696

Přednáška č. 1

ÚVOD

Znalosti o nebezpečí, které hrozí jak uživatelům Internetu, tak i poskytovatelům síťových služeb jsou v současnosti již nepostradatelné. Bez těchto znalostí není možné ochránit svá citlivá data před zcizením a zneužitím a není možné spolehlivě provozovat síťové služby.

Co to jsou citlivá data?
Kde se nacházejí?
Kdo k nim může chtít získat přístup?
Proč k nim může chtít získat přístup?
Jak k nim může získat přístup?
Jak mu v tom můžeme zabránit?

Bezpečnostní problematika má podporu v zákonech ČR a při veškerých činnostech týkajících se práce s daty a užívání výpočetní technikz je nutné na to pamatovat:

Zákon č. 40/2009 Sb., trestní zákoník
§ 230 Neoprávněný přístup k počítačovému systému a nosiči informací
§ 231 Opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat
§ 232 Poškození záznamu v počítačovém systému a na nosiči informací a zásah do vybavení počítače z nedbalosti
§ 182 Porušení tajemství dopravovaných zpráv

Viz.: http://www.mvcr.cz/clanek/sbirka-zakonu.aspx

Některé základní hrozby

Hrozba: Keyloger
Viz.: http://www.actualspy.com/index.html

Obrana:
-Zapamatovaná hesla v prohlížeči chránit heslem (Master password)
-LiveCD
Viz: http://nimblex.net/, http://www.puppylinux.com/

Hrozba: HW keylogery

Viz: http://www.keelog.com/ps2_hardware_keylogger.html,
http://www.keydevil.com/how-it-works.html

Obrana: Vizuální kontola počítače a infrastruktury.

Hrozba: Odposlech dat přenášených po síti

Viz: Wireshark http://www.wireshark.org,

Obrana: Šifrování přenášených dat (SSL, Ipsec, ccrypt, GPG)

Hrozba: Připojení souborového systému po nabootování z CD

Obrana: Zaheslovat bios, zabránit ve fyzickém přístupu k počítači

Hrozba: Mámení přístupových hesel (phishing)

Obrana: Nepřistupovat bezrozmyslu k jakémukoli WEBu, neotvírat bezrozmyslu přílohy e-mailů.

Hrozba: Přímé průniky do operačních systémů založené na zneužití chyb používaného software.

Viz.: http://isc.sans.org/survivaltime.html

Obrana: Aktualizace software, instalace lokálního firewallu, antiviru a software pro analýzu útoků.

Hrozba: Sociální inženýrství

Obrana: Identifikace volajícího, resp. odesílatele e-mailu.

Hrozba: Útoky na mobilní zařízení (mobilní telefony, mp3 přehrávače, fotoaparáty)

Viz.: Conficker

Obrana: Zdravý rozum a antivirový software.

Přednáška č. 2

ZABEZPEČENÍ KLIENTA (Windows XP)

1. HESLA

Silná hesla

Jak vytvořit silné heslo?
http://en.wikipedia.org/wiki/Password_strength
http://www.microsoft.com/protect/fraud/passwords/create.aspx

Jak dlouho trvá prolomení hesla v závislosti na jeho síle a použitých prostředcích.
http://www.lockdown.co.uk/?pg=combi

Kontrola síly hesla:
https://www.microsoft.com/protect/fraud/passwords/checker.aspx?WT.mc_id=Site_Link

Generování bezpečného hesla pomocí karty:
http://www.savernova.ch/online-password-card/logowebcard.php?id=159&lang=en

Základní požadavky na vlastnosti hesla (heslová politika):

Minimální délka hesla 8 znaků
Minimální životnost hesla (většinou mezi 1 a 7 dny)
Maximální životnost hesla (většinou ne více než 42 dnů)
Porovnávaná historie hesel by neměla být menší než 6

LAB:

Analyza implicitniho hesla studenta, proc je treba ho zmenit

Nastavit heslovou politiku:

Ovládací panely - Nástroje pro správu - Místní zásady zabezpečení

Ophcarck

Přednáška č. 3

2. SOUBOROVÝ SYSTÉM

Používat NTFS souborový systém.

