NetSikkerhedstest for Eksempel A/S

1. oktober til 26. oktober 2005

Henrik Lund Kramshøj

NetSikkerhedstest for Eksempel A/S: 1. oktober til 26. oktober 2005

af Henrik Lund Kramshøj

Indholdsfortegnelse

Kapitel 1. Fortrolighed

Alle informationer, som er indeholdt i denne rapport, er fortrolige. Informationerne vil kun være tilgængelige for personer, som er direkte involveret i scanningen, og som er sikkerhedsgodkendte.

Informationerne indeholdt i denne rapport vil kun blive videregivet til tredjemand efter samtykke fra Henrik Kramshøj eller dennes stedfortræder.

Kapitel 2. Scanningen

Scanningen er foretaget med en række forskellige værktøjer - blandt andet en portscanner som alene tjener det formål at kontrollere, hvilke porte der svarer, samt forsøge at konstatere hvilket operativsystem der bruges på baggrund af TCP/IP fingeraftryk.

Derudover benyttes et decideret penetrationsværktøj, som kontrollerer de forskellige porte mod en database med sårbarheder. Dette værktøj tester også i hundredvis af forskellige exploits. Det vil sige, at det konstaterer, hvorvidt forudsætningerne er til stede for, at en hacker kan udnytte et kendt hul.

Udover benyttelsen af værktøjer udføres en lang række manuelle tests og søgninger i eksterne databaser. Dette gøres dels for at kontrollere resultatet fra scanningsværktøjerne, dels for at kontrollere om der er nyopdagede huller og dels for at supplere den ufuldstændige information et program eller en enkelt database råder over.

Hvor det er muligt er der opgivet referencer til producentens egne sider omkring beskrivelse af kendte sårbarheder. Disse er suppleret med Common Vulnerabilities and Exposures indeksnumre (CVE/CAN), der fungerer som krydsreference mellem internationalt anerkendte sårbarhedsdatabaser. Beskrivelsen af de enkelte CVE kan tilgås via søgeformularer på adressen http://cve.mitre.org/cve

Kapitel 3. Forudsætninger

Afhængig af de informationer der er tilgængelige om opbygningen af det scannede netværk forud for NetSikkerhedsanalysen taler man om henholdsvis White, Grey og Black Box testning.

Black Box testen involverer en sikkerhedstestning af et netværk uden nogen form for insider viden om systemet udover den IP-adresse, der ønskes testet. Dette svarer til den situation en fjendtlig hacker vil stå i og giver derfor det mest realistiske billede af netværkets sårbarhed overfor angreb udefra.

I den anden ende af skalaen har vi White Box testen. I dette tilfælde har sikkerhedsspecialisten både før og under testen fuld adgang til alle informationer om det scannede netværk. Analysen vil derfor kunne afsløre sårbarheder, der ikke umiddelbart er synlige for en almindelig angriber. En White Box test er typisk mere omfattende end en Black Box test og forudsætter en højere grad af deltagelse fra kundens side.

En Grey Box test er som navnet siger et kompromis mellem en White Box og en Black Box test. Typisk vil sikkerhedsspecialisten udover en IP-adresse være i besiddelse af de mest grundlæggende systemoplysninger: Hvilken type af server der er tale om (mail-, webserver eller andet), operativ systemet og eventuelt om der er opstillet en firewall foran serveren.

Kapitel 4. Sårbarhedsanalysens omfang

Denne sårbarhedsanalysen er foretaget på indersiden af firewall og omfatter følgende IP-adresser/servere:

- 192.168.1.1
- 192.168.1.11
- 192.168.1.12
- 192.168.1.13
- 192.168.1.14

Oversigten inkluderer både interne og eksterne adresser for at beskrive sammenhængen mellem de eksterne kendte adresser og indersiden af firewall.

