



The background features a photograph of the Indian Institute of Technology (IIT) Kharagpur's main building, which is white with a flag flying from a pole.

NPTEL ONLINE CERTIFICATION COURSES

Course Name: Ethical Hacking

Faculty Name: Prof. Indranil Sen Gupta

Department : Computer Science and Engineering

Topic

Lecture 56: The NMAP Tool: A Relook (Part I)

Logos: IIT Kharagpur logo, Swayam logo, and a circular emblem.

CONCEPTS COVERED

- Introduction to NMAP
- Basic NMAP features
- Host discovery using NMAP

Logos: IIT Kharagpur logo, Swayam logo, and a circular emblem.

Introduction to Network Mapper (NMAP)

- NMAP is a free, open-source tool for vulnerability scanning and network discovery.
- Network administrators use NMAP for a variety of reasons:
 - Essentially a port scanning tool.
 - The packets that are sent out return with IP addresses and a wealth of other data.
 - Can be used to:
 - Discover hosts that are available on a network, and services that they offer.
 - Find open ports and detect security risks.
 - Determine OS versions.
 - Variety of other things ...



3

The History

- NMAP is a well-known and freely available security scanner developed by Gordon Lyon in 1997.
 - Available on: <https://nmap.org>
 - Several versions released since then.
- Generic command to run NMAP on command prompt:
`nmap [scan types] [options] <host or network ...>`



4

The Main NMAP Features

A. Host Discovery

- Which hosts are alive? --- Various approaches are available

B. Port Scanning

- What services are available? --- By enumerating the open ports

C. Service and Version Detection

- Which version is running? --- Identify application name and version number

D. OS Detection

- Which OS version is running? --- Also identify some hardware characteristics



5

(A) Host Discovery using NMAP



6

What is Host Discovery?

- The most basic step in network mapping.
 - Multiple hosts are queried (called **ping sweep** operation)
- Various host scan techniques are supported by NMAP:
 - a) ICMP sweep
 - b) Broadcast ICMP
 - c) Non-Echo ICMP
 - d) TCP sweep
 - e) UDP sweep

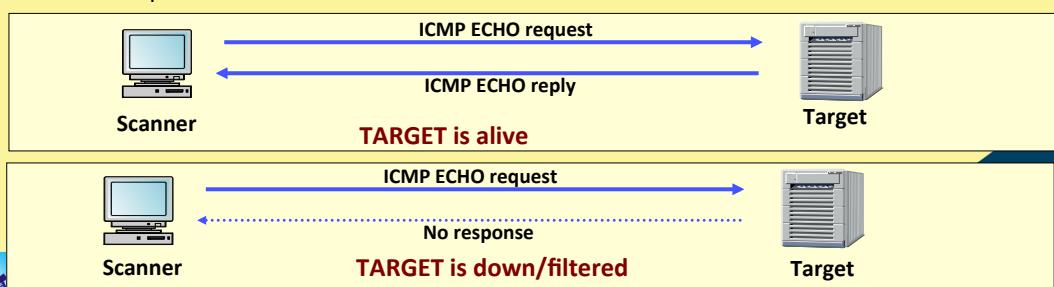


7

(a) Host discovery using ICMP Sweep

- How it works?
 - Send out an **ICMP ECHO request** (ICMP type 8)
 - If an **ICMP ECHO reply** (ICMP type 0) is received → **TARGET IS ALIVE**
 - No response is received → **TARGET IS DOWN**

- Easy to implement
- Rather slow
- Easy to block



8

- To perform ICMP echo sweep **-PE** option is used.
- We send an ICMP echo request from 10.5.23.251 to 10.5.23.209.
- In response to this 10.5.23.209 replies with an ICMP echo reply.

```
root@root:~# nmap -PE 10.5.23.209 --packet-trace --disable-arp-ping
Starting Nmap 7.70 ( https://nmap.org ) at 2019-09-26 08:47 EDT
SENT (0.0664s) ICMP [10.5.23.251 > 10.5.23.209 Echo request (type=8/code=0) id=9047 seq=0] IP [ttl=41 id=15635 iplen=28 ]
RCVD (0.0666s) ICMP [10.5.23.209 > 10.5.23.251 Echo reply (type=0/code=0) id=9047 seq=0] IP [ttl=128 id=7838 iplen=28 ]
```

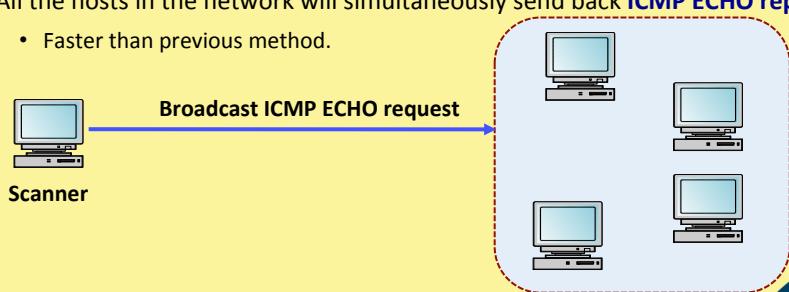


9

(b) Host discovery using Broadcast ICMP

- How it works?
 - Send out an **ICMP ECHO request** to the network and/or broadcast address.
 - All the hosts in the network will simultaneously send back **ICMP ECHO reply** packets.
 - Faster than previous method.

