3 Firewall/brandvägg, systemscanner och forensisk analys

Table of Contents

Betygsnivåer. VG: Klara alla frågor som ställts tillräckligt bra. G: En mindre undersökning, tex. bara en firewall behandlad i uppgift 3.2 samt inga uppgifter utförda eller felaktiga i uppgift 3.3.

3.1 Sammanfattning av uppgifterna i examinationen

Vi ska i denna laboration utvärdera några brandväggslösningar och utnyttja teknik vi lärt oss i föregående laborationer. Vi kan i uppgiften ha nytta av en systemscanner vilken kan hitta system- och konfigurationssvagheter.

Vi ska även i laborationen utföra en forensisk dataundersökning av några imagefiler (spegelkopior av datamedia) från en fingerad digital brottsplats.

När du är klar med uppgifterna så lägg dina svar från i labben i en mapp, komprimera mappen och lämna in den packade filen.

3.2 Firewall och systemscanning

Gör en Internetsökning på open source firewall eller free firewall. Tanka hem några brandväggslösningar som passar din datormiljö. Här är exempel på några sidor med brandväggar jag hittade:

- https://en.wikipedia.org/wiki/Comparison_of_firewalls
- https://en.wikipedia.org/wiki/List_of_router_and_firewall_distributions
- http://www.wilderssecurity.com/showthread.php?t=57655
- http://www.thefreecountry.com/security/firewalls.shtml

Installera och sätt upp några av dessa brandväggslösningar på din virtuella/fysiska dator eller i hemmanätverket/företaget. Använd gärna någon bok för hjälp eller resurser på internet för exempel på jämförelse och fallstudie.

Kör du GNU/Linux eller MacOS kan du testa med liknande brandväggslösningar och/eller netfilter/iptables om du har kunskap att sätta upp en sådan lösning. Referensinformation och tutorials om hur man gör finns på: http://www.netfilter.org. Detta ger en mycket kraftfull och flexibel lösning.

Om du har en enkel NAT-router (de flesta accesspunkter för hemmet eller mindre företag har en enklare firewall inbyggd) eller en fri/kommersiell brandvägg hemma eller i företaget, jämför även mot den om möjligt.
Ofta har operativsystemet en personlig firewall installerad redan som du också kan jämföra mot.

Att testa din egen dator/router/accesspunkt utifrån internet kan göras med en scan-tjänst som tex. shieldsup. Du kan även sätta din dator som DMZ eller direkt i WAN uttaget om den ska kunna nås utifrån utan inblandning av NAT-routern.

Du kan jämföra med tex. att ha den personliga firewallen påslagen och avslagen när du scannar med verktygen. Nessus letar dock endast efter sårbarheter på vissa portar.

Om du inte kan ordna eller har tillgång till en serverbaserad firewall så kan du redovisa det teoretiska runt en sådan. Du kan även attackera nb-hjo.du.se [130.243.36.2] som ligger bakom skolans firewall och testa vissa av attackverktygen.

Det är mycket svårt att testa firewalls och resultatet kan vara svårt att tolka. Du behöver lägga ner ett antal timmar på delmomentet (kursens totala antal timmar dividerat med antalet delmoment). Momentet har stor frihet i hur det utförs och du måste ha egna lösningar på de problemställningar som angivits, eftersom miljön för uppgiften kan vara väldigt olika studenter emellan.

Några verktyg vi kan att använda för att testa brandväggen är:

- Nmap, http://www.insecure.org/nmap/download.html – portscanner som med speciella växlar kan försöka ”gå igenom”filtreringen i en firewall.
- Nessus/NessusWX, http://www.nessus.org/ - systemscanner som hittar kända och okända system- och konfigurationssvagheter. Detta är inte ett verktyg för att testa en brandvägg men kan ge en bild av säkerhetsläget för öppna portar.
- FTester (Linux), länk till artikel som beskriver hur verktyget används - http://www.howtoforge.com/test_your_linux_firewall_with_ftester
- Verktyg i Kali Linux som tex. Firewalk.
- HoneyBOT, http://www.atomicsoftwaresolutions.com/ kan användas för att registrera och samla in attacker/trafik på olika portar.
- Webbsidor som: https://www.grc.com/shieldsup
- Eller verktyg fritt valda av er själv. Kali Linux har det mesta inbyggt redan, dock ej Nessus men det kan laddas ner och installeras med ett enkelt kommando.

Frågor

- Av vilken typ är brandväggarna?
- Vilka egenskaper/funktioner finns i dem?
- Vilka fördelar och nackdelar finns med respektive lösning?
- Din uppfattning om prestanda, autentisering, säkerhet, tjänster?
- Din uppfattning om gränssnitt, administration, dokumentation?
- Verifiera funktionen och ange ditt omdöme av de brandväggar du använt praktiskt i momentet. Dvs. testa firewallens funktioner praktiskt. Vad händer tex. om en scanning utförs mot victim? Hur ställer man in firewallskyddet osv.