Til yderligere information kan det bemærkes at den oplyste sammenhæng ikke er rigtig! Denne rapport der viser resultaterne fra testen hos Eksempel A/S udført med direkte tilkobling til det interne netværk kan således ikke direkte sammenholdes med rapporten der er udført fra Internet mod Eksempel A/S.

Sårbarhedsanalysen inkluderer en portscanning, servicebetingede manuelle tests, samt kortlægning af mulige DoS-angreb (Denial of Service).

Testen er udført fra serverummet og med direkte forbindelse til det interne netværk.

Testen er udført af Henrik Lund Kramshøj den 26. oktober 2005 hos Eksempel A/S.

Kapitel 5. Sikkerhedsevaluering

5.1. Sammendrag af IP-adresse 192.168.1.1

5.1.1. Forudsætninger

Kunden har ikke oplyst hvad type server der findes på denne IP-adresse.

5.1.2. Resultat

På denne IP-adresse blev følgende porte fundet åbne. Den angivne protokol er enten den typiske på denne port, eller den fundne service.

Port	Status	Service
25/tcp	open	smtp
80/tcp	open	http
135/tcp	open	msrpc
139/tcp	open	netbios-ssn
161/tcp	open	snmp
443/tcp	open	https
445/tcp	open	microsoft-ds
1027/tcp	open	IIS
1029/tcp	open	ms-lsa
1031/tcp	open	iad2
1059/tcp	open	nimreg
1428/tcp	open	informatik-lm
1432/tcp	open	blueberry-lm
1437/tcp	open	tabula
1536/tcp	open	ampr-inter
1921/tcp	open	unknown
2301/tcp	open	compaqdiag
3372/tcp	open	msdtc
3628/tcp	open	unknown
5005/tcp	open	unknown
5168/tcp	open	unknown
5169/tcp	open	unknown
6101/tcp	open	VeritasBackupExec
6129/tcp	open	unknown
8331/tcp	open	unknown
49400/tcp	open	compaqdiag
135/udp	open	epmap
137/udp	open	netbios-ns
138/udp	open	netbios-dgm

```
161/udp   open    snmp
445/udp   open    microsoft-ds
500/udp   open    isakmp
1047/udp  open    neod1
1048/udp  open    neod2
3000/udp  open    hbci
3456/udp  open    vat
32789/udp open    unknown
```

De resterende porte er ikke fundet tilgængelige.

5.1.3. Nærmere undersøgelse

Ved nærmere undersøgelse af IP-adressen blev operativsystemet identificeret yderligere som værende Microsoft Windows 2000.

Følgende systemoplysninger blev indsamlet:

- hostnavne: srv1
- Interne IP-adresser: 192.168.1.1

5.1.4. DoS - Denial of Service

Der er forsøgt enkelte ude af drift angreb på serveren.

5.1.5. Svagheder

Der er på serveren fundet sårbarheder.

- SMTP serveren er tilsyneladende ikke nødvendig for denne servers funktion og bør defor stoppes
- Webservere på port 80 og port 443 er tilsyneladende ikke nødvendige for denne servers funktion og bør defor stoppes
- Webserveren på port 80 afvikles med tilgængelig WebDAV funktionalitet, Internet Printing Protocol - printprotokol over HTTP, Frontpage extensions, IDA ISAPI filter

  Følgende CVE numre er relevante: CAN-2000-0649, CAN-2000-0114, CVE-2001-0500
- Port 445 microsoft-ds kan benyttes til at finde Security Identifier SID for systemet og yderligere udnyttes til at finde brugere på systemet:
  - `Administrator account name : Administrator (id 500)`
  - `Guest account name : Guest (id 501)`
  - `TsInternetUser (id 1000)`
  - `IUSR_BLK-SRV (id 1001)`

