SCANNING AND ENUMERATION

Hacking phases

1. Reconnaissance and footprinting
2. **Scanning and enumeration**
3. Gaining Access
4. Maintaining access/escalating privileges
5. Clearing traces

ISSES
Co-funded by the Erasmus+ Programme of the European Union

Scanning

- Scanning is a process of active probing a target network with the intent of revealing useful information and then using that information for later phases of the attack or the pen test.
- Scanning can be considered illegal if it negatively affects some system or part of the infrastructure (e.g. port/network scanning can be a sort of DoS attack)
- There should be a consent of/contract with the target.

ISSES

Co-funded by the
Erasmus+ Programme
of the European Union

Scanning

- Types of scan:
  - Network scan – detect active machines
  - Port scan – detect open ports on a machine
  - Vulnerability scan – find vulnerabilities, not exploiting them (this is penetration)
- **Key tool – nmap**
- Other tools – zenmap, zmap, pOf, hping3,…

ISSES
Co-funded by the Erasmus+ Programme of the European Union

Network scan - Checking for live systems

- Wardialing – find computers connected via modem
- Wardriving – searching WiFi networks
- Using ping, fping (Linux, MAC), Megaping (Windows),…
- Port scanning

```
$ fping -aeg 192.168.86.0/24
192.168.86.1 (10.3 ms)
192.168.86.2 (16.4 ms)
192.168.86.12 (27.7 ms)
192.168.86.21 (17.4 ms)
192.168.86.11 (173 ms)
192.168.86.20 (82.7 ms)
192.168.86.31 (0.04 ms)
192.168.86.30 (14.3 ms)
192.168.86.32 (16.4 ms)
192.168.86.35 (16.9 ms)
```

ISSES
Co-funded by the Erasmus+ Programme of the European Union

Using ping

- ICMP Echo Request and Echo reply
- If successful, machine is alive
- If not successful, machine is not active, or packets are blocked by firewall or ping disabled
- Various options: set size, set time between packets, set IP version,…

```
ping 8.8.8.8
nmap -sP -v 8.8.8.8
```

ISSES
Co-funded by the Erasmus+ Programme of the European Union

ping options (Linux version)

- `-4  Use IPv4 only.`
- `-6  Use IPv6 only.`
- `-B  Allow pinging a broadcast address.`
- `-c  count`
- `-i  interval`
- `-I  interface`
- `-M  pmtudisc_opt (want, don't)`
- `-s  packetsize`

- Other: man ping, ping -h

ISSES
Co-funded by the Erasmus+ Programme of the European Union

nmap tool - ping sweep

- Can be detected by firewall or IDS
- ping a range of addresses and ports

```
nmap -sP -PE -PA<port numbers> <starting-endingIP>
  nmap -sP -PE -PA21,23,80,3389 192.168.10.1-128
```

```
pavle@pavle-ideapad:~$ nmap -sP -PE -PA21,23,80,3389 192.168.1.1-255
Warning:  You are not root -- using TCP pingscan rather than ICMP

Starting Nmap 7.60 ( https://nmap.org ) at 2018-11-19 19:13 CET
Nmap scan report for _gateway (192.168.1.1)
Host is up (0.081s latency).
Nmap scan report for 192.168.1.100
Host is up (0.015s latency).
Nmap scan report for 192.168.1.105
Host is up (0.047s latency).
Nmap scan report for 192.168.1.107
Host is up (0.24s latency).
Nmap scan report for 192.168.1.111
Host is up (0.0018s latency).
Nmap done: 255 IP addresses (5 hosts up) scanned in 23.12 seconds
```

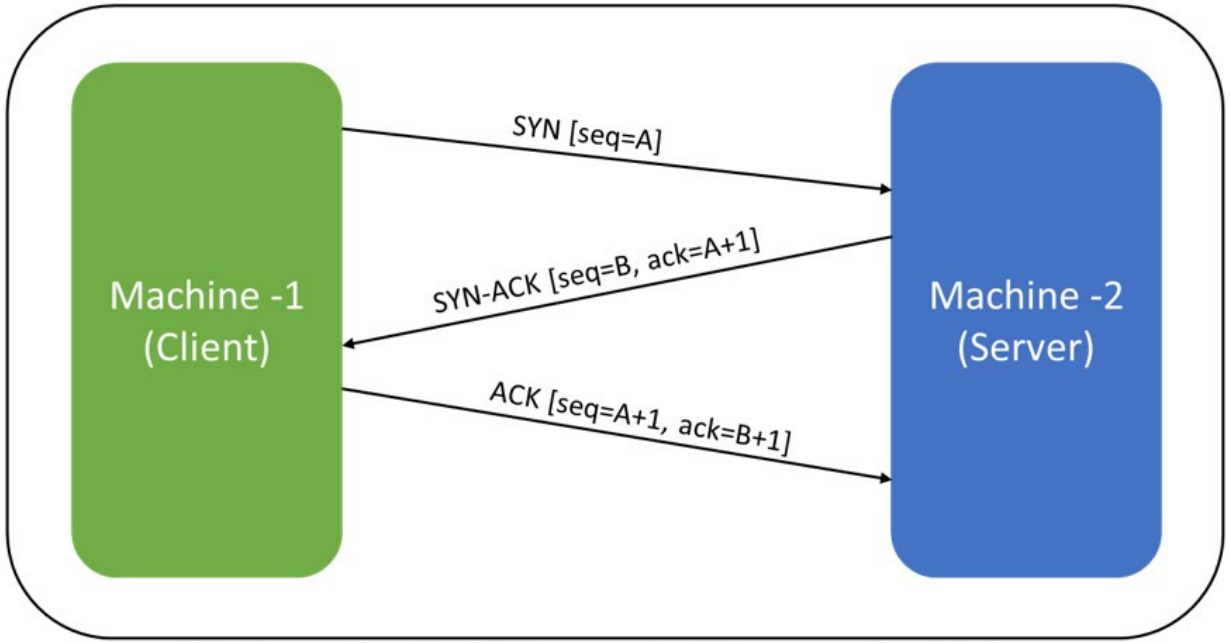
Scanning

- Full-open scan
- Stealth or half-open scan
- Xmas tree scan
- FIN scan
- NULL scan
- Idle Scanning
- ACK scanning
- UDP scanning

ISSES

Co-funded by the
Erasmus+ Programme
of the European Union

Background – TCP handshake



TCP Connection Establishment using Three-way Handshake

- TCP flags
  - SYN
  - ACK
  - URG
  - PSH
  - FIN
  - RST

ISSES
Co-funded by the Erasmus+ Programme of the European Union

TCP FLAGS

SYN	Initiates a connection between two hosts to facilitate communication.
ACK	Acknowledge the receipt of a packet.
URG	Indicates that the data contained in the packet is urgent and should process immediately.
PSH	Instructs the sending system to send all buffered data immediately.
FIN	Tells the remote system about the end of the communication. In essence, this gracefully closes a connection.
RST	Reset a connection.

TCP Handshake behaviour

- Open ports should respond to a SYN message with a SYN/ACK.
- Closed ports should respond to a SYN message with a RST message.
- Firewalls and intrusion detection systems can have different behaviour
- There are some exchanges that are simply not documented, so behavior isn't guaranteed because it's not expected.

ISSES

Co-funded by the
Erasmus+ Programme
of the European Union

Full-Open scan

- Full three-way TCP handshake
- Detected by IDS and FW

```
nmap -sT -v <target IP address>
```

ISSES
Co-funded by the Erasmus+ Programme of the European Union

Stealth, Half-Open scan

- Stops after SYN-ACK message
- Sends RST after SYN-ACK
- Less noisy, creates less log at the target

```
nmap -sS -v <target IP address>
```

ISSES
Co-funded by the Erasmus+ Programme of the European Union

Xmas tree scan

- Send packets with URG PSH and FIN + port number
- Combination of flags makes no sense and there is no adequate response, so silence is expected
- New systems drop the packet, but some older systems send RST if the port is closed or nothing if it is opened

```
nmap -sX -v <target IP address>
```

ISSES
Co-funded by the Erasmus+ Programme of the European Union

FIN Scan

- Send FIN+Port number
- Passes through the firewalls without changes
- If port is open – no response
- If port is closed RST is expected as a response

```
nmap -sF -v <target IP address>
```

ISSES
Co-funded by the Erasmus+ Programme of the European Union

NULL Scan

- No flags are set in the scanning packet
- The result is similar to FIN scan

```
nmap -sN -v <target IP address>
```