Tento počítač (pravé tlačítko) - Spravovat - Správa disků

ke konverzi FAT na NTFS lze použít utilitu convert

3. SUŽBY

Vypnout nepotřebné služby:

Telnet
Universal Plug and Play Device Host
IIS (není implicitně instalován)
Netmeeting Remote Desktop Sharing
Remote Desktop Help Session Manager
Remote Registry
Routing & Remote Access
SSDP Discovery Service

Tento počítač - Spravovat - Služby

Některé obzvlášť choulostivé služby:

Sdílené prostředky:

Odstraňení sdílených položek:
Run - ddeshare.exe

Zákaz null session:
Run - regedit

zazálohovat registry (Soubor - Exportovat)

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\restrictanonymous nastavit na hodnotu 2

restrictanonymoussam ponechat hodnotu 1

Zakázat NetBios přes TCP/IP

Ovládací panel - Síťová připojení - Připojení k místní síti - Vlastnosti (pravé tlačítko) - TCP/IP - Vlastnosti - Upřesnit - WINS - Zakázat rozhraní NetBIOS nad protokolem TCP/IP

Pokud bude počítač pužíván pouze k přístupu do Internetu pomocí protokolů TCP/IP je vhodné
lanmanserver rovnou vypnout:

Server (lanmanserver) disable (pravé tlačítko na něj ve Služby)

Nebo přímo zakázat (odinstalovat) klienta pro Microsoftí sítě.

Vzdálený přístup k ploše:

Ovládací panely - Systém - Vzdálený přístup - Zakázat vzdálenou pomoc a vzdálenou plochu.

gpedit
Místní počítač zásady - Konfigurace poćítače - Šablony pro správu - Součásti systému windows - Terminálová služba - Povolit uživatelům vzdálené připojení pomocí terminálové služby (pravé tlačítko)

Otevřené porty lze vypsat příkazem:

netstat -a

Je nutné pečlivě ověřit, které porty odpovídají kterým službám. Nesmí být otevřen žádný port, který by nenáležel službě kterou chceme provozovat, ani žádný port o kterém nám není známo, ke které službě patří.

4. UŽIVATELÉ:

Smazat nepotřebné uživatele:

Tento počítač - Spravovat - Místní uživatelé a skupiny - Uživatelé

Disablovat uživatele Guest
(má smysl jen v doméně, nebo na počítačích které nepoužívají Simple File Sharing model)

U systémů které nejsou v doméně, jsou pokusy o vzdálené připojení donuceny použít implicitně Guest konto.

Zakázat zobrazování naposledy přihlášeného uživatele:
gpedit
Místní počítač zásady - Konfigurace poćítače - Nastavení systému windows - Nastavení zabezpečení - Místní zásady - Možnosti zabezpečení - Interaktivní přihlašování: nezobrazovat ...

5. AUTORUN/AUTOPLAY

Vypnout autorun:

gpedit.msc
Konfigurace počítače - Šablony pro správu - Systém - Vypnout automatické přehrávání

Nezabráníme tak však útokům, které zneužívají naivity uživatele:

autorun.inf:

```
[autorun]
;  Autoplay menu
action=Test autoplay: Spust Paint z flash disku
open=mspaint.exe
;  Pravé tlačítko na ikonu flash disku
shell\FromFlash=Test kontextu: Spust Paint z flash disku
shell\FromFlash\command=mspaint.exe
;  Co spustit po dvojkliku v “Tento počítač”
shell=FromFlash
icon=mspaint.exe
```

label=Test AutoPlay

Nebo spuštění kódu z takzvaných U3 zařízení, které se chovají jako USB hub s flash diskem a CD mechanikou s vloženým CD.

Definitivním řešením je zdá se zcela zakázat práci se souborem autorun.inf:

Vytvořit soubor zap.reg:

REGEDIT4
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\IniFileMapping\Autorun.inf]
@="@SYS:DoesNotExist"

a spustit ho.

Více informací viz.:

http://nickbrown-france.blogspot.com/2007_10_01_archive.html

6. TCP/IP:

Zakázat ICMP redirecty a detekci “Mrtvých” směrovačů:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters
EnableICMPRedirect nastavit na 0
DeadGWDetectDefault nastavit na 0
EnableSecurityFilters nastavit na 1

Přednáška č. 4:

(zopakování fungování směrování v IP protokolu)

7. FIREWALL:

Je bezpodmínečně nutné omezit přístup ze sítě pomocí správně nastaveného firewallu:

Připojení k místní síti - pravé tlačítko - Vlastnosti - Upřesnit - Nastavení (Brána firewall)

Ze sítě povolit přístup pouze ke službám které nabízíme (je vhodné přístupy filtrovat na základě IP adresy, pokud má být služba dostupná jen vybraným

uživatelům), a směrem do sítě povolit pouze protokoly klientů se kterými pracujeme.

