Penetrační testování

Bakalářská práce

Michal Zeman

Vedoucí bakalářské práce: Ing. Ladislav Beránek, Csc., MBA

Jihočeská univerzita v Českých Budějovicích

Pedagogická fakulta

Katedra informatiky

2010

Prohlášení

Prohlašuji, že svoji bakalářskou práci jsem vypracoval samostatně pouze s použitím pramenů a literatury uvedených v seznamu citované literatury.

Prohlašuji, že v souladu s § 47b zákona č. 111/1998 Sb. v platném znění souhlasím se zveřejněním své bakalářské práce, a to v nezkrácené podobě elektronickou cestou ve veřejně přístupné části databáze STAG provozované Jihočeskou univerzitou v Českých Budějovicích na jejích internetových stránkách.

V Českých Budějovicích dne 23. 4. 2010

Anotace

Práce se zabývá testováním zranitelnosti informačních systémů. Tyto systémy se dnes velmi rozšiřují a často obsahují citlivá data, která je třeba ochránit před útoky zvenčí nebo zevnitř. Jednou z metod zabezpečení je simulace těchto útoků — penetrační testování. Součástí práce je také seznámení se standardem OSSTMM[12], provedení penetračního testování na univerzitní síti a vyhodnocení získaných výsledků.

Abstract

This work deals with testing vulnerability of information systems. Nowadays, these systems are expanding and often contains sensitive data, which needs to be protected from external or internal attacks. One method of protection is to simulate these attacks — penetration testing. Part of the thesis is to acquaint with the OSSTMM standard, perform penetration testing on university network and evaluate the results.

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 panu Ing. Petru Břehovskému — konzultantovi pro bezpečnost systémů Ústavu aplikované informatiky Přírodovědecké fakulty — za rady, které mi dal pro praktickou část této bakalářské práce.

Obsah

Úvod

Předkládaná práce se zabývá problematikou bezpečnosti informačních systémů a možnostmi, jak zabezpečení prolomit. Praktická část obsahuje penetrační test provedený na Pedagogické fakultě a jeho vyhodnocení.

V první části dokumentu se nachází rozpis nejnebezpečnějších útoků, které je možné využít. Je zde nástin statistiky vývoje četnosti útoků a možností, jak se proti nebezpečným útokům bránit.

Druhá část se věnuje rozdělení a vysvětlení jednotlivých bezpečnostních testů. Kapitola slouží pro získání základních informací o rozsahu a možnostech jednotlivých bezpečnostních testů, jak se s nimi můžeme v komerční sféře setkat.

Třetí část je věnována OSSTMM (Open Source Security Testing Methodology Manual) manuálu a vysvětlení k čemu slouží, proč byl vyvinut a jeho využití v praxi.

Čtvrtá část se zabývá penetračním testem na PF JČU; od pasivního prohledávání přes výsledky jednotlivých testů až k závěrům, jak je fakulta zabezpečena a jaká opatření by bylo vhodné přijmout pro zvýšení bezpečnosti.

Součástí práce je rovněž DVD médium, které obsahuje veškerý software použitý při testování. Software zahrnuje i .iso obrazy dvou linuxových distribucí speciálně vyvinutých pro penetrační testování (Pentoo a BackTrack). Na médiu se rovněž nachází všechny generované zprávy automatizovaných testovacích nástrojů, rozdělených do složek podle IP adres pod názvem příslušného programu.

1. Bezpečnost informačních systémů

1.1 Bezpečnost obecně

Bezpečnost informačních systémů a vlastně vůbec všech informací na internetu je aktuálně velice často probíraným tématem. Současní crackeři (hackeři) se jen tak před něčím nezastaví a pořád se snaží vymýšlet nové a nové způsoby, jak se k citlivým informacím dostat. Citlivou informací přitom rozumíme cokoliv, čeho by mohl útočník zneužít ihned (rodná čísla, čísla sociálního pojištění [USA], čísla kreditních karet, hesla, …), případně v budoucnu pro získání dalších informací. V dnešní době velice rychle se rozvíjejících sociálních útoků tak můžeme citlivou informací nazvat s klidným svědomím i emailový kontakt či telefon. Ano, i těchto informací je možno využít, a například pomocí emailu lákat přístupová hesla a podobně. Této problematice se budeme více věnovat v kapitole 2.2 o social engeneeringu.

1.2 Kdo stojí za útoky

Ve všeobecném povědomí je dnes synonymum pro počítačového útočníka slovo hacker. Název však není zcela správný. Kdybychom se podívali na definici slova hacker, a na to co hlásají lidé, kteří si tak říkají, dozvěděli bychom se, že záměry skutečných hackerů jsou veskrze dobré. Hodně se o této problematice můžeme dozvědět z různých zdrojů na internetu — například „The Jargon File“[19], „Hackerův manifest“ a podobně. V podstatě je zde následující rozdíl: hacker je člověk, který má neobyčejné schopnosti a jeho zálibou a koníčkem je hledat chyby s systémech, sítích a bezpečnostních systémech. Hacker je velmi zručný v nabourávání se do systémů a činí to jen pro potěšení. Správný hacker se řídí pravidly „Hacker ethic“.

„HACKER ETHIC
(hackerská etika)

1. *Víra, že sdílení informací je správné a dobré, a že je etickou povinností hackerů dělit se o své poznatky psaním open-source a usnadňováním přístupu k informacím a počítačovým zdrojům v maximální možné míře.*
2. *Víra, že „nabourávání" do systémů pro pobavení a získání zkušeností je eticky v pořádku, dokud však nedojde k vandalismu, zcizení informací či porušení jejich utajení."*

(online zdroj: http://www.root.cz/clanky/hacker-kdo-to-je/)

Když si pozorně přečteme tato pravidla, kterými by se správný hacker měl řídit, je nám jasné, že hacker je nepostradatelný člověk pro správný vývoj software a fungování celé internetové společnosti. Zkusme si v krátkosti ukázat, jak „útok" hackera probíhá. Hacker naprogramuje kupříkladu nějaký exploit[4], který zneužije jistou chybu v konkrétním systému a dostane se k citlivým informacím. Hacker exploit zveřejní jakožto open-source a správci nabouraného systému pošle například email s tím, že jeho systém byl nabourán takovým a takovým způsobem. V emailu by měl správci co nejpodrobněji popsat, jak k prolomení došlo, aby byl schopen takový způsob pro příště znemožnit. S trochou nadsázky se tedy dá říci, že hacker správci pomohl a upozornil ho na chybu v jeho zabezpečení. Správný hacker je tedy skrytý bezpečnostní auditor.

Proti tomu v opozici stojí cracker, což je člověk s podobnými dovednostmi. Může se kupříkladu i řídit 1. bodem hackerovy etiky, ovšem liší se v chápání bodu 2, především jeho druhé části. Cracker se naboural do systému a pokusí se informací využít ve svůj prospěch.

Dnešní společnost ovšem toto rozdělení nerespektuje už jen z toho důvodu, že často samotný cracker o sobě prohlašuje, že je hacker, což není. Budeme se držet obecné definice a pravidel sepsaných samotnými hackery,

vyhneme se tak nesprávnému označování; člověka, který nabourává síť za účelem svého prospěchu, budeme nazývat cracker. Ještě by se slušelo dodat, že při současné legislativě se ani jeden většinou nedrží v mezích zákona a oba ho svým chováním porušují. V nedávné době například obletěl svět incident ohledně prolomení 64bitové GSM šifry německým hackerem Karstenem Nohlem. Tento skutečný hacker chtěl svým počinem upozornit operátory mobilních sítí, že je nejvyšší čas přijmout 128bitovou bezpečnější šifru pro mobilní komunikaci a zveřejnil software, který k prolomení šifry sám naprogramoval, a GSM šifrovací tabulku. Nyní je však obviněn a hrozí mu vězení. Zda je správné trestat člověka s dobrými úmysly, by si měl odpovědět soud i každý z nás sám. [16]

1.3 Četnost útoků

Zjistit, kolik bylo kupříkladu v roce 2009 napadených počítačů, je bohužel nemožné. Jediná dostupná čísla byla od institutu zabývajícího se internetovou bezpečností (CERT), ovšem tento institut přestal vydávat statistiku útoků v roce 2003. Pokud bychom vycházeli z trendu růstu počtu počítačových útoků, tak bychom se čistě teoreticky mohli dopočítat k číslu lehce přes 1 milion ohlášených útoků pro rok 2009. (Tento výpočet je brán ze statistik institutu CERT a ohlášeným útokem se rozumí zpráva, která se dostala přímo do tohoto institutu.) Jiné zdroje, které ovšem neuvádějí žádná čísla ani podmínky, hovoří o mnohem rapidnějších nárůstech. Obrovský nárůst počítačových útoků souvisí jednak s rostoucím počtem počítačových stanic připojených k síti, dostupností výkonného hardware, zrychlujícím se internetovým připojením a hlavně s používáním automatických nástrojů pro napadání počítačů. Každopádně zde stále hovoříme o zjištěných pokusech o útok, přičemž těch nezjištěných je jistě ještě mnohem více. Z toho vyplývá jediné — v dnešní době by měl každý uživatel a správce počítat s tím, že jeho počítač bude dříve či později terčem buď cíleného, nebo spíše náhodného útoku. [21]

2. Počítačové útoky

V druhé kapitole si ukážeme, jaké prostředky je schopen útočník využít k nabourání do našeho systému a jak se proti nim bránit. Rozdělení útoků v této práci je podle povahy a prostředků, které jsou při jednotlivých typech potřebné.

2.1 Brutal force attack — útok hrubou silou

Útok hrubou silou je jedním z nejjednodušších; jde o snahu uhádnout heslo. Hádání se provádí prostým zkoušením možných hesel. K zvýšení efektivity tohoto způsobu je vyvinuto mnoho software s obsáhlými slovníky nejpoužívanějších hesel. Takový software je pak schopen zkoušet obrovské množství kombinací znaků za jednotku času — odsud název útok hrubou silou. Útok je často účinný tehdy, jsou-li v systému používána slabá jména či hesla, například typu „admin“, „administrator“, nebo velice často používané „heslo“. Jediná možná a používaná ochrana proti takovému útoku je čekací doba mezi jednotlivými pokusy o zadání jména a hesla, případně úplné zablokování po několikátém chybném zadání. [15]

2.2 Social Engeneering — Sociální inženýrství

Český výraz sociální inženýrství je pouze doslovným překladem anglického originálu, se kterým se sice můžeme setkat, ale častěji se užívá původního anglického výrazu a tato práce nebude výjimkou. Social engeneering je v poslední době na obrovském vzestupu, co se týče pokusů o ovládnutí sítě. Pro úspěch útoků je nezbytná dobrá znalost prostředí a zainteresovaných osob, stejně jako „šikovnost“ útočníka. Má mnoho možností, jak se do sítě dostat a jeho provádění potřebuje snad jen notnou dávku drzosti. Útočník se snaží získat citlivé informace například tím, že se vydává za někoho jiného. Ukázkovým příkladem mohou být útočníkem zjištěná jména správců systému (často jsou uvedena na webových

stránkách). Útočník pak telefonuje nějakému zaměstnanci a vydává se za některého ze správců. Nic netušící uživatel pak prozradí svá přístupová hesla do dané aplikace, protože se domnívá, že hovoří se správcem, který jeho informace nezneužije. Dalším příkladem je vydávání se za poskytovatele připojení k internetu a žádání rekonfigurace nějakých klíčových aktivních síťových prvků. Tyto typy útoků však mohou být až finálním počinem útočníka a může jim předcházet „vytahování" potřebných informací ze zaměstnanců, pokud se nedají získat jinak — např. pokud nejsou uvedena jména správců na volně přístupném místě. To byla jen malá ukázka, jak si může útočník počínat — jakým způsobem konkrétně hodlá získat citlivá data záleží pouze na jeho představivosti, vynalézavosti a na tom, jak důvěryhodně si bude při svých pokusech počínat.

Do skupiny social engeneering útoků lze rovněž zařadit podvržené emaily, které jsou také hojně využívány pro získání informací. Konkrétně sem patří Phishing, ten sice neslouží jako prostředek k nabourání do sítě, ale v dnešní době se s ním každý setkává poměrně běžně. Útok je spojený s vykrádáním bankovních kont, je založený na sběru emailových adres roboty a následnému obesílání emaily, které vypadají skoro jako od peněžní instituce. Jediný rozdíl v emailech je ten, že žádají po uživateli osobní data, jako například PIN kód kreditní karty, přihlašovací údaje do internetového bankovnictví, nebo číslo kreditní karty; což banky nikdy nedělají. Pokud uživatel skutečně uvěří, že se jedná o pravdivý email a odpoví na něj, dojde ke zneužití poskytnutých informací a s největší pravděpodobností přijde o finance, které na účtu/kreditní kartě má.

U social engeneeringu je nejdůležitější nepodcenit jeho rozsah a význam. V současnosti je asi nejpoužívanějším cíleným útokem a těší se až překvapivě vysoké úspěšnosti, mimo jiné i díky tomu, že není v povědomí zaměstnanců ani široké veřejnosti. [10]

2.3 Hardware útoky

Jak už název napovídá, hardware útoky jsou fyzické zásahy do sítě — konkrétně se může jednat o prosté odcizení serveru. I sebelépe zabezpečená síť, ze které je schopen útočník ukrást server, je nezabezpečená. Z odcizeného serveru pak není žádný problém získat všechna data, ať vyjmutím disku nebo zrušením hesel a spuštěním počítače — hesla do BIOS (Basic Input — Output System) se vymažou restartem CMOS (Complementary Metal—Oxide—Semiconductor), hesla ze systému se odstraní např. jeho opětovnou instalací. [14]

Sem také patří útoky, které už trochu hraničí se skupinou následující (kapitola 2.4), konkrétně jde o síťové „napíchnutí" a „odposlouchávání"— sniffing. Těchto útoků je řada druhů a jde o to, zda jde o odposlouchávání a napíchnutí zároveň, nebo se jedná jen o odposlouchávání. Nejčastějšími druhy jsou:

2.3.1 Lokální sniffing

Odposlouchávání pomocí software na počítači oběti (nutná instalace tohoto software na konkrétní počítač).

2.3.2 Man-In-the-Middle (člověk uprostřed)

Sniffing, kdy dojde k přerušení sítě a následnému spojení přes útočníkův notebook, můstek nebo jiný hardware. Opět dochází k odposlouchávání a získávaní uživatelských jmen a hesel. Je nutný fyzický zásah do sítě, což není často možné. Využívá se nejčastěji na nějakých významných síťových uzlech, kde napáchá největší škodu.

2.3.3 Packet sniffing

Nejjednodušší sniffing, který využívá charakteristiky sítě typu Ethernet, kdy jsou data (pakety) posílány celé skupině počítačů a ne jen konkrétnímu stroji, pro který jsou přímo určena (platí v nepřepínané síti — síť s aktivním prvkem typu hub[9] [5]). Poté za pomocí programů (např. Sniffit) je možné tyto pakety odposlouchávat a pokud nejsou kryptované je přihlašovací jméno a heslo do systému jednoduše čitelné. [13]

2.4 Software útoky

2.4.1 DNS spoofing

DNS spoofing je typ softwarového útoku, který je nejčastěji součástí síťového odposlouchávání (sniffingu). Funguje na principu podvržení IP adresy odpovědi DNS serveru (Domain Name Server — překládá doménová jména na IP adresy). Způsobů provedení je mnoho a s trochou šikovnosti lze přesměrovat provoz i mimo lokální síť, na které je útok prováděn. Koncový uživatel se však neptá přímo DNS serveru, ale DNS Resolveru, který je běžnou součástí OS (operační systém). Pro provedení útoku budeme potřebovat zjistit hned řadu věcí:

- IP adresu DNS serveru, ta je pro každý počítač v síti stejná, takže není velký problém si ji zjistit.
- Jakým protokolem jsou data přenášena, častěji se používá UDP[20], méně často pak TCP[18] (UDP je pro útočníka jednodušší — nepoužívá sekvenční čísla).
- ID dotazu, což je 16bitové číslo (65536 možností).
- Port, ze kterého se DNS Resolver dotazuje.