ISSES
Co-funded by the Erasmus+ Programme of the European Union

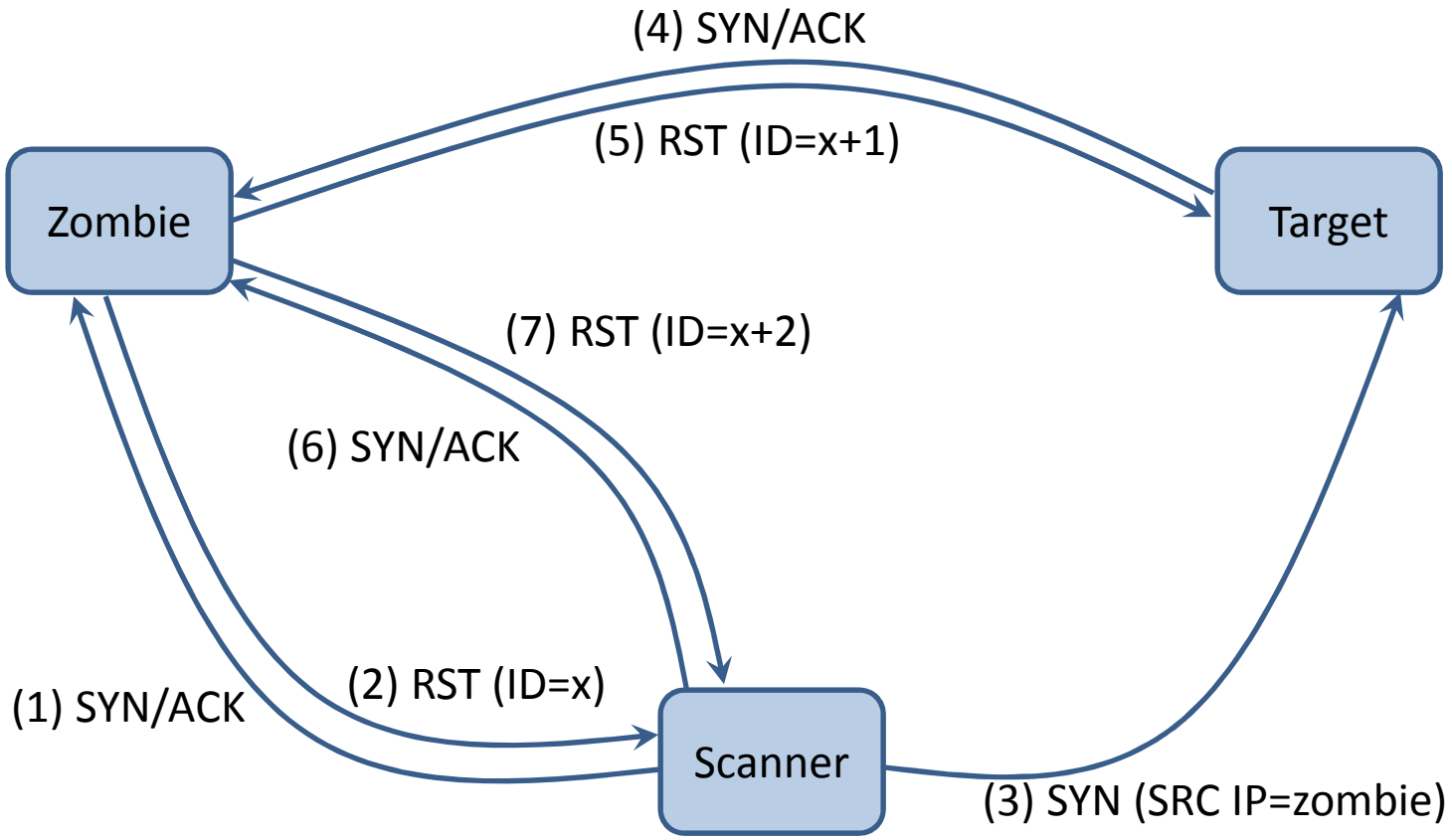
Idle Scan (1)

- Attacker is hidden behind the zombie host. Target does not know who is actually doing the scanning.
- Exploits IP Identification field (used for IP fragmentation to detect fragments that belong to the same packet) – RFC6864
- IP ID field has to be unique for each packet
- IP ID field is incremented for each packet in the same stream (between the same sources and destinations)
- Latest versions of Linux, OpenBSD, Windows from Vista are randomizing IPID field and are not suitable as zombies

```
nmap -Pn -p- -sI zombie target
```

ISSES
Co-funded by the Erasmus+ Programme of the European Union

Idle Scan (2)



ISSES
Co-funded by the Erasmus+ Programme of the European Union

ACK scanning

- Used to detect stateful firewall on the path and its setup
- If ACK is sent to the non-existing TCP session on a specific host for both open and closed ports, RST is returned
- If nothing is returned, or if ICMP error codes are returned (e.g. unreachable) there is a Firewall in between.
- Firewalls can sometimes be avoided by fragmenting the packets (-f switch in nmap)

```
nmap -sA -T4 target
```

ISSES

Co-funded by the
Erasmus+ Programme
of the European Union

UDP scanning

- UDP is connectionless protocol. No handshake, no flags.
- Response to the UDP packet comes from the application
- It is still possible to detect the open UDP ports:
  - If UDP port P is open, when the UDP packet is sent to UDP port P, there is no response or there is some reasonable UDP packet
  - IF UDP port P closed, when the UDP packet is sent to UDP port P, ICMP Port Unreachable message is sent back

hping3 tool

- Tool that can create crafted TCP/UDP packets
- Possible to set any flag, protocol type and do the scan
- ACK scan with hping3:

Port 25 open
(RST received)

Port 23 closed
(ICMP unreach.)

```
pavle@pavle-ideapad:~$ sudo hping3 -c 1 -V -p 25 -s 5050 -A
using wlp2s0, addr: [redacted], MTU: 1500
HPING [redacted] (wlp2s0 [redacted]): A set, 40 headers + 0 data bytes
len=40 ip=147.91.1.120 ttl=62 DF id=29622 tos=0 iplen=40
sport=25 flags=R seq=0 win=0 rtt=7.8 ms
seq=294949866 ack=0 sum=7d6b urp=0

--- [redacted] hping statistic ---
1 packets transmitted, 1 packets received, 0% packet loss
round-trip min/avg/max = 7.8/7.8/7.8 ms
pavle@pavle-ideapad:~$ sudo hping3 -c 1 -V -p 23 -s 5050 -A
using wlp2s0, addr: [redacted], MTU: 1500
HPING [redacted] (wlp2s0 [redacted]): A set, 40 headers + 0 data bytes
ICMP Unreachable type=10 from ip=147.91.1.120 name=[redacted]

--- [redacted] hping statistic ---
1 packets transmitted, 1 packets received, 0% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
```

ISSES
Co-funded by the
Erasmus+ Programme
of the European Union

OS Fingerprinting (1)

- Identifying the operating system of the host
- Each operating system has some specific implementation details and specific networking behaviour. Multiple OS can have the same fingerprint.
- Can detect kernel version and not linux distribution
- Active and passive scans:
  - Active (more effective): send packets to the host and observe its behaviour and compare it to the database of OS fingerprints/responses
  - Passive (less effective): sniff the traffic to the host and compare it to the OS fingerprints

ISSES
Co-funded by the Erasmus+ Programme of the European Union

OS Fingerprinting (2)

- Fingerprinting analyses the following parameters:
  - IP TTL values
  - IP ID values
  - TCP Window size
  - TCP options (generally, in TCP SYN and SYN+ACK packets)
  - DHCP requests
  - ICMP requests
  - HTTP packets (generally, the User-Agent field)
  - Running services
  - Open port patterns

```
nmap -O target
```

ISSES
Co-funded by the Erasmus+ Programme of the European Union

Active fingerprinting - examples

```
pavle@pavle-ideapad:~$ sudo nmap -O [redacted]
[sudo] password for pavle:

Starting Nmap 7.60 ( https://nmap.org ) at 2018-11-30 12:35 CET
Nmap scan report for _gateway ([redacted])
Host is up (0.016s latency).
Not shown: 998 closed ports
PORT    STATE SERVICE
22/tcp  open  ssh
443/tcp open  https
MAC Address: 2C:23:3A:56:42:EC (Hewlett Packard)
Device type: switch
Running: HP Comware 7.X
OS CPE: cpe:/o:hp:comware:7.1
OS details: HP FlexFabric 5900CP switch (Comware 7.1)
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/
submit/ .
Nmap done: 1 IP address (1 host up) scanned in 5.43 seconds
```

```
[redacted]:~$ sudo nmap -O [redacted]

Starting Nmap 7.60 ( https://nmap.org ) at 2018-11-30 12:41 CET
Nmap scan report for [redacted]
Host is up (0.0088s latency).
All 1000 scanned ports on 91.187.154.130 are closed
MAC Address: 8C:BF:A6:DE:10:04 (Samsung Electronics)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: phone|general purpose|webcam|storage-misc
Running: Google Android 2.X, Linux 2.6.X, AXIS embedded, ZyXEL embedded
OS CPE: cpe:/o:google:android:2.2 cpe:/o:linux:linux_kernel:2.6 cpe:/o:linux:linux_kernel:2.6.17 cpe:/h:
axis:210a_network_camera cpe:/h:axis:211_network_camera cpe:/h:zyxel:nsa-210
OS details: Android 2.2 (Linux 2.6), Linux 2.6.14 - 2.6.34, Linux 2.6.17 (Mandriva), Linux 2.6.32, AXIS
210A or 211 Network Camera (Linux 2.6.17), ZyXEL NSA-210 NAS device
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 21.54 seconds
```

