5. hét: Aktív információgyűjtés: DNS enumeráció, hálózat szkennelése, portok szkennelése, szkennelési módok, szolgáltatások azonosítása, Nmap

Tartalom

1. host discovery
2. port scan
3. service detection
4. exploit/metasploit

1. DNS (Domain name system)

- Mire jó? Számok helyett (IP cim) szavakat ("domain" név) kelljen megjegyezni. Az átváltás a DNS feladata.
- Korábbi versenytársa: NetBIOS name. Ma már egy gép teljes NetBIOS neve a domén névből származik. https://technet.microsoft.com/en-us/library/cc959322.aspx
- Egy IP címnek több domén neve is lehet, tehát a domén név nem nélkülözhető.
- DNS-t használó alkalmazásszintű protokollok: HTTP, SMTP, FTP stb.
- Parancsok: host (Linux), nslookup (Windows), dig (Linux)
- A DNS szervert a DHCP adja.
- ICANN által akkreditált regisztrátorok: http://www.internic.net/

1.1. Fontosabb DNS rekord fajták (record types)

Összes: https://en.wikipedia.org/wiki/List_of_DNS_record_types

record type	description
A	A host IPv4 címe
AAAA	A host IPv6 címe
MX	A domén email szerverének domén neve (A rekord)
NS	A domén névszerverének a domén neve (A rekord)
CNAME	Canonical naming allows aliases to a host. Points to an existing A record.
PTR	Reverse DNS: IP cím alapján domén név lekérdezése. Meg lehet adni tartományt.

1.2. host parancs

1. Minden rekordfajta lekérdezése.
```
host -t any gmail.com
```
2. "A" record lekérdezése
```
host -t A gmail.com
```
3. MX record (SMTP szerver) lekérdezése
```
host -t MX gmail.com
```
4. DNS rotation (load balancing): több IP cím, mindig más sorrend. Pl.
```
host -t A cnn.com
```
5. CNAME rekord lekérdezése (minek az alias-a a lekérdezett név):
```
host -t CNAME www.facebook.com
```
6. A NS rekord (nameserver) lekérdezése
```
host -t NS market.hu
```
7. PTR rekord: Reverse lookup
```
host -t PTR 216.58.214.229
```
8. Egy IP tartomány (pl. 91.82.217.131-140) doménneveinek reverse lookup lekérdezése
```
for ip in $(seq 131 140); do \
host -t PTR 91.82.217.$ip; done
```
```
nmap -vv -Pn -sL 91.82.217.131-140
```
9. Zone transfer
   1. Névszerverek listázása
   ```
   host -t ns zonetransfer.me
   ```
   Kimenet:
   2. Zone transfer megpróbálása
   ```
   host -l zonetransfer.me nsztml.digi.ninja
   ```
   3. A zone transfer lehetőségét jelezheti a nyitott 53-as TCP port
   ```
   nc -v nsztml.digi.ninja 53
   ```

2. Scanning válaszok

2.1. Port states

- open: egy alkalmazás hallgat (listening) az adott porton, vár kapcsolatokra vagy datagramokra,
- closed: nincs hallgató (listening) alkalmazás az adott porton,
- filtered: tűzfal miatt nem megállapítható, hogy nyitott-e vagy zárt,
- egyéb: unfiltered, open|filtered, closed|filtered.

2.2. UDP válaszok

open	closed	filtered	non-live host
Az adott service szerint értelmes válasz.	• ICMP Type: 3, Code: 3 (Port unreachable)	• ICMP Type: 3, Code: 10 (Host administratively prohibited) • (semmi)	(semmi)

2.3. TCP válaszok

TCP flags	open	closed	filtered	non-live host
SYN	SYN+ACK	RST, RST+ACK	(semmi)	(semmi)
Inverse scans **non-windows** • FIN, URG, PUSH (xmas) • FIN • (null scan)	(semmi)	RST	(semmi)	(semmi)
Inverse scans **Windows** • FIN, URG, PUSH (xmas) • FIN • (null scan)	RST	RST	(semmi)	(semmi)
ACK	RST	RST	(semmi)	(semmi)
SYN+ACK (az idle scanben)	RST			
RST	(semmi)			

3. nmap

Olvasnivaló: Nmap Reference Guide (man nmap)

3.1. Mire jó?

- (live) host discovery,
- scanning for open ports,
- service/version detection: service protocol, application name, application version number,
- OS detection: using its OS fingerprint database
- network traceroute. Állítható port és protokoll.

3.2. Használata

- Transport protocol port numbers: https://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers
- timing template

timing template	jelentése	késleltetés
-T0	paranoid (IDS evasion).	5 perc
-T1	sneaky (IDS evasion)	15 mp
-T2	polite	0,4 mp
-T3	normal (default), parallelization	
-T4	aggressive	
-T5	insane	

- --max-retries javasolt értéke: 0
- --max-rate: legfeljebb hány csomag mp-enként
- -n reverse DNS kihagyása
- IPv4 address specification

hogyan	példa	példa jelentése
Egy host.	192.168.0.1.	
Network of adjacent hosts using CIDR notation	192.168.0.1/24.	192.168.0.0 to 192.168.0.255
octet range addressing	192.168.2-4,6.1.	192.168.2.1, 192.168.3.1, 192.168.4.1, and 192.168.6.1.
Multiple host specifications	192.168.2.1 172.168.3-5,9.1	

- outputs: interactive output, normal output (-oN), XML output (-oX), grepable output (-oG)

3.2.1 Live host discovery

- Ping scan (ping sweep): ICMP echo request más hálózatba, ARP scan azonos hálózatba. (-sn: ping scan (no port scan), -n: no DNS lookup)

```
nmap -sn -n --max-retries 0 169.254.192.150-180
```

- Reverse DNS scan (-Pn: port scan (no ping scan), -sL: list scan)

```
nmap -Pn -sL 192.168.152.1-254
```

3.2.2 Scanning for open ports

- TCP syn scan (-n: no DNS lookup, -Pn: port scan (no ping scan))

```
nmap -n -Pn -sS --max-retries 0 --max-rate 1 \
-p 80,3389 45.33.32.156 -oX scanme.xml
```

- UDP scan, itt most: NetBIOS name query (NBTSTAT), udp 137 (-sU) (-Pn: port scan (no ping scan), -sL: list scan). A -sV (service detection) mindig ajánlott UDP esetében!

```
nmap -nvv -Pn -sU -sV -p 137 45.33.32.156 -oX udppc
```

3.2.3 Service/version detection

- Névszerver 53-as UDP portja (host -t ns example.com)

```
nmap -n -Pn -sU -sV -T1 -p U:53 127.0.0.1 \
-oX sv.xml
```

3.2.4 OS detection (OS fingerprinting)

-

```
nmap -n -vv -O 127.0.0.1 -oX osdet.xml
```

3.2.5 Network traceroute

-

```
nmap -sn --traceroute wikipedia.org
```

4. Feladatok

Válaszold meg az alábbi kérdéseket az órán kihúzott cégről.

1. A levelezőszerverének IP címét is tartalmazó, 10 db IP címből álló tartomány reverse DNS lookup lekérdezése.
2. A webszerverén port teszt végrehajtása az alábbi portokon: remote desktop (tcp 3389), NetBIOS name query (udp 137), HTTP (tcp 80).
3. A névszerverén a DNS szolgáltatást milyen nevű és verziójú alkalmazás szolgáltatja?