- Most routers block this.
- Windows ignore these requests.



10

(c) Host discovery using Non-ECHO ICMP

- How it works?

- Instead of ICMP ECHO request, the scanner sends out other types of ICMP messages.
 - The target will respond to such messages.
- **Approach 1:** Send ICMP type 13 messages (**TIMESTAMP**)
 - The scanner queries current time to the target.
- **Approach 2:** Send ICMP type 17 messages (**ADDRESS MASK REQUEST**)
 - The scanner queries subnet mask to the target (this feature is used by diskless workstations during booting)



11

- To perform ICMP non echo sweep **-PP** and **-PM** option are used.

- **-PP** is used for ICMP timestamp request (type 13)
- **-PM** is used for address mask request (type 17)

```
File Edit View Search Terminal Help
root@root:~# nmap -PP 10.5.23.209 --packet-trace --disable-arp-ping
Starting Nmap 7.70 ( https://nmap.org ) at 2019-09-26 08:48 EDT
SENT (0.0335s) ICMP [10.5.23.251 > 10.5.23.209] Timestamp request (type=13/code=0) id=25777 seq=0 orig=0 recv=0 trans=0] IP [ttl=59 id=21382 iplen=40 ]
RCVD (0.0335s) ICMP [10.5.23.209 > 10.5.23.251] Timestamp reply (type=14/code=0) id=25777 seq=0 orig=0 recv=2697838338 trans=2697838338] IP [ttl=128 id=8845 iplen=40 ]
```



12

```

File Edit View Search Terminal Help
root@root:~# nmap -PM 10.5.23.209 --packet-trace --disable-arp-ping
Starting Nmap 7.70 ( https://nmap.org ) at 2019-09-26 08:50 EDT
SENT (0.0346s) ICMP [10.5.23.251 > 10.5.23.209 Address mask request ( type=17/code=0) id=38772 seq=0 mask=0.0.0.0] IP [ttl=53 id=17281 iple n=32 ]
SENT (1.0361s) ICMP [10.5.23.251 > 10.5.23.209 Address mask request ( type=17/code=0) id=33338 seq=0 mask=0.0.0.0] IP [ttl=44 id=34607 iple n=32 ]
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 2.04 seconds
root@root:~#

```



13

(d) Host discovery using TCP Sweep

- How it works?
 - The scanner sends out **TCP SYN** or **TCP ACK** packet to the target.
 - The port number can be suitably selected to prevent blocking by firewall.
 - Typical port numbers used: 21, 22, 23, 25, 80
- A drawback:
 - Firewalls can **spoof a RESET packet** for an IP address, so TCP Sweep may not be reliable.



14

- TCP sweep can be performed using two options:
 - **-PS** : for TCP SYN sweep
 - **-PA** : for TCP ACK sweep
- We show example with the **-PS** option.
 - We just show the command and final output.
 - Many other lines of information may be generated.
- We can also see why any port is closed/open using **--reason** option.
- TCP sweep is also used by default port scanning options:
 - **-sT, -p, -Pn**



15

(i) TCP Sweep using **-PS** (TCP SYN) : closed port

```

File Edit View Search Terminal Help
root@root:~# nmap -PS -p22 10.5.23.209 --packet-trace --disable-arp-ping
Starting Nmap 7.70 ( https://nmap.org ) at 2019-09-26 08:51 EDT
SENT (0.0356s) TCP 10.5.23.251:47643 > 10.5.23.209:22 S ttl=58 id=150
63 iplen=44 seq=1888104618 win=1024 <mss 1460>
RCVD (0.0357s) TCP 10.5.23.209:22 > 10.5.23.251:47643 RA ttl=128 id=1
0914 iplen=40 seq=0 win=0
Nmap scan report for 10.5.23.209
Host is up (0.00016s latency).

PORT      STATE SERVICE
22/tcp    closed ssh
MAC Address: F8:B1:56:D7:2B:77 (Dell)
  
```



16

(ii) TCP Sweep using -PS (TCP SYN) : open port

```
File Edit View Search Terminal Help
root@root: # nmap -PS -p135 --packet-trace 10.5.23.209
Starting Nmap 7.70 ( https://nmap.org ) at 2019-09-26 08:35 EDT
SENT (0.0351s) TCP 10.5.23.251:63314 > 10.5.23.209:135 S ttl=57 id=57
742 iplen=44 seq=1578174756 win=1024 <mss 1460>
RCVD (0.0352s) TCP 10.5.23.209:135 > 10.5.23.251:63314 SA ttl=128 id=
4866 iplen=44 seq=2352554629 win=8192 <mss 1460>
Nmap scan report for 10.5.23.209
Host is up (0.00015s latency).

PORT      STATE SERVICE
135/tcp    open  msrpc
MAC Address: F8:B1:56:D7:2B:77 (Dell)

Nmap done: 1 IP address (1 host up) scanned in 0.04 seconds
```