ISSES

Co-funded by the
Erasmus+ Programme
of the European Union

Passive fingerprinting

- Different OSs use different initial values for TTL or initial TCP window size
- Tool pOf

```
pavle@pavle-ideapad:~/Downloads/p0f-3.09b$ sudo p0f -i enx503eaa41e537
--- p0f 3.09b by Michal Zalewski <lcamtuf@coredump.cx> ---

[+] Closed 1 file descriptor.
[+] Loaded 322 signatures from '/etc/p0f/p0f.fp'.
[+] Intercepting traffic on interface 'enx503eaa41e537'.
[+] Default packet filtering configured [+VLAN].
[+] Entered main event loop.

.-[ [redacted] -> [redacted] (syn+ack) ]-
|
| server   = [redacted]/443
| os       = Linux 2.6.x
| dist     = 2
| params   = none
| raw_sig  = 4:62+2:0:1460:mss*4,7:mss,sok,ts,nop,ws:df:0
|
`----

.-[ [redacted] -> [redacted] (mtu) ]-
|
| server   = [redacted]/443
| link     = Ethernet or modem
| raw_mtu  = 1500
|
`----

.-[ [redacted] -> [redacted] (uptime) ]-
|
| server   = [redacted]/443
| uptime   = 46 days 5 hrs 55 min (modulo 49 days)
| raw_freq = 1000.00 Hz
|
`----
```

Banner grabbing

- Grab what the service is returning about itself
- Can be done using telnet on specific port
- Useful for detecting software/OS versions
- Banners can be hidden
- Online tool: https://www.netcraft.com/
- Other tools:
  - Xprobe (Linux)
  - Maltego

```
pavle@pavle-ideapad:~/Downloads/p0f-3.09b$ telnet [redacted] 80
Trying [redacted]...
Connected to [redacted].
Escape character is '^]'.
dummy
HTTP/1.1 400 Bad Request
Date: Fri, 30 Nov 2018 12:17:29 GMT
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16
Content-Length: 226
Connection: close
Content-Type: text/html; charset=iso-8859-1

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>400 Bad Request</title>
</head><body>
<h1>Bad Request</h1>
<p>Your browser sent a request that this server could not understand.<br />
</p>
</body></html>
Connection closed by foreign host.
```

```
pavle@pavle-ideapad:~/Downloads/p0f-3.09b$ telnet [redacted] 22
Trying [redacted]...
Connected to [redacted].
Escape character is '^]'.
SSH-2.0-OpenSSH_7.4
```

ISSES
Co-funded by the Erasmus+ Programme of the European Union

nmap version scan

- connect to the port and, as necessary, issue the correct protocol commands to get the application banner back.

```
$ nmap -sV 192.168.86.32
Starting Nmap 7.70 ( https://nmap.org ) at 2018-07-14 20:51 MDT
Nmap scan report for billthecat.lan (192.168.86.32)
Host is up (0.0083s latency).
Not shown: 995 closed ports
PORT     STATE SERVICE       VERSION
22/tcp   open  ssh           OpenSSH 7.4 (protocol 2.0)
88/tcp   open  kerberos-sec  Heimdal Kerberos (server time: 2018-07-15 02:51:39Z)
445/tcp  open  microsoft-ds?
```

ISSES

Co-funded by the
Erasmus+ Programme
of the European Union

nmap scripts

- Allows users to write (and share) simple scripts (using the Lua programming language) to automate a wide variety of networking tasks.
- https://nmap.org/nsedoc/

```
nmap --script http-form-fuzzer --script-args 'http-form-fuzzer.targets={1={path=/},2={path=/register.html}}' -p 80 <host>

This script attempts to fuzz fields in forms it detects (it fuzzes one field at a time).
In each iteration it first tries to fuzz a field with a string, then with a number.
In the output, actions and paths for which errors were observed are listed, along with
names of fields that were being fuzzed during error occurrence. Length and type
(string/integer) of the input that caused the error are also provided.
We consider an error to be either: a response with status 500 or with an empty body,
a response that contains "server error" or "sql error" strings. ATM anything other than
that is considered not to be an 'error'.
TODO: develop more sophisticated techniques that will let us determine if the fuzzing was
successful (i.e. we got an 'error'). Ideally, an algorithm that will tell us a percentage
difference between responses should be implemented.
```

Script Output

```
PORT   STATE SERVICE REASON
80/tcp open  http    syn-ack
| http-form-fuzzer:
|   Path: /register.html Action: /validate.php
|     age
|       integer lengths that caused errors:
|         10000, 10001
|     name
|       string lengths that caused errors:
|         40000
|   Path: /form.html Action: /check_form.php
|     fieldfoo
|       integer lengths that caused errors:
|_        1, 2
```

Categories

auth
broadcast
brute
default
discovery
dos
exploit
external
fuzzer
intrusive
malware
safe
version
vuln

Scripts (show 602)

Libraries (show 139)

ISSES

Co-funded by the Erasmus+ Programme of the European Union

Sniffing network traffic

ISSES

Co-funded by the
Erasmus+ Programme
of the European Union

Sniffing

- Viewing raw packet content. Limited for the encrypted packets (TLS, IPsec,…)
- All the packets on the machine where the sniffer is can be captured
- Switched network – only those in the same collision domain (port)
- SPAN/Mirror ports
- Optical network taps
- Lawful interception

ISSES

Co-funded by the
Erasmus+ Programme
of the European Union

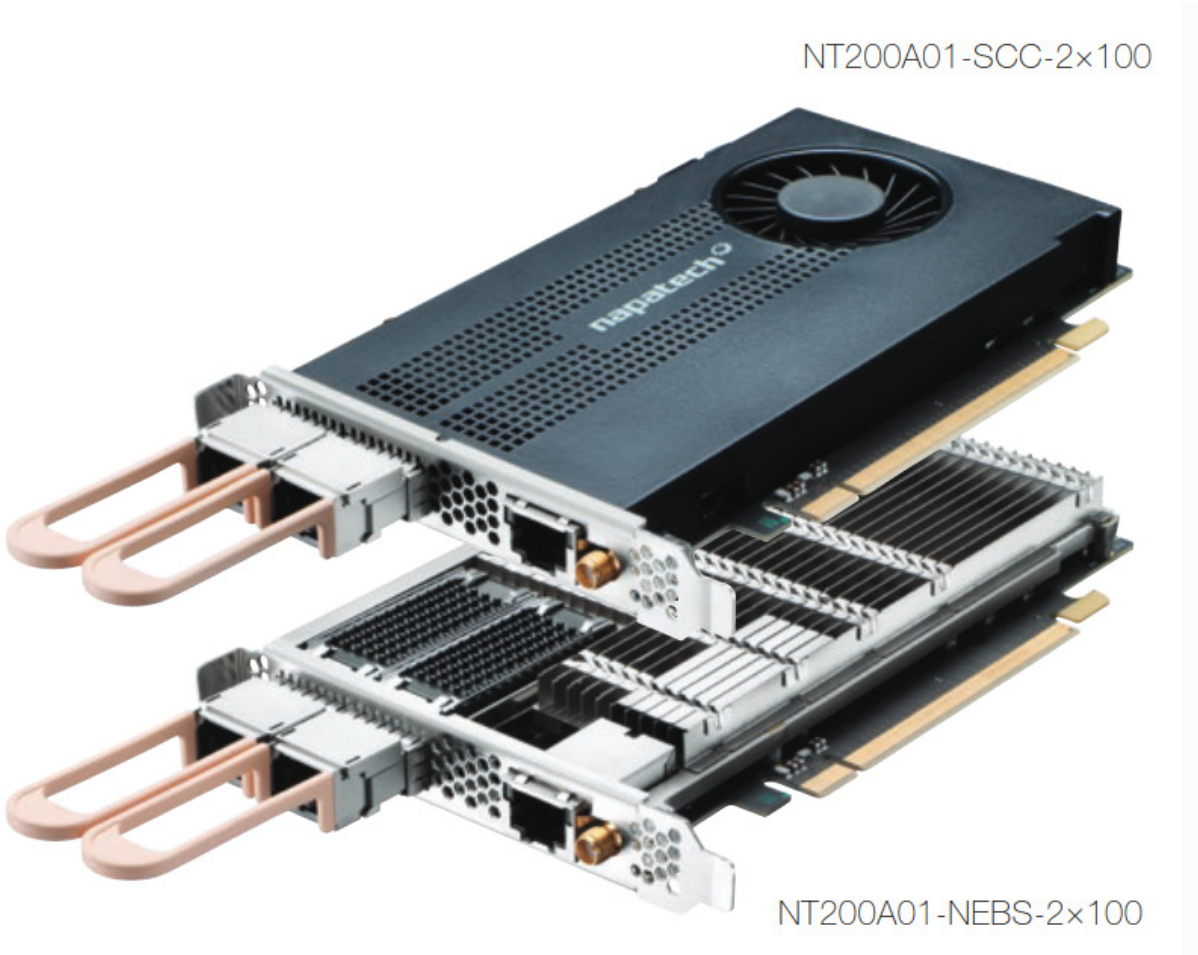
Sniffers

- wireshark/tshark (based on dumpcap)
- tcpdump (less protocol decoding)
- WinDump
- OmniPeek
- DSniff
- EtherApe
- NetWitness
- …