8. AUDITING/LOGOVÁNÍ:

Je vhodné logovat vybrané události, které v případě pokusů o neoprávněný přístup pomohou při identifikaci problému:

Přihlášení k účtu (Úspešné/Neúspěšné)
Změny v účtech. resp. management uživatelů (Úspešné/Neúspěšné)
Přístupy k oběktům (Úspešné)
Změny politik (Úspešné/Neúspěšné)
Použití privilegií (Úspešné/Neúspěšné)
Systémové události (Úspešné/Neúspěšné)

Ovládací panely - Nástroje pro správu - Místní zásady zabezpečení - Místní zásady - Zásady auditu - Auditovat přístup k objektům

9. ŠIFROVÁNÍ SOUBORŮ:

Na adresář: pravé tlačítko - Vlastnosti - Upřesnit - Šifrovat

10. AKTUALIZACE SYSTÉMU

Ovládací panely – Automatické aktualizace

11. ANTIVIRUS/ANTISPYWARE

Antivirus, antispywre:
http://www.microsoft.com/security/products/mse.aspx

Nástroj na odstranění škodlivého software (malware).

http://www.microsoft.com/security/malwareremove/default.aspx

Přednáška č. 5

12. KLIENTSKÉ PROGRAMY

Browser:
Centrum zabezpečení - Možnosti Internetu
nebo přímo z prohlížeče: Nástroje - Možnosti Internetu
Nastavení Zón:
Internet Zone Settings
Secure Zone Settings

http://surfthenetsafely.com/ieseczone8.htm
Sporné:
META REFRESH
File download

Přidat počítače do Secure Zone

Mimochodem souborovou cache lze využít ke stahování flash videa.

Privoxy
http://www.privoxy.org

Sandboxie

13. OVĚŘENÍ ZABEZPEČENÍ

Microsoft baseline security analyzer

ESET SysInspector
http://www.eset.com/download/sysinspector

14. DALŠÍ ZDROJE INFORMACÍ

Windows XP Security Guide:
http://www.microsoft.com/downloads/details.aspx?familyid=2d3e25bc-f434-4cc6-a5a7-09a8a229f118&displaylang=en

XP Checklist:
http://labmice.techtarget.com/articles/winxpsecuritychecklist.htm

Zabezpečení sítě:
http://www.microsoft.com/windowsxp/using/security/learnmore/smbsecurity.mspx
http://www.microsoft.com/windowsxp/using/networking/security/features.mspx

http://technet.microsoft.com/cs-cz/security/default.aspx

UNIX

1. SILNÁ HESLA

/etc/pam.d/common-password:

password required pam_cracklib.so retry=3 minlen=10
        difok=3 dcredit=-1 ucredit=-1 lcredit=-1

difok počet znaků, kterými se musí lišit od minulého hesla
dcredit čísla
ucredit velká písmena
lcredit malá písmena
ocredit ostatní znaky
-1 znamená minimálně jeden znak tohoto typu
1 credit pro znaky daného typu (heslo může být při použití daných znaků kratší)

/etc/login.defs:
PASS_MAX_DAYS 40
PASS_MIN_DAYS 0
PASS_WARN_AGE 7

apt-get install libpam-cracklib
apt-get install libcrack2
apt-get install wbritish

2.SOUBOROVÝ SYSTÉM

Vždy používat souborový systém s žurnálem

Srovnání výkonnosti:
http://www.debian-administration.org/articles/388

Bezpečnost:
user, group, others
rwx
SUID, SGID bits

find / -type f \(-perm -2 -o -perm -20 \)
find / -type d \(-perm -2 -o -perm -20 \)

find / -type f \(-perm -004000 -o -perm -002000 \)

mount -o nosuid zeus:/athena /usr/athena

hard links to SUID binaries
find ... -links +1

Sticky bit
ACL
Šifrování:

Loop-AES
DM-Crypt
Truecrypt
Crypto-FS
Enc-FS

(http://www.debianadmin.com/filesystem-encryption-tools-for-linux.html)

NFS
Samba

3. SLUŽBY

/etc/initttab
/etc/init.d

sysv-rc-conf sluzba off/on

update-rc.d

/etc/inetd.conf

4. UŽIVATELÉ

/etc/passwd
/etc/shadow

useradd, userdel
adduser, deluser

5. AUTOSTART

Desktop - Preferences

6. TCP/IP

/proc/sys/net/ipv4:
ip_forward
icmp_echo_ignore_all

Přednáška č. 6

7. FIREWALL

Iptables

Výpis konfigurace:

iptables -L

Akceptování paketů již navázaných spojení:

iptables -A INPUT -m conntrack --ctstate ESTABLISHED,RELATED -j ACCEPT

Povolení připojení na port ssh zvenku:

iptables -A INPUT -p tcp ––dport ssh -j ACCEPT

Blokování všeho ostatního:

iptables -A INPUT -j DROP

Povolení komunikace s Loopbackem (první pravidlo v pořadí):

iptables -I INPUT 1 -i lo -j ACCEPT

pf

8. AUDIT/LOGOVÁNÍ

btmp,wtmp:

Pokud soubory neexistují, nic se neloguje.
Soubory lze vytvořit např. programem touch.