Port 135: MSRPC
 (Microsoft
 Remote
 Procedure Call)



17

(iii) TCP Sweep using -PS with --reason option

```
File Edit View Search Terminal Help
root@root: # nmap -PS -p22 10.5.23.209 --reason
Starting Nmap 7.70 ( https://nmap.org ) at 2019-09-26 08:37 EDT
Nmap scan report for 10.5.23.209
Host is up, received arp-response (0.00017s latency).

PORT      STATE SERVICE REASON
22/tcp    closed ssh      reset ttl 128
MAC Address: F8:B1:56:D7:2B:77 (Dell)

Nmap done: 1 IP address (1 host up) scanned in 0.04 seconds
root@root: # nmap -PS -p135 10.5.23.209 --reason
Starting Nmap 7.70 ( https://nmap.org ) at 2019-09-26 08:37 EDT
Nmap scan report for 10.5.23.209
Host is up, received arp-response (0.00017s latency).

PORT      STATE SERVICE REASON
135/tcp   open  msrpc   syn-ack ttl 128
MAC Address: F8:B1:56:D7:2B:77 (Dell)

Nmap done: 1 IP address (1 host up) scanned in 0.04 seconds
root@root: #
```



18

(e) Host discovery using UDP Sweep

- How it works?
 - The scanner sends a UDP datagram to the target.
 - If no **ICMP PORT UNREACHABLE** message is received → **TARGET IS ALIVE**
 - If an **ICMP PORT UNREACHABLE** message is received → **TARGET IS DOWN**
- Routers can drop UDP packets as they cross the Internet.
 - Many UDP services do not respond.
 - Firewalls typically drop UDP packets (except DNS).
 - Not very reliable



19

- To perform UDP sweep **-PU** option is used.
- The **-sU** option also uses UDP sweep.
- In the example, unreachable means the UDP port is considered as closed.

```
File Edit View Search Terminal Help
root@root:~# nmap -PU -p135 10.5.23.209 --packet-trace --disable-arp-ping
Starting Nmap 7.70 ( https://nmap.org ) at 2019-09-26 09:02 EDT
SENT (0.0406s) UDP 10.5.23.251:35066 > 10.5.23.209:40125 ttl=55 id=57
462 ipLen=28
RCVD (0.0408s) ICMP [10.5.23.209 > 10.5.23.251 Port unreachable (type =3/code=3) ] IP [ttl=128 id=461 ipLen=56 ]
```



20

More on Host Detection

- By default NMAP uses all types of sweep operations in common scanning options such that it can get better details about any system.
- Commands that use all types (except UDP sweep) are **-sP**, **-sn**, **-sL**, **-Pn**, etc.
- We will show example of **-sP** command.
 - This is used to print whether all or specific hosts are up and running.

21



```
File Edit View Search Terminal Help
root@root:~# nmap -sP 10.5.23.180-210
Starting Nmap 7.70 ( https://nmap.org ) at 2019-09-26 07:16 EDT
Nmap scan report for 10.5.23.183
Host is up (0.0013s latency).
MAC Address: 04:92:26:6E:39:FC (Unknown)
Nmap scan report for 10.5.23.186
Host is up (0.00031s latency).
MAC Address: F8:B1:56:D7:29:1C (Dell)
Nmap scan report for 10.5.23.194
Host is up (0.00052s latency).
MAC Address: A4:5D:36:CF:75:14 (Hewlett Packard)
Nmap scan report for 10.5.23.203
Host is up (0.016s latency).
MAC Address: 18:66:DA:2D:C5:F8 (Dell)
Nmap scan report for 10.5.23.209
Host is up (0.00014s latency).
MAC Address: F8:B1:56:D7:2B:77 (Dell)
Nmap done: 31 IP addresses (5 hosts up) scanned in 0.49 seconds
root@root:~#
```

22



```
File Edit View Search Terminal Help
root@root: # nmap -sn 10.5.23.209 --packet-trace --disable-arp-ping
Starting Nmap 7.70 ( https://nmap.org ) at 2019-09-26 07:58 EDT
SENT (0.0016s) ICMP [10.5.23.251 > 10.5.23.209 Echo request (type=8/code=0) id=48998 seq=0] IP [ttl=37 id=4096 iplen=28]
SENT (0.0017s) TCP 10.5.23.251:36797 > 10.5.23.209:443 S ttl=53 id=53664 iplen=44 seq=2649164987 win=1024 <mss 1460>
SENT (0.0018s) TCP 10.5.23.251:36797 > 10.5.23.209:80 A ttl=42 id=25327 iplen=40 seq=0 win=1024
SENT (0.0019s) ICMP [10.5.23.251 > 10.5.23.209 Timestamp request (type=13/code=0) id=11069 seq=0 orig=0 recv=0 trans=0] IP [ttl=39 id=43055 iplen=40]
RCVD (0.0018s) ICMP [10.5.23.209 > 10.5.23.251 Echo reply (type=0/code=0) id=48998 seq=0] IP [ttl=128 id=31703 iplen=28]
NSOCK INFO [0.0020s] nssock_iiod_new2(): nssock_iiod_new (IOD #1)
```

All type of sweep options are used with **-sn** except UDP.
--packet-trace gives the details.



