
67/udp  open|filtered dhcps
68/udp  open|filtered dhcpc
69/udp  open|filtered tftp
80/tcp  filtered        http
110/tcp filtered        pop3

Interesting ports on 88.146.126.4:
PORT    STATE           SERVICE
22/tcp  filtered        ssh
23/tcp  filtered        telnet
25/tcp  filtered        smtp
53/tcp  filtered        domain
53/udp  open|filtered domain
67/udp  open|filtered dhcps
68/udp  open|filtered dhcpc
69/udp  open|filtered tftp
80/tcp  filtered        http
110/tcp filtered        pop3

Interesting ports on 88.146.126.5:
PORT    STATE           SERVICE
22/tcp  filtered        ssh
23/tcp  filtered        telnet
25/tcp  filtered        smtp
53/tcp  closed          domain
53/udp  open|filtered domain
```

```
67/udp  open|filtered dhcps
68/udp  open|filtered dhcpc
69/udp  open|filtered tftp
80/tcp  filtered      http
110/tcp filtered      pop3

Interesting ports on 88.146.126.6:
PORT    STATE         SERVICE
22/tcp  filtered      ssh
23/tcp  filtered      telnet
25/tcp  filtered      smtp
53/tcp  closed        domain
53/udp  open|filtered domain
67/udp  open|filtered dhcps
68/udp  open|filtered dhcpc
69/udp  open|filtered tftp
80/tcp  filtered      http
110/tcp filtered      pop3

Interesting ports on 88.146.126.7:
PORT    STATE         SERVICE
22/tcp  filtered      ssh
23/tcp  filtered      telnet
25/tcp  filtered      smtp
53/tcp  filtered      domain
53/udp  open|filtered domain
67/udp  open|filtered dhcps
68/udp  open|filtered dhcpc
69/udp  open|filtered tftp
80/tcp  filtered      http
110/tcp filtered      pop3

Interesting ports on 88.146.126.9:
PORT    STATE         SERVICE
22/tcp  filtered      ssh
23/tcp  filtered      telnet
25/tcp  filtered      smtp
53/tcp  filtered      domain
53/udp  open|filtered domain
67/udp  open|filtered dhcps
68/udp  open|filtered dhcpc
```

```
69/udp  open|filtered tftp
80/tcp  filtered      http
110/tcp filtered      pop3

Interesting ports on 88.146.126.100:
PORT    STATE         SERVICE
22/tcp  filtered      ssh
23/tcp  filtered      telnet
25/tcp  filtered      smtp
53/tcp  filtered      domain
53/udp  open|filtered domain
67/udp  open|filtered dhcps
68/udp  open|filtered dhcpc
69/udp  open|filtered tftp
80/tcp  filtered      http
110/tcp filtered      pop3

Interesting ports on 88.146.126.101:
PORT    STATE         SERVICE
22/tcp  filtered      ssh
23/tcp  filtered      telnet
25/tcp  filtered      smtp
53/tcp  filtered      domain
53/udp  open|filtered domain
67/udp  open|filtered dhcps
68/udp  open|filtered dhcpc
69/udp  open|filtered tftp
80/tcp  filtered      http
110/tcp filtered      pop3

Interesting ports on 88.146.126.106:
PORT    STATE         SERVICE
22/tcp  filtered      ssh
23/tcp  filtered      telnet
25/tcp  filtered      smtp
53/tcp  filtered      domain
53/udp  open|filtered domain
67/udp  open|filtered dhcps
68/udp  open|filtered dhcpc
69/udp  open|filtered tftp
80/tcp  filtered      http
```

```
110/tcp filtered      pop3

# Nmap run completed at Tue Apr 25 01:34:48 2006 -- 10 IP addresses (10 hosts
up) scanned in 2920.250 seconds
```

Nmap pro UDP scany používá 0 bytové UDP pakety. Když obdržíme chybovou hlášku *ICMP_PORT_UNREACHABLE* je port uzavřený, jinak je port otevřený(nebo filtrovaný, ale v tomto případě bez chybových hlášek).

Zdá se mi, že nastavení všech strojů je úplně stejné a dá se do jisté míry říci, že to zřejmě bude jeden stroj s vícero IP adresami.

4.3 Testování bezpečnosti aplikací

Z předešlých testů víme, že www.southgate.cz má alias services.southgate.cz. Podíváme se tedy jestli webový server podporuje šifrovanou variantu http(https). To zjistíme jednoduše pomocí netcatu.