/var/log/wtmp (last)
/var/log/btmp (lastb)

syslogd – syslogd, klogd
syslogd -r

kill -SIGNAL ‘cat /var/run/syslogd.pid‘

SIGNAL: SIGHUP, SIGTERM, SIGUSR1

/etc/syslog.conf

daemon.debug /usr/adm/daemons

*.=debug /usr/adm/debug

mail.*;mail.!=info /usr/adm/mail
news.info;news.!crit /usr/adm/news

. @hostname
(/etc/services: syslog 514/udp)

Analýza logů:

http://www.loganalysis.org/

LogSentry

9. ŠIFROVÁNÍ SOUBORŮ A JEJICH INTEGRITA

http://www.debian-administration.org/articles/49

Aide
http://www.cs.tut.fi/~rammer/aide.html
http://sourceforge.net/projects/aide/

Tripwire
http://www.tripwire.org/
http://sourceforge.net/projects/tripwire/

Integrit
http://integrit.sourceforge.net/texinfo/integrit.html

10. AKTUALIZACE SYSTÉMU

http://www.debian.org/security/

/etc/apt/sources.list:

deb http://security.debian.org/ distribuce/updates ...
deb-src http://security.debian.org/ distribuce/updates ...

apt-get update
apt-get upgrade

11. ANTIVIRUS/ANTISPYWARE

Chkrootkit
Clam Antivius (ClamAV) - email
http://www.clamav.net/

12. KLIENTSKÉ PROGRAMY

13. OVĚŘENÍ ZABEZPEČENÍ

CIS
http://www.cisecurity.org/tools2/linux/CIS_Debian_Benchmark_v1.0.pdf

http://www.nongnu.org/tiger/
http://packages.debian.org/tiger

Debian: checksecurity

Unix hardening
Sentry
OpenWall

14. DALŠÍ ZDROJE INFORMACÍ

Přednáška č. 7

MONITOROVÁNÍ A DETEKCE

1. LOGY

Analýza:
Sawmill (http://www.sawmill.net)

psad (http://cipherdyne.org/psad/)

2. IDS

lokální IDS, síťové IDS, hybridy

2.1 LOKÁLNÍ IDS

OSSEC HIDS
http://www.ossec.net/

2.2 IDS

Dva základní způsoby sběru dat v přepínaných sítích:

- zrcadlení portu (mirroring, SPAN)
- větvení sítě (network TAP)

Dva typy IDS

- IDS založené na pravidlech (signaturách)
- IDS založená na profilu (detekce anomálií)

nedefinuje pouze činnosti, které nejsou povoleny, ale i činnosti, které povolené jsou

Problémy:
- falešné pozitivní detekce
- vysokorychlostní prostředí
- potíže s detekcí neznámých hrozeb

TCPDUMP

tcpdump -r soubor.pcap
- načtení dat ze souboru

tcpdump -tt
- čas v UNIX formátu (date -r Uxformat)

tcpdump -n
- neprovádí konverzi IP adres a portů do symbolického formátu

tcpdump -S
- uvádí původní (nenormalizované) sekvenční číslo TCP paketů

tcpdump -v (-vv. -vvv)
- podrobnější informace

tcpdump -x
- zobrazení obsahu paketu hexadecimálně

tcpdump -s0

- zachytávat celý paket

tcpdump -w soubor.pcap

- uložit zachycená data do souboru

Výrazy:

(detekce aplikací běžících na nestandardních portech, detekce peer to peer aplikací atd.