23

Some other NMAP commands for host discovery

```
File Edit View Search Terminal Help
root@root: # nmap -sL 10.5.23.209-215
Starting Nmap 7.70 ( https://nmap.org ) at 2019-09-26 09:05 EDT
Nmap scan report for 10.5.23.209
Nmap scan report for 10.5.23.210
Nmap scan report for 10.5.23.211
Nmap scan report for 10.5.23.212
Nmap scan report for 10.5.23.213
Nmap scan report for 10.5.23.214
Nmap scan report for 10.5.23.215
Nmap done: 7 IP addresses (0 hosts up) scanned in 0.00 seconds
root@root: #
```

-sL: listing the IP of any range or subnet (list scan)



24

```

File Edit View Search Terminal Help
root@root: # nmap -PN 10.5.23.209-235
Starting Nmap 7.0 ( https://nmap.org ) at 2019-09-26 09:10 EDT
Nmap scan report for 10.5.23.209
Host is up (0.00031s latency).
Not shown: 996 closed ports
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
5357/tcp   open  wsdapi
MAC Address: F8:B1:56:D7:2B:77 (Dell)

Nmap scan report for 10.5.23.222
Host is up (0.00018s latency).
All 1000 scanned ports on 10.5.23.222 are closed
MAC Address: 20:47:47:59:10:3D (Dell)

Nmap scan report for 10.5.23.225
Host is up (0.00013s latency).
All 1000 scanned ports on 10.5.23.225 are closed
MAC Address: 00:25:64:94:C8:74 (Dell)

Nmap done: 27 IP addresses (3 hosts up) scanned in 2.14 seconds

```

-PN : Check firewall and print open ports if firewall is off; else print the active IPs.



Activated
Go to Settings

25

```

File Edit View Search Terminal Help
root@root: # nmap -sn 10.5.23.209-230
Starting Nmap 7.0 ( https://nmap.org ) at 2019-09-26 10:25 EDT
Nmap scan report for 10.5.23.209
Host is up (0.00022s latency).
MAC Address: F8:B1:56:D7:2B:77 (Dell)
Nmap scan report for 10.5.23.225
Host is up (0.00047s latency).
MAC Address: 00:25:64:94:C8:74 (Dell)
Nmap done: 22 IP addresses (2 hosts up) scanned in 0.64 seconds
root@root: #

```

Multiple host discovery (by specifying list)

```

File Edit View Search Terminal Help
root@root: # nmap -sn 10.5.23.209,203
Starting Nmap 7.0 ( https://nmap.org ) at 2019-09-26 10:26 EDT
Nmap scan report for 10.5.23.203
Host is up (0.00050s latency).
MAC Address: 18:66:DA:2D:C5:F8 (Dell)
Nmap scan report for 10.5.23.209
Host is up (0.00032s latency).
MAC Address: F8:B1:56:D7:2B:77 (Dell)
Nmap done: 2 IP addresses (2 hosts up) scanned in 0.01 seconds
root@root: #

```

Multiple host discovery (by specifying range)



26

NMAP Command Options for Host Discovery

- **-sI:** List Scan - simply list targets to scan
- **-sP:** Ping Scan - go no further than determining if host is online
- **-PN:** Treat all hosts as online -- skip host discovery
- **-PS/PA/PU [portlist]:** TCP SYN/ACK or UDP discovery to given ports
- **-PE/PP/PM:** ICMP echo, timestamp, and netmask request discovery probes
- **-PO [protocol list]:** IP Protocol Ping
- **-n/-R:** Never do DNS resolution/Always resolve [default: sometimes]
- **--dns-servers <serv1[,serv2],...>:** Specify custom DNS servers
- **--system-dns:** Use OS's DNS resolver
- **-sU:** UDP Scan



27



NPTEL ONLINE CERTIFICATION COURSES

Thank you!

The slide features the NPTEL logo at the top right, which includes the text "FREE ONLINE EDUCATION swayam स्वैयम् भारत, उन्नति भारत". Below the logo, the text "NPTEL ONLINE CERTIFICATION COURSES" is displayed in orange. A large, stylized blue "Thank you!" is centered in the lower right area. The background is yellow with a blue diagonal stripe on the left side.