```
c:\Tools\netcat\Win\netcat>nc -v www.southgate.cz 443
services.southgate.cz [10.108.15.4] 443 (https): connection refused
```

HTTPS není serverem podporována.

Nyní jsem změnil na svém testovacím počítači operační systém na Slackware. Budeme testovat server pomocí nástroje whisker. V základní nastavené konfiguraci whisker zkouší standardní adresáře a cesty, jestli jsou k dispozici.

```
-- whisker / v1.4.0 / rain forest puppy / www.wiretrip.net --
- Loaded script database of 1968 lines

= - = - = - = - = - =
= Host: 88.146.126.9
- Directory index: /

= Server: Apache/1.3.34 (Debian) PHP/4.3.10-16

-  www.apache.org
```

```
+ 404 Not Found: GET /cfdocs/
+ 404 Not Found: GET /scripts/
+ 404 Not Found: GET /cfcache.map
+ 404 Not Found: GET /cfide/Administrator/startstop.html
+ 404 Not Found: GET /cfappman/index.cfm
+ 404 Not Found: GET /cgi-bin/
+ 404 Not Found: HEAD /_vti_inf.html
+ 404 Not Found: HEAD /_vti_pvt/
+ 404 Not Found: HEAD /mall_log_files/order.log
+ 404 Not Found: HEAD /PDG_Cart/
+ 404 Not Found: HEAD /quikstore.cfg
+ 404 Not Found: HEAD /orders/
+ 404 Not Found: HEAD /Admin_files/order.log
+ 404 Not Found: HEAD /WebShop/
+ 404 Not Found: HEAD /pw/storemgr.pw
+ 404 Not Found: HEAD /bigconf.cgi
+ 404 Not Found: HEAD /icat
+ 404 Not Found: HEAD /cgi-local/
+ 404 Not Found: HEAD /htbin/
+ 404 Not Found: HEAD /cgibin/
+ 404 Not Found: HEAD /cgis/
+ 404 Not Found: HEAD /cgi/
+ 404 Not Found: HEAD /cgi-win/
+ 404 Not Found: HEAD /manage/cgi/cgiproc
+ 404 Not Found: HEAD /wwwboard/
+ 404 Not Found: HEAD /logs/
+ 404 Not Found: HEAD /database/
+ 404 Not Found: HEAD /databases/
+ 403 Forbidden: HEAD /.htaccess
+ 404 Not Found: HEAD /docs/
+ 404 Not Found: HEAD /~root/
+ 404 Not Found: HEAD /ws_ftp.ini
+ 404 Not Found: HEAD /WS_FTP.ini
+ 404 Not Found: HEAD /search97.vts
+ 404 Not Found: HEAD /search.vts
+ 404 Not Found: HEAD /search97cgi/s97_cgi
+ 404 Not Found: HEAD /webcart/
+ 404 Not Found: HEAD /webcart-lite/
+ 404 Not Found: HEAD /reviews/newpro.cgi
+ 404 Not Found: HEAD /piranha/secure/passwd.php3
+ 404 Not Found: HEAD /srchadm
```

```
+ 404 Not Found: HEAD /users/scripts/submit.cgi
+ 404 Not Found: HEAD /bb-dnbd/
+ 404 Not Found: HEAD /session/admnlogin
+ 404 Not Found: HEAD /wwwthreads/
+ 404 Not Found: HEAD /ss.cfg
+ 404 Not Found: HEAD /ncl_items.html
+ 404 Not Found: HEAD /test/test.cgi
+ 404 Not Found: HEAD /php/
+ 404 Not Found: HEAD /mlog.phtml
+ 404 Not Found: HEAD /mylog.phtml
+ 404 Not Found: HEAD /HyperStat/stat_what.log
+ 404 Not Found: HEAD /Stats/
+ 404 Not Found: HEAD /WebTrend/
+ 404 Not Found: HEAD /analog/
+ 404 Not Found: HEAD /cache-stats/
+ 404 Not Found: HEAD /easylog/easylog.html
+ 404 Not Found: HEAD /hit_tracker/
+ 404 Not Found: HEAD /hitmatic/
+ 404 Not Found: HEAD /hitmatic/analyse.cgi
+ 404 Not Found: HEAD /hyperstat/stat_what.log
+ 404 Not Found: HEAD /log/
+ 404 Not Found: HEAD /logfile/
+ 404 Not Found: HEAD /logfiles/
+ 404 Not Found: HEAD /logger/
+ 404 Not Found: HEAD /logging/
+ 404 Not Found: HEAD /logs/access_log
+ 404 Not Found: HEAD /ministats/admin.cgi
+ 404 Not Found: HEAD /scripts/weblog
+ 404 Not Found: HEAD /server_stats/
+ 404 Not Found: HEAD /stat/
+ 404 Not Found: HEAD /statistics/
+ 404 Not Found: HEAD /stats/
+ 404 Not Found: HEAD /super_stats/access_logs
+ 404 Not Found: HEAD /trafficlog/
+ 404 Not Found: HEAD /ustats/
+ 404 Not Found: HEAD /w3perl/admin
+ 404 Not Found: HEAD /webaccess/access-options.txt
+ 404 Not Found: HEAD /weblog/
+ 404 Not Found: HEAD /weblogs/
+ 404 Not Found: HEAD /webstats/
+ 404 Not Found: HEAD /wstats/
```