BPF

aritmetika a booleovské operátory: +, -, *, /, &, |

logické operárory: &&, ||

relační operátory: <, <=, >=, >

bitový posun: >>, <<

negace: !

závorky: (,)

Paket s cílovým portem 22:
tcp[2:2] = 22
nebo tcp dst port 22
ale: tcp[2:2]>=20 and tcp[2:2]<=30 (pakety s TCP porty od 20 do 30)

IP paket s hodnotou TTL = 1:
ip[8] = 1

Paket s IP verze 4 a žádnou volbou:
ip[0] = 0x45

Paket jehož první datový bajt je roven 1:
tcp[(tcp[12] >>4)*4] = 1

(vezmeme 12 bajt hlavičky, který obsahuje její délku ve 32bitových slovech v horních 4 bitech. Posuneme o 4 bajty vlevo a horní čtveřici vyplníme 0. Protože se jedná o počet 32bitových, resp. 4bajtových slov, délku hlavičky obdržíme, když uvedenou hodnotu vynásobíme 4, což je zároveň offset prvního datového bajtu)

(http://www.sans.org/security-resources/tcpip.pdf)

Zkrácené výrazy:

net, host, port
src, dst

host A or host B
host A and not host B
src host A
src host A and tcp port telnet
net MOJESIT and not net MOJESIT (provoz mezi MOJESIT a ostatnimi uzly, nebo sitemi)

Velkokapacitní záchyt a analýza útoků offline, nebo pozdější forenzní analýza.

Počátky IDS:
Detekce červa Slammer (MSSQL na portu 1434/UDP a je délky 376bajtů):
udp[4:2] = 384 and dst port 1434 and src net MOJESIT

Detekce SSH spojení na nestandardních portech (backdoor):
??? tcp [((tcp[12] & 0xf0)>>2]):4] = 0x5353482D

tcpslice, tcpflow, tcpjoin

tcpslice:
umožňuje vybrat data za určitý časový interval

tcpflow:
umožňuje extrahovat TCP streamy

tcpjoin:
umožňuje spojit dva soubory generované tcpdumpem

Přednáška č. 8:

Architektura IDS

- jednovrstevná
- vícevrstevná
- peer to peer

Senzory
zisk a předání dat (tcpdump)

Agenti

analýza vstupů získaných ze senzorů

Manažer

správa dat
generování výstrahy
korelace událostí
monitorování ostatních komponent
řídící konzole

Způsoby detekce:

- porovnávání signatur
- porovnávací pravidla
- porovnávání založené na profilu

Implementace:

Cisco IDS
IBM ISS
Imperva Secure Sphere

Snort
IDS založený na pravidlech, signatury používá pouze k identifikaci typu uskutečněného útoku

Režimy:

sniffer: snort -d
logger: snort -dev -l /adresar
ids: snort -dev -l /adresar -c snort.conf

Komponenty:
packet capture engine (libpcap, winpcap)

preprocesory
- co bude provedeno s laždým paketem (analýza, změna, odmítnutí, generování výstrahy)

modifikace URI a URL do standardního formátu
stavová analýza TCP/IP
detekce skenerů portů
dekódovaní paketů (např. RPC, telnet)

detekční jednotka
dekódování paketů
aplikace pravidel na pakety a data

output pluginy
generování informací které budou zobrazeny v analýze

Pravidla:
SID

snort.conf
.rules

alert tcp any any -> 192.168.1.0/24 111 (content:”|00 01 86 a5|”; msg: “mountd access”;)
header options

header:
alert, log, pass

tcp,udp,icmp
source -> dest port (1:1024 port range)

->, <>

options:
logto
ttl – test TTL
dsize – test velikosti datové části paketu
content – vyhledání paternu v datové části paketu
icode – test pole TYPE ICMP paketu
msg – zpráva uvedená v alertu a logu

IPS

monitoruje síť a pokud dojde k události, přijme opatření podle definovaných pravidel

iptables + fwsnort

snort + modul flexresp2

3. HONEYPOTY

- nízkointeraktivní

honeyd

- vysoceinteraktivní

HIHAT (high interaction honeypot analysis toolkit)
konvertuje libovolnou PHP aplikaci do WEB high-interaction honeypotu

4. HONEYNETY

Darknet
http://www.team-cymru.org/Services/darknets.html
Network Telescope
http://www.caida.org/research/security/telescope/

Literatura:
C. Endorf, E. Schultz, J. Mellander: Detekce a prevence počítačového útoku , Grada, ISBN 80-247-1035-8

Přednáška číslo 9:

REAKCE NA INCIDENTY A FORENZNÍ ANALÝZA

CÍLE

Potvrdit, nebo vyvrátit zda k incidentu skutečně došlo

Shromáždit přesné a objektivní informace

Nastavit mechanizmy získávání a zpracování důkazů

Zachovat privátnost informací garantovanou zákonem

Minimalizovat dopady incidentu na normální fungování organizace

Umožnit stíhání útočníků

Vytvořit podrobné protokoly a doporučení

METODOLOGIE

1. PŘÍPRAVA

Dostatečně se připravit ještě před tím, než k incidentu dojde.