V praxi to však není zcela totožné a díky implementaci DNS Resolveru často nepotřebujeme znát úplně všechny výše uvedené informace.

Často nám stačí jen to nejzákladnější — tím je ID dotazu a port.

Získání těchto klíčových informací je dnes již poměrně složité, dříve bylo možné na Windows platformě odchytit a zjistit oboje velice snadno, protože ID nebylo náhodné číslo. Ovšem současné Service Pack (aktualizační — opravné balíčky pro Microsoft Windows) už tyto chyby odstranily a ID je pseudonáhodné číslo.

Port, na který se dotazy posílají, se dá zjistit skenováním portů (síť bez firewall[5]), případně zkoušením nejpoužívanějších rozsahů portů.

Dalším způsobem, jak oboje zjistit, je odeslání dotazu DNS serveru na doménu kterou vlastní útočník. Na adrese je umístěn sniffer, který vše sdělí zpět útočníkovi.

Poslední věc, kterou je potřeba zajistit pro úspěšný útok, je, aby útočníkem zfalšovaná DNS odpověď dorazila dříve, než odpověď legitimní. Není to problém, pokud je útočník na stejné LAN jako oběť. Pokud tomu tak není, musí následovat tipování a prodloužení času na legitimní odpověď DNS serveru. Prodloužení odpovědi DNS serveru se provádí nejčastěji pomocí Denial-of-Service útoků (DoS — bude vysvětleno později v 2.4.6), které se snaží DNS server vyřadit z provozu nebo ho minimálně zatížit natolik, aby nedocházelo k rychlé odpovědi.

Všechny typy útoků na koncového uživatele probíhají velice podobně jen s drobnými obměnami. Na začátku útoku je nutné zjistit port a ID dotazu, útočník se většinou spokojí s portem, protože zjištění ID je komplikované. Pak spustí DoS útok na DNS server, který se tím snaží vyřadit případně zpomalit. Nyní začne posílat na cíl falšované DNS odpovědi s ID, které se bude měnit, než je ID uhádnuto. Následně útočník čeká na další dotaz nebo mu podvrhne jiný odkaz, aby toto urychlil. Útok má vyšší efektivitu, pokud se provádí z více počítačů současně.

Nyní přicházejí drobné modifikace:

- Využití sekce Additional records[1] — přidává do falšované odpovědi další adresy (využívá se pro urychlování DNS služeb). Útočník pak obdrží odpověď od serveru s dalšími dodatkovými adresami, které souvisí s původním dotazem.
- Mnohonásobné dotazování (dnes nefunkční) vedlo k vyšší pravděpodobnosti uhádnutí ID dotazu, protože existovalo více stejných dotazů (s jinými ID) a tím pádem i více ID správných odpovědí.

DNS spoofing je útok, který vede k přesměrovaní uživatele na jinou stránku, než předpokládá. Může vést například k zjištění přihlašovacích údajů do internetového bankovnictví a jiných stránek vyžadujících autentifikaci. (Je nutné vytvořit nešifrovanou kopii originálních stránek, aby uživatel skutečně vložil jméno a heslo v domnění, že přistupuje na původní stránky — využití social engeneeringu.) U neaktualizovaných a starších systémů bylo dokonce možné přistoupit na počítač bez autentifikace. Ta proběhla tím, že útočník byl považován za DNS server. [9]

2.4.2 ARP cache poisoning (Otrávení ARP paměti)

ARP — Address Resolution Protocol

Protokol ARP se používá pro překlad IP adres na MAC (Media Access Control — unikátní číslo pro každé síťové zařízení) adresy. Překlad je využíván v síti s aktivním prvkem typu switch[17] (přepínaný Ethernet), kdy switch zjišťuje podle MAC adres uložených v paměti (ARP cache), jakému počítači jsou data určena, jakou má IP adresu a na jakém portu se počítač nachází. (O přidělování portu k MAC se stará CAM paměť — bude vysvětleno při dalším typu útoku.)

Pozn. Tento typ sítě je rozdílný od typu s hubem (nepřepínaný Ethernet), kdy jsou pakety posílány celému segmentu sítě, nedochází tedy k překladu IP na MAC, protože překlad není zapotřebí. Nepřepínaný Ethernet je ale náchylný

k odposlouchávání, jak bylo popsáno výše.

ARP je již poměrně starým protokolem a byl navrhnut bez bezpečnostních mechanizmů, proto je dosti zranitelný.

Pro názorný příklad máme síť o 3 počítačích — počítač útočníka, počítač oběti a bránu připojenou na internet, přes kterou musí všechny počítače přistupovat, pokud chtějí do internetu. Na začátku útoku se pošle oběti paket, ve kterém se tvrdí, že brána má stejnou MAC, jako útočník. Poté se pošle paket bráně, že MAC adresa oběti je stejná, jako útočníkova. Tím se docílí toho, že switch bude posílat veškerá data přes útočníka, který si je může prohlédnout, poté přidělit správné adresy a odeslat zpět, aby se data neztratila (oběť nepozná, že něco není v pořádku). Jediné, co si musí útočník hlídat, je, aby nedošlo k smazání otrávené ARP cache ve switchi. Toho se docílí tím, že se posílají ARP Replay pakety neustále za sebou s daným časovým rozestupem (obvykle jednotky vteřin). Pro hromadný ARP cache poisoning (otrávení paměti) se používají ARP Gratuious Replay pakety; jsou běžnými ARP Replay (ARP odpověď), s tím rozdílem, že jim nepředcházel žádný ARP Request (ARP žádost). V ARP Gratuious Replay paketech je nastavená universální MAC adresa (FF:FF:FF:FF:FF:FF), takže je přijmou všechny počítače a pokud již existuje z IP adresy oběti záznam, tak se univerzální MAC změní na MAC adresu útočníka.

Útok v praxi funguje výše popsaným způsobem a využívá se k němu potřebného software — Ettercap, Ethereal a Dniff. Zmíněný software je volně k dispozici na internetu, takže útočník zde má volné pole působnosti a může prohlížet veškerou komunikaci mezi počítači v síti. [6]

Pozn. Program Ettercap ve skutečnosti nezaznamenává veškerou komunikaci mezi počítači (považuje to za nadbytečné). Jediné co kontroluje a uchovává jsou přihlašovací jména a hesla a také, kam s heslem uživatel přistupuje. Tímto vlastně útočníkovi ještě usnadňuje práci. Ten se po odfiltrování nepotřebného balastu dostává přímo k tomu, proč celý cache poisoning dělal — k přístupovým jménům a heslům oběti.

2.4.3 Port Stealing (Kradení portu) — alias MAC Flooding

Již z názvu je jasné, že při útoku jde útočníkovi o kradení portu. Opět je tento útok možný pouze na přepínaném Ethernetu, protože se k němu využívá switch. Switch si při každém přijetí paketu aktualizuje CAM (Content Addressable Memory) tabulku, která uchovává odesílatelovu MAC adresu a port, na kterém se nachází. Útočník toho využije tím, že začne posílat pakety, které budou mít útočníkovu MAC jako cílovou a jako odesílatelova bude uvedena MAC oběti. Tím docílí, že switch podle nastavení MAC předpokládá, že oběť je na portu odkud byl paket poslán a podle toho upraví CAM tabulku. Pak nastane to, že switch bude data posílat útočníkovi namísto oběti. Útočník si data prohlédne, opraví CAM tabulku korektním ARP paketem a odešle data oběti. Port Stealing útok je ovšem dost náročný na uchování konzistence dat, protože při komunikaci oběti směrem ke switchi se vždy přepíše CAM tabulka na správné adresy. Navíc je na správné hodnoty přepisuje i útočník a poté je zase přepisuje na špatné, aby mohlo k prohlížení paketů docházet a zároveň, aby je obdržela i oběť. Opakované přepisování CAM tabulky tak může vést k tomu, že některá data nejsou útočníkem zachycena. [7]

Pozn. U některých přístrojů dochází k zahlcení CAM paměti a switch pak přestane posílat data kontrolovaně (jen jednomu počítači podle MAC adresy), ale posílá je celému segmentu sítě podobně jako hub a nekontroluje MAC adresy ani odesílatele, ani příjemce.

2.4.4 DHCP Spoofing

Pozn. DHCP (Dynamic Host Configuration Protocol) — protokol, který slouží k přidělování síťových parametrů koncovému zařízení.

Útok zakládá na tom, že v LAN síti může existovat a fungovat více DHCP serverů. Když se oběť poprvé připojuje do sítě, pošle paket DHCP Discover, jenž slouží k zjištění, jaké DHCP servery se na síti nachází. Paket je odeslán s nesměrovou adresou, takže projde celou sítí. DHCP

servery na tento paket odpoví DHCP Offer paketem, kde jsou nabídnuty parametry pro připojení. Počítač si však nevybírá ze všech přijatých možností, ale reaguje pouze na první DHCP Offer paket — funguje princip nejrychlejšího. Nejrychlejšímu DHCP serveru pak zašle DHCP Request s žádostí o parametry pro připojení. Server odpoví DHCP Ack paketem a spojení je navázáno. Když útočník chce do systému zasáhnout, jediné co k úspěchu potřebuje, je zajistit, aby jeho falešný DHCP server byl tím nejrychlejším, který odpoví na paket DHCP Discover.

V praxi je ovšem problém zastihnout okamžik, kdy se oběť poprvé připojuje do sítě. Při běžné komunikaci totiž posílá oběť už jen DHCP Request pakety k serveru, který jí naposledy přidělil parametry. Když nastane tato situace, jediná útočníkova možnost spočívá v tom, že čeká, až oběti vyprší doba platnosti IP adresy (lease time — jeden z parametrů nastavení DHCP serverů; doba se může lišit, ale většinou bývá několik hodin, maximum pak bývá 1 den). Aby si útočník zajistil, že jeho falešný DHCP server odpoví jako první, vyřadí korektní DHCP servery z provozu posíláním požadavků na přidělení parametrů, než dojde k jejich vyčerpání. Když má DHCP server vyčerpané možnosti přidělení parametrů, přestane odpovídat na DHCP Discover a zároveň není schopen oběti prodloužit platnost parametrů, protože má žádosti, které byly před ní.

Pozn. Nejpohodlnější pro útočníka je využít toho během delší doby, kdy nejsou klienti (oběti) připojeni — např. víkend.

Po připojení oběti na falešný DHCP server s podvrženou výchozí branou — gateway (gateway — brána; slouží pro spojení dvou sítí s rozdílným protokolem, nejčastěji jako spojení LAN s internetem) a přesměrování provozu přes útočníka lze pomocí speciálního software (Ettercap) sledovat data jdoucí do internetu. [8]

Pozn. Při DHCP spoofingu není schopen útočník sledovat data, která jdou z internetu k oběti, protože data jsou posílána na skutečnou gateway a nikoliv přes útočníka. Pro obousměrné sledování dat je třeba využít jiného útoku, například již popisovaného DNS spoofingu.

2.4.5 Buffer Overflow (Přetečení vyrovnávací paměti)

Tento typ útoku se týká z větší části Linuxových systémů, kde Buffer Overflow představuje větší nebezpečí. Útok spočívá v naplnění proměnné větší hodnotou, než proces očekává. Při vhodně zvolených datech vede přetečení až k neoprávněnému vykonávání příkazů na cílovém počítači. Pokud má pak napadený proces práva superuživatele, mají je i prováděné příkazy. Tento problém je téměř výlučně způsoben chybně napsanou aplikací, kdy program nekontroluje formát dat, ale rovnou je vkládá do paměti. Konkrétních typů známých chyb u používaných programů je velké množství, ale naprostá většina je jich dnes již opravených a proto útok nefunguje. Útok je tedy úspěšný pokud cílový systém není aktualizovaný. [5]

2.4.6 DoS — Denial of service (odepření služby)

DoS útoky ne zcela zapadají do kategorie pro získání neoprávněného přístupu. Tyto útoky totiž nejsou samy o sobě schopné poskytnout ani zachytit přihlašovací jména a hesla, ale často jsou využívány v kombinaci s jinými, kdy je třeba zahltit a vyřadit z provozu nějakou část sítě. DoS útok je vždy prováděn se špatným úmyslem, protože slouží výhradně k tomu, aby napadená služba nebo část sítě nebyla schopna obsluhovat běžné uživatele. DoS útok je také často využíván jako poslední možnost při nepodařenému útoku, kdy je oběť alespoň poškozena, když se útočníkovi nepodařilo do sítě dostat jiným způsobem. Útoky jsou častěji prováděny na Windows servery, protože ty jsou mnohem náchylnější k jejich působení. DoS útoků je rovněž využíváno pro „zametení stop“. Když se útočník dostane do systému, tak po sobě většinou zanechá nějaké stopy, pokud se mu podaří zhroutit systém pomocí DoS útoku, zbude po něm stop mnohem méně a samotný DoS útok je prakticky nemožné vystopovat.

DoS útoky je možné rozdělit do 3 základních skupin:

- Útoky využívající chyb implementace TCP/IP — Ping of Death, Teardrops Attacks
- Útoky využívající nedostatky ve specifikaci TCP/IP — SYN Attack, Land Attack
- Brutal force attack — útok hrubou silou — Smurf

Útoky využívající chyb implementace TCP/IP

Ping of Death

Příkazu ping se využívá hojně pro zjištění zda vzdálený server pracuje. Útočník provede při útoku to, že překročí maximální povolenou velikost ping paketu (specifikace IP protokolu uvádí maximální přípustnou velikost 65 536 bajtů). Takový nestandardně velký paket pak odešle na cíl. Ten může na cíli napáchat velkou škodu a může vést ke zhroucení nebo zamrznutí celého systému. Útok je však již hodně starý a drtivá většina operačních systémů má proti němu záplaty, které ho znemožní.

Teardrops Attack

Tento útok je novější a využívá slabiny při opětovném sestavování IP paketů, které byly rozděleny na více částí. Každý kus IP paketu je totožný s původním, jen v sekci offset obsahuje informaci, jaký rozsah bajtů z původního paketu nese. Teardrop program pak vytváří sérii fragmentů, které se překrývají — položky offset jsou chybně vyplněny a překrývají se. Při opětovném sestavování na cílovém serveru může dojít k zhroucení některých systémů.

Útoky využívající nedostatky ve specifikaci TCP/IP

SYN Attack

SYN Attack využívá skutečnosti, že při navazování komunikace mezi dvěma systémy dochází k „třífázovému handshakingu“ (three way handshake). Ten funguje tak, že aplikace, která chce posílat a přijímat data od vzdáleného počítače, pošle synchronizační SYN paket. Příjemce na něj odpoví TCP SYN—ACK, což je potvrzovací paket, na který čeká odpověď od iniciátora spojení v podobě ACK paketu. Až teprve po ukončení procesu jsou schopné aplikace mezi sebou posílat a přijímat data. Útočník této skutečnosti využije tak, že začne na cílový systém posílat SYN pakety, které mají ovšem vyplněnou neplatnou IP adresu odesílatele — vylepšení s neplatnou IP se nazývá **Land attack**. Na neplatnou IP posílá systém SYN—ACK pakety a čeká na odpověď, která ovšem nepřijde. Nenavázaná spojení systém nezahazuje, ale dává je do fronty (obvykle bývá velice krátká) a čeká na odpověď. Po chvíli nastane situace, kdy útočník zaplní frontu a legitimní uživatel již nedokáže navázat spojení. Z fronty jsou žádosti odebrány pouze dvěma způsoby, buď přijetím ACK paketu, nebo po uplynutí časového intervalu interního časovače, který pak smaže nevyřízené požadavky. Časovač bývá obvykle nastaven na relativně dlouhé intervaly. Při konstantním posíláním žádostí od útočníka se tak vytvoří fronta, která se ani není schopna pomocí interního časovače zcela promazávat a legitimní uživatelé nebudou obslouženi.