```
+ 404 Not Found: HEAD /wusage/
+ 404 Not Found: HEAD /wwwlog/
+ 404 Not Found: HEAD /wwwstats/
+ 404 Not Found: HEAD /access-log
+ 404 Not Found: HEAD /access.log
+ 404 Not Found: HEAD /awebvisit.stat
+ 404 Not Found: HEAD /dan_o.dat
+ 404 Not Found: HEAD /hits.txt
+ 404 Not Found: HEAD /log.htm
+ 404 Not Found: HEAD /log.html
+ 404 Not Found: HEAD /log.txt
+ 404 Not Found: HEAD /logfile
+ 404 Not Found: HEAD /logfile.htm
+ 404 Not Found: HEAD /logfile.html
+ 404 Not Found: HEAD /logfile.txt
+ 404 Not Found: HEAD /logger.html
+ 404 Not Found: HEAD /stat.htm
+ 404 Not Found: HEAD /stats.htm
+ 404 Not Found: HEAD /stats.html
+ 404 Not Found: HEAD /stats.txt
+ 404 Not Found: HEAD /webaccess.htm
+ 404 Not Found: HEAD /wwwstats.html
+ 404 Not Found: HEAD /bin/
- Directory index: /admin/

+ 404 Not Found: HEAD /Admin_files/
+ 404 Not Found: HEAD /DMR/
+ 404 Not Found: HEAD /StoreDB/
+ 404 Not Found: HEAD /Web_store/
+ 404 Not Found: HEAD /access/
+ 404 Not Found: HEAD /account/
+ 404 Not Found: HEAD /accounting/
+ 404 Not Found: HEAD /administrator/
+ 404 Not Found: HEAD /app/
+ 404 Not Found: HEAD /apps/
+ 404 Not Found: HEAD /archive/
+ 404 Not Found: HEAD /asp/
+ 404 Not Found: HEAD /atc/
+ 404 Not Found: HEAD /backup/
+ 404 Not Found: HEAD /bak/
+ 404 Not Found: HEAD /beta/
```

```
+ 404 Not Found: HEAD /buy/
+ 404 Not Found: HEAD /buynow/
+ 404 Not Found: HEAD /c/
+ 404 Not Found: HEAD /cart/
+ 404 Not Found: HEAD /ccard/
+ 404 Not Found: HEAD /config/
+ 404 Not Found: HEAD /counter/
+ 404 Not Found: HEAD /credit/
+ 404 Not Found: HEAD /customers/
+ 404 Not Found: HEAD /dat/
+ 404 Not Found: HEAD /data/
+ 404 Not Found: HEAD /db/
+ 404 Not Found: HEAD /dbase/
+ 404 Not Found: HEAD /doc-html/
+ 404 Not Found: HEAD /down/