28



NPTEL ONLINE CERTIFICATION COURSES

Course Name: Ethical Hacking

Faculty Name: Prof. Indranil Sen Gupta

Department : Computer Science and Engineering

Topic

Lecture 57: The NMAP Tool: A Relook (Part II)

CONCEPTS COVERED

- Post scanning using NMAP
- Various ways to carry out port scan



Port Scanning using NMAP



3

Introduction

- To determine what services are running or LISTENing.
 - Each running TCP service is associated with a port number, which *listens* for incoming connections.
 - Each running UDP service is associated with a port number.
- Various port scanning techniques in NMAP:
 - a) TCP Connect scan
 - b) TCP SYN scan
 - c) TCP Stealth scan
 - d) FTP Bounce scan



4

(a) TCP Connect scan

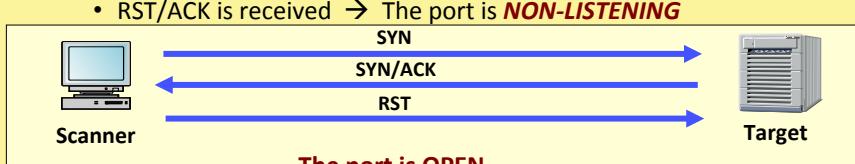
- How it works?
 - Use basic TCP connection establishment mechanism.
 - Complete 3-way handshake.
- Easy to detect by inspecting the system log.



5

(b) TCP SYN scan

- How it works?
 - Do not establish complete connection (half-open scanning).
 - SYN/ACK is received → The port is **LISTENING**
 - Immediately terminate connection by sending RST.
 - RST/ACK is received → The port is **NON-LISTENING**



6

- The **-sT** scan uses both TCP SYN and TCP ACK packets.
- It also uses ICMP ECHO sweep for checking if host is up or not.

```
root@root:~# nmap -sT -p22 10.5.23.209
Starting Nmap 7.70 ( https://nmap.org ) at 2019-09-26 09:30 EDT
Nmap scan report for 10.5.23.209
Host is up (0.00015s latency).

PORT      STATE SERVICE
22/tcp    closed ssh
MAC Address: F8:B1:56:D7:2B:77 (Dell)

Nmap done: 1 IP address (1 host up) scanned in 0.06 seconds
root@root:~# nmap -sT -p135 10.5.23.209
Starting Nmap 7.70 ( https://nmap.org ) at 2019-09-26 09:31 EDT
Nmap scan report for 10.5.23.209
Host is up (0.00020s latency).

PORT      STATE SERVICE
135/tcp   open  msrpc
MAC Address: F8:B1:56:D7:2B:77 (Dell)

Nmap done: 1 IP address (1 host up) scanned in 0.07 seconds
root@root:~#
```

Acti
Go to

7



```
File Edit View Search Terminal Help
root@root:~# nmap -sT -p22 10.5.23.209 --packet-trace --disable-arp-ping
Starting Nmap 7.70 ( https://nmap.org ) at 2019-09-26 09:25 EDT
SENT (0.0337s) ICMP [10.5.23.251 > 10.5.23.209 Echo request (type=8/code=0) id=25072 seq=0] IP [ttl=38 id=51804 iplen=28 ]
SENT (0.0339s) TCP 10.5.23.251:59547 > 10.5.23.209:443 S ttl=45 id=22375 iplen=44 seq=4247547709 win=1024 <mss 1460>
SENT (0.0341s) TCP 10.5.23.251:59547 > 10.5.23.209:80 A ttl=51 id=56071 iplen=40 seq=0 win=1024
CONN (0.0356s) TCP localhost > 10.5.23.209:22 => Operation now in progress
CONN (0.0357s) TCP localhost > 10.5.23.209:22 => Connection refused
Nmap scan report for 10.5.23.209
Host is up (0.00020s latency).
```

-sT packet trace
for closed port

```
PORT      STATE SERVICE
22/tcp    closed ssh
```



8

```
root@root:~# nmap -sT -p135 10.5.23.209 --packet-trace --disable-arp-ping
Starting Nmap 7.70 ( https://nmap.org ) at 2019-09-26 09:27 EDT
SENT (0.0333s) ICMP [10.5.23.251 > 10.5.23.209 Echo request (type=8/code=0) id=31901 seq=0] IP [ttl=50 id=18265 iplen=28 ]
SENT (0.0335s) TCP 10.5.23.251:53552 > 10.5.23.209:443 S ttl=58 id=17007 iplen=44 seq=1685614607 win=1024 <mss 1460>
SENT (0.0336s) TCP 10.5.23.251:53552 > 10.5.23.209:80 A ttl=49 id=51078 iplen=40 seq=0 win=1024
CONN (0.0354s) TCP localhost > 10.5.23.209:135 => Operation now in progress
CONN (0.0355s) TCP localhost > 10.5.23.209:135 => Connected
Nmap scan report for 10.5.23.209
Host is up (0.00024s latency).

PORT      STATE SERVICE
135/tcp    open  msrpc
MAC Address: F8:B1:56:D7:2B:77 (Dell)
```

-sT packet trace
for open port



9

(c) TCP Stealth scan

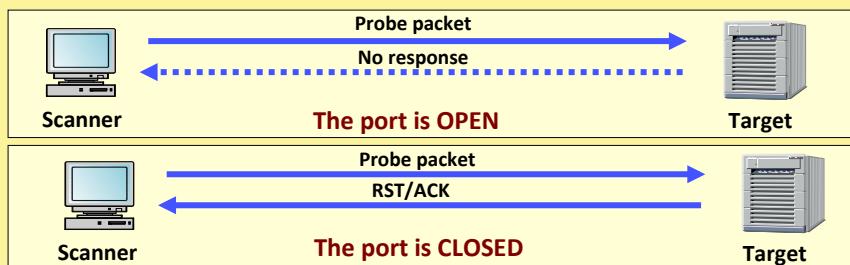
- Basic idea:
 - Carry out port scanning while avoiding detection.
 - Try to hide themselves among normal network traffic.
 - Not to be logged (stealth).
- How it works?
 - Flag probe packets (also known as *Inverse Mapping*)
 - Response is sent back only by closed port.
 - Intruder determines what services do not exist, and can infer the ones that exist.
 - Slow scan rate
 - Difficult to detect, and needs long history log.