Útoky hrubou silou

Smurf

Útok smurf je zaměřen na vlastnost, která se nazývá všeobecné adresování (direct broadcast addessing). Útočník zaplaví síť ping pakety s broadcast cílovou adresou. Nastavení adresy způsobí, že na síti oběti budou routery šířit ping pakety každému počítači. Pokud je pak síť vel-

ká, dojde k jejímu značnému zatížení. Celý útok se dá ještě vylepšit tím, že odesílatelem může být zfalšovaná adresa nějaké jiné sítě a ta pak bude zahlcena odpověďmi ze sítě první. Útočník je tak schopen omezit provoz na obou sítích prakticky zároveň.

Výčet známých a používaných DoS útoků je rozsáhlejší, ale práce nepojednává jen o DoS útocích a proto bude zmíněný výpis a popis útoků stačit. Ještě je nutné ovšem zmínit jednu významnou modifikaci DoS útoků a tou je **DDoS (Distributed Denial—of—service)**. Tento útok využívá stejných postupů jako DoS, jen je ještě mnohem zákeřnější v tom, že se provádí z většího množství počítačů najednou. Když se u DDoS útoku hovoří o větším počtu, máme na mysli desítky, stovky či dokonce tisíce počítačů. Útočník takto velké množství počítačů neovládá pochopitelně sám, ale nějakou dobu před samotným útokem šíří internetem program — tzv. zombie. Zombie se pak na popud útočníka aktivuje a zasype oběť přívalem dat. [14]

2.5 Obrana proti útokům

V této části si ukážeme některé způsoby, jak je možné se proti výše uvedeným útokům bránit.

2.5.1 Brutal force attack — útok hrubou silou

Nejjednodušší obranou je nepoužívání jednoduchých jmen a hesel, což není až tak úplně obrana, jako spíše dobrá rada. Jediná možná a používaná skutečná ochrana proti Brutal force útoku je pak čekací doba mezi jednotlivými pokusy o zadání jména a hesla, případně úplné zablokování po několikátém chybném zadání.

2.5.2 Social engeneering — sociální inženýrství

Ochrana proti social engeneering je velice složitá a vlastně neexistuje přesný postup, jak se útokům vyvarovat. Asi nejúčinnějším způsobem, jak útoky omezit je školení zaměstnanců. Když zaměstnanec ví, že právě on by se mohl stát obětí pravděpodobně si dá větší pozor, aby k tomu nedošlo. Dalším způsobem je samozřejmě kontrola proti vniknutí do objektu, bezpečnostní kamery a podobně. Útočník si ovšem nepočíná nijak podezřele a je velmi obtížné rozeznat, že má nekalé úmysly. Ovšem jsou typy útoků, proti kterým je i proškolený zaměstnanec bezbranný — například pokud je útočník z řad jeho kolegů.

Pozn. Social engeneering s útočníkem v jádru firmy nebyl uváděn jako konkrétní útok, protože není prováděn zvenčí a útočník je pak součástí bezpečnosti firmy. Takový útok je velmi specifický a neexistují žádné postupy, jak zaměstnanec — útočník bude při útoku postupovat, neboť to vše záleží jen na jeho postavení, informacích a možnostech, ke kterým se ze své pracovní pozice dostane.

2.5.3 Hardware útoky

Hardware útoky jsou prováděny striktně přímo ve firmě, proto jedinými bezpečnostními možnostmi je, aby se útočník nedokázal dostat na místa, která by mohl zneužít — mít zabezpečené síťové uzly a servery.

Pozn. Podle nejnovějších průzkumů je útočník schopen zcela překonfigurovat (přístupová práva, jména a hesla) server během 1 minuty a 20 sekund.

Základním předpokladem k zajištění bezpečnosti je zamezit komukoliv bez autorizovaného přístupu, aby se pohyboval v blízkosti serveru, například i po výpadku proudu, nebo podobném incidentu — tyto incidenty mohou být fingovány útočníkem.

2.5.4 Software útoky

Software útoky také většinou probíhají z LAN daného cíle, takže nejjednodušší ochranou je útočníka do sítě nepustit. Zabezpečení všech možných síťových zásuvek po celé budově cíle a jejich kontrola, případně odpojení těch nevyužívaných. Další nadstavbou pak může být využití ověřování uživatelů pomocí protokolu EAPOL (Extensible Authentication Protokol Over LAN). Samotný protokol neurčuje konkrétní způsob autentizace, proto k ní může sloužit heslo, čipová karta nebo USB token, totožnost se pak ověřuje na autentizačním serveru. Když se útočník pokouší o útok zvenčí, je nezbytné mít pro ochranu kvalitní firewall.

Většině druhů útoků se ještě dá zabránit nastavením firewallu a aktivních prvků. To platí především pro DoS a DDoS, kterým jiným způsobem, než nastavením firewall a aktivních prvků zabránit nelze. Další obranou, která je možná pouze u profesionálních zařízení (např. dražší modely prvků Cisco), je omezení množství určitých typů paketů — konkrétní typ volíme podle útoku a vnitřních potřeb sítě. Vzhledem k tomu, že omezení není možné provést všude, nebudeme se jimi detailně zabývat. Obecně používaná nastavení, která jsou dostupná i na levnějších zařízeních, jsou pak omezení UDP z internetu — ochrana proti UDP Flood, filtrování neplatných IP adres firewallem — Land Attack, nebo vypnutí Broadcast adresování — Smurf.

Proti starším, ale i novějším typům útoků je pak důležitá ochrana pomocí instalace aktualizací, to ovšem již dnes považujeme za samozřejmost a předpokládáme, že důležité systémy jsou opravované posledními dostupnými aktualizacemi výrobců. [9]

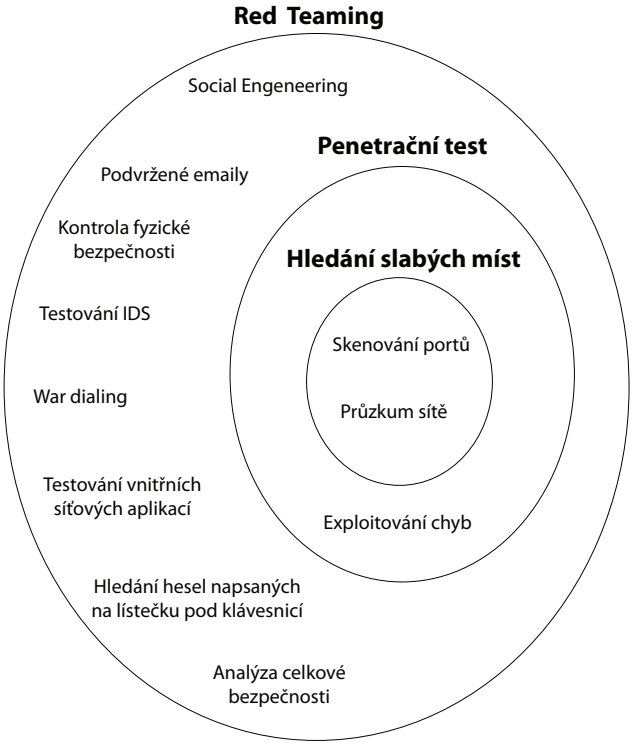
Pozn. Při aktualizacích je důležité brát v potaz, že nejen operační systém, ale i ostatní programy je třeba aktualizovat. Neméně důležitá je pak kontrola a aktualizace firmware síťových prvků.

3. Bezpečnostní testy

Bezpečnostní testy jsou způsob, jak zjistit stávají bezpečnost sítě. Bezpečnostní testy mají různý rozsah a různé zaměření. Abychom se dokázali v problematice orientovat, ukážeme si v této kapitole kategorizaci bezpečnostních testů a popíšeme si jejich jednotlivé druhy.

3.1 Rozdělení podle prováděných úkonů

Při rozdělení pouze podle rozsahu testování použitých metod můžeme testy v zásadě dělit na 3 druhy. Prvním z nich je **Hledání slabých míst** (vulnerability assessment, vulnerability audit) trošku obsáhlejším je **Penetrační test** (pen testing) a nejkomplexnějším testem je pak **Red Teaming**. Přehledné rozdělení včetně prováděných činností můžeme vidět na následujícím obrázku. Rozdělení je velmi jednoduché, ale nezahrnuje všechny okolnosti, které je třeba zohlednit. Ovšem jako jednoduché naznačení rozdělení testů má dostatečnou vypovídající hodnotu a pro svou jednoduchost je i často využíváno.

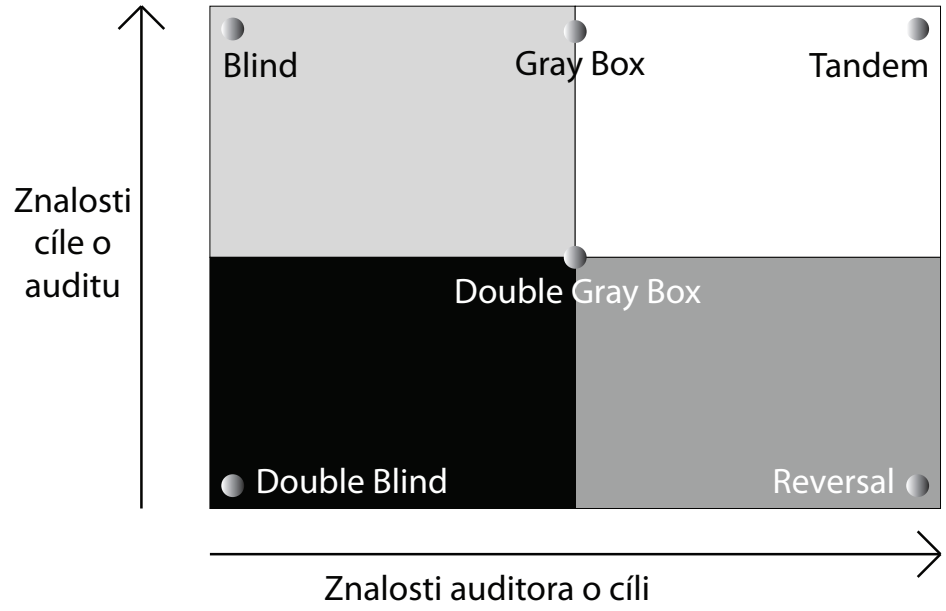


Z obrázku vyplývá, že rozdíl mezi hledáním slabých míst a penetračním testem spočívá v tom, že při penetračním testu je využito (zneužito) vyhledaných slabých míst a jejich pomocí se dále pokouší auditor získat kontrolu nad systémem (typicky administrátorská přístupová práva). Penetrační test zdaleka nezohledňuje všechna potenciální nebezpečí, jak to činí Red Teaming. V praxi však často bývá prováděn jen penetrační test, protože velký rozsah Red Teamingu posouvá testy do jiné cenové kategorie. Často rozsah penetračního testu postačuje pro zjištění úrovně zabezpečení, protože útoky jsou i přes dnešní vzestup social engineeringu stále nejčastěji prováděny z internetu. Pokud má ovšem firma nebo instituce zájem o rozsáhlé prozkoumání bezpečnosti je Red Teaming asi jediným skutečným a hlavně komplexním testem bezpečnosti. [2]

3.2 Rozdělení podle znalostí obou zainteresovaných stran

Toto rozdělení je o poznání složitější a využívá ho právě OSSTMM manuál, který je nedílnou součástí práce. V souladu s pravidly přepisování (překládání) OSSTMM budou uvedeny nejprve anglické názvy jednotlivých testů a specifických anglických výrazů a až poté české ekvivalenty.

Pozn. České ekvivalenty jsou uváděny pouze tehdy, jsou-li používané, doslovný překlad anglických výrazů by byl matoucí a kontraproduktivní.



Nejprve je třeba definovat, co znamenají jednotlivé pomyslné osy. Osa x reprezentuje auditorovy znalosti o cíli. Osa y reprezentuje informovanost o připravovaném útoku. Nyní je možné začít objasňovat jednotlivé druhy testů.

3.2.1 Blind

Auditor se zabývá cílem bez předchozích znalostí obrany, bezpečnostních výhod a kanálů — dle OSSTMM existují 3 kanály (COMSEC[3], PHYSEC[13], HUMSEC[10]). Cíl je připraven na audit a v předstihu zná, všechny detaily auditu, včetně předpokládaného průběhu. „Blind" audit primárně testuje dovednosti auditora. Rozsah a hloubka „Blind" auditu může být pouze taková, nakolik je auditor schopen aplikovat své znalosti a jak dovolí jeho efektivita. V COMSEC a SPECSEC[14] je tento typ testu často referován jako „Ethical Hacking" (etický hacking) a v dalších PHYSEC a HUMSEC je popisován jako „War Gaming" nebo „Role Playing".

3.2.2 Double Blind

Auditor se zabývá cílem bez předchozích znalostí obrany, bezpečnostních výhod a kanálů. Cíl není vyrozuměn o průběhu testu, které kanály budou testovány, nezná rozsah testu, ani odkud bude test veden. „Double Blind" audit testuje jednak dovednosti a znalosti auditora a také připravenost cíle na neočekávané útoky a zásahy do sytému. Rozsah a hloubka „Double Blind" auditu může být pouze tak obsáhlá, jak je auditor schopen aplikovat své znalosti a jak dovolí jeho efektivita. Tento test je označován jako „Black Box Audit" nebo „Penetration Test" (Penetrační test).

3.2.3 Gray Box

Auditor se zabývá testem s omezenými znalostmi cíle, jeho obrany a bezpečnostních výhod, ale s plnou znalostí kanálů. Cíl je připraven na audit a v předstihu zná, všechny detaily auditu, včetně předpokládaného průběhu. „Gray Box" audit testuje jednak dovednosti a znalosti auditora a také připravenost cíle na neočekávané útoky a zásahy do sytému. Tento druh testu je velmi efektivní. Rozsah a hloubka testu záleží na množství a kvalitě poskytnutých informací auditorovi a cíli, stejně jako na aplikaci auditorových znalostí a jeho efektivitě. Tento typ je často referován jako „Vulnerability Test" (hledání slabých míst) a je nejčastěji prováděn samotným cílem jako sebehodnocení.

3.2.4 Double Gray Box

Auditor se zabývá testem s omezenými znalostmi cíle, jeho obrany a bezpečnostních výhod, ale s plnou znalostí kanálů. Cíl je upozorněn v předstihu na rozsah a typ testování a je seznámen s časovým plánem, ale neví, jaké kanály budou testovány a odkud budou testy provedeny. „Double Gray Box" audit testuje jednak dovednosti a znalosti auditora, ale především připravenost cíle na neočekávané útoky a zásahy do systému. Test je velmi efektivní. Rozsah a hloubka testu záleží na množství

a kvalitě poskytnutých informací auditorovi a informacích poskytnutých cíli stejně jako na aplikaci auditorových znalostí a jeho efektivitě. Test je také znám jako „White Box Audit“.

3.2.5 Tandem

Auditor a cíl jsou předem upozorněni na všechny detaily ohledně testování i popisu zabezpečení. „Tandem“ audit testuje ochranu a správce cíle. Ale nemůže otestovat připravenost cíle na neznámé a neočekávané útoky. Test je velmi důkladný, protože auditor má přesné a podrobné informace o cíli a jejich reakcích. Rozsah a hloubka testu záleží na množství a kvalitě poskytnutých informací auditorovi (průhlednost), stejně jako na aplikaci jeho znalostí a jeho efektivitě. Toto je často známo jako „In-House Audit“ nebo jako „Crystal Box Audit“ a auditor je většinou součástí bezpečnostního týmu, často jeden ze správců.

3.2.6 Reversal

Auditor ví naprosto všechny potřebné informace o procesech a zabezpečení cíle. Oproti tomu cíl neví absolutně nic, ani jaký test bude proveden, ani kdy a v jakém rozsahu. Test je především o zkoumání připravenosti na nepředpokládané útoky. Rozsah a hloubka testu závisí na množství a kvalitě poskytnutých informací auditorovi (průhlednost), stejně jako na aplikaci jeho znalostí a jeho kreativitě. Test je také často nazýván „Red Teaming“. [4]

Jak si můžeme všimnout, oba pohledy rozdělení jsou velice důležité a rozdílné a to je důvod, proč se využívají a existují oba. Jak by se mohlo zdát, definování jednotlivých testů je velice striktní, ale opak je pravdou. Proto je velice důležité si u všech testů předem definovat a stanovit jaké testy se budou provádět a s jakým obeznámením jednotlivých stran, u skutečných útoků to samozřejmě možné není. V praxi by asi nejkom-

plexnějším testem byl Red Teaming z pohledu rozsahu, ale zároveň penetrační test z hlediska znalostí obou stran. Takový test by nejvíce vypovídal o opravdové snaze útočníka proniknout do systému i bez jeho znalostí (cíl by mu je neposkytl), ale zároveň by využil naprosto všech možností proniknutí včetně social engeneeringu.

