# Auditarea Securitatii Retelelor

- Colectarea de informatii
- Scanare si enumerare

# Colectarea de informatii

- **Activitate pasiva** – nu se interactioneaza cu tinta
- Obtinerea de informatii utile in desfasurarea atacurilor:
  - Adresele IP externe ale companiei tinta (+ ISP-ul)
  - Subdomenii alocate
  - Numere de telefon si adrese de email ale angajatilor
  - Profile ale angajatilor (site-uri de socializare)
  - Metadate in documentele publice
  - Statii si servicii active in retea (pentest intern)
- Exemple:
  - Google hacking
  - Interogari Whois
  - Interogari DNS
  - Baze de date publice: Netcraft.com , zone-h.com
  - Inspectare site web
  - Network Sniffing

# Google Hacking

**Google Dorks:**

- **site:** - restrictioneaza rezultatele cautarii doar la site-ul specificat - ex: *site:pub.ro error*
- **intitle: / allintitle:** - cuvintele cautate se afla in titlul paginilor raspuns - ex: *intitle:"index of" config "parent directory"*
- **inurl: / allinurl:** - cuvintele cautate se afla in URL-ul paginilor raspuns - ex: *inurl:backup intitle:index.of*
- **filetype:** - specifica extensia fisierului cautat - ex: *filetype:doc site:pub.ro*
- **Incluziune explicita: + “”** - ex: *+123456 "yahoo.com" site:pastebin.com*
- **Excluziune explicita: -** - ex: *+virus -biology*

http://www.google.com/help/operators.html
http://www.hackersforcharity.org/ghdb/

# Google Hacking - Exercitii

1. Cautati toate fisierele de tip *xls* ce pot fi accesate de pe site-ul *xyz* 2. Verificati daca pe site-ul *xyz* se poate face directory browsing
3. Gasiti adrese de email ale angajatilor din firma *xyz*
4. Cautati toate posturile pe site-ul *softpedia.com* ale unei persoane gasite la cautarea anterioara
5. Gasiti subdomenii ale domeniului *xyz*
6. Faceti o cautare dupa expresia: *mysql dump filetype:sql* . Ce obtineti? 7. Cautati camere live pe web:

   *inurl:/view/index.shtml*

   *inurl:viewerFrame?Mode=*
8. Exersati tool-urile din Backtrack din directorul:

   */pentest/enumeration/google/*

# Interogari Whois

Se pot obtine informatii despre compania tinta precum:

- Servere de nume
- Intervalul de adrese IP alocat
- Locatia si adresa firmei
- Persoane de contact (nume, telefon, email)

**Exemplu:**

whois cisco.com

whois 128.107.241.185

**Exercitiu:**

Identificati spatiile de adrese IP alocate firmei *xyz*

# Interogari DNS

Utilitare: *dig, host, nslookup*

Tipuri de inregistrari DNS: ***A, NS, MX, PTR, AXFR***, etc

**Exemple:**

- Dorim sa aflam serverele de email pentru domeniul *pub.ro*:

  *dig pub.ro mx*

  *host –t mx pub.ro*

- Cerem serverului *ns1.roedu.ro* sa faca reverse DNS pentru IP-ul 141.85.166.60:

  *dig @ns1.roedu.net ptr 60.166.85.141.in-addr.arpa*

  *host 141.85.166.60*

**Exercitii:**

- Care sunt serverele de nume ale domeniului *xyz*?
- Pentru fiecare server de nume descoperit anterior, faceti cerere de transfer de zona (type=axfr)
- Exersati tool-ul urmator pentru extragerea de informatii DNS:

  */pentest/enumeration/dnsenum/dnsenum.pl*

# Scanare si enumerare

Activitati care implica interactiune cu tinta

Cereri repetate pentru obtinerea a diverse informatii:

- Statii pornite in retea (live hosts)
- Porturi deschise
- Versiuni ale serviciilor care ruleaza
- Sistemul de operare
- Network shares
- Local users
- …

# Host Discovery

Tehnica de a descoperi daca o statie/server este pornita si conectata la retea.

- ARP Ping
- ICMP Ping
- TCP SYN Ping
- UDP Ping

# ARP Ping

- Functioneaza numai in reteaua locala.
- Da rezultate false daca *proxy-arp* este configurat pe echipamentele de retea.
- **Tools:**
  - arping
  - nmap -PR

**Exercitiu:**

- Folosind metoda *ARP Ping* verificati daca statia victima este activa in retea sau nu.
- Vizualizati cu *tcpdump* dialogul ARP.

# ICMP Ping

RFC 792

**Echo request:**

nmap -sP -PE 192.168.1.1

ping 192.168.1.1

hping --icmp -C 8 -K 0 192.168.1.1

**Timestamp request:**

nmap -sP -PP 192.168.1.1

hping --icmp -C 13 -K 0 192.168.1.1

**Netmask request:**

nmap -sP -PM 192.168.1.1

# TCP SYN Ping

**TCP SYN Ping**

nmap –sP -PS80 192.168.1.1

hping -S -p 80 192.168.1.1

netcat -vv 192.168.1.1 80

telnet 192.168.1.1 80

**TCP SYN Ping, port deschis**

-------> SYN ------>

<------- SYN / ACK <------

**Port inchis**

-------> SYN ------>

<------- RST <------

Ambele raspunsuri indica prezenta statiei scanate

**Exercitiu**

- Porniti firewall-ul de pe statia victima si debifati orice exceptie • Faceti share la un folder de pe statia victima
- Verificati daca victima este ‘live’ folosind *arping.* Rezultate? • Verificati daca victima este ‘live’ folosind *ping.* Rezultate?
- Verificati daca victima este ‘live’ folosind *netcat* pe portul 445*. Rezultate?*