10

- How it can be done?

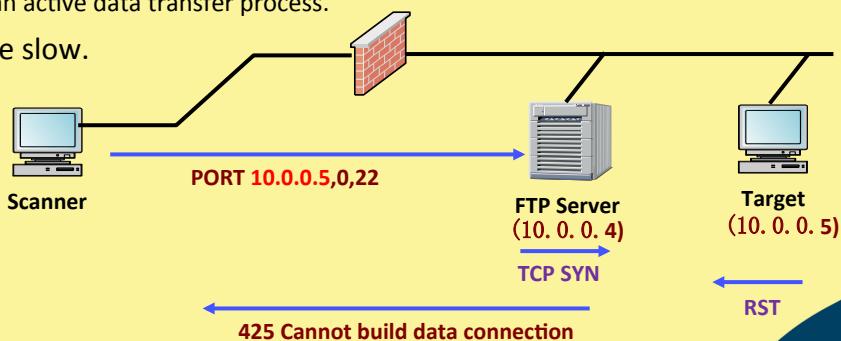
- RFC793 talks about how to handle wrong packets.
 - Closed ports → Reply with a RESET packet
 - Open ports → Ignore any packet in question
- Various ways:
 - Send a RST scan packet.
 - Send a FIN probe with FIN flag set.



11

(d) FTP Bounce scan

- How it works?
 - Connect to a FTP server, and establish a control connection, and ask the FTP server to initiate an active data transfer process.
- Quite slow.



12

Other port scanning options in NMAP

```
File Edit View Search Terminal Help
root@root:~# nmap -p135-200 10.5.23.209
Starting Nmap 7.70 ( https://nmap.org ) at 2019-09-26 09:52 EDT
Nmap scan report for 10.5.23.209
Host is up (0.00026s latency).
Not shown: 64 closed ports
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
MAC Address: F8:B1:56:D7:2B:77 (Dell)

Nmap done: 1 IP address (1 host up) scanned in 1.17 seconds
root@root:~#
```

Specify the port numbers to be scanned using **-p** option



13

```
File Edit View Search Terminal Help
root@root:~# nmap -F 10.5.23.209
Starting Nmap 7.70 ( https://nmap.org ) at 2019-09-26 09:53 EDT
Nmap scan report for 10.5.23.209
Host is up (0.00030s latency).
Not shown: 96 closed ports
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
5357/tcp   open  wsdapi
MAC Address: F8:B1:56:D7:2B:77 (Dell)

Nmap done: 1 IP address (1 host up) scanned in 1.18 seconds
root@root:~#
```

Scan fewer ports than the default scan using **-F** option (fast mode)



14

```

File Edit View Search Terminal Help
root@root:~# nmap --top-ports 3 10.5.23.209
Starting Nmap 7.70 ( https://nmap.org ) at 2019-09-26 09:54 EDT
Nmap scan report for 10.5.23.209
Host is up (0.00016s latency).

PORT      STATE SERVICE
23/tcp    closed telnet
80/tcp    closed http
443/tcp   closed https
MAC Address: F8:B1:56:D7:2B:77 (Dell)

Nmap done: 1 IP address (1 host up) scanned in 0.04 seconds
root@root:~#

```

Scan most common ports using **--top-ports** option



15

```

File Edit View Search Terminal Help
root@root: # nmap -sO 10.5.23.209
Starting Nmap 7.70 ( https://nmap.org ) at 2019-09-26 10:30 EDT
Nmap scan report for 10.5.23.209
Host is up (0.00034s latency).
Not shown: 237 closed protocols
PROTOCOL STATE      SERVICE
1      open        icmp
2      open|filtered igmp
4      open|filtered ipv4
6      open        tcp
17     open        udp
41     open|filtered ipv6
50     open|filtered esp
51     open|filtered ah
69     open|filtered sat-mon
101    open|filtered ifmp
107    open|filtered a/n
132    open|filtered sctp
138    open|filtered manet
161    open|filtered unknown
186    open|filtered unknown
192    open|filtered unknown

```

IP protocol scan using **-sO** option



16

NMAP Command Options for Port Scanning

- Scan Techniques:
 - -sS/sT/sA/sW/sM: TCP SYN/Connect()/ACK/Window/Maimon scans
 - -sN/sF/sX: TCP Null, FIN, and Xmas scans
 - -b <FTP relay host>: FTP bounce scan
- Port specification and Scan Order:
 - -p <port ranges>: Only scan specified ports
 - Ex: -p22; -p1-65535; -p U:53,111,137,T:21-25,80,139,8080
 - -F: Fast mode - Scan fewer ports than the default scan
 - -r: Scan ports consecutively - don't randomize
 - --top-ports <number>: Scan <number> most common ports



17

NPTEL ONLINE CERTIFICATION COURSES

Thank you!