3.3 Jiné používané testy

Do této kategorie patří testy, se kterými je možné se setkat, ovšem nejdou ani do jednoho z předchozích rozdělení zařadit. Patří sem samozřejmě více testů, ale budou uvedeny dva nejčastěji používané.

3.3.1 Bezpečnostní audit

Prvním z testů je bezpečnostní audit, test je rozsahem velice podobný penetračnímu testu, ovšem probíhá „zevnitř". Auditor obdrží administrátorská práva a zkoumá bezpečnost systému zevnitř a nepokouší se do něho proniknout, ale najít slabá místa přímo uvnitř samotného systému.

3.3.2 Systémové testy

Tyto testy jsou ovšem dost odlišné od běžného penetračního testu a zabývají se pouze konkrétní částí systému. Například systémový test webové aplikace, který testuje jen a pouze konkrétní webovou aplikaci, ale zkoumá ji velice podrobně (mnohem podrobněji než penetrační test). Testování se soustředí jednak na známé chyby, ale také na hledání chyb nových. Systémové testy jsou velice náročné na auditora, protože hledání nových chyb je velice složitý problém, který vyžaduje opravdu vysoké znalosti problematiky. Testy jsou často využívány zákazníky, kteří žádají zjištění bezpečnosti konkrétních částí systému, ze kterých považují útok za nejpravděpodobnější a nejničivější. [22]

4. OSSTMM

Open Source Security Testing Methodology Manual — v této části práce si řekneme něco o manuálu, který je určený pro veškeré bezpečnostní testy. Ukážeme si zde úryvky manuálu, abychom se stručně a výstižně dozvěděli, k čemu přesně má manuál sloužit a jaké jsou jeho možnosti.

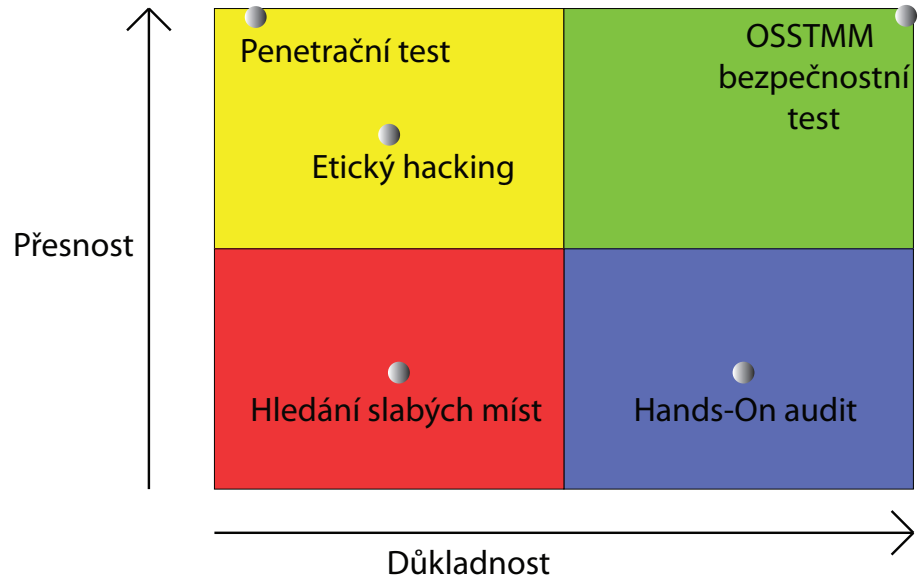
Pozn. Veškerý text je přímo převzatý z OSSTM manuálu a je přeložen autorem práce.

4.1 Představení OSSTMM

OSSTMM poskytuje metodologii pro celý bezpečností test, v manuálu uváděný jako OSSTMM audit. OSSTMM audit je přesným měřením bezpečnosti na operační úrovni. Pomocí této metodologie jsou prováděny testy, které jsou celistvé a opakovatelné. Od svého vzniku má již tisíce recenzentů. Od roku 2005 není OSSTMM brán pouze jako framework pro etický hacking, ale stává se metodologií pro zajištění bezpečnosti na operační úrovni.

4.2 Účel OSSTMM

Primárním důvodem existence manuálu je poskytnout odbornou metodologii pro přesnou charakteristiku bezpečnosti pomocí zkoumání a vyhodnocování výsledků testů. Manuál je adaptabilní na všechny možné typy auditů, včetně penetračního testu, etického hackingu, bezpečnostního zhodnocení, vyhodnocení zranitelnosti, red-teamingu, blue-teamingu a podobných. Je napsaný jako bezpečnostní výzkumný dokument a je projektován na faktické bezpečnostní ověřování a prezentaci na profesionální úrovni.



Sekundární účel je poskytovat směrnice, které při správném dodržování dovolí auditorovi vykonávat kvalifikovaný OSSTMM audit. Tyto směrnice existují pro zajištění následujícího:

1. Test byl vedený důsledně.
2. Test zahrnul všechny nezbytné kanály.
3. Test vyhověl zákonům dané země.
4. Výsledky jsou kvantifikovatelené.
5. Výsledky jsou konzistentní a opakovatelné.
6. Výsledky obsahují jen fakta odvozená ze samotných testů.

4.3 Výsledky a jejich certifikace

Výsledky testů bývají často doprovázené doporučenými řešeními problémů nebo návrhů konzultanta. Doporučená opatření nejsou povinná, protože často neexistuje ucelené řešení, které by bylo schopno zohlednit jak pohled auditora, tak pohled správců systému, kteří můsí dodržet jistá opatření v rámci potřeb pro správný chod sítě.

Prověření bezpečnosti zkoumaného cíle by mělo vyústit závěrečnou bezpečnostní zprávou — STAR (Security Test Audit Report).

STAR vyžaduje následující informace:
1. Datum a čas testu
2. Testovací období
3. Auditory a analytiky provádějící testování
4. Typ testu
5. Rozsah testu
6. Zkušební Index (metoda cílového výpočtu)
7. Testované kanály
8. Testované vektory
9. Ověřený test a metrické výpočty operační ochranné úrovně, kontrolu ztrát a bezpečnostní omezení
10. Informaci, které testy byly dokončeny, nedokončeny, či jen částečně dokončeny a jak dalece
11. Případné problémy s ohledem na test a platnost výsledků
12. Přesnost testování
13. Procesy, které ovlivňují bezpečnostní omezení
14. Všechny neznámé či anomálie

Certifikace a akreditace závěrečné zprávy

Aby mohl test a závěrečná zpráva STAR získat certifikaci a akreditaci, je nezbytné, aby bylo STAR podepsáno auditorem (auditory) či analytiky, kteří provedli test. Zpráva STAR musí také splnit požadavky zprávy uvedené v této příručce. STAR může být předloženo institutu ISECOM k recenzi a oficiální OSSTMM certifikaci. Certifikace nezaručuje, že byla provedena celá škála testů, garantuje pouze, že ze závěrečné zprávy bude patrné, které testy proběhly, které nikoliv a získáme jejich výsledky, resp. odůvodnění proč nebyly provedeny.

Kvalifikovaný OSSTMM audit poskytuje následující výhody:
1. Slouží jako důkaz faktického testu
2. Auditor nese zodpovědnost za výsledky testu
3. Poskytuje jasný výsledek klientovi
4. Poskytuje komplexní pohled na bezpečnost testovaného subjektu
5. Poskytuje pochopitelné metriky

4.4 Závěr

Výše uvedené slouží jako ukázka z OSSTMM. Z pochopitelných důvodů nemá smysl na tomto místě předkládat další ukázky z manuálu. Pokud má čtenář skutečný zájem se o metodice dozvědět více, má možnost přímo na stránkách ISECOM, kde získá plné znění manuálu. [4]

5. Penetrační test

Kapitola obsahuje postupy a výsledky (nikoliv hodnocení — kapitola 6) penetračního testu provedeného na PF JČU v Českých Budějovicích.

Cílem testu bylo zjištění stavu zabezpečení a odolnosti PF vůči útokům zvenčí.

Test zahrnuje použití běžných testovacích postupů jakými jsou pasivní i aktivní prohledávání sítě, testování automatickými nástroji a částečně také exploitování zjištěných nedostatků.

Test nezahrnuje programování vlastních exploitů, objevování dosud nezjištěných chyb v zabezpečení, DoS (DDoS) útoky a nevěnuje se bezdrátovým sítím, ani síti uvnitř fakulty. Vnitřní LAN fakulty nebyl zkoumán z důvodu nepovolení tohoto testování ze strany správců.

Technické detaily testu

Penetrační test probíhal převážně v období 16. 11. 2009—6. 12. 2009

Test byl prováděn na přenosném počítači značky Asus, modelové označení A8 — H, technické parametry počítače: Intel Celeron M 420 @ 1,6 GHz, 1024 MB DDR2 RAM, Atheros AR5006EG Wireless Network Adapter (MAC 00-15-AF-02-2A-B1), Realtec RTL8168/8111 PCI-E Gigabit Ethernet NIC (MAC 00-17-31-95-18-FE), OS Microsoft Windows XP Professional SP3. Některé testy byly spouštěny pod linuxovou platformou pod systémem Pentoo-i686-2009.0_beta a Backtrack 4 Pre-final (obrazy jsou na přibaleném DVD). Počítač byl připojen k internetu společností STARNET České Budějovice přes router Asus GL-32 a vystupoval pod IP adresou 92.62.224.12. Některé testy byly prováděny na připojení od společnosti JHComp při použití routeru TP-LINK TL-WR642G s vnější IP adresou 88.146.207.2.

5.1 Testy prováděné na celém rozsahu

5.1.1 Pasivní prohledávání

Pasivní prohledávání spočívá v zjištění co možná nejvíce dostupných informací, aniž by to prohledávaná strana mohla zjistit. Tyto informace jsou uloženy v registrech a databázích na internetu.

whois

Program slouží k získání informací z centrálního registu

```
C:\dig>whois 160.217.96.1
% This is the RIPE Database query service.
% The objects are in RPSL format.
%
% The RIPE Database is subject to Terms and Conditions.
% See http://www.ripe.net/db/support/db-terms-conditions.pdf

% Note: This output has been filtered.
% To receive output for a database update, use the „-B" flag.
% Information related to ‚160.217.0.0 – 160.217.255.255'

inetnum: 160.217.0.0 – 160.217.255.255
netname: JCU-TCZ
descr: University of South Bohemia
descr: Ceske Budejovice
country: CZ
admin-c: JM13374-RIPE
tech-c: PS1575-RIPE
status: ASSIGNED PI
mnt-by: TENCZ-MNT
remarks: Please report network abuse – > abuse@jcu.cz
source: RIPE # Filtered

person: Jan Marek
address: Univesity of South Bohemia
address: Academic Computer Centre
address: Branisovska 31
address: Ceske Budejovice
address: 370 05
address: The Czech Republic
phone: +420 387772080
fax-no: +420 385310348
abuse-mailbox: abuse@jcu.cz
nic-hdl: JM13374-RIPE
source: RIPE # Filtered
```

```
person: Petr Simek
address: University of South Bohemia
address: Academic Computer Centre
address: Branisovska 31
address: Ceske Budejovice
address: 370 05
address: The Czech Republic
phone: +420 387772083
fax-no: +420 385300348
abuse-mailbox: abuse@jcu.cz
nic-hdl: PS1575-RIPE
source: RIPE # Filtered

% Information related to ‚160.216.0.0/15AS2852‘

route: 160.216.0.0/15
descr: UNOB-TCZ + JCU-TCZ
origin: AS2852
mnt-by: AS2852-MNT
remarks: Please report abuse — > abuse@cesnet.cz
source: RIPE # Filtered
```

Jak si můžeme všimnout, informace se bohužel nevztahují přímo na PF, nýbrž na celou Jihočeskou univerzitu a jediné, co se dozvíme, jsou jména správců a kontakty na ně. Je to způsobené tím, že registrátor domény je Jihočeská univerzita a Pedagogická fakulta spadá pod ni.

Pozn. Informace je možné zjistit i online, například na nic.cz.

Dig, nslookup

Z neznámého důvodu nelze použít na prozkoumání sítě ani jeden z programů, vždy dojde k přerušení spojení. Při použití online nslookup (http://network-tools.com/nslook/Default.asp) ovšem již nějaké výsledky dostaneme, ale opět se vztahují na celou univerzitu.

Answer records

name	class	type	data		time to live
pf.jcu.cz	IN	MX	preference: exchange:	12801 ax.virusfree.cz	3600s (1h)
pf.jcu.cz	IN	MX	preference: exchange:	12817 bx.virusfree.cz	3600s (1h)
pf.jcu.cz	IN	MX	preference: exchange:	12833 cx.spamfree.cz	3600s (1h)
pf.jcu.cz	IN	MX	preference: exchange:	12849 dx.spamfree.cz	3600s (1h)

Authority records

name	class	type	data	time to live
jcu.cz	IN	NS	taurus.zf.jcu.cz	3600s (1h)
jcu.cz	IN	NS	eros.zcu.cz	3600s (1h)
jcu.cz	IN	NS	virgo.jcu.cz	3600s (1h)

Additional records

name	class	type	data	time to live
virgo.jcu.cz	IN	A	160.217.1.10	3600s (1h)
taurus. zf.jcu.cz	IN	A	160.217.161.1	3600s (1h)

Když se podíváme na výsledky, vidíme jména nameserverů pro celou univerzitu, nameservery jsou označeny zkratkou NS. Dále také jména poštovní serverů — jsou označeny zkratkou MX. Nyní tedy zkusíme dát dotaz pro celou jcu.cz.

Answer records

name	class	type	data		time to live
jcu.cz	IN	SOA	server:	virgo.jcu.cz	3600s (1h)
			email:	hostmaster@jcu.cz	
			serial:	1265002389	
			refresh:	10800	
			retry:	1800	
			expire:	1814400	
			minimum ttl:	7200	
jcu.cz	IN	NS	virgo.jcu.cz		3600s (1h)
jcu.cz	IN	NS	taurus.zf.jcu.cz		3600s (1h)
jcu.cz	IN	NS	eros.zcu.cz		3600s (1h)
jcu.cz	IN	MX	preference:	12833	3600s (1h)
			exchange:	cx.spamfree.cz	
jcu.cz	IN	MX	preference:	12849	3600s (1h)
			exchange:	dx.spamfree.cz	
jcu.cz	IN	MX	preference:	12801	3600s (1h)
			exchange:	ax.virusfree.cz	
jcu.cz	IN	MX	preference:	12817	3600s (1h)
			exchange:	bx.virusfree.cz	

Authority records

[none]

Additional records

name	class	type	data	time to live
virgo.jcu.cz	IN	A	160.217.1.10	3600s (1h)
taurus.zf.jcu.cz	IN	A	160.217.161.1	3600s (1h)

Na první pohled by se mohlo zdát, že máme z obou dotazů totožné výsledky, ale není tomu tak, neboť jsme navíc získali část s informacemi o serveru. Z těch se dá zjistit datum poslední aktualizace, ovšem za předpokladu, že je sériové číslo uvedené ve standardním formátu. V tomto případě tomu tak není, proto jednoduše informaci o poslední aktualizaci nezískáme a jedině dlouhodobé pozorování by nám mohlo napovědět něco o chování správců.

Další věc, kterou je třeba ověřit, je fungování rekurzivních dotazů na nameserverech. Po vyzkoušení rekurzivního dotazu zjistíme, že tyto dotazy jsou skutečně povolené a můžeme se tedy ptát nameserverů Jiho-

české univerzity na ostatní servery na internetu. Rekurzivní dotazy by měly sloužit pouze k interním účelům a pro ostatní by měly být zakázané. Je hned několik důvodů proč je mít zakázané:

- Může dojít k nadměrnému zatížení serveru rekurzivními dotazy.
- Útočník může skrýt svou identitu pomocí rekurzivních dotazů a získat informace o cíli a jeho identita bude schována za nameserver.
- Útočník jich může využít při DDoS útoku.

