Anteckningar

Vecka 1 - Introduktion

Mest använda IPS/IDS är Snort och Suricata. System för att få in regler till IPS/IDS är Pull pork och oinkmaster.

Security Onion är ett kit som innehåller antivirus, IPS, IDS, loggning, brandvägg o.s.v.

Honetrap är nästa nivå av honepots. Den sparar resultat efter körning.

Vi får 16 adresser per grupp för hosts. Smidigt att köra NAT på ett privat management VLAN. En port för mirroring till IDS (datorn för analyssystemet security onion). Den servern ska även ha en riktig address som är åtkomlig. Ett par honeypot kanske.

Han vill ha rapport om brandväggsregler och SNORT-regler. LaTeX-skriven rapport. Två veckor från nu.

Maltego är ett verktyg som letar efter krossreferenser. Hämta information på nätet och mata in i maltego.

Vecka 2 - Pentesting

För 20-30 år sedan hade man en synkron hotbild - enade stater mot andra enade stater, stat mot stat, företag mot företag eller person mot person. Efter elfte septemper-attacken såg man att stater kan gå mot enskilda personer, enskilda personer kunde hota sammanslutna stater m.m. Det har blivit svårt att förutse beteendent. Tidigare kretsade intresset kring stater - idag ligger det i kunskap om produktutveckling m.m.

Hacktivism

Organisationer som vill framhäva något - få ut sitt budskap. Innan sociala medier m.m. var en grupp väldigt homogen. Antingen tillhörde man en grupp eller inte. Idag finns inte samma lojalitet bland grupper - en person kan röra sig kring flera grupper / nätverk.

Cyber warfare

Stuxnet var det första riktiga cybervapnet. Ursprunget tycks vara USA och Israel. Målet var att förstöra Irans kärnanrikningsanläggning. Mjukvaran var väldigt inriktad för ett specifikt system och kördes aldrig någon annanstans. Spreds via ett USB-minne. Viruset spelade in all data den kom över och sedan spelade den upp datan igen - men i bakgrunden plockade det bort säkringar och körde systemet så att det havererade.

Botnets

Infekterade datorer som är del i ett nätverk av andra datorer. Alla maskiner kommunicerar med så kallade command and control servrar. CC-servrar är distribuerade och ofta svåra att stänga ned.

Övrigt

Ransomware, Phishing, Vishing, Web exploits m.m, social engineering, spearphishing.

IT-säkerhetsprinciper

Vart drar du gränsen? En information system perimiter förklarar vad som räknas till dina system som du litar på och resten av världen.

Terminologi

- Weakness
    - En sårbarhet som möjliggör en attack
- Exposure
    - En åtkomstpunkt till sårbarheten
- Vulnerability
    - En instans av sårbarheten
- Exploit
    - Ett sätt att utnyttja sårbarheten
- 0-Day
    - Noll dagar från att sårbarheten tillkännagivits
- Threat
    - Ett potentiellt event som hotar ett system
- Risk
    - Sannolikhet att ett hot genomförs

Hacker-typer

- Hacktivists
- Black-hat
- White-hat
- Grey-hat
- Script kiddies
- Suicide hackers

Standarder

- NIST 800-115
    - Planering
    - Upptäcka
    - Attacken
    - Rapportering
- EC-Council, CE|H (Certified Ethical Hacker - vanligast)

    - Undersökning
    - Scanning
    - Få åtkomst
    - Upprätthåll åtkomst
    - Sopa igen spåren
    - Rapportering
- PTES
- Open Source Security Testing Methodology Manual (OSSTMM)
- ISO / IEC 17799:2005 och 27000-serien
- Payment Card Industry Data Security Standard (PCI DSS)

Rapport

Resultatet bör få VDn att inse att kostnaden ger resultat. De bör få förståelse för vad som händer. Rapporten bör ha innehåll för följande grupper:

- Manager CIO
- Middle manager
- Engineer Administrator
    - Windows server
    - Database admin
    - Web admin
    - Linux admin

Vecka 2 - Repetition nätverksprotokoll

En UDP-tjänst svarar med ICMP "Port unreachable" om exempelvis DNS-förfrågningar fås. TCP svarar med Reset Ack (döda förbindelsen). Normal avstängning är Fin Ack.

ARP

Närmst nätverket använder vi ofta ARP. ARP hittar MAC-adressen som hör till en IP-adress. ARP frågar nätverket genom en broadcast och litar på ett unicast-svar, något som är osäkert. Man kan *flood:a* en router och PC med tillverkade svar för att få ut sin egna MAC-adress genom så kallad ARP-poisoning. Detta används vanligtvis för så kallade MITM-attacker. Man kan motverka detta till viss grad genom att låsa tabellen i routern efter en enda uppdatering (learning mode - LM). ARP Watch är ett verktyg som kan kontrollera paket för att jämföra MAC-adresser. Verktyget varnar om någon utger sig för att vara någon annan.

ICMP

ICMP är informationsmeddelanden så som ping (ICMP request och ICMP response). Det har inga portnummer, ingen client / server etc.

0: Echo Reply 5: Destination Unreachable 6: Source Quench 7: Redirect 8: Echo 11: Time exceed ...

Source quenche - be källan att lugna ner sig (roll back / kick back). Detta ligger i drivrutinen. Vi kan använda detta för att skicka ut detta meddelande till andra på nätverket.

Error:

- Host unreachable
  - router skickar detta när den inte får svar på ARP
- Port unreachable
  - host som tar mot paketet skickar detta när porten inte används
- Admin prohibited
  - enligt spec. det som ett brandvägg ska skicka om request nekas
- Redirect
  - default gateway skickar vidare ett paket till en mer optimal route
  - default gateway skickar redirect till hosten för att den ska använda optimal route
- Fragmentation required, DF flag set
- Time exceeded
  - traceroute använder TTL och kan använda TCP / UDP / portar etc
  - Routern där TTL går över till 0 skickar ICMP time exceeded in transit
- Reassembly time exceeded

Farliga ICMP

Smurf-attack är en amplifikationsattack där man använder broadcast-addresser för att skicka spoofade paket (stora ping etc.).

WinFreez är en attack där man utnyttjar ICMP redirect för att skicka alla paket från ett offer till offret själv.

Tribe Flood Network (TFN) använder ICMP reply för att styra ett botnet som skickar ICMP echo request floods, UDP-floods och TCP:SYN-floods m.m. till ett offer.

Loki använder ICMP request / reply för dold kommunikation

ICMP kan alltså användas för recon, DoS och en s.k. covert channel.

NMAP

NMAP skannar ett nätverk och kan identiferar tjänster och OS som körs. NMAP

```
# Visa användning
nmap | less

# Skanna igenom ett nätverk
nmap 194.47.149.0/26

# Använd en serie IP-adresser att skicka ifrån (decoys)
nmap target-ip -D decoy-ip1,decoy-ip2
```

NMAP script engine är ett kompetent verktyg vi bör använda.

Banner grabbing kallas metoden att testa en öppen tjänst för att se vad servern ger för svar i form av banner som kan innehålla intressant information.