Shromáždění nástrojů a postupů pomocí kterých budeme na incident reagovat a úpravy systémů a sítí, které jsou incidentem ohroženy

Vytvořit tým, který se bude incidentem zabývat, definovat procedury a připravit nástroje, které budeme během řešení incidentu používat.

Příklady:

http://csirt.cesnet.cz

Identifikace vitálních oblastí.

Zabezpečení systémů.

Hardware

Software

Kopie disku:

Safeback, EnCase, DiskPro, dd

Prohlížení souborů:

Quckview Plus, HandyVue

Ovladače

2. DETEKCE INCIDENTŮ

Odhadnout, zda se jedná o incident.

Zaznamenat všechno co jsme schopni zjistit.
Jedná se například o:

Aktuální datum a čas

Kdo, nebo jaký prostředek incident zaznamenal

Podstatu incidentu

Kdy k incidentu došlo

Jakého hardware a software se incident týká

Kontakty na zúčastněné osoby

3. POČÁTEČNÍ REAKCE

Provést prvotní analýzu, zajistit informace, které nejsou trvalého charakteru (včetně

svědectví zúčastněných) a potvrdit zda skutečně došlo k incidentu.

Ověřit, kterých systémů se incident přímo, či nepřímo týká, kteří uživatelé se ho účastní a definovat dopad, který bude incident mít na fungování společnosti.

Jak důležité jsou napadené systémy

Jak citlivé jsou ukradené, nebo porušené informace

Kdo je potencionálním útočníkem

Zda je o incidentu informována veřejnost

Úroveň neoprávněného přístupu získaná útočníkem

Schopnosti útočníka

Jak velké výpadky systému je možné tolerovat

Celkové finanční ztráty

4. FORMULACE STRATEGIE

Na základě všech známých faktů určit nejlepší reakci.

Reakce musí být odsouhlasena vrcholovým managementem

5. DUPLIKACE KRITICKÝCH DAT

Rozhodnout, zda je nutné kvůli pozdějšímu zkoumání vytvořit fyzickou kopii dat, nebo získat důkazy online.

Analýza „živých“ dat versus analýza duplikátu systému

Ještě před tím, než bude provedena duplikace systému, je třeba získat živá data z běžícího systému:

Obsahy registrů a vyrovnávacích pamětí

Obsah operační paměti

Informace o síťových spojeních

Informace o běžících procesech

Obsah disků

Obsah výměnných a zálohovacích médií

Systémový čas	date, time	date
Kdo je přihlášen?	loggedon	w
Otevřené sokety	netstat	netstat –anp
Seznam procesů, které sokety otevřely	fport	lsof
Seznam běžících procesů	pslist	ps
Přehled připojených systémů	nbtstat	netstat
Záznam provedených kroků	doskey	script, vi, histrory

Duplikování systému

V neobsazeném prostotu disku se mohou nacházet informace, které mohou mít na výsledek pátrání poměrně značný vliv**.**

Tři různé způsoby:

Vyjmeme odpovídající médium z napadeného systému a zduplikujeme ho v počítači

používaném k vyšetřování.

Duplikát provedeme na napadeném systému, poté co do něho připojíme náš pevný disk.

Zduplikujeme relevantní médium pomocí uzavřeného síťového spojení na počítač používaný

k vyšetřování.

Počítač použitý k vyšetřování (172.17.11.6):

netcat –l –p 7000 > /mnt/dukazy/disk1.dd

Zkoumaný počítač (nabootováno z CD ROM):

dd if=/dev/hda | nc 172.17.11.6 7000

Analýza netbiosu:

Určit geometrii důkazního média (pevného disku, který chcete zkoumat)

Určit bootovací sekvenci systému

Nástroje používané k duplikování důkazů musí splňovat následující požadavky:

Aplikace musí umožňovat duplikovat každý bit originálního média. Obraz musí obsahovat všechna data obsažená na disku. Od počátku disku až po služební stopu.

Aplikace se musí spolehlivě vyrovnat s chybami čtení. Jestliže se ani po několika pokusech nepodaří poškozený sektor přečíst, musí být vynechán, identifikován a místo něho musí být do výstupních dat umístěn sektor přesně stejné délky obsahující „výplň“.

Aplikace nesmí žádným způsobem modifikovat data na originálním médiu.

