Universitatea Politehnica Bucuresti
Facultatea de Automatica si Calculatoare
Master – Securitatea Retelelor Informatice Complexe

Auditarea Securitatii Retelelor

Laborator 1

- Colectarea de informatii
- Scanare si enumerare

Adrian Furtună, Ph.D.
adif2k8@gmail.com

Partea 1: 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)
- Tehnici:
  - 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 in your SQL syntax“`
  - intitle: / allintitle:
    - cuvintele cautate se afla in titlul paginilor raspuns
    - Ex: `intitle:"index of“ intext:”parent directory”`
  - 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

Alegeti un site preferat: *xyz*

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 subdomenii ale domeniului *xyz*
4. Faceti o cautare dupa expresia: `mysql dump filetype:sql .` Ce obtineti?
5. Cautati camere live pe web:
   ```
   inurl:/view/index.shtml
   inurl:viewerFrame?Mode=
   ```
6. Instalati si testati Foca:
   http://www.informatica64.com/foca/

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 companiei *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:
  1. Care sunt serverele de nume ale domeniului *xyz*?
  2. Pentru fiecare server de nume descoperit anterior, faceti cerere de transfer de zona (type=axfr)
  3. Exersati tool-ul urmator pentru extragerea de informatii DNS:
     - /pentest/enumeration/dnsenum/dnsenum.pl

Partea 2: 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
  - …

Descoperirea statiilor din retea

- Tehnica de a descoperi daca o statie/server este pornita si conectata la retea.
  - ARP Ping
  - ICMP Ping
  - TCP SYN Ping
  - UDP Ping

Scanarea porturilor

- Tipuri de scanari
  - SYN scan
  - Connect scan
  - ACK 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 de catre un firewall stateless sau ACL
- 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**

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

Nmap – optiuni (1)

- 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’)

Nmap – optiuni (2)

- Detectarea versiunii serviciilor:
  - `nmap -sV 192.168.1.1`

- Detectarea sistemului de operare:
  - `nmap -O 192.168.1.1`

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

- Folosind o singura comanda *nmap* scanati intreg subnetul la care este conectata placa de retea vmnet8.
  - Obtineti urmatoarele informatii:
    - Statiile active
    - Porturile deschise
    - Versiunile serviciilor care ruleaza
    - Sistemul de operare
    - Rezultatele scripturilor de discovery (--script discovery)
  - Scrieti rezultatele intr-un fisier

Intrebari

?