ISSES

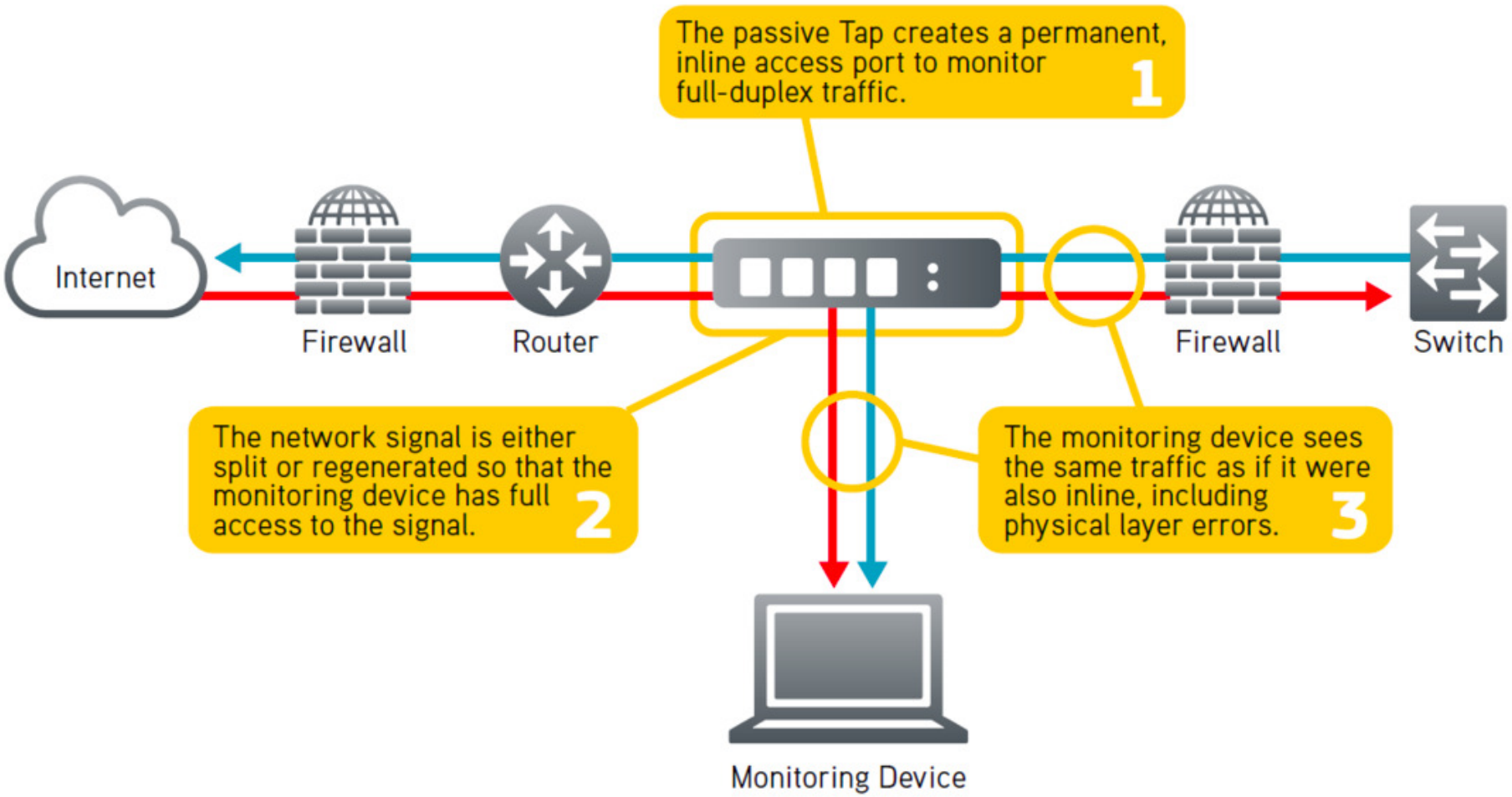
Co-funded by the
Erasmus+ Programme
of the European Union

Network capturing cards



ISSES
Co-funded by the
Erasmus+ Programme
of the European Union

Inline fibre taps



ISSES
Co-funded by the Erasmus+ Programme of the European Union

Capturing performance

- wireshark writes to disk (slow) and can drop packets (on links with higher than 1Gbps capacity)
- tshark (command line tools) are faster (less drop)
- dumpcap is faster than wireshark/tshark
- Improve with SSD or RAM disk

Co-funded by the Erasmus+ Programme of the European Union

Raw packet capture

	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.1	224.0.0.1	IGMPv2	60	Membership Query, general
2	0.452735	192.168.1.100	239.255.255.250	IGMPv2	46	Membership Report group 239.255.255.250
3	8.954918	192.168.1.100	224.0.0.252	IGMPv2	46	Membership Report group 224.0.0.252
4	19.501665	192.168.1.100	192.168.1.1	DNS	85	Standard query 0x536c A teredo.ipv6.microsoft.com
5	20.515067	192.168.1.100	192.168.1.1	DNS	85	Standard query 0x536c A teredo.ipv6.microsoft.com
6	21.529327	192.168.1.100	192.168.1.1	DNS	85	Standard query 0x536c A teredo.ipv6.microsoft.com
7	23.541703	192.168.1.100	192.168.1.1	DNS	85	Standard query 0x536c A teredo.ipv6.microsoft.com
8	24.445788	Inventec_a0:a5:1a	Tp-LinkT_f0:38:3e	ARP	42	Who has 192.168.1.1? Tell 192.168.1.100
9	24.446220	Tp-LinkT_f0:38:3e	Inventec_a0:a5:1a	ARP	60	192.168.1.1 is at 94:0c:6d:f0:38:3e
10	25.226923	Inventec_a0:a5:1a	Broadcast	ARP	42	Who has 192.168.1.1? Tell 192.168.1.100
11	25.227270	Tp-LinkT_f0:38:3e	Inventec_a0:a5:1a	ARP	60	192.168.1.1 is at 94:0c:6d:f0:38:3e
12	25.229506	fe80::d892:9a79:df0…	ff02::1:3	LLMNR	84	Standard query 0xfe1b A wpad
13	25.229835	192.168.1.100	224.0.0.252	LLMNR	64	Standard query 0xfe1b A wpad
14	25.230504	fe80::d892:9a79:df0…	ff02::1:3	LLMNR	84	Standard query 0x8ac9 A wpad
15	25.230809	192.168.1.100	224.0.0.252	LLMNR	64	Standard query 0x8ac9 A wpad
16	25.335811	fe80::d892:9a79:df0…	ff02::1:3	LLMNR	84	Standard query 0x8ac9 A wpad
17	25.335915	192.168.1.100	224.0.0.252	LLMNR	64	Standard query 0x8ac9 A wpad
18	25.336260	fe80::d892:9a79:df0…	ff02::1:3	LLMNR	84	Standard query 0xfe1b A wpad
19	25.336345	192.168.1.100	224.0.0.252	LLMNR	64	Standard query 0xfe1b A wpad
20	25.541265	192.168.1.100	192.168.1.255	NBNS	92	Name query NB WPAD<00>
21	25.541717	192.168.1.100	192.168.1.255	NBNS	92	Name query NB WPAD<00>
22	26.302299	192.168.1.100	192.168.1.255	NBNS	92	Name query NB WPAD<00>
23	26.302470	192.168.1.100	192.168.1.255	NBNS	92	Name query NB WPAD<00>
24	27.066867	192.168.1.100	192.168.1.255	NBNS	92	Name query NB WPAD<00>
25	27.067006	192.168.1.100	192.168.1.255	NBNS	92	Name query NB WPAD<00>
26	27.550311	192.168.1.100	192.168.1.1	DNS	85	Standard query 0x536c A teredo.ipv6.microsoft.com
27	27.833517	192.168.1.100	192.168.1.1	DNS	83	Standard query 0x2ee1 A officecdn.microsoft.com
28	28.845112	192.168.1.100	192.168.1.1	DNS	83	Standard query 0x2ee1 A officecdn.microsoft.com
29	29.859189	192.168.1.100	192.168.1.1	DNS	83	Standard query 0x2ee1 A officecdn.microsoft.com
30	31.871536	192.168.1.100	192.168.1.1	DNS	83	Standard query 0x2ee1 A officecdn.microsoft.com
31	35.880752	192.168.1.100	192.168.1.1	DNS	83	Standard query 0x2ee1 A officecdn.microsoft.com
32	40.030967	192.168.1.100	255.255.255.255	DHCP	342	DHCP Inform - Transaction ID 0xc0aa0291
33	43.041243	192.168.1.100	255.255.255.255	DHCP	342	DHCP Inform - Transaction ID 0xc0aa0291
34	52.048743	fe80::d892:9a79:df0…	ff02::1:3	LLMNR	84	Standard query 0x268a A wpad

```
0000  94 0c 6d f0 38 3e 00 a0  d1 a0 a5 1a 08 00 45 00   ··m·8>·· ·····E·
0010  00 47 02 3d 00 00 40 11  00 00 c0 a8 01 64 c0 a8   ·G·=··@· ·····d··
0020  01 01 eb f9 00 35 00 33  83 fa 53 6c 01 00 00 01   ·····5·3 ··Sl····
0030  00 00 00 00 00 00 06 74  65 72 65 64 6f 04 69 70   ·······t eredo·ip
0040  76 36 09 6d 69 63 72 6f  73 6f 66 74 03 63 6f 6d   v6·micro soft·com
0050  00 00 01 00 01                                    ·····
```

