České vysoké učení technické v Praze

Fakulta elektrotechnická

Penetrační testy sítě podle OSSTMM

Obsah

Úvod

Tato semestrální práce má za cíl shrnout výsledky penetračních testů, které jsem provedl na menší síti (cca 50 počítačů) na střední škole, kde jsem studoval. Dále bych chtěl shrnout bezpečností problémy, které jsem objevil a najít k nim doporučení, jak je odstranit.

Metodika

Pro svou práci jsem zvolil postup podle metodiky OSSTM (Open Source Security Testing Methodology Manual) verze 2.2.

OSSTMM

OSSTMM je metodika pro provádění bezpečnostních testů a měření. Testy jsou rozděleny do pěti sekcí:

- **Information security testing** (*jak organizace funguje, kolik dat musí spravovat, profily zaměstnanců*)
- **Process security testing** (*co všechno o sobě organizace navenek prozrazuje, sociální inženýrství*)
- **Internet technology security testing** (s*kenování sítě, hledání bezpečnostních slabin, pokusy o průnik a získání citlivých dat*)
- **Communications security testing** (*telefony, hlasové schránky, faxy*)
- **Wireless security testing** (*elekromagnetické vyzařování, Wi-fi, Bluetooth, bezdrátové periferie*)
- **Physical security testing** (*zabezpečení prostor, dveře, ploty, monitorovací zařízení, alarmy*)

Ve své práci jsem se zabýval pouze sekcí **Internet technology security**, která se dělí na moduly:

1. Network surveying (*struktura sítě, doménová jména, IP adresy serverů)*
2. Port scanning (*které porty jsou otevřené, nastavení firewallu)*
3. Service identification (*identifikace běžících služeb)*
4. System Identification (*identifikace operačního systému*)
5. Vulnerability research (*nalezení potenciálních zranitelností podle běžících služeb a OS)*
6. Internet application testing (*nalezení chyb v aplikacích vytvořených danou organizací)*
7. Router testing (*jaké pakety propouští router do/z vnitřní sítě, co je zakázáno/povoleno)*
8. Trusted system testing (*nalezení systémů, které jsou závislé na dalších systémech)*
9. Firewall testing (*otestování ACL, podobné jako sekce Router testing)*
10. Intrusion Detection System Testing (*druhy paketů, které nejsou pomocí IDS testovány)*
11. Containment Measures Testing (*bezpečnost před viry a trojskými koni)*
12. Password Cracking (*ověření síly hesel pomocí automatických nástrojů)*
13. Denial of Service Testing (*systémy, které jsou zranitelné DoS)*
14. Security Policy Review (*ověření bezpečnostní politiky vůči aktuálnímu stavu*)