Do pasivního prohledávání lze ještě zařadit informace, které jsme schopni získat při použití vyhledávače, např. Goggle. Takové prohledávání není v práci zahrnuto.

5.1.2 Aktivní prohledávání

Aktivní způsob prohledávání může již být zjistitelný v logu zkoumaných strojů, tím pádem na sebe útočník při používání těchto nástrojů může upozornit.

Při penetračním testu bylo třeba zajistit prověření bezpečnosti všech počítačů na PF, k tomuto účelu v prvé řadě posloužil program Angry IP, který nám ukázal veškeré „živé“ stroje v C rozsahu IP adres[2], kterým PF disponuje. Ukážeme si výsledky:

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


Scanned 160.217.96.1 – 160.217.96.255
23.11.2009 13:25:12

IP Ping Hostname

160.217.96.1 33 ms romeo.pf.jcu.cz
```

```
160.217.96.2 26 ms home.pf.jcu.cz
160.217.96.3 22 ms dbs.pf.jcu.cz
160.217.96.5 23 ms turbol.pf.jcu.cz
160.217.96.6 26 ms ki1.pf.jcu.cz
160.217.96.7 27 ms amos.pf.jcu.cz
160.217.96.9 21 ms licsvr.pf.jcu.cz
160.217.96.12 26 ms jelinek.pf.jcu.cz
160.217.96.15 22 ms thecus.pf.jcu.cz
160.217.96.16 27 ms hp4p.pf.jcu.cz
160.217.96.17 36 ms hp300x.pf.jcu.cz
160.217.96.18 30 ms urban.pf.jcu.cz
160.217.96.22 27 ms polaris.pf.jcu.cz
160.217.96.25 26 ms alcor.pf.jcu.cz
160.217.96.26 23 ms vesela.pf.jcu.cz
160.217.96.27 21 ms harazimova.pf.jcu.cz
160.217.96.28 19 ms sue.pf.jcu.cz
160.217.96.29 23 ms raid.pf.jcu.cz
160.217.96.31 21 ms wifi3.pf.jcu.cz
160.217.96.36 21 ms dariusova.pf.jcu.cz
160.217.96.39 21 ms podatelna.pf.jcu.cz
160.217.96.41 19 ms havelkova.pf.jcu.cz
160.217.96.42 26 ms ir2018ki.pf.jcu.cz
160.217.96.46 38 ms vancura.pf.jcu.cz
160.217.96.47 29 ms vanicek.pf.jcu.cz
160.217.96.49 27 ms chladek.pf.jcu.cz
160.217.96.57 33 ms hasek.pf.jcu.cz
160.217.96.60 20 ms debian.pf.jcu.cz
160.217.96.61 20 ms svobodova.pf.jcu.cz
160.217.96.62 30 ms avs2000.pf.jcu.cz
160.217.96.68 19 ms tesar.pf.jcu.cz
160.217.96.70 21 ms kozelkova.pf.jcu.cz
160.217.96.71 21 ms matenova.pf.jcu.cz
160.217.96.72 24 ms icha.pf.jcu.cz
160.217.96.74 21 ms dhclient08.pf.jcu.cz
160.217.96.75 24 ms svec.pf.jcu.cz
160.217.96.76 26 ms array1.pf.jcu.cz
160.217.96.77 24 ms pc1613.pf.jcu.cz
160.217.96.80 27 ms pc1612.pf.jcu.cz
160.217.96.83 22 ms pc1614.pf.jcu.cz
160.217.96.84 28 ms pc1615.pf.jcu.cz
160.217.96.85 31 ms babkova.pf.jcu.cz
160.217.96.86 40 ms array2.pf.jcu.cz
```

```
160.217.96.87 39 ms j505.pf.jcu.cz
160.217.96.92 21 ms pokus.pf.jcu.cz
160.217.96.94 25 ms pc1616.pf.jcu.cz
160.217.96.96 22 ms NewHome.pf.jcu.cz
160.217.96.98 24 ms j203.pf.jcu.cz
160.217.96.110 21 ms pc1600.pf.jcu.cz
160.217.96.111 29 ms pc1601.pf.jcu.cz
160.217.96.112 21 ms pc1602.pf.jcu.cz
160.217.96.114 19 ms pc1603.pf.jcu.cz
160.217.96.115 22 ms pc1604.pf.jcu.cz
160.217.96.116 20 ms pc1605.pf.jcu.cz
160.217.96.118 33 ms pc1607.pf.jcu.cz
160.217.96.119 42 ms pc1608.pf.jcu.cz
160.217.96.120 44 ms pc1609.pf.jcu.cz
160.217.96.121 41 ms pc1610.pf.jcu.cz
160.217.96.123 34 ms pc1611.pf.jcu.cz
160.217.96.126 27 ms sauron.pf.jcu.cz
160.217.96.130 38 ms rudaprac.pf.jcu.cz
160.217.96.139 35 ms gollum.pf.jcu.cz
160.217.96.142 28 ms jiri-jelinek.pf.jcu.cz
160.217.96.145 23 ms mickova.pf.jcu.cz
160.217.96.146 22 ms ryplova.pf.jcu.cz
160.217.96.151 23 ms dektaj.pf.jcu.cz
160.217.96.152 21 ms deksek.pf.jcu.cz
160.217.96.153 48 ms brychtova.pf.jcu.cz
160.217.96.155 28 ms kiweb.pf.jcu.cz
160.217.96.161 21 ms beranek.pf.jcu.cz
160.217.96.176 27 ms laura.pf.jcu.cz
160.217.96.177 25 ms turbo.pf.jcu.cz
160.217.96.178 44 ms wvc.pf.jcu.cz
160.217.96.179 31 ms eamos.pf.jcu.cz
160.217.96.183 25 ms pexa.pf.jcu.cz
160.217.96.190 32 ms udrzba.pf.jcu.cz
160.217.96.192 39 ms sramhauserova.pf.jcu.cz
160.217.96.198 29 ms vojtova.pf.jcu.cz
160.217.96.199 33 ms bizhub282.pf.jcu.cz
160.217.96.212 23 ms pavlicek.pf.jcu.cz
160.217.96.213 25 ms hbinter.pf.jcu.cz
160.217.96.218 23 ms geogr2.pf.jcu.cz
160.217.96.220 25 ms pouzar.pf.jcu.cz
160.217.96.229 30 ms spata.pf.jcu.cz
160.217.96.232 33 ms objednavky.pf.jcu.cz
```

```
160.217.96.233 31 ms avs2.pf.jcu.cz
160.217.96.234 28 ms wifi5.pf.jcu.cz
160.217.96.238 23 ms cerny.pf.jcu.cz
160.217.96.241 25 ms netdrive.pf.jcu.cz
160.217.96.242 26 ms ir2018kbi.pf.jcu.cz
160.217.96.244 23 ms access.pf.jcu.cz
160.217.96.245 22 ms geo4.pf.jcu.cz
160.217.96.249 38 ms cekal.pf.jcu.cz
160.217.96.250 29 ms wifi2.pf.jcu.cz
160.217.96.254 30 ms net96-gw.pf.jcu.cz
```

Z výsledků vyplývá jedna zajímavost — každý počítač na PF má vlastní vnější IP adresu, jedná se tedy o velké množství počítačů připojených do sítě s vlastní IP adresou. Počítače jsou pojmenovány tak, že jejich uspořádání je zřejmé — počítače pojmenované příjmením jsou pracovní stanice zaměstnanců, počítače s označením pc a číslem jsou studentské stanice v počítačových učebnách. Ještě jsou zde „unikátní" stroje, kterým je třeba věnovat zvýšenou pozornost (romeo, home, raid, kiweb, …).

5.1.3 Závěr k testování celého rozsahu adres

Je zřejmé, že „živých" strojů je na PF velmi mnoho, proto bylo třeba před důkladným zkoumáním všech počítačů vytvořit nějaká omezení, kterými stroji ze zabývat povrchně a naopak, které otestovat co nejdůkladněji. Po konzultaci tohoto problému s Ing. Břehovským (bylo zvoleno nejrozumnější řešení) — celý rozsah IP byl otestován automatickým nástrojem Nessus a počítače, které vykázaly problémy středního nebo vysokého stupně, byly podrobeny důkladnému zkoumání. Takových počítačů bylo na fakultě celkem 9, jimi se budeme podrobně zabývat ve zbývající části práce.

Jak je zřejmé, práce se rozdělí do 9 větví, které budou představovat jednotlivé počítače s bezpečnostními nedostatky. Na jednom z nich (romeo.pf.jcu.cz — 160.217.96.1) si ukážeme další testy podrobně, u ostatních jen velmi stručně. Opatření jsou učiněna z důvodů omezení rozsahu práce. Jednotlivé počítače jsou řazeny podle IP adresy.

5.2 romeo.pf.jcu.cz — 160.217.96.1

5.2.1 netcat

Jako první z dalších testů bude uveden test programem netcat, též známým pod svou přezdívkou „Swiss army knife".

```
C:\Tools\netcat>nc www.pf.jcu.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>
<p>Your browser sent a request that this server could not understand.<br />
</p>
<hr>
<address>Apache/2.2.9 (Debian) PHP/5.2.6-1+lenny3 with Suhosin-Patch
mod_ssl/2.2
.9 OpenSSL/0.9.8g Server at romeo.pf.jcu.cz Port 80</address>
</body></html>
```

Podstatnou informaci tvoří až závěr celého výsledku, kde se dozvídáme, jaké služby a v jakých verzích na stroji běží.

5.2.2 nmap (Zenmap)

Následuje program pro scan portů, využit byl asi nejznámější a nejpoužívanější z nich a to nmap s GUI[7] pro Windows — Zenmap.

```
C:\Tools\nmap>nmap — T Aggressive — A — v — p 1-65535 160.217.96.1

Starting Nmap 5.00 ( http://nmap.org ) at 2009-11-24 19:52 St°ednÝ Evropa
(bý×nř Řas)
NSE: Loaded 30 scripts for scanning.
Initiating Ping Scan at 19:52
Scanning 160.217.96.1 [4 ports]
```

```
Completed Ping Scan at 19:52, 0.13s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 19:52
Completed Parallel DNS resolution of 1 host. at 19:52, 0.03s elapsed
Initiating SYN Stealth Scan at 19:52
Scanning romeo.pf.jcu.cz (160.217.96.1) [65535 ports]
Discovered open port 53/tcp on 160.217.96.1
Discovered open port 21/tcp on 160.217.96.1
Discovered open port 993/tcp on 160.217.96.1
Discovered open port 995/tcp on 160.217.96.1
Discovered open port 110/tcp on 160.217.96.1
Discovered open port 443/tcp on 160.217.96.1
Discovered open port 80/tcp on 160.217.96.1
Discovered open port 22/tcp on 160.217.96.1
Discovered open port 143/tcp on 160.217.96.1
SYN Stealth Scan Timing: About 2.78% done; ETC: 20:11 (0:18:06 remaining)
SYN Stealth Scan Timing: About 6.96% done; ETC: 20:11 (0:16:55 remaining)
SYN Stealth Scan Timing: About 10.27% done; ETC: 20:10 (0:15:27 remaining)
SYN Stealth Scan Timing: About 14.57% done; ETC: 20:09 (0:14:28 remaining)
SYN Stealth Scan Timing: About 18.28% done; ETC: 20:09 (0:13:29 remaining)
SYN Stealth Scan Timing: About 22.97% done; ETC: 20:09 (0:12:38 remaining)
SYN Stealth Scan Timing: About 27.70% done; ETC: 20:09 (0:11:47 remaining)
SYN Stealth Scan Timing: About 32.29% done; ETC: 20:08 (0:10:56 remaining)
SYN Stealth Scan Timing: About 37.59% done; ETC: 20:08 (0:10:04 remaining)
Discovered open port 465/tcp on 160.217.96.1
SYN Stealth Scan Timing: About 43.59% done; ETC: 20:09 (0:09:13 remaining)
SYN Stealth Scan Timing: About 48.14% done; ETC: 20:08 (0:08:22 remaining)
SYN Stealth Scan Timing: About 53.64% done; ETC: 20:09 (0:07:32 remaining)
SYN Stealth Scan Timing: About 58.56% done; ETC: 20:08 (0:06:40 remaining)
SYN Stealth Scan Timing: About 63.86% done; ETC: 20:08 (0:05:50 remaining)
SYN Stealth Scan Timing: About 69.15% done; ETC: 20:08 (0:04:59 remaining)
SYN Stealth Scan Timing: About 74.21% done; ETC: 20:08 (0:04:07 remaining)
SYN Stealth Scan Timing: About 79.43% done; ETC: 20:08 (0:03:17 remaining)
SYN Stealth Scan Timing: About 84.61% done; ETC: 20:08 (0:02:28 remaining)
SYN Stealth Scan Timing: About 89.75% done; ETC: 20:08 (0:01:39 remaining)
SYN Stealth Scan Timing: About 94.96% done; ETC: 20:08 (0:00:49 remaining)
Completed SYN Stealth Scan at 20:08, 964.39s elapsed (65535 total ports)
Initiating Service scan at 20:08
Scanning 10 services on romeo.pf.jcu.cz (160.217.96.1)
Completed Service scan at 20:09, 37.83s elapsed (10 services on 1 host)
Initiating OS detection (try #1) against romeo.pf.jcu.cz (160.217.96.1)
Retrying OS detection (try #2) against romeo.pf.jcu.cz (160.217.96.1)
160.217.96.1: guessing hop distance at 7
Initiating Traceroute at 20:09
Completed Traceroute at 20:09, 10.05s elapsed
Initiating Parallel DNS resolution of 7 hosts. at 20:09
Completed Parallel DNS resolution of 7 hosts. at 20:09, 0.05s elapsed
NSE: Script scanning 160.217.96.1.
NSE: Starting runlevel 1 scan
Initiating NSE at 20:09
Completed NSE at 20:09, 4.30s elapsed
NSE: Script Scanning completed.
Host romeo.pf.jcu.cz (160.217.96.1) is up (0.026s latency).
```

```
Interesting ports on romeo.pf.jcu.cz (160.217.96.1):
Not shown: 65525 filtered ports
PORT STATE SERVICE VERSION
21/tcp open ftp ProFTPD
|_ ftp-bounce: server forbids bouncing to low ports <1025
|_ ftp-anon: Anonymous FTP login allowed
22/tcp open ssh OpenSSH 5.1p1 Debian 5 (protocol 2.0)
| ssh-hostkey: 1024 af:0c:a9:7d:6a:a4:21:59:6d:d1:e7:31:74:4d:19:fc (DSA)
|_ 1024 0a:95:0c:cd:be:14:96:cc:35:65:8c:32:80:64:fe:14 (RSA)
53/tcp open domain ISC BIND 4.X
80/tcp open http Apache httpd 2.2.9 ((Debian) PHP/5.2.6-1+lenny3 with
Suho
sin-Patch mod_ssl/2.2.9 OpenSSL/0.9.8g)
| html-title: Pedagogick\xE1 fakulta Jiho\xE8esk\xE9 univerzity
|_ Requested resource was http://www.pf.jcu.cz/
110/tcp open pop3 Courier pop3d
|_ pop3-capabilities: USER STLS IMPLEMENTATION(Courier Mail Server) UIDL
PIPELIN
ING LOGIN-DELAY(10) TOP
143/tcp open imap Courier Imapd (released 2008)
|_ imap-capabilities: THREAD=ORDEREDSUBJECT QUOTA STARTTLS
THREAD=REFERENCES UID
PLUS ACL2=UNION SORT ACL IMAP4rev1 IDLE NAMESPACE CHILDREN
443/tcp open ssl/http Apache httpd 2.2.9 ((Debian) PHP/5.2.6-1+lenny3
with Suho
sin-Patch mod_ssl/2.2.9 OpenSSL/0.9.8g)
| html-title: 302 Found
|_ Did not follow redirect to https://www.pf.jcu.cz
465/tcp open ssl/smtp Postfix smtpd
|_ smtp-commands: EHLO romeo.pf.jcu.cz, PIPELINING, SIZE 10485760, ETRN,
AUTH LO
GIN PLAIN, AUTH=LOGIN PLAIN, ENHANCEDSTATUSCODES, 8BITMIME, DSN
993/tcp open ssl/imap Courier Imapd (released 2008)
|_ sslv2: server still supports SSLv2
|_ imap-capabilities: THREAD=ORDEREDSUBJECT QUOTA AUTH=PLAIN
THREAD=REFERENCES U
IDPLUS ACL2=UNION SORT ACL IMAP4rev1 IDLE NAMESPACE CHILDREN
995/tcp open ssl/pop3 Courier pop3d
|_ pop3-capabilities: USER STLS IMPLEMENTATION(Courier Mail Server) UIDL
PIPELIN
ING LOGIN-DELAY(10) TOP
|_ sslv2: server still supports SSLv2
Warning: OSScan results may be unreliable because we could not find at
least 1 o
pen and 1 closed port
Device type: general purpose|WAP|printer
Running (JUST GUESSING) : Linux 2.6.X|2.4.X (93%), Gemtek embedded (91%),
Siemen
s embedded (91%), Linksys Linux 2.4.X (90%), Aastra embedded (87%),
Linksys embe
dded (85%), Xerox embedded (85%)
Aggressive OS guesses: Linux 2.6.27 (93%), Linux 2.6.15 – 2.6.26 (92%),
```