ISSES

Co-funded by the Erasmus+ Programme of the European Union

Raw packet capture

```
▸ Frame 69: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
▸ Ethernet II, Src: JuniperN_ee:b4:00 (00:12:1e:ee:b4:00), Dst: Raspberr_35:29:90 (b8:27:eb:35:29:90)
▾ Internet Protocol Version 4, Src: 117.102.69.54, Dst: 147.91.72.131
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▾ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
      0000 00.. = Differentiated Services Codepoint: Default (0)
      .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
    Total Length: 40
    Identification: 0x1ae2 (6882)
  ▾ Flags: 0x4000, Don't fragment
      0... .... .... .... = Reserved bit: Not set
      .1.. .... .... .... = Don't fragment: Set
      ..0. .... .... .... = More fragments: Not set
      ...0 0000 0000 0000 = Fragment offset: 0
    Time to live: 234
    Protocol: TCP (6)
    Header checksum: 0xdf72 [validation disabled]
    [Header checksum status: Unverified]
    Source: 117.102.69.54
    Destination: 147.91.72.131
▾ Transmission Control Protocol, Src Port: 46041, Dst Port: 80, Seq: 0, Len: 0
    Source Port: 46041
    Destination Port: 80
    [Stream index: 16]
    [TCP Segment Len: 0]
    Sequence number: 0    (relative sequence number)
    [Next sequence number: 0    (relative sequence number)]
    Acknowledgment number: 0
    0101 .... = Header Length: 20 bytes (5)
  ▾ Flags: 0x002 (SYN)
      000. .... .... = Reserved: Not set
      ...0 .... .... = Nonce: Not set
      .... 0... .... = Congestion Window Reduced (CWR): Not set
      .... .0.. .... = ECN-Echo: Not set
      .... ..0. .... = Urgent: Not set
      .... ...0 .... = Acknowledgment: Not set
      .... .... 0... = Push: Not set
      .... .... .0.. = Reset: Not set
    ▸ .... .... ..1. = Syn: Set
      .... .... ...0 = Fin: Not set
      [TCP Flags: ··········S·]
    Window size value: 14600
    [Calculated window size: 14600]
    Checksum: 0x30af [unverified]
    [Checksum Status: Unverified]
    Urgent pointer: 0
  ▾ [Timestamps]
      [Time since first frame in this TCP stream: 0.000000000 seconds]
      [Time since previous frame in this TCP stream: 0.000000000 seconds]
```

Botnet C&C communication

```
37 131.643498429 185.244.39.10   147.91.72.158   TCP   70 151 → 54742 [PSH, ACK] Seq=32 Ack=166 Win=15616 Len=4 TSval=121158153 TSecr=2147754160
38 131.643664783 147.91.72.158   185.244.39.10   TCP   66 54742 → 151 [ACK] Seq=166 Ack=36 Win=29312 Len=0 TSval=2147787614 TSecr=121158153
39 131.673990019 185.244.39.10   147.91.72.158   TCP   67 151 → 54742 [PSH, ACK] Seq=36 Ack=166 Win=15616 Len=1 TSval=121158184 TSecr=2147787614
40 131.674131009 147.91.72.158   185.244.39.10   TCP   66 54742 → 151 [ACK] Seq=166 Ack=37 Win=29312 Len=0 TSval=2147787644 TSecr=121158184
```

```
▸ Frame 37: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface 0
▸ Ethernet II, Src: JuniperN_ee:b4:00 (00:12:1e:ee:b4:00), Dst: Raspberr_31:dc:dc (b8:27:eb:31:dc:dc)
▸ Internet Protocol Version 4, Src: 185.244.39.10, Dst: 147.91.72.158
▸ Transmission Control Protocol, Src Port: 151, Dst Port: 54742, Seq: 32, Ack: 166, Len: 4
▾ Data (4 bytes)
    Data: 50494e47
    [Length: 4]
```

```
0000  b8 27 eb 31 dc dc 00 12  1e ee b4 00 08 00 45 00   ·'·1·· ·  ·····E·
0010  00 38 bf 66 40 00 37 06  c7 61 b9 f4 27 0a 93 5b   ·8·f@·7·  ·a··'··[
0020  48 9e 00 97 d5 d6 75 e4  07 79 06 86 44 16 80 18   H·····u·  ·y··D···
0030  00 7a 1a 51 00 00 01 01  08 0a 07 38 ba 09 80 04   ·z·Q····  ···8····
0040  20 b0 50 49 4e 47                                  ·PING
```

```
▸ Frame 41: 71 bytes on wire (568 bits), 71 bytes captured (568 bits) on interface 0
▸ Ethernet II, Src: Raspberr_31:dc:dc (b8:27:eb:31:dc:dc), Dst: JuniperN_ee:b4:00 (00:12:1e:ee:b4:00)
▸ Internet Protocol Version 4, Src: 147.91.72.158, Dst: 185.244.39.10
▸ Transmission Control Protocol, Src Port: 54742, Dst Port: 151, Seq: 166, Ack: 37, Len: 5
▾ Data (5 bytes)
    Data: 504f4e470a
    [Length: 5]
```

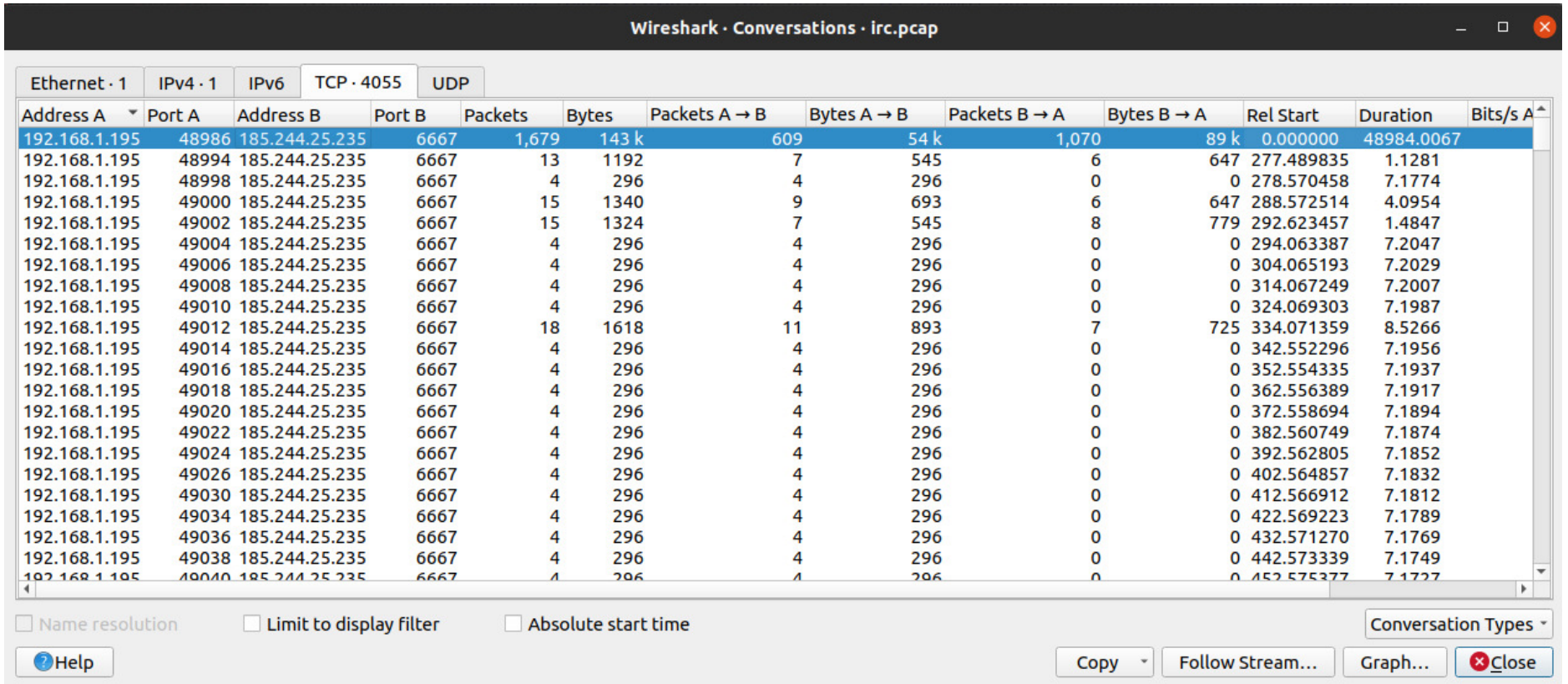
```
0000  00 12 1e ee b4 00 b8 27  eb 31 dc dc 08 00 45 00   ·······'  ·1····E·
0010  00 39 06 2d 40 00 40 06  77 9a 93 5b 48 9e b9 f4   ·9·-@·@·  w··[H···
0020  27 0a d5 d6 00 97 06 86  44 16 75 e4 07 7e 80 18   '·······  D·u··~··
0030  00 e5 bd 23 00 00 01 01  08 0a 80 04 a3 7d 07 38   ···#····  ·····}·8
0040  ba 28 50 4f 4e 47 0a                              ·(PONG·
```