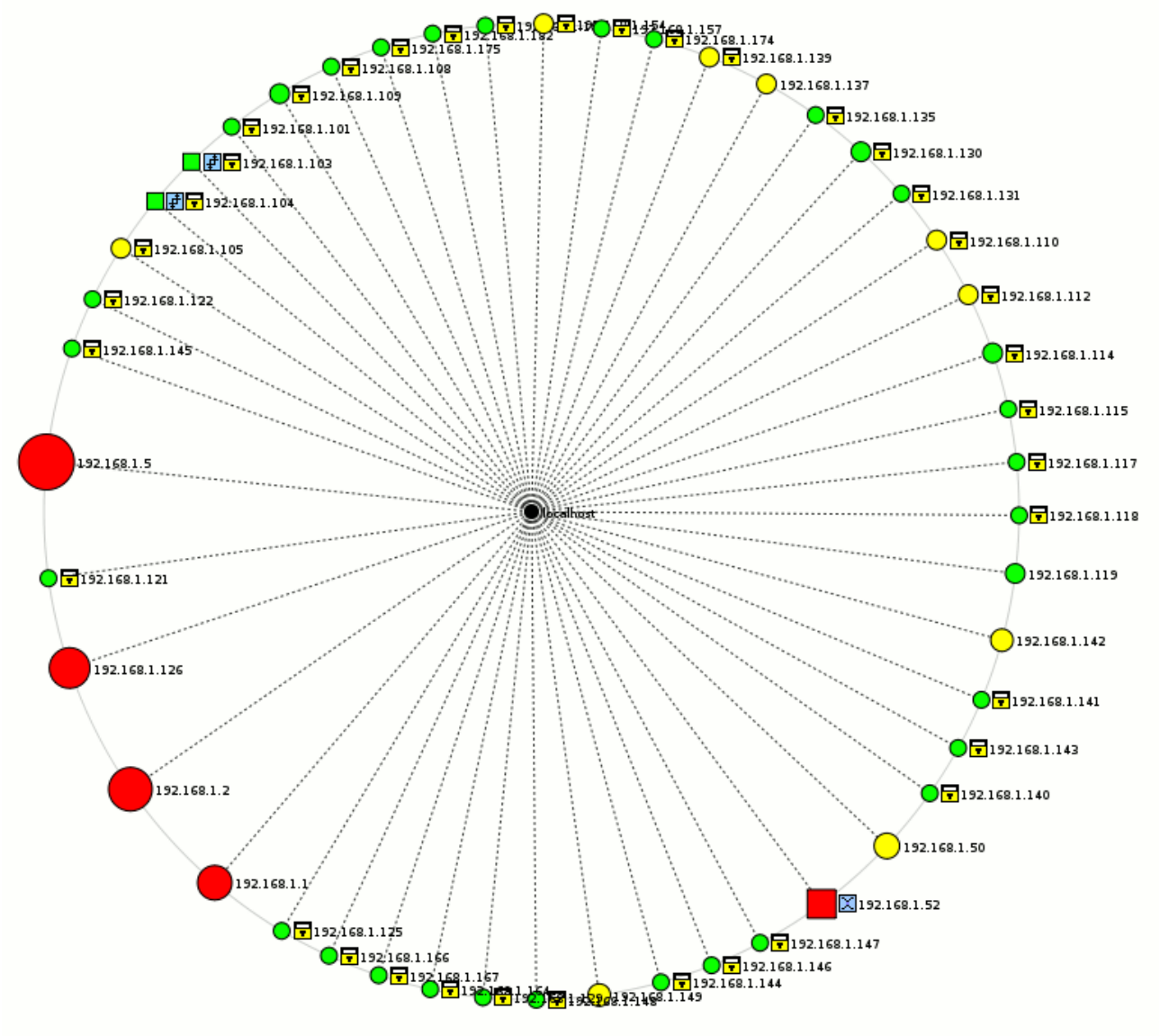
Poznámky psané kurzívou v závorkách jsou velmi obecné a nepřesné. Slouží jen pro představu, čeho se daná sekce/modul týká. Podrobnosti v dokumentu OSSTMM.

Výsledky testování

Testování jsem prováděl na IP rozsahu 192.168.1.0/24, kde se v době testování nacházelo 46 běžících počítačů.

Default gateway do Internetu se nechází na adrese 192.168.1.1. Na gateway běží NAT, který překládá interní adresy na externí adresu 80.95.246.154. Testy bylo zjištěno, že provoz ven do Internetu není nijak omezen. Dovnitř jsou povoleny porty (21/tcp, 25/tcp, 443/tcp, 2121/tcp, 993/tcp) vedoucí na stroj 192.168.1.1.

Podrobnější pohled na topologii v následujícím diagramu:



grafický výstup programu Zenmap

Detaily o počítačích zjištěné skenováním portů pomocí nástroje Nmap (případně Zenmap):

IP adresa	**192.168.1.1 (gw.gybot.cz)**		
otevřené porty	21/tcp	ftp	vsftpd 2.0.5
	22/tcp	ssh	OpenSSH 4.3p2 Debian 9etch3 (protocol 2.0)
	25/tcp	smtp	Sendmail 8.13.8/8.13.8/Debian-3
	53/tcp	domain	ISC BIND 9.3.4-P1.1
	80/tcp	http	Apache httpd 2.2.3 ((Debian) PHP/4.4.4-8+etch6 mod_ssl/2.2.3 OpenSSL/0.9.8c)
	106/tcp	pop3pw	Poppassd 1.8.5
	110/tcp	pop3	UW Imap pop3d 2003.83
	143/tcp	imap?	
	443/tcp	ssl	OpenSSL (SSLv3)
	587/tcp	smtp	Sendmail 8.13.8/8.13.8/Debian-3
	993/tcp	ssl	OpenSSL (SSLv3)
	995/tcp	ssl	OpenSSL (SSLv3)
	2121/tcp	ftp	vsftpd 2.0.5
operační systém	Linux 2.6.13 - 2.6.27		
poznámka	gateway pro celou síť poštovní server pro doménu gybot.cz na Apache dostupný zranitelný SquirrelMail (https://gw.gybot.cz/mail) FTP server podporující anonymní přihlášení, zranitelnost nepoužívané DNS, zranitelné cache poisoning		