Aplikace musí být schopna prodělat testování a analýzu na vědecké úrovni. Výsledky musí být opakovatelné a musí být možnost je potvrdit třetí stranou (pokud je to nutné).

Vytvořený obraz (kopie) musí být ochráněn kontrolním součtem, nebo signaturou. Kontrolní součet (signatura) může být vytvářena během kopírování dat (Safeback), nebo až po skončení celého procesu (dd a md5sum).

6. PÁTRÁNÍ

Provést analýzu dat za účelem odhalení toho, co se vlastně stalo, kdo je za incident odpovědný a jak je mu možné do budoucna zabránit.

Zjistit kdo, co, kdy, kde a jak měl s daným incidentem souvislost.

Chyby, kterým je třeba se při zpracování důkazů vyhnout:

Změna časových značek systému ještě před tím, než je zaznamenáte

Zrušení podezřelých procesů

Aplikace záplat systému před dokončením analýzy dat

Nezaznamenání příkazů zadaných během vyšetřování

Požití neprověřených příkazů a binárních kódů

Přepsání potenciálních důkazů, například instalací software na důkazní média

Přepsání potenciálních důkazů spuštěním programů, které ukládají své výstupy na důkazní média.

Fyzická analýza (vyhledávání řetězců na disku):

Všechny URL nalezené na analyzovaném médiu

Všechny e-mail adresy nalezené na médiu

Všechny řetězce obsahující specifická klíčová slova relevantní případu

Logická analýza (analýza souborů daného souborového systému.

7. IMPLEMENTACE BEZPEČNOSTNÍCH OPATŘENÍ

Aktivně izolovat útočníkovi systémy a zabránit tak rozšíření incidentu.

Metody:

odpojení od sítě

funkční izolace napadeného počítače

filtrování provozu na síti (fishbowling)

Pokud shromažďujeme důkazy pro případné soudní, nebo administrativní jednání, je třeba tak učinit tak ještě *před tím*, než implementujeme bezpečnostní opatření.

8. MONITOROVÁNÍ SÍTĚ

Monitorovat síťové aktivity za účelem průzkumu a neutralizace incidentu.

Kde, jak a co monitorovat.

Analýza síťových spojení:

tcpdump

Jsou některá pole hlaviček IP datagramů podezřelá?

- Je podezřelá odchozí IP adresa?
- Nedochází ke zbytečným fragmentacím?
- Nemají některé pakety podezřelou délku?

Jsou některá pole hlaviček TCP segmentů podezřelá?

- Odpovídají cílové porty segmentů provozovaným službám?

Odpovídají data v síti RFC standardům?

Nejsou časové informace o paketech podezřelé?

9. OBNOVA

Vrátit napadený systém do původního funkčního stavu a jeho zabezpečení.

Před obnovou, je třeba přesně znát rozsah poškození, typ a umístění poškozeného systému.

10. PROTOKOLOVÁNÍ

Pečlivě zdokumentovat všechny kroky pátrání a přijatých bezpečnostních opatření

Kompletně zdokumentovat průběh incidentu.

11. POUČENÍ

Analyzovat celý proces případu, poučit se z chyb a napravit všechny bezpečnostní

nedostatky systému.

Přednáška č. 10.

AUIDIT/PENETRAČNÍ TEST

1. Metodika OSSTMM
http://www.isecom.org/osstmm/

Smlouva
- souhlas s testováním, podrobný popis toho, co a kdy testovat
- kontakty
- odkud budou testy probíhat (IP adresy)

1.1 Rozsah testů

Testovací plán
- časový harmonogram testů

1.2 Informace o organizaci

- WHOIS
- DNS

1.3 Přítomnost organizace v Internetu

- WEB servery, FTP servery atd.
- veřejně dostupné informace (noviny, články, konference, chaty, produkty)

1.4 Analýza dostupných dokumnetů

- telefonní seznamy
- e-mail adresy
- osobný stránky zaměstnanců
- analýza zveřejňovaných dokumentů
- extrakce skrytých dat z dokumentů zveřejňěných organizací
(Black Hat Europe 2009: Tactical Fingerprinting Using Metadata. Hidden Info and Lost Data – Chema Alonso, Enrique Rando)

1.5 Testování technologií

- identifikace technologií organizace dostupných z Internetu
- skenování portů

skenování portů
nmap

detekce typů a verzí služeb a operačních systémů

nmap -sV
nmap -sC
NetCat
nmap -O

Pasivní

odposlech
Siphon

Fyzicky

prohledávání odpadků
poslouchání zaměstnanců
pozorování

Sbírání informací přímým kontaktem

1.6 Testování služeb

Automatizované nástroje

Nessus
OpenVas

Testování konkrétních služeb a aplikací

Autentizace
Relace
Manipulace se vstupy
Manipulace s výstupy
Prosakování informací