ISSES

Co-funded by the Erasmus+ Programme of the European Union

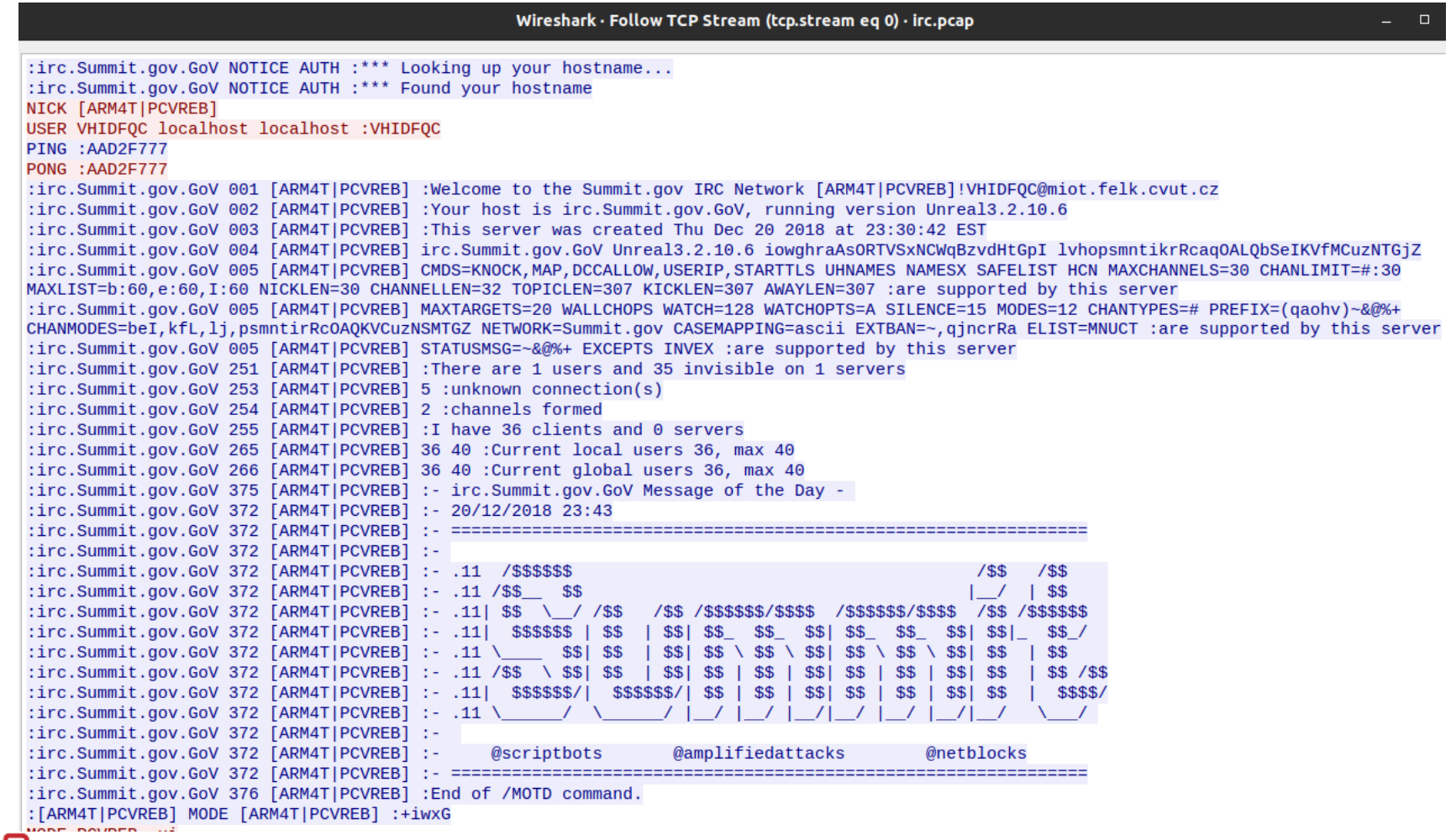
Use Statistics/Conversations/Follow Stream

- Botnet CnC based on IRC



ISSES
Co-funded by the Erasmus+ Programme of the European Union

Use Statistics/Conversations/Follow Stream



ISSES

Co-funded by the Erasmus+ Programme of the European Union

Other techniques

- Vulnerability scanners (Nessus, OpenVAS)
- Network mappers
- …

ENUMERATION

Hacking phases

1. Reconnaissance
    1. Passive (public info)
    2. Active (engaging the target – calls, emails,…)
2. Scanning and **enumeration**
3. Gaining Access
4. Maintaining access/escalating privileges
5. Clearing traces

ISSES
Co-funded by the Erasmus+ Programme of the European Union

Enumeration

- Gaining in-depth information from a target system by exploiting active services
- Can be illegal
- Can expose the attacker/tester
- Knowledge about the operating systems and service internals are required

```
Password:
Last login: Tue Nov  6 12:05:03 2018 from 2001:798:3::96
-------------
W A R N I N G
-------------

THIS IS A NON-PUBLIC COMPUTER SYSTEM.

This computer system, including all related equipment, network devices
(specifically including network and Internet access), are provided only for
authorized use.

All computer systems may be monitored for all lawful purposes, including to
ensure that their use is authorized, for management of the system, to
facilitate protection against unauthorized access, and to verify security
procedures, survivability and operational security.

Monitoring includes active attacks by authorized personnel and their entities
to test or verify the security of the system. During monitoring, information
may be examined, recorded, copied and used for authorized purposes.

All information, including personal information, placed on or sent over this
system may be monitored.

Uses of this system, authorized or unauthorized, constitutes consent to
monitoring of this system.

Unauthorized use may subject you to criminal prosecution.

Evidence of any such unauthorized use collected during monitoring may be used
for administrative, criminal or other adverse action.

Use of this system constitutes consent to monitoring for these purposes.

If you are unsure if you are an authorized user, you should presume you are
not and disconnect immediately.
```

ISSES
Co-funded by the Erasmus+ Programme of the European Union

Enumeration techniques

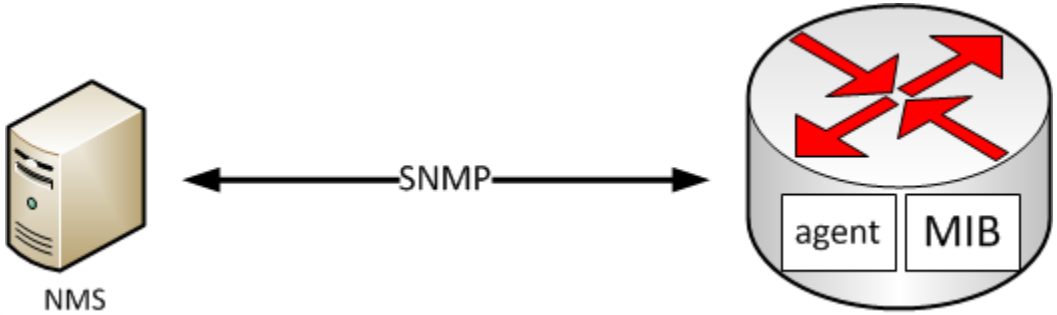
- Try default passwords (hundreds of thousands of devices use default factory passwords – Mirai, linkedin)
- Look for the info from:
  - DNS
  - Email (SMTP, POP3)
  - SNMP
  - NTP
  - LDAP
  - Web servers
  - Other protocols…
- Knowledge about these protocols is desirable

Rank	Password	Frequency
1	123456	753,305
2	linkedin	172,523
3	password	144,458
4	123456789	94,314
5	12345678	63,769

ISSES
Co-funded by the Erasmus+ Programme of the European Union

SNMP enumeration

- Simple Network Management Protocol
  - v1 – RFC 1157
  - v2 - RFC 3416 - 3418
  - v3 – RFC – 3410 - 3418
- Transport protocol UDP
  - port 161: send and receive
  - port 162: traps