IP adresa	**192.168.1.2**		
otevřené porty	42/tcp	wins	Microsoft Windows Wins
	53/tcp	domain	Microsoft DNS
	88/tcp	kerberos-sec	Microsoft Windows kerberos-sec
	135/tcp	msrpc	Microsoft Windows RPC
	139/tcp	netbios-ssn	
	389/tcp	ldap	
	445/tcp	microsoft-ds	Microsoft Windows 2003 microsoft-ds
	464/tcp	kpasswd5?	
	593/tcp	ncacn_http	Microsoft Windows RPC over HTTP 1.0
	636/tcp		
	1026/tcp	msrpc	Microsoft Windows RPC
	1027/tcp	ncacn_http	Microsoft Windows RPC over HTTP 1.0
	1047/tcp	msrpc	Microsoft Windows RPC
	1049/tcp	msrpc	Microsoft Windows RPC
	1050/tcp	msrpc	Microsoft Windows RPC
	1057/tcp	msrpc	Microsoft Windows RPC
	3268/tcp	ldap	
	3269/tcp		
	3389/tcp	microsoft-rdp	Microsoft Terminal Service
operační systém	Microsoft Windows Server 2003 SP1 or SP2		
poznámka	DNS pro celou síť server s Active Directory,		

IP adresa	192.168.1.5 (JAZSERVER.jazucebna)		
otevřené porty	25/tcp	smtp	Microsoft ESMTP 5.0.2195.4453
	80/tcp	http	Microsoft IIS webserver 5.0
	88/tcp	kerberos-sec	Microsoft Windows kerberos-sec
	135/tcp	msrpc	Microsoft Windows RPC
	139/tcp	netbios-ssn	
	280/tcp	http	GoAhead-Webs embedded httpd
	389/tcp	ldap	
	443/tcp	https?	
	445/tcp	microsoft-ds	Microsoft Windows 2000 microsoft-ds
	464/tcp	kpasswd5?	
	593/tcp	ncacn_http	Microsoft Windows RPC over HTTP 1.0
	636/tcp	tcpwrapped	
	1026/tcp	mstask	Microsoft mstask
	1029/tcp	ncacn_http	Microsoft Windows RPC over HTTP 1.0
	1071/tcp	msrpc	Microsoft Windows RPC
	1086/tcp	mstask	Microsoft mstask
	1100/tcp	msrpc	Microsoft Windows RPC
	1119/tcp	mstask	Microsoft mstask
	1137/tcp	msrpc	Microsoft Windows RPC
	1145/tcp	msrpc	Microsoft Windows RPC
	3268/tcp	ldap	
	3269/tcp	tcpwrapped	
	3372/tcp	msdtc?	
	3389/tcp	microsoft-rdp	Microsoft Terminal Service
	4321/tcp	rwhois?	
	5555/tcp	freeciv?	
	8080/tcp	http-proxy	Microsoft ISA Server http proxy
operační systém	Microsoft Windows 2000|Me		
poznámka	server, který nepatří škole a v nejbližší době se bude rušit, tudíž jsem ho ani nějak podrobně neřešil		

IP adresa	192.168.1.50		
otevřené porty	23/tcp	telnet?	
	80/tcp	http	HP Jetdirect httpd
	280/tcp	http	HP Jetdirect httpd
	515/tcp	printer	
	631/tcp	http	HP Jetdirect httpd
	9100/tcp	jetdirect?	
operační systém	HP LaserJet 4050 or 4000n printer		
poznámka			

IP adresa	**192.168.1.52**		
otevřené porty	21/tcp 80/tcp 139/tcp 427/tcp 443/tcp 515/tcp 631/tcp 9100/tcp 50001/tcp	ftp http netbios-ssn? tcpwrapped tcpwrapped tcpwrapped http jetdirect? unknown	Konica Minolta Bizhub printer ftpd Konica Minolta Bizhub printer http config Konica Minolta Bizhub printer http config
operační systém	Konica Minolta Bizhub C450 copier		
poznámka			

Klientské počítače nebudu řeait samostatně, vyberu pouze jeden jako reprezentativní vzorek.

IP adresa	**192.168.1.109**		
otevřené porty	139/tcp 445/tcp	netbios-ssn microsoft-ds	 Microsoft Windows XP microsoft-ds
operační systém	Microsoft Windows XP SP2		
poznámka	klientský počítač		

Nalezená bezpečnostní rizika

Následuje výčet potenciálních rizik, které se na síti vyskytly a návrh jejich řešení:

Cíl	celá síť
Problém	Vzhledem k tomu, že síť je propojena neadministrovanými switchi, které nepodporují žádnou formu port security nebo DAI, není problém provést útok metodou *ARP poisoning* a dostat se do postavení *man-in-the-middle* a následně odposlouchávat komunikaci mezi kterýmikoli dvěma stanicemi. Tímto způsobem se může útočník dostat ke všem citlivým datům, která jsou na síti přenášena (hesla, e-maily apod.).
Navrhované řešení	1. Nákup switchů, které podporují DHCP snooping, případně nějakou formu DAI (Dynamic ARP Inspection). Tím se zabrání tomu, aby útočník mohl rozesílat do sítě falešné ARP pakety, tudíž se nedostane do postavení MITM. 2. Provizorním řešením je nastavení nejdůležitějších položek v ARP cache každého počítače staticky. Nejdůležitější data jsou pravděpodobně cílena na bránu do Internetu, případně Windows server (adresy 192.168.1.1 a 192.168.1.2). Těmto adresám lze na klientských stanicích s Windows nastavit staticky MAC pomocí nějakého skriptu, který se spouští po startu systému (*příkaz: arp -s 192.168.1.1 00:30:4F:50:B4:AC).*