```
Linux 2.
6.27 (Ubuntu 8.10) (92%), Linux 2.6.18 (92%), Linux 2.6.18 – 2.6.27
(91%), Linux
 2.6.21 (91%), Linux 2.6.26 (91%), Gemtek P360 WAP or Siemens Gigaset
SE515dsl w
ireless broadband router (91%), Linux 2.6.16 – 2.6.20 (90%), Linux
2.6.18-8.el5
(Red Hat Enterprise Linux 5) (90%)
No exact OS matches for host (test conditions non-ideal).
Uptime guess: 22.432 days (since Mon Nov 02 09:47:10 2009)
Network Distance: 7 hops
TCP Sequence Prediction: Difficulty=188 (Good luck!)
IP ID Sequence Generation: All zeros
Service Info: OS: Linux

TRACEROUTE (using port 53/tcp)
HOP RTT ADDRESS
1 0.00 RT-G32 (192.168.1.1)
2 0.00 10.5.157.89
3 0.00 pvt.starnet.cz (92.62.224.30)
4 16.00 ge0-1-s140.bb1.pop1.cb.sloane.cz (213.192.26.1)
5 16.00 v104.bb1.pop1.sve.sloane.cz (62.240.161.193)
6 …
7 31.00 r50ol-pos9-0-stm16.cesnet.cz (195.113.156.142)
8 31.00 romeo.pf.jcu.cz (160.217.96.1)

Read data files from: C:\Tools\nmap
OS and Service detection performed. Please report any incorrect results
at http:
//nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1026.02 seconds
 Raw packets sent: 197346 (8.686MB) | Rcvd: 1571 (70.264KB)
```

Jak si můžeme všimnout, bylo zvoleno co možná nejvíce funkcí pro jedno spuštění, proto je výsledek poměrně nepřehledný. Pokusíme si vysvětlit, co jaká část znamená a co je nejpodstatnější. Ze zadání příkazu `C:\Tools\nmap>nmap – T Aggressive – A – v – p 1-65535 160.217.96.1` je patrné, že byla zvolena agresivní cesta testování portů — je mnohem větší riziko, že správci pohyb na síti zaznamenají. V našem případě to nebylo na škodu, protože správci o testování věděli a nebyl důvod se skrývat. Další parametry jsou pro zapnutí detekce operačního systému, tracerouting a specifikace, které porty se mají otestovat, v našem případě 1—65535. Z výsledků je čitelné, jaké TCP porty jsou na adrese otevřené — 21, 22, 53, 80, 110, 143, 443, 465, 993 a 995 — a pro jaké služby slouží.

Pokud se dostaneme na úplný konec výsledků, můžeme vidět traceroute, tedy cestu, kudy jdou pakety od auditora až po romeo.pf.jcu.cz.

```
21/tcp open ftp ProFTPD
|_ ftp-bounce: server forbids bouncing to low ports <1025
|_ ftp-anon: Anonymous FTP login allowed
```

Tato pasáž je vůbec asi tím nejdůležitějším, co se dá z výsledků zjistit. Vidíme, že je povolen ftp-bounce scan na porty přes 1024 a že je povoleno anonymní FTP[6]. Těmito skutečnostmi se budeme zabývat v kapitole 5.2.4 o zneužití chyb na romeo.pf.jcu.

5.2.3 Nessus

Jako poslední si budeme prezentovat výsledky z automatického nástroje Nessus. Program je velmi používaným nástrojem i u profesionálů, má velkou podporu, časté aktualizace a je asi nejlepším nástrojem, který je dnes na internetu volně dostupný (volně dostupná verze má jistá omezení — např. v maximálním počtu IP adres, které je možné najednou otestovat). Testů bylo samozřejmě provedeno ještě více a všechny na této IP adrese jsou dostupné na přiloženém DVD ve vlastní složce.

Pro úplnost je ještě třeba dodat, že zde budou uvedeny jen části zprávy z programu Nessus, konkrétně to budou ta rizika, která dosahují minimálně střední úrovně. [11]

Anonymous FTP Enabled

Synopsis :

Anonymous logins are allowed on the remote FTP server.

Description :

This FTP service allows anonymous logins. Any remote user may connect and authenticate without providing a password or unique credentials. This allows a user to access any files made available on the FTP server.

Solution :

Disable anonymous FTP if it is not required. Routinely check the FTP server to ensure sensitive content is not available.

Risk factor :

Medium / CVSS Base Score : 5.0
(CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N)

Plugin output :

The contents of the remote FTP root are :
drwxr-xr-x 3 ftp ftp 16 Jan 27 1999 mnt
dr-xr-sr-x 11 ftp ftp 100 Sep 29 2004 pub
-rw-r--r- — 1 ftp ftp 166 Mar 7 2000 welcome.msg

CVE : CVE-1999-0497
Other references : OSVDB:69

Nessus ID : 10079

FTP Privileged Port Bounce Scan

Synopsis :
The remote FTP server is vulnerable to a FTP server bounce attack.

Description :
It is possible to force the remote FTP server to connect to third parties using the PORT command.

The problem allows intruders to use your network resources to scan other hosts, making them think the attack comes from your network.

See also :
http://archives.neohapsis.com/archives/bugtraq/1995_3/0047.html
http://archives.neohapsis.com/archives/bugtraq/2002-10/0367.html
http://www.cert.org/advisories/CA-1997-27.html

Solution :
See the CERT advisory in the references for solutions and workarounds .

Risk factor :
High / CVSS Base Score : 7.5
(CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P)

Plugin output :
The following command, telling the server to connect to 169.254.74.43 on port 10794:

PORT 169,254,74,43,42,42

produced the following output:

200 PORT command successful

CVE : CVE-1999-0017
BID : 126
Other references : OSVDB:71

Nessus ID : 10081

Jak můžeme vidět, Nessus upozornil na 2 stejné věci jako nmap — na FTP-bounce scan (zde dokonce i na privilegované porty) a na anonymní FTP. Jednu věc ovšem Nessus přidává a to je podpora slabých SSL[16] šifer.

SSL Weak Cipher Suites Supported

Synopsis :
The remote service supports the use of weak SSL ciphers.

Description :
The remote host supports the use of SSL ciphers that offer either weak encryption or no encryption at all.

See also :
http://www.openssl.org/docs/apps/ciphers.html

Solution :
Reconfigure the affected application if possible to avoid use of weak ciphers.

Risk factor :
Medium / CVSS Base Score : 5.0
(CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N)

Plugin output :
Here is the list of weak SSL ciphers supported by the remote server :

```
Low Strength Ciphers (< 56-bit key)
SSLv3
EXP-EDH-RSA-DES-CBC-SHA Kx=DH(512) Au=RSA Enc=DES(40) Mac=SHA1 export
EXP-DES-CBC-SHA Kx=RSA(512) Au=RSA Enc=DES(40) Mac=SHA1 export
EXP-RC2-CBC-MD5 Kx=RSA(512) Au=RSA Enc=RC2(40) Mac=MD5 export
EXP-RC4-MD5 Kx=RSA(512) Au=RSA Enc=RC4(40) Mac=MD5 export
TLSv1
EXP-EDH-RSA-DES-CBC-SHA Kx=DH(512) Au=RSA Enc=DES(40) Mac=SHA1 export
EXP-DES-CBC-SHA Kx=RSA(512) Au=RSA Enc=DES(40) Mac=SHA1 export
EXP-RC2-CBC-MD5 Kx=RSA(512) Au=RSA Enc=RC2(40) Mac=MD5 export
EXP-RC4-MD5 Kx=RSA(512) Au=RSA Enc=RC4(40) Mac=MD5 export
```

The fields above are :

{OpenSSL ciphername}
Kx={key exchange}
Au={authentication}
Enc={symmetric encryption method}
Mac={message authentication code}
{export flag}

Nessus ID : 26928

Nyní se pustíme do závěrečného zhodnocení a pokusíme se zjištěné nedostatky využít tak, abychom získali něco, co bychom neměli.

5.2.4 Zneužití chyb — romeo

V této kapitole si ukážeme zda zjištěné nedostatky byly prokázány a co nám jejich využití umožňuje.

Pozn. Opatření, jak nedostatkům předejít zde nebude ukázáno, problematice bude věnována samostatná kapitola 6.

Anonymní FTP, SSL šifry

Anonymní FTP je skutečně povolené, ovšem nepodařilo se mi získat žádná data, která by neměla patřit do mých rukou či do rukou kohokoliv, kdo se pomocí FTP anonymně připojí. U SSL šifer jsem ovšem nebyl schopen prokázat jejich použití. Abych toho byl schopen musel bych být připojen na lokální síť PF, což mi správci nebylo umožněno.

FTP Bounce Scan

Při zjišťování fungování scanu byl opět využit program Nmap, který v sobě má intergrovaný příkaz pro otestovaní FTP Bounce Scanu.

```
C:\Tools\nmap>nmap — v — b anonymous:anon@160.217.96.1 160.217.96.15
Hint: if your bounce scan target hosts aren't reachable from here, remem-
ber to u
se — PN so we don't try and ping them prior to the scan

Starting Nmap 5.00 ( http://nmap.org ) at 2009-11-17 10:37 St°ednÝ Evropa
(bý×nř
 Řas)
Resolved FTP bounce attack proxy to 160.217.96.1 (160.217.96.1).
NSE: Loaded 0 scripts for scanning.
Initiating Ping Scan at 10:37
Scanning 160.217.96.15 [4 ports]
Completed Ping Scan at 10:37, 0.17s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 10:37
Completed Parallel DNS resolution of 1 host. at 10:37, 0.03s elapsed
Attempting connection to ftp://anonymous:anon@160.217.96.1:21
```

```
Connected:220 ::ffff:160.217.96.1 FTP server ready
Login credentials accepted by FTP server!
Initiating TCP FTP bounce scan against thecus.pf.jcu.cz (160.217.96.15)
at 10:37

Your FTP bounce server doesn't allow privileged ports, skipping them.
Your FTP bounce server doesn't allow privileged ports, skipping them.
Your FTP bounce server doesn't allow privileged ports, skipping them.
Your FTP bounce server doesn't allow privileged ports, skipping them.
recv problem from FTP bounce server: No such file or directory
recv problem from FTP bounce server: No such file or directory
recv problem from FTP bounce server: No such file or directory
recv problem from FTP bounce server: No such file or directory
recv problem from FTP bounce server: No such file or directory
recv problem from FTP bounce server: No such file or directory
recv problem from FTP bounce server: No such file or directory
recv problem from FTP bounce server: No such file or directory
recv problem from FTP bounce server: No such file or directory
recv problem from FTP bounce server: No such file or directory
recv problem from FTP bounce server: No such file or directory
Discovered open port 30000/tcp on 160.217.96.15
recv problem from FTP bounce server: No such file or directory
recv problem from FTP bounce server: No such file or directory
recv problem from FTP bounce server: No such file or directory
recv problem from FTP bounce server: No such file or directory
recv problem from FTP bounce server: No such file or directory
recv problem from FTP bounce server: No such file or directory
recv problem from FTP bounce server: No such file or directory
recv problem from FTP bounce server: No such file or directory
recv problem from FTP bounce server: No such file or directory
recv problem from FTP bounce server: No such file or directory
recv problem from FTP bounce server: No such file or directory
recv problem from FTP bounce server: No such file or directory
Discovered open port 10617/tcp on 160.217.96.15
recv problem from FTP bounce server: No such file or directory
recv problem from FTP bounce server: No such file or directory
recv problem from FTP bounce server: No such file or directory
recv problem from FTP bounce server: No such file or directory
recv problem from FTP bounce server: No such file or directory
recv problem from FTP bounce server: No such file or directory
recv problem from FTP bounce server: No such file or directory
recv problem from FTP bounce server: No such file or directory
recv problem from FTP bounce server: No such file or directory
recv problem from FTP bounce server: No such file or directory
recv problem from FTP bounce server: No such file or directory
recv problem from FTP bounce server: No such file or directory
Discovered open port 10566/tcp on 160.217.96.15
Discovered open port 5550/tcp on 160.217.96.15
recv problem from FTP bounce server: No such file or directory
recv in recvtime: StßvajÝcÝ p°ipojenÝ bylo vynucený ukonŕeno vzdßlenřm
hostitelem.
 (10054)
```

```
send in bounce_scan: StßvajÝcÝ p°ipojenÝ bylo vynucený ukonŕeno vzdßlenřm
hostitelem.
 (10054)
Our FTP proxy server hung up on us! retrying
Attempting connection to ftp://anonymous:anon@160.217.96.1:21
Connected:220 ::ffff:160.217.96.1 FTP server ready
Login credentials accepted by FTP server!
recv problem from FTP bounce server: No such file or directory
recv problem from FTP bounce server: No such file or directory
recv problem from FTP bounce server: No such file or directory
recv problem from FTP bounce server: No such file or directory
recv problem from FTP bounce server: No such file or directory
recv problem from FTP bounce server: No such file or directory
recv problem from FTP bounce server: No such file or directory
recv problem from FTP bounce server: No such file or directory
recv problem from FTP bounce server: No such file or directory
recv problem from FTP bounce server: No such file or directory
recv problem from FTP bounce server: No such file or directory
Discovered open port 1300/tcp on 160.217.96.15
recv problem from FTP bounce server: No such file or directory
recv problem from FTP bounce server: No such file or directory
recv problem from FTP bounce server: No such file or directory
recv problem from FTP bounce server: No such file or directory
recv problem from FTP bounce server: No such file or directory
recv problem from FTP bounce server: No such file or directory
recv problem from FTP bounce server: No such file or directory
recv problem from FTP bounce server: No such file or directory
recv problem from FTP bounce server: No such file or directory
recv problem from FTP bounce server: No such file or directory
recv problem from FTP bounce server: No such file or directory
recv problem from FTP bounce server: No such file or directory
Discovered open port 9593/tcp on 160.217.96.15
recv problem from FTP bounce server: No such file or directory
recv problem from FTP bounce server: No such file or directory
recv problem from FTP bounce server: No such file or directory
recv problem from FTP bounce server: No such file or directory
recv problem from FTP bounce server: No such file or directory
recv problem from FTP bounce server: No such file or directory
recv problem from FTP bounce server: No such file or directory
recv problem from FTP bounce server: No such file or directory
recv problem from FTP bounce server: No such file or directory
recv problem from FTP bounce server: No such file or directory
recv problem from FTP bounce server: No such file or directory
recv problem from FTP bounce server: No such file or directory
Discovered open port 1154/tcp on 160.217.96.15
Discovered open port 366/tcp on 160.217.96.15
recv problem from FTP bounce server: No such file or directory
recv in recvtime: StßvajÝcÝ p°ipojenÝ bylo vynucený ukonŕeno vzdßlenřm
hostitelem.
 (10054)
send in bounce_scan: StßvajÝcÝ p°ipojenÝ bylo vynucený ukonŕeno vzdßlenřm
hostitelem.
```