+ 200 OK: HEAD /download/
+ 404 Not Found: HEAD /downloads/
+ 404 Not Found: HEAD /employees/
+ 404 Not Found: HEAD /exe/
+ 404 Not Found: HEAD /file/
+ 404 Not Found: HEAD /files/
+ 404 Not Found: HEAD /forum/
+ 404 Not Found: HEAD /fpadmin/
+ 404 Not Found: HEAD /ftp/
+ 404 Not Found: HEAD /guestbook/
+ 404 Not Found: HEAD /guests/
+ 404 Not Found: HEAD /home/
+ 404 Not Found: HEAD /htdocs/
+ 404 Not Found: HEAD /html/
+ 404 Not Found: HEAD /ibill/
+ 404 Not Found: HEAD /idea/
+ 404 Not Found: HEAD /ideas/
+ 404 Not Found: HEAD /incoming/
+ 404 Not Found: HEAD /info/
+ 404 Not Found: HEAD /install/
+ 404 Not Found: HEAD /intranet/
+ 404 Not Found: HEAD /jave/
+ 404 Not Found: HEAD /jdbc/
+ 404 Not Found: HEAD /lib/
+ 404 Not Found: HEAD /library/
```

```
+ 404 Not Found: HEAD /login/
+ 404 Not Found: HEAD /mail/
+ 404 Not Found: HEAD /mall_log_files/
+ 404 Not Found: HEAD /manual/
+ 404 Not Found: HEAD /marketing/
+ 404 Not Found: HEAD /msql/
+ 404 Not Found: HEAD /new/
+ 404 Not Found: HEAD /odbc/
+ 404 Not Found: HEAD /old/
+ 404 Not Found: HEAD /oracle/
+ 404 Not Found: HEAD /order/
+ 404 Not Found: HEAD /outgoing/
+ 404 Not Found: HEAD /pages/
+ 404 Not Found: HEAD /passwords/
+ 404 Not Found: HEAD /perl/
+ 404 Not Found: HEAD /private/
+ 404 Not Found: HEAD /pub/
+ 404 Not Found: HEAD /public/
+ 404 Not Found: HEAD /purchase/
+ 404 Not Found: HEAD /purchases/
+ 404 Not Found: HEAD /pw/
+ 404 Not Found: HEAD /register/
+ 404 Not Found: HEAD /registered/
+ 404 Not Found: HEAD /reseller/
+ 404 Not Found: HEAD /retail/
+ 404 Not Found: HEAD /root/
+ 404 Not Found: HEAD /sales/
+ 404 Not Found: HEAD /search/
+ 404 Not Found: HEAD /sell/
+ 404 Not Found: HEAD /setup/
+ 404 Not Found: HEAD /shop/
+ 404 Not Found: HEAD /shopper/
+ 404 Not Found: HEAD /site/iissamples/
+ 404 Not Found: HEAD /software/
+ 404 Not Found: HEAD /source/
+ 404 Not Found: HEAD /sql/
+ 404 Not Found: HEAD /store/
+ 404 Not Found: HEAD /support/
+ 404 Not Found: HEAD /temp/
+ 404 Not Found: HEAD /test/
+ 404 Not Found: HEAD /test-cgi/
```

```
+ 200 OK: HEAD /tmp/
+ 404 Not Found: HEAD /tools/
+ 404 Not Found: HEAD /tree/
+ 404 Not Found: HEAD /updates/
+ 404 Not Found: HEAD /usage/
+ 404 Not Found: HEAD /user/
+ 404 Not Found: HEAD /users/
+ 404 Not Found: HEAD /web/
+ 404 Not Found: HEAD /web800fo/
+ 404 Not Found: HEAD /webadmin/
+ 404 Not Found: HEAD /webboard/
+ 404 Not Found: HEAD /webdata/
+ 404 Not Found: HEAD /website/
+ 404 Not Found: HEAD /www/
+ 404 Not Found: HEAD /www-sql/
+ 404 Not Found: HEAD /wwwjoin/
+ 404 Not Found: HEAD /import/
+ 404 Not Found: HEAD /zipfiles/
+ 404 Not Found: HEAD /passwd
+ 404 Not Found: HEAD /passwd.txt
+ 404 Not Found: HEAD /password
+ 404 Not Found: HEAD /password.txt