- Attackera med Nmap, Nessus eller lämpligt verktyg utifrån, kontrollera firewall-loggen och verktygslogg. Tänk på att när du attackerar med Nmap så måste du använda TCP paket (ACK scans tex.) som är formaterade att kunna gå igenom firewallen.
  Principen bakom en ACK scan är att lura firewallen att insidan redan har en uppkoppling SYN (som den inte har) mot utsidan och att utsidan svarar med SYN-ACK eller bara ACK. Vissa brandväggar kan i detta scenario släppa igenom trafik, speciellt om de är av typen stateless.

Redovisning
Skriv en rapport som jämför/utvärderar firewall-lösningarna. Du bör om möjligt ha med minst 3 olika brandväggar i jämförelsen, helst av olika typ. Dvs. personlig, NAT-router, serverbaserad etc. Där den serverbaserade i många fall troligen blir en teoretisk jämförelse. Tänk på att skyddet kan finnas på olika nivåer som stateless/stateful och i applikationslagret. Om du även kan utföra en sårbarhetsscanning mot någon victim-dator så är det bra.

3.3 Digital forensics - MBR (Master Boot Record)

Vi ska utföra en forensisk dataundersökning av några imagefiler (spegelkopior av datamedia). En digital brottsplatsundersökning liknar i stort en vanlig brottsplatsundersökning. De tre steg som normalt utförs vid en digital brottsplatsundersökning är:

1. Samla in och kopiera data utan att förstöra eller förändra orginaldata och bevis därmed försvinner eller blir ogiltigt.
2. Analysera kopiorna (inriktningen sker ofta utifrån brottsmisstanken). Gärna med olika verktyg för att verifiera samma resultat.
3. Skriv en rapport över de resultat undersökningen gav.

Punkt ett har redan utförts av din medarbetare i detta fall. Ladda hem och packa upp filen forensic_cases.zip som finns i samma mapp som labben. I filen finns 6 binära filer som skall undersökas.

Case-0 till och med case-3 representerar endast första sektorn, dvs. MBR (Master Boot Sector) från ett lagringsmedium som hårddisk, USB minne, diskett etc. Med ledning av informationen bör du kunna lista ut en hel del om vilket media den sparade sektorn kommer ifrån.
Till din hjälp kan du använda en hex-editor eller annat forensiskt verktyg som låter dig undersöka data på låg nivå. Lite information om hur det kan se ut i MBR finns här:
http://en.wikipedia.org/wiki/Master_boot_record

Verktyg som är lämpliga för detta arbete är:

- Active Disk editor - http://www.disk-editor.org/ - Ett väldigt bra verktyg för att läsa metadata om lagringsmedia.Välj Actions > Open in disk editor.
- DiskExplorer, http://www.runtime.org – ger lite bättre hjälp än WinHex, välj File-> Image -> All files (*.*) för att öppna *.dat-filer.
- WinHex, http://www.x-ways.com/ – en manual finns även (winhex.pdf)
- FTK Imager, http://accessdata.com/product-download
- En lista med hex editorer, http://en.wikipedia.org/wiki/Comparison_of_hex_editors
- Andra liknande verktyg, det finns fler att välja på.

Redovisning
Försök hitta så mycket MBR-information som möjligt från innehållet i varje fil. Presentera resultatet från din undersökning i en tabell eller annat lämpligt format.

3.4 Digital forensics - Forensiskt case

I filen filen forensic_cases.zip består case-4 och case-5 av spegelkopior (image) från disketter.

Din första uppgift blir att ta hashen på dessa (MD5 eller SHA1) så integriteten av mediat du undersöker kan garanteras, spar hash-informationen till en fil, verifiera gärna hashen med fler verktyg.

Din andra uppgift blir att undersöka dessa case (case-4 och case-5 filerna) efter bevis om en man (ägaren till disketterna) som sysslar med ”computer stalking”, dvs. förföljer någon på nätet via e-mail etc. I detta case skall det dels finnas en bild på offret - en kvinna och några e-mail som verkligen inte skulle vara roliga att få!

Verktyg som är lämpliga för detta arbete är:

- Forensic ToolKit (FTK) och FTK imager: http://www.accessdata.com. Detta är professionella verktyg för undersökning av datamedia. FTK-Forensic_Toolkit-1.81.6 som finns i lab-mappen fungerar i demoläge upp till 5000 filer och FTK imager är fri att använda. Bra hjälp ingår i programmen.
- OSForensics: http://www.osforensics.com/
- WinHex (Xways forensics) funkar, men inte så bra (restriktiv licens).
- Autopsy och The Sleuth Kit: http://www.sleuthkit.org/ - är avancerade verktyg (grafiska och console) för både Windows och Linux.
- Hashtab: http://implbits.com/ - beräknar hash.
- EXIF InfoTip eller ExifTool, använd sökmotor för att hitta.
- Andra liknande verktyg, det finns fler att välja på.

Mer information, verktyg etc. och tillvägagångssätt finns på följande platser:

- http://www.forensicswiki.org/
- https://en.wikipedia.org/wiki/Computer_forensics

Redovisning

- Fiska ut (extrahera) bevisen (de otrevliga e-mailen och bilden) med hjälp av verktygen.
- Vad heter mannen som sysslar med ”computer stalking”?
- Bifoga filer med hashsumman på de två kopiorna.
- Vilken Exif information finns det i bilder?

Skriv en rapport med dina resultat och förklaringar där du hänvisningar till de funna bevisen.