```
 (10054)
Our FTP proxy server hung up on us! retrying
Attempting connection to ftp://anonymous:anon@160.217.96.1:21
Connected:220 ::ffff:160.217.96.1 FTP server ready
Login credentials accepted by FTP server!
recv problem from FTP bounce server: No such file or directory
recv problem from FTP bounce server: No such file or directory
recv problem from FTP bounce server: No such file or directory
recv problem from FTP bounce server: No such file or directory
recv problem from FTP bounce server: No such file or directory
recv problem from FTP bounce server: No such file or directory
recv problem from FTP bounce server: No such file or directory
recv problem from FTP bounce server: No such file or directory
recv problem from FTP bounce server: No such file or directory
recv problem from FTP bounce server: No such file or directory
recv problem from FTP bounce server: No such file or directory
Discovered open port 3404/tcp on 160.217.96.15
Discovered open port 20222/tcp on 160.217.96.15
recv problem from FTP bounce server: No such file or directory
recv problem from FTP bounce server: No such file or directory
recv problem from FTP bounce server: No such file or directory
recv problem from FTP bounce server: No such file or directory
recv problem from FTP bounce server: No such file or directory
recv problem from FTP bounce server: No such file or directory
recv problem from FTP bounce server: No such file or directory
recv problem from FTP bounce server: No such file or directory
recv problem from FTP bounce server: No such file or directory
recv problem from FTP bounce server: No such file or directory
recv problem from FTP bounce server: No such file or directory
Discovered open port 4449/tcp on 160.217.96.15
recv problem from FTP bounce server: No such file or directory
recv problem from FTP bounce server: No such file or directory
recv problem from FTP bounce server: No such file or directory
recv problem from FTP bounce server: No such file or directory
recv problem from FTP bounce server: No such file or directory
recv problem from FTP bounce server: No such file or directory
recv problem from FTP bounce server: No such file or directory
recv problem from FTP bounce server: No such file or directory
recv problem from FTP bounce server: No such file or directory
recv problem from FTP bounce server: No such file or directory
recv problem from FTP bounce server: No such file or directory
Discovered open port 16018/tcp on 160.217.96.15
recv problem from FTP bounce server: No such file or directory
recv in recvtime: StßvajÝcÝ p°ipojenÝ bylo vynucený ukonŘeno vzdßlenřm
hostitelem.
(10054)
send in bounce_scan: StßvajÝcÝ p°ipojenÝ bylo vynucený ukonŘeno vzdßlenřm
hostitelem.
 (10054)
Our socket descriptor is dead and we are out of retries. Giving up.
```

```
Host thecus.pf.jcu.cz (160.217.96.15) is up (0.031s latency).
Interesting ports on thecus.pf.jcu.cz (160.217.96.15):
PORT STATE SERVICE
366/tcp open odmr
1062/tcp closed veracity
1154/tcp open unknown
1300/tcp open unknown
3371/tcp closed unknown
3404/tcp open unknown
4449/tcp open unknown
5050/tcp filtered mmcc
5550/tcp open sdadmind
6156/tcp filtered unknown
6839/tcp closed unknown
7778/tcp closed unknown
8080/tcp filtered http-proxy
8651/tcp closed unknown
9593/tcp open unknown
10566/tcp open unknown
10617/tcp open unknown
16018/tcp open unknown
20222/tcp open unknown
30000/tcp open unknown
52848/tcp closed unknown