+ 200 OK: HEAD /status/
```

Nenašli jsme žádné adresáře, které by mohli pro nás obsahovat něco zajímavého. Také hned v prvních řádkách jsme si potvrdili, že jde o server Apache a nová věc pro nás je i použitý operační systém.

Další krok který jsem podnikl, bylo použití automatizovaných nástrojů. Test serveru jsem podrobil třemi nástroji – Nikto, Nessus, N-Stealth. Výsledky testů jsou přiloženy na CD médiu, protože jejich výpis je rozsáhlý. Důležité výsledky, které jsem získal, jsem zařadil do následující kapitoly.

4.4 Doporučení

V několika případech služba předala do internetu mnohem více informací o vnitřním uspořádání než by ve skutečnosti měla. Informace o vnitřní architektuře může potenciálnímu útočníkovi pomoci k tomu, aby mohl směrovat přesně své viry nebo červi. Je vždy lepší dávat do internetu jen tolik informací, kolik je potřeba.

Zdá se, že jeden stroj bude zároveň webovým a poštovním serverem (pravděpodobně na tom stroji poběží jistě ještě další služby). Pokud by tedy potencionální útočník směřoval svůj útok na tento stroj, je dost pravděpodobné, že by došlo k přerušení veškerých služeb, které na tomto stroji běží. Nejen webový server Apache a pošta, ale podle dns výpisu by se jednalo o irc, ftp, sql atd. Mé doporučení je, aby webový server běžel sám na jednom stroji. Nebo se alespoň pokusit o rozmístění služeb na jiné stroje.

Je zde také pouze jediný poštovní server. V případě DoS útoku by nebylo možné doručit poštu do domény southgate.cz. Doporučoval bych vytvořit ještě jeden poštovní server, který by nebyl na stejné podsíti a který by také běžel na zcela jiném stroji.

4.5 Zranitelnosti

4.5.1 DNS internal zone information (důležitost – vysoká)

Domnívám se, že by server neměl dávat žádné informace o vnitřním prostředí komukoliv, kdo o ně požádá. V našem případě se dostaneme přímo k IP adresám vnitřní sítě