18



The slide features a blue and yellow diagonal banner on the right side. At the top of the banner is the logo of the Indian Institute of Technology (IIT) Kharagpur, which includes a tree and the text "INDIAN INSTITUTE OF TECHNOLOGY KHARAGPUR 1951". To the right of the IIT logo is the "swayam" logo, which includes the text "FREE ONLINE EDUCATION" and "swayam" with a graduation cap icon, along with the tagline "शिक्षण मार्ग, ज्ञान मार्ग". Further to the right is a circular emblem featuring a flower design.

NPTEL ONLINE CERTIFICATION COURSES

Course Name: Ethical Hacking

Faculty Name: Prof. Indranil Sen Gupta

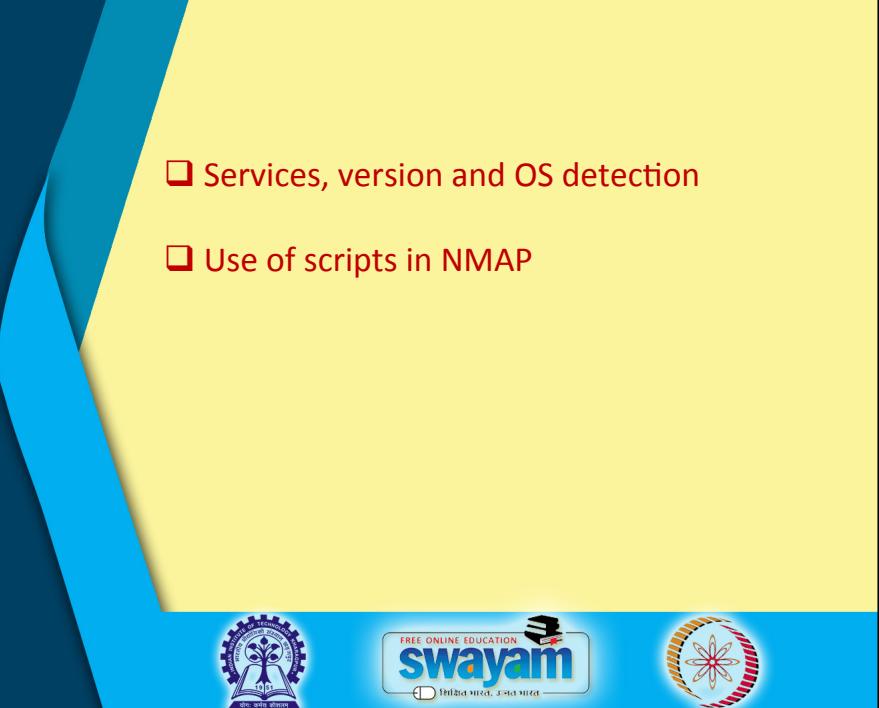
Department : Computer Science and Engineering

Topic

Lecture 58: The NMAP Tool: A Relook (Part III)

CONCEPTS COVERED

- Services, version and OS detection
- Use of scripts in NMAP



(C) Services, Version and OS Detection



3

Introduction

- Some operating systems respond with specific messages in response to certain requests.
 - Helps in identification.
- TCP/IP fingerprinting (IP stack implementation will response differently).
 - FIN probe, Bogus Flag probe
 - TCP initial sequence number sampling, TCP initial window, ACK value
 - ICMP error quenching, message quoting, ICMP echo integrity
 - IP: DF, TOS, Fragmentation



4

Some Specific Examples

- **ACK:** sending ***FIN/PSH/URG*** to a closed port
 - Most OS → ACK with the same sequence number.
 - Windows → ACK with sequence number + 1
- **Type of Service:** Probing with ***ICMP_PORT_UNREACHABLE*** message
 - Most OS → Returns with TOS = 0.
 - Linux → Returns with TOS = 0xC0.



5

```

File Edit View Search Terminal Help
root@root: # nmap -O 10.5.23.209
Starting Nmap 7.70 ( https://nmap.org ) at 2019-09-26 09:57 EDT
Nmap scan report for 10.5.23.209
Host is up (0.00041s latency).
Not shown: 996 closed ports
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
5357/tcp   open  wsdapi
MAC Address: F8:B1:56:D7:2B:77 (Dell)
Device type: general purpose
Running: Microsoft Windows 10
OS CPE: cpe:/o:microsoft:windows_10
OS details: Microsoft Windows 10 1507 - 1607
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 7.01 seconds