Cíl	192.168.1.1 – ftp
Problém	FTP démon *vsftpd 2.0.5* na serveru 192.168.1.1 podporuje anonymní přihlášení, a to dokonce i z vnějšku sítě. Zároveň obsahuje zranitelnost (podrobnosti zde), která by případně mohla vést DoS celého serveru.
Navrhované řešení	FTP server není údajně využíván, doporučeno rovnou vypnout a na vstupním firewallu zakázat jeho porty. Jinak upgradovat na novější verzi a zakázat anonymní přihlášení.

Cíl	192.168.1.1 – http
Problém	Na serveru běží zranitelná aplikace *SquirrelMail verze 1.4.9a*, která je napadnutelná pomocí útoku *Cross-site scripting* (CVE-2007-1262).
Navrhované řešení	Pokud není SquirrelMail využíván, doporučeno zrušit. Jinak upgrade na novější verzi.

Cíl	192.168.1.1 – dns
Problém	Aplikace: BIND 9.3.4-P1.1 DNS démon je napadnutelný pomocí útoku *DNS cache poisoning* (CVE-2007-2926).
Navrhované řešení	Podle všeho není DNS na stroji 192.168.1.1 využíváno. Doporučeno vypnout. Jinak upgrade na novější verzi.

Cíl	192.168.1.5 (JAZSERVER.jazucebna)	
Problém	Podle všeho nebyl tento stroj posledních minimálně 7 let aktualizován. Následuje výčet zranitelností, pomocí kterých by případný útočník mohl nad tímto serverem převzít kontrolu:	
	CVE-2003-0717 CVE-2004-0212 CVE-2007-0040 CVE-2007-3028 CVE-2005-1983 CVE-2005-2120 CVE-2003-0533 CVE-2003-0605 CVE-2003-0528 CVE-2003-0715 CVE-2005-1984 CVE-2005-2150 CVE-2006-1315 CVE-2006-1314 CVE-2008-4250	CVE-2006-3439 CVE-2005-1206 CVE-2002-0071 CVE-2006-1184 CVE-2006-0034 CVE-2005-1980 CVE-2005-1979 CVE-2005-1978 CVE-2005-2119 CVE-2004-0124 CVE-2003-0807 CVE-2004-0116 CVE-2003-0813 CVE-2003-0818
Navrhované řešení	Vzhledem k tomu, že pro server není do budoucna žádné využití, doporučeno **okamžitě odpojit** od sítě.	

Závěr

Ve své práci jsem se z časových důvodů zaměřil jen na nejvíce rizikové zranitelnosti. Bezpečnostní slabiny, které neznamenají přímé nebezpečí, například prozrazování informací v bannerech běžících služeb, jsem vědomě opomněl.

Objevil jsem nejdůležitější bezpečnostní rizika a navrhl postupy k jejich řešení. Zároveň jsem ale neměl čas procházet všechny detaily do podrobností, tudíž jsem některý slabiny mohl přehlédnout.

Použité materiály

[1] Pete Herzog. Open Source Security Testing Methodology Manual. ISECOM, 2006. [online] http://www.isecom.org/mirror/osstmm.en.2.2.zip

[2] Marek Kocián. Metodiky testování bezpečnosti. [online] http://is.muni.cz/th/99189/fi_b/bak.pdf

[3] Petr Šťastný. Útoky s využitím protokolu DNS. [online] http://www.pweb.cz/a/38/utoky-s-vyuzitim-protokolu-dns-1-dns-spoofing-cache-poisoning.html

[4] Martin Haller. Bráníme se odposlechu: obrana na switch. [online] http://www.lupa.cz/clanky/branime-se-odposlechu-obrana-na-switchi/

Použité nástroje

- Nmap (http://nmap.org/)
- Zenmap (http://nmap.org/zenmap/)
- Wireshark (http://www.wireshark.org/)
- Ettercap (http://ettercap.sourceforge.net/)
- Cain (http://www.oxid.it/cain.html)
- Nessus (http://www.nessus.org/nessus/)
- Nikto (http://www.cirt.net/nikto2)
- THC-Hydra (http://freeworld.thc.org/thc-hydra/)