ISSES
Co-funded by the Erasmus+ Programme of the European Union

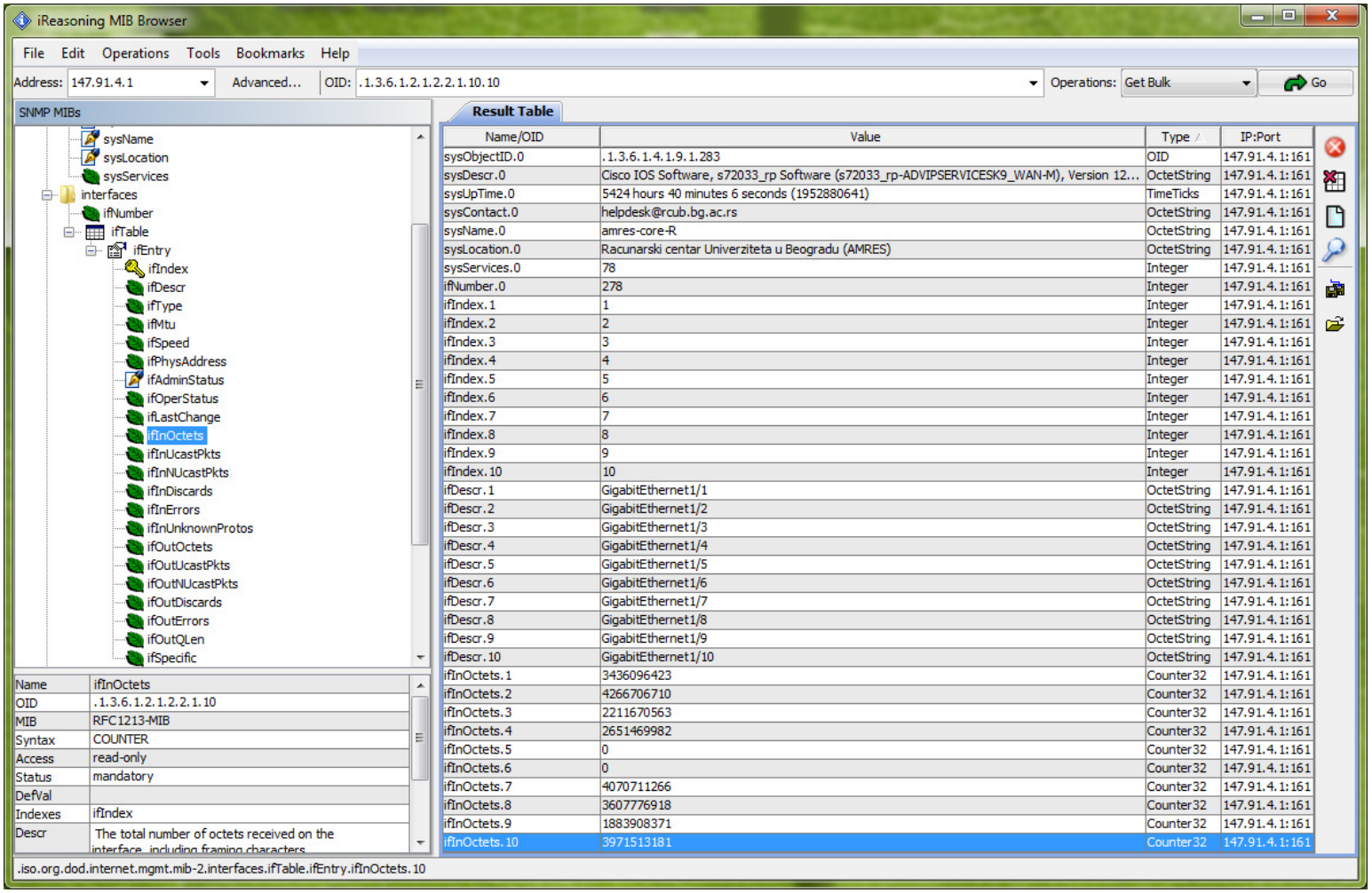
Getting information from SNMP

1. Sniff the network traffic
2. If SNMPv1 or v2 is used, read the community strings
3. If SNMPv3 try default community values
4. Use SNMP browser to read the device/service parameter

- The following can be extracted through SNMP:
  - Network resources such as hosts, routers, and devices
  - File shares
  - ARP tables
  - Routing tables
  - Device-specific information
  - Traffic statistics

ISSES
Co-funded by the Erasmus+ Programme of the European Union

MIB Browser



ISSES

Co-funded by the Erasmus+ Programme of the European Union

Getting information from DNS

- Regular DNS queries using `dig` or `nslookup` – UDP 53
- Zone transfers – whole tables moved as between primary and secondary DNS servers (often disabled by DNS admin) – TCP 53

```
Microsoft Windows [Version 6.0.6001]
Copyright (c) 2006 Microsoft Corporation.  All rights reserved.

C:\Users\sean>nslookup
Default Server:  lisa.portugal.belair.com
Address:  196.132.132.10
> server ns1.fubar.com
Default Server:  ns1.rancidbutter.com
Address:  xxx.xxx.xxx.xxx

> set type=any
> ls -d example.com
[ns1.fubar.com]
 example.com.               SOA     ns1.rancidbutter.com
logs.rancidbutter.com. (2008102800 14400 7200 3600000 86400)
 example.com.               MX      0    example.com
 example.com.               NS      ns1.rancidbutter.com
 example.com.               NS      ns2.rancidbutter.com
 example.com.               A       yyy.yyy.yyy.yyy
 cpanel                     A       yyy.yyy.yyy.yyy
 ftp                        A       yyy.yyy.yyy.yyy
 localhost                  A       127.0.0.1
 mail                       CNAME   example.com
 webdisk                    A       yyy.yyy.yyy.yyy
 webmail                    A       yyy.yyy.yyy.yyy
```

```
pavle@pavle-ideapad:~$ nslookup
> server 147.91.1.5
Default server: 147.91.1.5
Address: 147.91.1.5#53
> set type=any
> ls -d rcub.bg.ac.rs
The 'ls' command is not implemented.
>
```

ISSES

Co-funded by the Erasmus+ Programme of the European Union

Simple script to get all DNS records in a network from reverse DNS

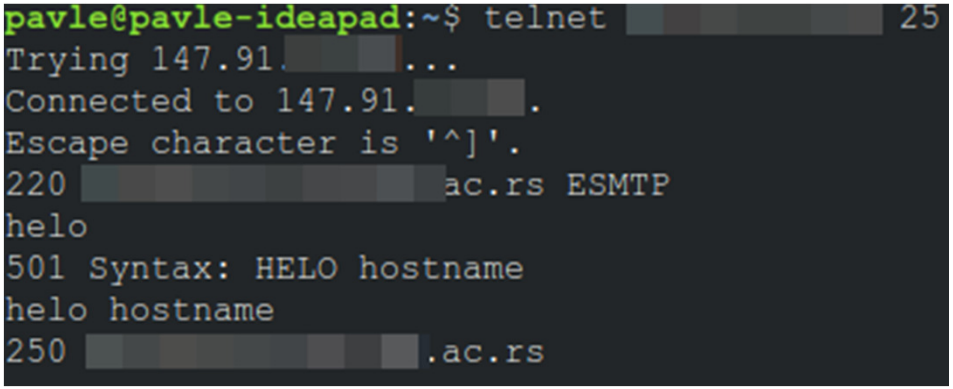
```
#!/usr/local/bin/py3.5
import os
import sys
import subprocess

addr_range = ''
rev_dns_addr = ''

# wrapper command is: rDNSwrap network addr (192.168.1)
addr_range = sys.argv[1]

for i in range (0,256):
  rev_dns_addr=addr_range+'.'+str(i)
  result=subprocess.run(['nslookup', rev_dns_addr], stdout=subprocess.PIPE)
  print(result.stdout)
```

ISSES

Co-funded by the Erasmus+ Programme of the European Union

Getting information from SMTP

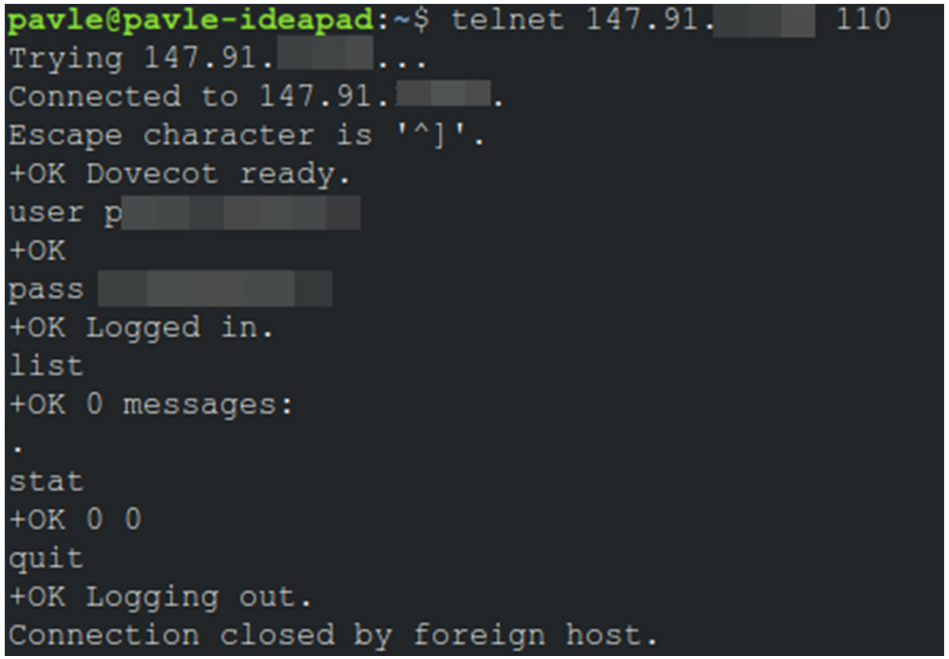
- Try to connect to mail server using SMTP
- Some SMTP commands
  - HELO – identify sender domain name
  - VRFY – verify the availability of the server
  - RCPT – specify message recipient
  - …
  - Metasploit: smtp_enum