# UDP Ping

**Exemplu:**

nmap –sP –PU 9999 192.168.1.1

(--send-ip)

hping --udp –p 9999 192.168.1.1

**Situatia 1:**

-------> UDP packet ------>

<------- no response <------

**=> firewall** sau

**=> statie activa si port deschis**

**Situatia 2:**

-------> UDP packet ------>

<------- ICMP port unreachable <------

**=> statie activa si port inchis**

# Tipuri de scanari

- SYN Scan
- Connect scan
- ACK Scan
- NULL Scan, FIN Scan, Xmas Scan
- UDP Scan

# SYN Scan / Connect Scan

**Connect scan** (complete 3-way handshake)

nmap -sT -p 445 192.168.1.1

telnet 192.168.1.1 445

netcat 192.168.1.1 445

*(nu necesita drepturi de root)*

**SYN scan** (half-connect)

nmap -sS -p 445 192.168.1.1

hping -S -p 445 192.168.1.1

**Connect scan, port deschis**

-------> SYN ------>
<------- SYN / ACK <--------
-----> ACK ------> --
-----> RST ------>

**SYN scan, port deschis** -

------> SYN ------>
<------- SYN / ACK <--------
-----> RST ------>

**Port inchis**

-------> SYN ------>
<------- RST <------

# ACK Scan

- Verifica daca un port este filtrat sau nu de catre firewall
- Nu ofera nici o informatie despre starea portului (inchis/deschis)
- Exemplu:

  nmap –sA –p 445 192.168.1.1

**Situatia 1:**

-------> ACK ------>

<------- RST <------

**=> Firewall OFF, port deschis**

sau

**=> Firewall OFF, port inchis**

**Situatia 2:**

-------> ACK ------>

<------- no response or ICMP error msg <------

=> **Firewall ON**

# NULL Scan, FIN Scan, Xmas Scan

RFC 793

- NULL Scan – toate flag-urile TCP sunt 0
- FIN Scan – flag-ul FIN este setat
- Xmas Scan – flag-urile FIN, PUSH si URG sunt setate

**Exemplu:**
nmap –sX –p 445 192.168.1.1

**Situatia 1:**
-------> NULL/FIN/Xmas ------>
<---X-- dropped <------
**=> port deschis si firewall OFF** sau
**=> firewall ON**

**Situatia 2:**
-------> NULL/FIN/Xmas ------>
<------- RST <------
**=> port inchis, firewall OFF**

**Situatia 3:**
-------> NULL/FIN/Xmas ------>
<------- ICMP unreachable <------
**=> firewall ON**

# UDP Scan

Acelasi principiu ca la UDP Ping

**Exemplu:**

nmap –sU –p 53 192.168.1.1

**Situatia 1:**

-------> UDP packet ------>
<------- no response <------
**=> firewall sau**
**=> statie activa si port deschis**

**Situatia 2:**

-------> UDP packet ------>
<------- ICMP port unreachable <------
**=> statie activa si port inchis**

# Alte optiuni *nmap* (1)

- Detectarea versiunii serviciilor:

  nmap **–sV** 192.168.1.1

- Detectarea sistemului de operare:

  nmap **–O** 192.168.1.1

# Alte optiuni *nmap* (2)

- Specificarea target-ului: nmap 192.168.1-254.1-254
  nmap 192.168.0.0/16 nmap –iL iplist.txt
- Specificarea porturilor: nmap –p21,22,80,445 192.168.1.1
  nmap –p1-65535 192.168.1.1 *(implicit nmap scaneaza 1660 porturi)*
- Scrierea rezultatului scanarii intr-un fisier:
  nmap –oN output.txt 192.168.1.1
- Viteza de scanare:
  nmap –T<0-5> 192.168.1.1 *(mai mare inseamna mai rapid)*
- Fara rezolvare DNS: nmap –n 192.168.1.1
  *(mai rapida si mai putin „zgomot")*

# Exercitiu (nmap)

- **Folosind nmap faceti o singura scanare care sa indeplineasca conditiile:**
  - Target: ip-urile 1,5,7,20-25 din subnetul masinii virtuale atacator
  - Porturi: TCP 21,80,139,445 si de la 1024 la 1030
  - Tipul scanarii: full connect
  - Scrieti rezultatele in fisierul output.txt
  - Viteza de scanare sa fie mica (-T2)
  - Parallel scan?

- **In paralel porniti Wireshark si vizualizati packetele care se transmit**
  - Deduceti ‘ce se intampla’

# Enumerare

- Interogarea serviciilor descoperite pentru a obtine informatii disponibile

- Vom folosi scripturi nmap (.nse):
  dpkg –L nmap
  => /usr/share/nmap/scripts

- Categorii de scripturi:
  *default, discovery, auth, safe, intrusive, exploit, dos, vuln*

- **Exemple:**

nmap --script smb-enum-shares.nse -p 445 –n 192.168.1.1
nmap --script smb-enum-users.nse -p 445 –n 192.168.1.1
nmap --script discovery 192.168.1.1
nmap --script dns-zone-transfer.nse
--script-args dnszonetransfer.domain=abc.xyz.com -
p 53 ns.xyz.com

# Exercitiu

- Scanati intreg subnetul la care este conectata placa de retea *vmnet8.*
- Obtineti urmatoarele informatii:
  - Statii active
  - Porturi deschise
  - Versiuni ale serviciilor care ruleaza
  - Sistemul de operare
  - Rezultatele scripturilor de *discovery*