1.6.1 WEB

Metodika OWASP
http://www.owasp.org
OWASP_Testing_Guide_v3
Získávání informací

1.6.1.1 Web mirroring

GNU wget

http://www.gnu.org/software/wget/

HTTRACK
http://www.httrack.com/

Vyhledávače
http://www.google.com

1.6.1.2 Identifikace aplikací

1.6.1.3 Analýza chybových hlášení

1.6.1.4 Testování konfiguračního managementu
SSL, databázové porty, soubory se starými zálohami
administrátorská rozhraní

1.6.1.5 Testování logiky

1.6.1.6 Testování autentizačních mechanizmů

nešifrované autentizační údaje
hrubá síla
síla šifer

1.6.1.7 Testování autorizace

path traversal
obcházení autorizačního schématu
eskalace privilegií

1.6.1.8 Testování managementu relací

cookies, session fixation, dostupné parametry relace (SESSIONID)

1.6.1.9 Testování validace dat

XSS
SQL Injection
LDAP, ORM, XML, SSI Xpath, IMAP/SMTP, Code injection
OS Commanding
Buffer overflow

1.6.1.10 Testování DoS

Zamykání uživatelských účtů

zaplnění disků
alokace zdrojů

1.6.1.11 Testování služeb

XML
SOAP

Ajax

Automatizované nástroje

w3af
http://w3af.sourceforge.net/

sqlmap
http://sqlmap.sourceforge.net/

Proxy server

BurpSuite
http://portswigger.net/suite/
WebScarab

http://www.scribd.com/doc/28590479/Black-Hat-Webcast-Pen-Testing-the-Web-with-Firefox

Komerční:

Accunetix web vulnerability scanner

E-mail (viz. viry a sociální inženýrství)

Přednáška č. 11

1.6.2 Databáze

Scuba
http://www.imperva.com/products/scuba.html

AppDetective

1.6.3 VoIP

http://www.voipsa.org/

1.6.4 Router/Firewall

- odolnost proti útokům směrovaným na samotný IDS
- testování pravidel
- kapacitní testy
- testování autentizace

hping

Firewall Tester FTester
http://www.secguru.com/link/firewall_and_ids_testing_tool

1.7 Testování důvěry

1.8 Testování IDS

- pokrytí
- pravděpodobnost falešných poplachů
- pravděpodobnost úspěšné detekce útoku
- odolnost proti útokům směrovaným na samotný IDS
- schopnost zpracovávat velké toky dat
- schopnost korelovat události
- schponost detekovat nové, dosud neznámé útoky
- schopnost správně identifikovat útok
- schopnost detekovat zdroje útoků
- kapacitní testy NIDS

Nástroje:
Snot
Sneeze
Stick
Mucus
IDSWakeup

Fpg (http://www.geschke-online.de/FLoP/fpg.8.html)
snortspoof.pl
(http://trac.cipherdyne.org/trac/fwsnort/browser/fwsnort/branches/fwsnort-1.0.3/snortspoof.pl)

1.9 Testování možnosti průniku škodlivého kódu

- e-mail
- web

- Antivir
- sap 27
- eicar (http://www.eicar.org)

1.10 Testování síly hesel

- cracking

John the Ripper
http://www.openwall.com/john/

- hrubá síla (bruteforce)

Hydra
http://www.thc.org/thc-hydra/

1.11 Testování DoS

1.12 Testování klientů

http://bcheck.scanit.be/bcheck/
Metasploit Framework

http://nsslabs.com/browser-security

1.13 Kontrola bezpečnostních politik

SSA (OVAL)
http://www.security-database.com/ssa.php

1.14 Testování komunikační bezpečnosti

- VoIP
- PBX
- faxy
- e-mail
- hlasové schránky

1.15 Testování bezdrátových sítí

- EMR

Tempest

- 802.11
- Bluetooth
- Klávesnice, myš
- RFID
- Mobilní zařízení

- infrared

1.16 Fyzická bezpečnost

Perimetr
Vstupy/výstupy
Ploty, brány, osvětlení, kamery
Nemonitorované oblasti

Testy monitorovacích zařízení

Testy vstupních zařízení

Testy alarmů

Sociální Inženýrství

VisualSniffer www.biovisualtech.com
Etherape http://etherape.sourceforge.net