ISSES
Co-funded by the Erasmus+ Programme of the European Union

Email – POP3 information

- POP3 commands
  - USER <username>
  - PASS <password>
  - STAT
  - LIST
  - RETR
  - DELE
  - RSET
  - TOP
  - QUIT



ISSES
Co-funded by the Erasmus+ Programme of the European Union

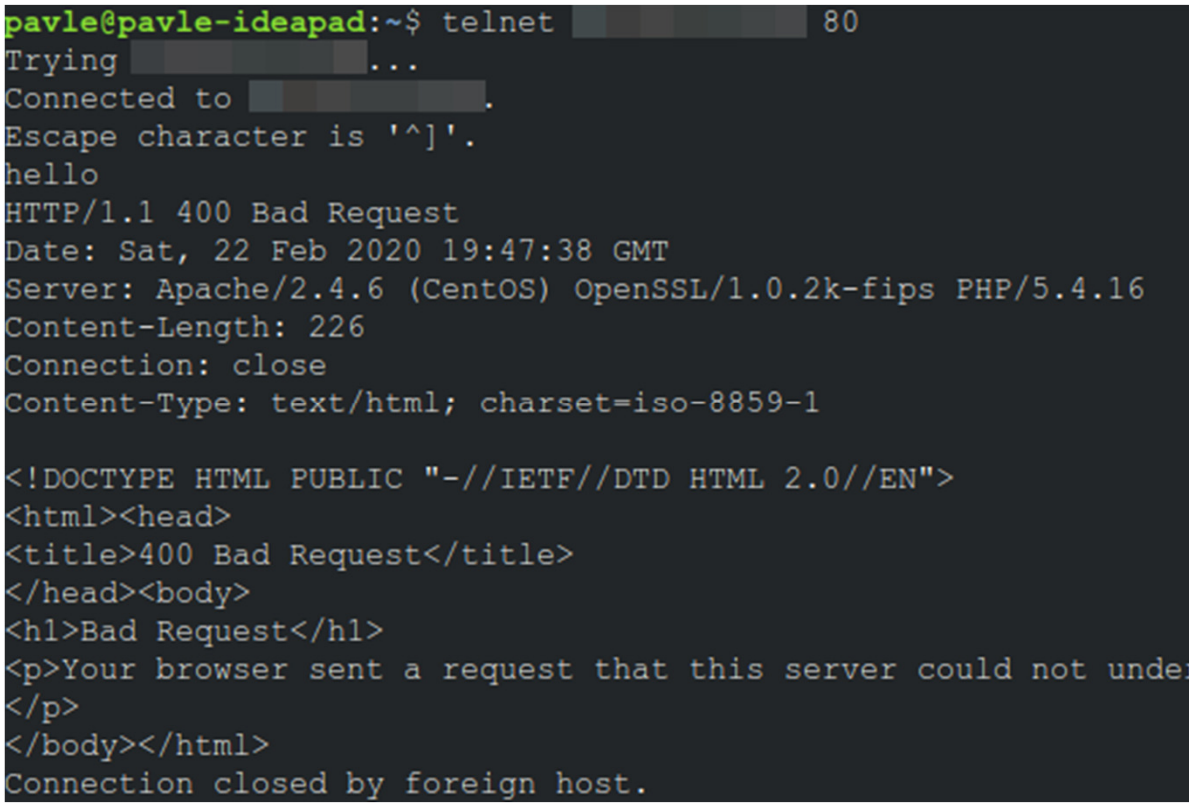
Active directory / LDAP

- Stores users, profiles, passwords,…
- LDAP – TCP/UDP 389
- LDAP tools:
  - Jxplorer
  - LDAP admin tool
  - LDAP Account manager
  - Active directory explorer

ISSES
Co-funded by the Erasmus+ Programme of the European Union

Web server enumeration

- Various tools for spidering/web crawling:
  - Screaming Frog
  - Apify
  - DeepCrawl
  - Wild Shark
  - Scraper,…



ISSES
Co-funded by the Erasmus+ Programme of the European Union

SMB enumeration

- Server Message Block (SMB) – protocol for file, printer sharing
- Different versions on Windows 7, 8, 10.
- 33 SMB-related nmap scripts included in the implementation of nmap
- Metasploit smb tools

```
pavle@pavle-ideapad:~$ nmap --script smb-enum-shares.nse -p445 192.168.1.0/24
Starting Nmap 7.80 ( https://nmap.org ) at 2020-11-05 16:30 CET
Nmap scan report for _gateway (192.168.1.1)
Host is up (0.0090s latency).

Nmap scan report for 192.168.1.144
Host is up (0.016s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds

Host script results:
| smb-enum-shares:
|   account_used: guest
|   \\192.168.1.144\Backup:
|     Type: STYPE_DISKTREE
|     Comment:
|     Users: 0
|     Max Users: <unlimited>
|     Path: C:\storage\backup
|     Anonymous access: READ/WRITE
|     Current user access: READ/WRITE
|   \\192.168.1.144\Configfiles:
|     Type: STYPE_DISKTREE
|     Comment:
|     Users: 0
|     Max Users: <unlimited>
|     Path: C:\storage\.config
|     Anonymous access: READ/WRITE
|     Current user access: READ/WRITE
|   \\192.168.1.144\Downloads:
|     Type: STYPE_DISKTREE
|     Comment:
|     Users: 0
|     Max Users: <unlimited>
|     Path: C:\storage\downloads
|     Anonymous access: READ/WRITE
|     Current user access: READ/WRITE
|   \\192.168.1.144\IPC$:
|     Type: STYPE_IPC_HIDDEN
|     Comment: IPC Service (OpenELEC)
|     Users: 1
|     Max Users: <unlimited>
|     Path: C:\tmp
|     Anonymous access: READ/WRITE
|     Current user access: READ/WRITE
```

ISSES

Co-funded by the Erasmus+ Programme of the European Union

Getting information from NetBIOS

- Used to access information from a remote computer in LAN
- Enabled by default, but best practice is to filter over WAN ports
- Runs over TCP (NBT – NetBIOS over TCP)
  - UDP 137 – name services
  - UDP 138 – datagram services
  - TCP 139 – session services

```
pavle@pavle-ideapad:~$ nmblookup -A 192.168.1.108
Looking up status of 192.168.1.108
        PAVLE-PC        <00> -         B <ACTIVE>
        WORKGROUP       <00> - <GROUP> B <ACTIVE>
        PAVLE-PC        <20> -         B <ACTIVE>
        WORKGROUP       <1e> - <GROUP> B <ACTIVE>

        MAC Address = CC-AF-78-30-D0-DB
```

ISSES
Co-funded by the Erasmus+ Programme of the European Union

NetBIOS names

Name	Hex Code	Type	Information
<computername>	00	U	Workstation Service
<computername>	01	U	Messenger Service
<\\--__MSBROWSE__>	01	G	Master Browser
<computername>	03	U	Messenger Service
<computername>	06	U	RAS Server Service

```
pavle@pavle-ideapad:~$ nmblookup -A 192.168.1.100
Looking up status of 192.168.1.100
        CUBOX-VAMP      <00> -          B <ACTIVE>
        CUBOX-VAMP      <03> -          B <ACTIVE>
        CUBOX-VAMP      <20> -          B <ACTIVE>
        ..__MSBROWSE__. <01> - <GROUP> B <ACTIVE>
        WORKGROUP       <1d> -          B <ACTIVE>
        WORKGROUP       <1e> - <GROUP> B <ACTIVE>
        WORKGROUP       <00> - <GROUP> B <ACTIVE>

        MAC Address = 00-00-00-00-00-00
```

ISSES
Co-funded by the Erasmus+ Programme of the European Union

NetBIOS scanning tools

- SuperScan - https://www.filecroco.com/download-superscan/
- Hyena - https://www.systemtools.com/hyena/download.htm
- Winfingerprint - https://packetstormsecurity.com/files/38356/winfingerprint-0.6.2.zip.html
- NetBIOS enumerator - http://nbtenum.sourceforge.net/
- Nsauditor - http://www.nsauditor.com/

ISSES
Co-funded by the Erasmus+ Programme of the European Union