```
pc.davidos.southgate.cz. 86400   IN      A       10.108.18.108
dchub.southgate.cz.      86400   IN      CNAME   services.southgate.cz
dude.southgate.cz.       86400   IN      A       10.108.15.7
firewall.southgate.cz.   86400   IN      A       10.108.15.3
forum.southgate.cz.      86400   IN      CNAME   services.southgate.cz
pc.pupik.southgate.cz.   86400   IN      A       10.108.15.15
pc.pambroz.southgate.cz. 86400   IN      A       10.108.17.117
```

Jelikož útočník zná vnitřní IP adresy, jeho útok může mít přesnější cíl.

Tento výsledek může být chybnou konfigurací nebo chybou samotného DNS serveru. Tato chyba by měla být odstraněna co nejdříve.

4.5.2 DNS recursive query (důležitost – středně vysoká)

DNS server by měl být nakonfigurován tak, aby nepovoloval rekurzivní dotazy z okolního světa. Porušení tohoto pravidla by mohlo vést k útoku cache poisoning, což by mohlo mít fatální následky.

Vypnutí služby rekurzivních dotazů, je jednoduchým krokem ve všech verzích DNS serverů od Microsoftu a ve všech verzích BIND(unixová varianta DNS) nad verzi 4.0.

Existují další možné řešení:

- Použití dvou DNS serverů (jeden na rekurzivní dotazy pro interní použití a jeden pro držení informací o southgate.cz ostatnímu světu).

- Použití dvou nezávislých DNS služeb běžící na jednom stroji(každá by běžela na jiném síťovém zařízení)

Co může potencionální útočník udělat, je uvedeno v kapitole 4.2.1.

4.5.3 Nižší verze serveru Apache (důležitost – střední)

Server Apache běží ve verzi 1.3.34. I když je tato verze ještě stále udržovaná, bylo by na místě zvážit nainstalování novější verze.

4.5.4 Nižší verze PHP (důležitost – střední)

Verze php, která je na serveru nainstalována je ve verzi 4.3.10-16. Momentálně je dostupná vyšší verze php a to 4.4.2. Při instalaci nové verze by se mohlo zvážit, zda nenainstalovat rovnou verzi 5.1.2.

4.5.5 Aktivní debug mód na Apache (důležitost – nízká)

Na http serveru Apache je povolen Debug mód. Server tak podporuje TRACE a TRACK. Metody se používají k debugování serverových konexí. Útočník může zneužít tyto funkce k získání přístupu k informacím v http hlavičkách jako jsou cookies a ověřovací data.

4.5.6 Zjištění verze DNS (důležitost – nízká)

Bylo možné určit verzi BIND(unixová varianta DNS). Doporučoval bych změnit konfiguraci tak, aby nebylo možné provádět fingerprinting.

TCP/IP je poměrně pevně stanovený protokol, ale některé jeho části nejsou přesně definované. To dává programátorům operačních systémů jistou volnost, která vede k nekonzistenci jednotlivých řešení. Různé systémy tak reagují na vzniklé situace různými způsoby.

Pochopitelně za normálních okolností musí docházet ke správné a přesně stanovené komunikaci, jinak bychom se nedohodli, ale existuje řada případů, kdy dokážeme navodit neočekávanou situaci a získat ze systému reakci, podle níž můžeme odhadnout, o jaký systém se jedná.

4.6 Závěr penetračního testu

Během testu jsme neobjevili žádné skutečné hrozby nebo vážně zranitelná místa. Také jsme nenašli žádnou stopu o předešlém kompromitování strojů.

Zjistili jsme, že výskyt southgate.cz na Internetu je schován za firewallem a je dobře zabezpečen. Našli jsme ale několik chyb v nastavení, které by se měli opravit.

Pokus byl proveden větším počtem univerzálních nástrojů. Což spolu s dostatkem informací má podle mého názoru lepší výsledky než použití automatizovaných nástrojů. Všechny tyto nástroje jsou běžně dostupné.

Společně se změnami v konfiguraci bych doporučoval ještě nasazení IDS(systém detekce průniku) na klíčové části sítě. Existují útoky, které nejsou vidět v logových souborech firewallů (jelikož jsou prováděny na aplikační úrovni), ale mohou být rozeznány pomocí IDS.

Při detekci útoku dále hrají roli logové soubory firewallů a samozřejmě důležitou roli hraje i schopnost porozumění těmto souborům. To spolu s IDS umožňuje porovnávat různé události vzhledem k určitým pravidlům(čas, zdrojová adresa, cílová adresa, port atd.).

Závěr

Nástroje a monitorovací systémy jsou jednou stranou mince bezpečnosti informačních systémů. Druhá strana mince je lidský faktor. Bezpečnostní administrátoři musí totiž kontrolovat údaje z logových souborů (zařízení,systémů), sledovat nové trendy, neustále aktualizovat a testovat jejich vlastní nastavení. Ti, kteří tak nedělají, se vystavují vysokému riziku napadení. To může způsobit ztrátu cenných informací jako jsou například osobní údaje. Ty jsou na dnešním trhu ohromě ceněné.

Útočníci jsou ve většině případech o krok napřed. Proto je téměř každý webový server napadnutelný. I přes to se bezpečnostní administrátoři musí snažit o to, aby co nejvíce zabránili snaze potencionálního útočníka uspět. I sebemenší překážky mohou odradit různé pokusy o útok. Napadá mě paralela v běžném životě. Pokud necháme v automobilu klíčky a odejdeme na 2 hodiny od vozu, je dost pravděpodobné, že při návratu vůz nebude na svém místě. Naopak i sebemenší překážka, může odradit potencionálního lupiče.