Read data files from: C:\Tools\nmap
Nmap done: 1 IP address (1 host up) scanned in 1801.58 seconds
 Raw packets sent: 4 (152B) | Rcvd: 1 (28B)
```

Scan byl veden proti IP adrese 160.217.96.15 — thecus.pf.jcu.cz. Pokud se zadíváme důkladně na výsledky a především na poslední část, můžeme přehledně zjistit, které porty jsou otevřené. Zde je třeba zdůraznit, že by se určitě dalo portů najít více, ale pro demonstraci nebyl volen vyšší počet opakování, který by byl zapotřebí k zjištění dalších portů. Co je ovšem nejpodstatnější, že Nmap byl schopen odhalit otevřené porty i s číslem nižším než 1024, o kterých tvrdil, že jejich scanování je zakázáné (viz kapitola 5.2.2). Scan poskytne útočníkovi možnosti aktivního scanování sítě s tím, že u správců zkoumané sítě bude jako odesílatel požadavků uvedena IP 160.217.96.1, tedy romeo.pf.jcu.cz. Z toho vyplývá, že se za server může schovat jakýkoli útočník z celého světa a scanovat přes něj celý internet. Při takové činnosti by jednak zatěžoval server, ale co je horší — podezřelým by byla fakulta a „schováním identity“ by bránila vystopování a dopadení útočníka.

5.3. home.pf.jcu.cz — 160.217.96.2

Nyní si ve zkratce ukážeme, jaké problémy můžeme najít na dalším stroji na fakultě.

Otevřené porty: 21, 22, 23, 80, 443, 2401, 3306, 6666, 8180

Zjištěné nedostatky (Nessus): Detekce SSL ve verzi 2, použití slabých SSL šifer a povolenou metodu HTTP[8] Trace/Track v debuggeru.

Zneužití chyb: Oveření použití verze protokolu a slabých šifer jsem bohužel nebyl schopen — nutnost připojení na lokální síť PF. HTTP Trace/Track je povolen, ale jeho zranitelnosti při využití Cross-Site-Tracing jsem nedokázal ověřit, neboť vyžaduje pokročilé programování scriptů. Dostupné scripty nebylo možné již spuštět, protože byly programovány pro starší verze prohlížečů a z nějakého důvodu s novějšími již nekomunikují.

5.4 turbol.pf.jcu.cz — 160.217.96.5

Otevřené porty: 21, 22, 53, 80, 110, 143, 443, 465, 993, 995

Zjištěné nedostatky (Nessus): Povolená metoda HTTP Trace/Track v debuggeru a prošlé certifikáty SSL.

Zneužití chyb: Vypršelou platnost certifikátu SSL jsem nebyl schopen ověřit, ale bylo by vhodné aby tuto skutečnost správce zkontroloval. HTTP Trace/Track je vysvětlen výše.

5.5 thecus.pf.jcu.cz — 160.217.96.15

Otevřené porty: 21, 443, 631, 1194, 2000, 3260

Filtrované porty: 25, 135, 136, 137, 138, 139, 445

Zjištěné nedostatky (Nessus): Detekce SSL ve verzi 2, použití slabých SSL šifer, povolení anonymního FTP (port 2000) a XAMPP[21] výchozí FTP účet.

Zneužití chyb: SSL protokol a šifry jsou vysvětleny výše. Anonymní FTP a výchozí XAMPP účet je skutečně povolen, ale po připojení na server jsem viděl pouze kořenové adresáře a žádný z nich jsem nebyl schopen otevřít. Práva jsou pro anonymní uživatele tedy nastavena správně.

5.6 kiweb.pf.jcu.cz — 160.217.96.155

Otevřené porty: 80, 82

Zjištěné nedostatky (Nessus): Povolená metoda HTTP Trace/Track v debuggeru.

Zneužití chyb: Je již popsáno výše.

5.7 turbo.pf.jcu.cz — 160.217.96.177

Otevřené porty: 22

Zjištěné nedostatky (Nessus): SSH[15] protocol version 1 session key retrieval — běžící SSH dovoluje navázání spojení i přes verzi 1.

Zneužití chyb: Bohužel jsem nemohl ověřit, zda SSH dovolí navázat spojení přes verzi 1, tudíž jsem ani nebyl schopen odhalit její nedostatečné zabezpečení. Pro ověření SSH bych musel být připojen na lokální síť PF, což mi nebylo umožněno.

5.8 wvc.pf.jcu.cz — 160.217.96.178

Otevřené porty: 22, 80, 111, 60044

Filtrované porty: 25, 135, 136, 137, 138, 139, 445

Zjištěné nedostatky (Nessus): Povolená metoda HTTP Trace/Track v debuggeru.

Zneužití chyb: Je již popsáno výše.

5.9 eamos.pf.jcu.cz — 160.217.96.179

Otevřené porty: 22, 80

Zjištěné nedostatky (Nessus): Povolená metoda HTTP Trace/Track v debuggeru.

Zneužití chyb: Je již popsáno výše.

5.10 netdrive.pf.jcu.cz — 160.217.96.241

Otevřené porty: 21, 22, 80, 111, 515, 702, 1024, 2049

Filtrované porty: 25, 135, 136, 137, 138, 139, 445

Zjištěné nedostatky (Nessus): Nedostatky při konfiguraci NFS[11] share. Obsah share je čitelný a je možné ho vzdáleně připojit, neboť k tomu nejsou nutná administrátorská práva — jedná se o připojení na portu vyšším než 1024, v tomto případě na portu 2049. Dále je přítomen „Guest“ učet pro připojení k FTP na portu 21.

Zneužití chyb: NFS jsem ani nezkoumal, neboť stejný obsah je sdílen přes „Guest“ účet na FTP, proto je i nepodstatné, zda NFS je chybně nakonfigurováno, protože zajisté se dostaneme k datům přes FTP. Po připojení na FTP jsem se dostal prakticky k celému obsahu. V některých složkách se nachází velice zajímavé materiály, které by dle mého názoru neměly patřit do rukou každému „Guestovi“, který se na FTP připojí. Jedná se o licencovaný software (Avast, MS Office, MS Windows), učební materiály několika vyučujících fakulty, zálohy z eamosu a z celé DM1, zálohy některých vyučujících, webmasterů. Objevuje se i hudba, filmy a nějaké torrenty. Po důkladném prozkoumání všemožných souborů jsem se byl schopen dostat asi celkem k 3600 emailům ze 7 účtů od 3 různých jedinců. Většina emailů pochází sice z let starších (2004), ale jeden emailový učet je díky způsobu zazálohovaní (záložní soubory z Mozzila Thunderbird) prakticky plně funkční a je schopen přijímat zcela aktuální emaily a dovoluje útočníkovi zacházet s nimi dle uvážení. Jediné co nelze, je emaily

odesílat. Další materiály, které jsem byl schopen získat byl funkční IM (protokol ICQ) účet, na který je možné se připojit, získat kompletní historii rozhovorů a potenciálně citlivých informací. Dalším problémem je sdílení záloh z eamosu a DM1, tyto zálohy jsou zaheslované archivy, v dnešní době výkonného hardware není vhodné ani zaheslované zálohy uchovávat takto volně přístupné. Navíc díky skutečnosti, že snad každý student má účet na eamosu, útočník velice rychle získá uživatelská jména všech studentů. A co je možná ještě zajímavější, „Guest" má ve většině případů práva i na zápis, takže je možné (i aktuální) zálohy velice jednoduše a rychle smazat. Nedokáži odhadnout, zda jsou tyto zálohy využívány v případě problému, ale rozhodně ne každý by je měl být schopen mazat z disku.

6. Shrnutí výsledků a doporučená opatření

Znovu se budeme zabývat zjištěnými nedostatky sítě, tentokrát ale s ohodnocením, jaké závažnosti chyba je. Nebudeme brát v úvahu závažnost, kterou ukládají jednotlivým problémům automatické programy, ale budeme se jim věnovat z toho pohledu, jakou chybu může běžný útočník jednoduše využít a kterou nikoliv. Součástí každého popisu chyby bude i doporučení pro správce, jak chybě předejít a jak ji napravit.

6.1 Windows NT FTP „Guest" účet — kritická

„Guest" účet se vyskytuje na IP adrese 160.217.96.241 — netdrive.pf.jcu.cz. Díky tomuto účtu se dostaneme ke skutečně citlivým datům, jak bylo popsáno výše. Takto nastavené FTP považuji jednoznačně za největší problém v celém zabezpečení PF JČU. Je neskutečně jednoduché se k informacím dostat, stačí jednoduchý a volně dostupný software — FileZilla a několik emailových klientů (Microsoft Outlook Express, Mozzila Thunderbird, The Bat) a jsme schopni získat přes 3000 emailů vyučujících a webmastera. Ještě jednou upozorním na licencovaný software, který je možné z adresy rovněž stáhnout, což by mělo být umožněno pouze zaměstnancům fakulty případně studentům, ale každopádně ne všem na celém světě.

Doporučená opatření: V podstatě jsou 2 možnosti, jak se s problémem vypořádat, jeden je definitivní — tím je zakázání „Guest" účtu. Zakázání účtu ovšem nemusí být možné z interních důvodů fungovanání serveru (s těmito podrobnostmi nejsem seznámen). Druhá možnost je nechat účet povolený a striktně kontrolovat, co bude mít „Guest" uživatel k dispozici pro čtení a zápis. S tím úzce souvisí i školení zaměstnanců, jak s daty na podobných místech zacházet, aby nemohl každý kopírovat a číst jejich zálohy, jak je tomu v současném stavu — nastavování práv pro jednotlivé skupiny uživatelů a podobné detaily sdílení dat.

6.2 FTP Bounce Scan — velmi vysoká

FTP bounce scan je funkční na adrese 160.217.96.1 — romeo.pf.jcu.cz. Nebezpečnost Bounce scanu jsem ohodnotil jako velmi vysokou, protože útočníkovi dovoluje víc než je zdrávo, ovšem nedosahuje na kritickou hodnotu, protože útočník nemůže získat žádné informace. Zároveň není FTP bounce scan na romeo.pf.jcz.cz ničím unikátní, na internetu se vyskytuje řada serverů, které stejné scany také dovolují. Každopádně nastavení není v žádném případě korektní a takto by nemělo fungovat.

Doporučená opatření: Jednoznačně tuto možnost zakázat. Pokud je využívána k nějaké nutné činnosti, tak by bylo na místě zvážit překonfigurování a nahrazení jiným způsobem, neboť FTP bounce scan, obzvlášť na portech nižších než 1024, by fungovat neměl. Navíc hrozí objevení nějakým robotem a zveřejnění serveru na seznam, následně vysoké vytížení a zneužívání serveru PF k ilegálním útokům.

6.3 DNS Rekurzivní dotazy — střední

DNS by neměl umožňovat rekurzivní dotazy z okolního světa. Stávající konfigurace by mohla potenciálně vést k zneužití při cache poisoningu, což by mohlo mít nemalé důsledky.

Doporučená opatření: Vypnutí rekurzivních dotazů je jednoduchý krok konfigurace všech DNS verzí od společnosti Microsoft a BIND od verze 4.0. Pokud je třeba mít rekurzivní dotazy pro regulérní chod sítě zapnuté, existují jistá alternativní řešení:

- Prvním je použití dvou DNS serverů, kdy jeden by fungoval pouze pro rekurzivní dotazy v interním prostředí a druhý by komunikoval s ostatním světem s vypnutými rekurzivními dotazy.
- Druhou možností je použití dvou nezávislých DNS služeb na jednom stroji.

6.4 SSL, SSH — střední

Jedná se především o starší verze SSL protokolu a použití slabých šifer. V jednom případě jde o neplatný certifikát. Útočník by mohl odposlechnout a prolomit zabezpečenou komunikaci, kdyby bylo využito starší verze/slabých šifer. U SSH se jedná o zpětnou kompatibilutu při navazování spojení s verzí 1, která není bezpečná.

Doporučená opatření: Doporučil bych správcům projít hlášení ohledně SSL, zkontrolovat jejich nastavení a zabezpečení na jednotlivých serverech a pokud jsou skutečně použity slabé šifry, bylo by adekvátní je nahradit. To stejné platí pro starší verze. U SSH je třeba zakázat kompatibilitu s verzí 1, neboť představuje zbytečné bezpečnostní riziko.

6.5 Aktivní Apache debug mód — nízká

Na Apache serveru je povolený debug mód, jedná se konkrétně o stroje home, turbol, kiweb, wvc a eamos. Aktivní debug mód dovoluje metody HTTP Trace/Track. Tyto metody slouží k debugování serverových konexí, ale dají se zneužít pro získání informací z HTTP hlaviček či cookies (Cross-site-tracing XST — většinou javaScript, který získává informace z cookies).

Doporučená opatření: Pokud není tato metoda nutná, bylo by rozumnější ji jako preventivní opatření zakázat.

6.6 Zastaralá verze PHP — neznámá

Problematika se týká hned několika serverů PF — romeo, home, turbol, wvc a eamos. Na serverech je pravděpodobně použita neauktuální verze PHP (konkrétně se jedná o verze 5.2.6, 5.2.4 nebo starší), tyto verze mají známé bezpečnostní chyby, jejich přítomnost však přes několik pokusů nebyla ověřena. S velkou pravděpodobností se jedná o neexistující chyby

ve službách, které ani nemusí běžet na PHP — to dokládám skutečností, že na existenci chyb upozornil jen jeden program. Další možností je, že jsou skutečně přítomny starší verze, ale jsou udržovány bezpečnostními záplatami, které program neověřoval (nedokázal ověřit).

Doporučená opatření: I přes nepodloženost bych doporučil správcům, aby prošli seznam zjištěných chyb z programu Shadow Security Scanner (přiloženo na DVD) a zkontrolovali bezpečnostní záplaty. Jako předběžné opatření bych doporučil (pokud je to možné) nainstalovat PHP v nejnovější dostupné verzi, která je bezpečnější, než verze předcházející.

6.7 Závěr z penetračního testování

Během penetračního testu na Pedagogické fakultě jsem narazil na několik závažných problémů — problémy nejsou přímo způsobeny nedostatky v zabezpečení, ale spíše chybným nastavením služeb (viz „Guest“ účet).

Bylo by vhodné, aby na tento popud správci systému zkontrolovali veškeré popsané i nepopsané nedostatky (PHP) a přijali patřičná opatření proti zjištěným skutečnostem.

Aby závěry z penetračního testování byly co nejpřesnější, bylo použito velké množství nástrojů, všechny jsou dostupné zdarma na internetu (několik z nich v omezené trial verzi) a jejich použité verze jsou přiloženy na DVD.

Závěr

V dnešní moderní době hraje stále větší roli zabezpečení poskytnutých informací. Ty jsou cennější díky neustálému růstu používání internetu k platbám, studiu a komunikaci.

Velkou roli v bezpečnosti hraje lidský faktor, a to jak ze strany sociotechnik, tak ze strany správců a kvality jejich odváděné práce. Správce systému by měl být neustále v pohotovosti, kontrolovat logové soubory a snažit se udržovat systém bezpečný častými aktualizacemi. Nedílnou součástí jeho práce by mělo být i sledování nejnovějších trendů v bezpečnosti a přizpůsobování se jim. Výše zmíněné faktory jsou velmi důležité a jsou základem bezpečného systému.

Dalším faktorem ochrany je bezpečnostní testování. Penetrační test, který byl proveden na PF JČU, by měl sloužit spíše jako podnět k profesionálním testům. Při testování byly odhaleny nedostatky v nastavení a zabezpečení sítě — to i při velmi malém rozsahu a hloubce testování. Test nebyl proveden důkladněji z několika důvodů. V prvé řadě správci auditorovi nedovolili potřebný prostor pro provedení testování z vnitřní LAN fakulty. Takové testování by bylo z hlediska bezpečnosti mnohem důležitější než jen testování z vnější sítě. Za druhé — test byl časově omezen, proto se v něm objevují nepřesnosti, a test není dotažen k dokonalosti co se zneužití některých chyb týče. Posledním důvodem byla nezkušenost auditora, který test vedl. I přes veškerá omezení dokázal test ukázat vypovídající výsledky o zabezpečení PF.

Výsledky v některých případech upozorňují na vysoká rizika nastavení v síti, což je vzhledem k charakteru informací, které se na falkultě nachází, na poměrně velkou. Proto bych zde v závěru rád apeloval na správce Pedagogické fakulty, ale nejen na ně, aby se zkusili zabývat výsledky mé práce a předešli zjištěným rizikům a pokud možno zařídili ještě další testování rozsáhlejšího a důkladnějšího charakteru.

Seznam použité literatury

[1] DOSTÁLEK, Rndr. Libor, et al. Velký průvodce protokoly TCP/IP : Bezpečnost. 2. aktualizované vydání. Praha : Computer Press, 2003. 571 s. ISBN 80-7226-849-X.

[2] HARRIS, Shon, et al. Manuál Hackera. Z anglicého originálu přeložil Tomáš Znamenáček. 1. vydání. Praha : Grada Publishing a. s., 2008. 399 s. ISBN 978-80-247-1346-5.

[3] SCAMBRAY, Joel; MCCLURE, Stuart; KURTZ, George. Hacking bez tajemství. Z anglického originálu přeložil Petr Břehovský, Josef Pojsl, Radek Čevela. 2. aktualizované vydání. Praha : Computer Press, 2002. 625 s. ISBN 80-7226-644-6.

[4] OSSTMM 3 LITE : Introduction and Sample to the Open Source Security Testing Methodology Manual [online]. New York, USA : ISECOM, 3. 8. 2008 [cit. 1. 10. 2009]. Dostupné z WWW: <http://www.isecom.org/mirror/OSSTMM_3.0_LITE.pdf>.

[5] Odposloucháváme data na přepínaném Ethernetu 1. Lupa.cz : Server o českém Internetu [online]. 13. 6. 2006 [cit. 7. 11. 2009]. Dostupný z WWW: <http://www.lupa.cz/clanky/odposlouchavame-data-na-prepinanem-ethernetu-1/>.

[6] Odposloucháváme data na přepínaném Ethernetu 2. Lupa.cz : Server o českém Internetu [online]. 20. 6. 2006 [cit. 8. 11. 2009]. Dostupný z WWW: <http://www.lupa.cz/clanky/odposlouchavame-data-na-prepinanem-ethernetu-2/>.

[7] Odposloucháváme data na přepínaném Ethernetu 3. Lupa.cz : Server o českém Internetu [online]. 27. 6. 2006 [cit. 9. 11. 2009]. Dostupný

z WWW: <http://www.lupa.cz/clanky/odposlouchavame-data-na-prepinanem-ethernetu-3/>.

[8] Odposloucháváme data na přepínaném Ethernetu 4. Lupa.cz : Server o českém Internetu [online]. 5. 7. 2006 [cit. 9. 11. 2009]. Dostupný z WWW: <http://www.lupa.cz/clanky/odposlouchavame-data-na-prepinanem-ethernetu-4/>.

[9] Odposloucháváme data na přepínaném Ethernetu 5. Lupa.cz : Server o českém Internetu [online]. 11. 7. 2006 [cit. 9. 11. 2009]. Dostupný z WWW: <http://www.lupa.cz/clanky/odposlouchavame-data-na-prepinanem-ethernetu-5/>.

[10] Sociální inženýrství — Web věnovaný problematice sociotechniky [online]. 2009 [cit. 10. 12. 2009]. Dostupné z WWW: <http://www.sociotechnika.ic.cz/>.

[11] Tenable Network Security [online]. 2002 [cit. 23. 11. 2009]. Dostupné z WWW: <http://nessus.org/nessus/>.

[12] Open Web Application Security Project [online]. 2006 [cit. 12. 1. 2010]. Dostupné z WWW: <http://www.owasp.org>.

[13] Connect [online]. 20. 7. 2007 [cit. 10. 12. 2009]. Nejznámější útoky v síti Ethernet. Dostupné z WWW: <http://connect.zive.cz/node/714>.

[14] Reboot.cz [online]. 29. 5. 2000 [cit. 12. 11. 2009]. Denial of Service Attack. Dostupné z WWW: <http://reboot.cz/howto/hacking/denial-of-service-attack/articles.html?id=18>.

[15] ISVS.CZ — Informační Systémy Veřejné Správy [online]. 2. 11. 2004 [cit. 12. 11. 2009]. ISVS.CZ — Informační Systémy Veřejné Správy —

Bezpečnost Informačních systémů — rizika(3. díl). Dostupné z WWW: <http://www.isvs.cz/bezpecnost/bezpecnost-informacnich-systemu-rizika-3-dil-.html>.

[16] Finanční noviny [online]. 29. 12. 2009 [cit. 8. 1. 2010]. Karsten Nohl odkryl detaily kódu, který chrání hovory v GSM. Dostupné z WWW: <http://www.financninoviny.cz/zpravodajstvi/telekomunikace/zpravy/karsten-nohl-odkryl-detaily-kodu-ktery-chrani-hovory-v-gsm/414239>.

[17] Fakulta informatiky Masarykovy univerzity [online]. 2003 [cit. 10. 12. 2009]. Sociotechnika (sociální inženýrství). Dostupné z WWW: <http://www.fi.muni.cz/usr/jkucera/pv109/2003p/xsimek3sociotechnika.htm>.

[18] Reboot.cz [online]. 23. 5. 2000 [cit. 12. 12. 2009]. Bezpečnost na internetu. Dostupné z WWW: <http://reboot.cz/howto/hacking/bezpecnost-na-internetu/articles.html?id=11>.

[19] Svět sítí [online]. 28. 10. 2007 [cit. 10. 11. 2009]. Penetrační testy v bezpečnostní analýze informačního systému. Dostupné z WWW: <http://www.svetsiti.cz/view.asp?rubrika=Technologie&clanekID=309>.

[20] Automatizace [online]. 2004 [cit. 10. 10. 2009]. Penetrační testy: aneb sám sobě hackerem. Dostupné z WWW: <http://www.automatizace.cz/article.php?a=206>.

[21] CERT [online]. 2009 [cit. 25. 9. 2009]. CERT Statistics. Dostupné z WWW: <http://www.cert.org/stats/>.

[22] MIKO, Karel Co přinese a nepřinese za užitečné informace penetrační test. Co přinese a nepřinese za užitečné informace penetrační test. Praha : DCIT, 2001 [cit. 9. 10. 2009]. Dostupné z WWW: <http://www.dcit.cz/files/bezpecnost/AFOI_2001_Miko.pdf>.

Rejstřík pojmů

1	Additional Records	Pole v DNS odpovědi, které slouží k urychlení fungování služby tím, že pošle přeložené další adresy, které souvisí s původním dotazem.
2	C rozsah IP adres	Rozsah IP adres, kde adresa má pevně dané první 3 části a poslední, čtvrtá část, slouží k identifikaci stanice. V tomto rozsahu je možné unikátně identifikovat 254 stanic.
3	COMSEC	Comunication Security — jeden z kanálů podle OSSTMM. Skládá se ze 2 sekcí — 1) Datové sítě; do kterých patří všechny sítě a komunikace, které probíhají přes pevný kabel. 2) Telekomunikace; sem patří všechny komunikace probíhající po telefonním kabelu.
4	Exploit	Program, případně sekvence příkazů, který je schopen zneužít programátorské chyby v software ku prospěchu útočníka.
5	Firewall	Software či hardware zařízení (případně oboje), které slouží k oddělení dvou sítí s odlišnou důvěryhodností. Nejčastěji jako oddělení vnitřní LAN od internetu.
6	FTP	File Transfer Protocol — slouží k přenosu souborů mezi počítači. Je to protokol z rodiny TCP/IP běžící na aplikační vrstvě.
7	GUI	Graphical User Interface — grafické uživatelské rozhraní; slouží k usnadnění a zpřehlednění práce s daným programem díky ovládání pomocí interaktivních grafických ovládacích prvků.

8	HTTP	Hypertext Transfer Protocol — slouží k výměně hypertextových dokumentů ve formátu HTML.
9	Hub	Rozbočovač — slouží k propojení více počítačů ve hvězdicové topologii, není schopen přidělovat síťové parametry. Odesílaná data jsou posílána všem počítačům v síti bez ohledu na adresáta.
10	HUMSEC	Human Security — jedna se sekcí PHYSSEC, konkrétně jeho druhá sekce. Testuje, kde jsou kanály fyzického (nikoliv elektronického) charakteru. Tato sekce zahrnuje prvky bezpečnosti, které vyžadují fyzickou námahu k tomu, aby jimi mohlo být manipulováno.
11	NFS	Network File System — protokol sloužící k vzdálenému přístupu k souborům přes počítačovou síť. Využívá se například pro vzdálené připojování síťových disků.
12	OSSTMM	Open Source Security Testing Methodology Manual — Manuál pro bezpečnostní testy vyvinutý společností ISECOM, za účelem stanovení jednotných pravidel všech bezpečnostních testů.
13	PHYSSEC	Physical Security — kanál podle OSSTMM skládající se ze dvou sekcí — 1) Lidská sekce; sekce zkoumající lidský faktor komunikace z pohledu fyzického i psychologického. 2) Fyzická sekce; testuje tam, kde jsou kanály fyzického (nikoliv elektronického) charakteru. Tato sekce zahrnuje prvky bezpečnosti, které vyžadují fyzickou námahu k tomu, aby jimi mohlo být manipulováno.

14 SPECSEC	Spectrum Security — kanál podle OSSTMM obsahující sekci Bezdrátové komunikace. Sekce se zabývá problematikou všech bezdrátových signálů v celém elektromagnetickém spektru.
15 SSH	Secure Shell — program a protokol sloužící k zabezpečení komunikace mezi dvěma počítači. Slouží k zprostředkování přístupu k příkazové řádce i přenosům souborů.
16 SSL	Secure Sockets Layer — vrstva, která poskytuje zabezpečenou komunikaci s šifrováním a autetizací. Využívá se při komunikaci pomocí HTTPS, což je zabezpečená varianta HTTP.
17 Switch	Sofistikovanější varianta hubu. Funguje ovšem odlišně a data na síti již nejsou rozesílána všem, ale switch je schopen kontrolovat adresáta a odesílat data pouze jemu. Další výhoda je, že je schopen přidělovat síťové parametry.
18 TCP	Transmission Control Protocol — základní protokol z rodiny TCP/IP, představuje transportní vrstvu. Tento protokol umožňuje navázat spojení pro přenos dat.
19 The Jargon File	Jedná se o souborné kompendium hackerského slangu. Vysvětluje spoustu pojmů, tradic, folkloru a humoru hackerské komunity.
20 UDP	User Datagram Protocol — další z rodiny TCP/IP protokolů. Je jednodušší než TCP, protože nedává záruku na datagramy a integritu dat. Nevyužívá k navázání spojení „three way handshake“.

21 XAMPP	Je to open source web server balíček. Zkratka je odvozena od částí, ze kterých se balíček skládá: X — multiplatformní, A — Apache HTTP Server, M — MySQL, P — PHP, P — Perl.

Použitý software

Angry IP Scanner	Scanner počítačů na rozsahu IPadres, funguje na principu hromadného ping
Cain & Abel	Slouží k obnově různých zapomenutých hesel pomocí odposlouchávání sítě
CesarFTP	FTP server
Crowbar	Nástroj pro odhalovaní hesel hrubou silou
Dig	Slouží k nalezení DNS záznamů
FileZilla	Pokročilý FTP klient
GFI Languard	Bezpečnostní scanner
Metasploit Framework	Framework sloužící k exploitování známých chyb v zabezpečení, pomocí integrovaných exploitů
Mozilla Thunderbird	Emailový klient
MS Outlook Express	Emailový klient (součást OS Windows)
Nessus	Bezpečnostní scanner
Netcat	Mocný nástroj využitelný pro mnoho činností pod protokoly TCP a UDP, má mnoho funkcí, je to základní hackerský nástroj
Nmap	Bezpečnostní scanner
Nstalker	Bezpečnostní scanner
N-Stealth	Bezpečnostní scanner
Paros	Proxy
Privoxy	Proxy
Putty	SSH a telnet klient

Scuba	Bezpečnostní scanner databází
Shadow Security Scanner	Bezpečnostní scanner
The Bat	Emailový klient
Vulnerability Scanner	Bezpečnostní scanner
Whois	Vyhledávač informací o doméně
Wikto	Bezpečnostní scanner
Wireshark	Program pro monitorování sítě[4]