  - `IWAM_BLK-SRV (id 1002)`
  - `ASPNET (id 1003)`

- Af de fundne brugere har 4 aldrig skiftet kodeord:
  - `TsInternetUser`
  - `IUSR_BLK-SRV`
  - `IWAM_BLK-SRV`
  - `ASPNET`
- Den eneste bruger der er låst er Guest brugeren
- HP/Compaq diagnostics på port 2301 og 49400 er en sikkerhedsrisiko fordi den afslører et væld af informationer om systemet. Såfremt den ikke benyttes aktivt bør den stoppes.
- SNMP på port 161 svarer med default community name 'public' og bør stoppes eller konfigureres til et andet community. Denne service afslører et væld af information om systemet.
- Det er tilladt at lave NULL session og dermed kan serveren tilgås som gæstebrugeren 'guest'. Se yderligere: CAN-1999-0504, CAN-1999-0506, CVE-2000-0222, CAN-1999-0505, CAN-2002-1117 og MS KB Article Q143474 (NT 4.0) og Q246261 (Windows 2000).

5.1.6. Anbefaling

Det anbefales at opdatere konfigurationen af serveren for at gøre det sværere for en angriber at undersøge denne:

- Overflødige services bør stoppes
- Det anbefales at serveren opdateres jævnligt
- Det anbefales at konfigurere de nødvendige services sikkert og derfor hærde serveren yderligere
- Det anbefales at serveren testes regelmæssigt, for at minimere risikoen for indbrud. Der findes jævnligt sårbarheder i de mest benyttede serverprogrammer

5.1.7. Risikovurdering

Vi har vurderet det samlede sikkerhedsniveau på denne host set fra denne forbindelse til at være medium.

Der er adgang til for mange porte og unødvendige services, det trækker ned i vurderingen.

5.1.7.1. Fortrolighed: Medium risiko

- Der er et antal services der trivielt kan spørges om information fra denne server. De almindelige adgangsveje til serveren er ikke blokeret tilstrækkeligt og en dedikeret angriber vil formentlig kunne udnytte de tilgængelige services til at skaffe sig adgang

5.1.7.2. Integritet: Lav risiko

- Serverens funktion er ukendt og derfor kan der ikke gives yderligere estimat på risikoen. Serveren bør hærdes behørigt såfremt data på serveren har værdi.

5.1.7.3. Tilgængelighed: Lav risiko

- Der er ikke yderligere bemærkninger til tilgængeligheden af systemet. Systemet viste ikke tegn på nedbrud eller forringet funktionalitet under testen.

Kapitel 6. Konklusion

Sikkerhedsniveauet på Jeres server/servere er vurderet til at være medium, primært fordi der er fundet unødvendige åbne services og megen unødvendig funktionalitet på serverne under testen.

Serverne giver således indtryk af ikke at være hærdet behørigt før placering på Internet!

Opbygningen af netværket virker ufornuftig med brug af hub fremfor switch og der hersker nogen tvivl om opbygningen af netværket. Den visuelle inspektion og placering gør det svært at indse om netværket er konfigureret fornuftigt.

Vi kan overordnet anbefale, at der tages følgende tiltag for at optimere sikkerheden på jeres installation:

- Den fysiske placering af Internetforbindelse og adskildelse mellem farlige forbindelser og interne netværk skal tydeliggøres - eksempelvis ved at flytte enhederne sammen og på separate hylder i serverrummet. Alternativt kan farvede kabler benyttes til at sikre at der ikke skabes forbindelse mellem eksterne netværk og routere der kan give adgang internt
- Det anbefales at benytte switche fremfor hubs til DMZ zoner - medmindre det er et bevidst valg for at lette implementering af IDS
- Firewalls bør indstilles til ikke at svare aktivt på portscan
- Det anbefales at hærde servere generelt før placering med adgang fra åbne netværk
- Fortsat have fokus på opdatering af software på servere - herunde at undgå at visse servere halter for langt bagefter. Det er ikke tidsvarende at benytte en NT server i produktion idag
- Hvis funktionalitet ikke benyttes kan services med fordel omkonfigureres eller stoppes
- Det anbefales at især webservere, navneservere og postservere testes regelmæssigt