Bezpečnost informačních systémů není statická záležitost, je to neustálý proces zdokonalování proti bezpečnostním rizikům, který zahrnuje oblast nejen technickou ale i organizační a personální..

Použitý software

Nessus	- standardní bezpečnostní scanner
N-Stealth	- standardní bezpečnostní scanner(freeware)
Nikto	- standardní bezpečnostní scanner
Nmap	- nástroj na rychlé mapování portů
Hping	- nástroj na síťové testování
Opera	- webový prohlížeč
Whisker	- bezpečnostní scanner pro webové servery
Traceroute(Tracert)	- standardní testovací nástroj
Ping	- standardní testovací nástroj
Nslookup	- standardní testovací nástroj pro DNS
Dig	- standardní testovací nástroj pro DNS
host	- standardní testovací nástroj pro DNS
whois	- standardní testovací nástroj
Apache	- webový server
WinXP	- operační systém
Slackware	- nekomerční linuxová distribuce(operační systém)

Použitá literatura a internetové zdroje

Literatura

[1] Joel Scambray, Mike Shema, Hacking bez tajemství, Computer Press, Brno, 2003

[2] Petr Břehovský, Praktický úvod TCP/IP, Kopp, 1995, České Budějovice

[3] Jiří Havelka a kolektiv, Výkladový slovník výpočetní techniky a komunikací, Computer Press, Brno 1997

[4] Libor Dostálek, Alena Kabelová, Velký průvodce protokoly TCP/IP DNS, Computer Press, Praha, 2000

Internetové zdroje

[5] Centrum internetové bezpečnosti, Dostupné na World Wide Web : <http://www.cert.org/>

[6] Informace o bezpečnosti, Dostupné na World Wide Web : <http://www.msn.cz/security/>

[7] Magazín informačních technologií, Dostupné na World Wide Web : <http://www.reboot.cz/>

[8] Informační server nejen pro administrátory, Dostupné na World Wide Web : <http://owebu.cz/bezpecnost/>

[9] Svět počítačů, Dostupné na World Wide Web : <http://www.pcworld.cz/>

[10] Bezpečnost Linuxu, Dostupné na World Wide Web : <http://atrey.karlin.mff.cuni.cz/seminar/OLD/Papers98/linux-attack/>

[11] Firma v oblasti bezpečnosti informačních technologií, Dostupné na World Wide Web : <http://www.actinet.cz >

[12] Průvodce pro začátečníky a administrátory, Dostupné na World Wide Web : <http://www.adminxp.cz/>

[13] Informační server o Linuxu, Dostupné na World Wide Web : <http://www.root.cz/>

[14] Vlastnosti IP adres, Dostupné na World Wide Web : <http://www.showmyip.com/>

[15] Vyhledávač, Dostupné na World Wide Web : <http://www.google.com/ >

[16] Vyhledávač doménových jmen a IP adres, Dostupné na World Wide Web : <http://www.geektools.com/>

[17] DNS testování, DNS nástroje, ping, trace, Dostupné na World Wide Web <http://www.dnsstuff.com/>

[18] Databáze známých bezpečnostních děr, Dostupné na World Wide Web <http://msgs.securepoint.com/bugtraq/>

[19] Databáze známých bezpečnostních děr, Dostupné na World Wide Web <http://cve.mitre.org/>

Použité výrazy

DNS - doménový pojmenovávací systém. Technologie či systém, který se používá k překladu doménových jmen.

DoS – Denial of Service, vysvětleno v teoretické části

DDoS – Distributed Denial of Service, vysvětleno v teoretické části

HTTP - Protokol určený k transportu hypertextových souborů po Internetu

ICMP – Protokol soužící k odhadování chyb v síti

IP – Protokol zajišťující správné doručování dat jednotlivým počítačům v síti

IP adresa – jednoznačná číselná identifikace počítače připojeného do sítě

Exploit - exploit je program, který „využívá" chyby ve specifickém softwaru

Firewall - Hardware či software (ev. obojí), který slouží k oddělení jedné sítě od druhé z důvodů bezpečnosti.

FQDN - Plné jméno počítače v síti Internet; jméno, které počítač plně v této síti identifikuje.

MX – Mail Exchange; ukazatel na poštovní server v DNS

NAT - Mechanismus umožňující redukci potřebného množství jedinečných IP adres. Umožňuje připojení do Internetu síti, která nemá unikátní IP adresy, jejich překladem do takových adres.

NS – jmenný server nebo-li DNS

OS – operační systém

Proxy server - Server v síti Internet, který funguje v této síti přesně jako cache na běžném počítači, samozřejmě s o mnoho řádů vyšší kapacitou. Proxy server má velkou kapacitu pro úschovu dat; informace z Internetu, které

jdou „přes něj", uloží a pokud jsou žádány příště, pouze si na cílovém místě ověří, zda nebyly změněny a poslouží jimi z lokálních zásob.

SMTP - Protokol pro správný a bezpečný přenos zpráv elektronické pošty přes Internet

UDP - Transportní protokol negenerující spojení, pracující nad IP v protokolu TCP/IP. Poskytuje nespolehlivou datagramovou službu – pakety mohou být duplikovány, ztraceny či obdrženy v jiném pořadí než vyslaném

TCP - Přenosový a komunikační protokol, který se stal jedním z nejpoužívanějších standardů.

Virus - Kód zapsaný s výslovným záměrem šířit sám sebe. Virus připojí sám sebe k hostitelskému programu a poté se pokusí šířit z počítače do počítače. Může poškodit hardware, software nebo informace.

Červ - Podtřída viru. Červ se obvykle šíří bez účasti uživatele, přičemž distribuuje své úplné kopie (případně pozměněné) v rámci sítí. Může spotřebovávat paměť nebo šířku pásma sítě, což může vést ke zhroucení počítače.