```

OS detection using the
-O option



6

```

File Edit View Search Terminal Help
root@root: # nmap -sV 10.5.23.209
Starting Nmap 7.70 ( https://nmap.org ) at 2019-09-26 10:14 EDT
Nmap scan report for 10.5.23.209
Host is up (0.00028s latency).
Not shown: 996 closed ports
PORT      STATE SERVICE      VERSION
135/tcp    open  msrpc        Microsoft Windows RPC
139/tcp    open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp    open  microsoft-ds Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)
5357/tcp   open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
MAC Address: F8:B1:56:D7:2B:77 (Dell)
Service Info: Host: DESKTOP-LRRL557; OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at h
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 22.14 seconds
root@root: #

```

Version detection using
the **-sV** option



7

NMAP Command Options for OS Detection

- Service / Version Detection:
 - -sV: Probe open ports to determine service/version info
 - --version-intensity <level>: Set from 0 (light) to 9 (try all probes)
 - --version-light: Limit to most likely probes (intensity 2)
 - --version-all: Try every single probe (intensity 9)
 - --version-trace: Show detailed version scan activity (for debugging)
- OS Detection:
 - -O: Enables OS detection
 - --osscan-limit: Limit OS detection to promising targets
 - --osscan-guess: Guess OS more aggressively



8

Use of Scripts in NMAP



9

What are NMAP Scripts?

- There are 1000s of scripts available with NMAP to perform various operation.
- The scripts can have their own specific requirements, like some services running, port requirements, etc.
- We have already seen an example earlier:
`--script vuln` to check vulnerability in a system.
- Any script can be run using the command:
`--script <script name> <port # if required> <target>`



10

```

File Edit View Search Terminal Help
root@root:~# nmap --script vuln 10.5.23.209
Starting Nmap 7.70 ( https://nmap.org ) at 2019-09-26 10:33 EDT
Pre-scan script results:
| broadcast-avahi-dos:
|   Discovered hosts:
|     224.0.0.251
|     After NULL UDP avahi packet DoS (CVE-2011-1002).
|     Hosts are all up (not vulnerable).
Nmap scan report for 10.5.23.209
Host is up (0.000082s latency).
Not shown: 996 closed ports
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
5357/tcp   open  wsddapi
MAC Address: F8:B1:56:D7:2B:77 (Dell)

Host script results:
|_smb-vuln-ms10-054: false
|_smb-vuln-ms10-061: ERROR: Script execution failed (use -d to debug)
|_smb-vuln-ms17-010:
  VULNERABLE:

```

Vulnerability scan using the **--script vuln** option



Activate WiFi

11

```

File Edit View Search Terminal Help
root@root:~# nmap -sV --script http-malware-host 10.5.23.209
Starting Nmap 7.70 ( https://nmap.org ) at 2019-09-26 10:35 EDT
Nmap scan report for 10.5.23.209
Host is up (0.00018s latency).
Not shown: 996 closed ports
PORT      STATE SERVICE      VERSION
135/tcp    open  msrpc        Microsoft Windows RPC
139/tcp    open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp    open  microsoft-ds Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)
5357/tcp   open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-malware-host: Host appears to be clean
|_http-server-header: Microsoft-HTTPAPI/2.0
MAC Address: F8:B1:56:D7:2B:77 (Dell)
Service Info: Host: DESKTOP-LRRL557; OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/.
Nmap done: 1 IP address (1 host up) scanned in 17.27 seconds
root@root:~#

```

Detecting malware infection using **--script http-malware-host** option



Activate WiFi

12

```

File Edit View Search Terminal Tabs Help
root@root:~ x root@root:~
root@root:~# nmap --script http-methods -p80 10.5.23.245
Starting Nmap 7.70 ( https://nmap.org ) at 2019-09-26 10:44 EDT
Nmap scan report for 10.5.23.245
Host is up (0.029s latency).

PORT      STATE SERVICE
80/tcp    open  http
| http-methods:
|_ Supported Methods: GET HEAD POST OPTIONS
MAC Address: 08:00:27:47:19:5E (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 7.59 seconds
root@root:~#

```

Check whether a host is running web server on a particular port using **--script http-methods** option



13

```

File Edit View Search Terminal Help
root@root:~# nmap --script smb-brute.nse -p445 10.5.23.245
Starting Nmap 7.70 ( https://nmap.org ) at 2019-09-26 10:43 EDT
Nmap scan report for 10.5.23.245
Host is up (0.085s latency).

PORT      STATE SERVICE
445/tcp   open  microsoft-ds
MAC Address: 08:00:27:47:19:5E (Oracle VirtualBox virtual NIC)

Host script results:
| smb-brute:
|_ msfadmin:msfadmin => Valid credentials
|_ user:user => Valid credentials

Nmap done: 1 IP address (1 host up) scanned in 602.50 seconds
root@root:~#

```

Guess username and password using **--script smb-brute.nse** option
(This is possible only if port 445 is open, and takes a long time)



14

Some Issues

- For System Administrators to detect scanning:
 - Examine logs for suspicious packets
 - Identify connections not properly terminated
 - Analyze ports usage
- For scanners to avoid detection:
 - Randomize the sequence of ports being scanned
 - Slow scan: exceed the site detection threshold in IDS, 2 packets/day/site!
 - Use spoofed address in attack
 - Coordinated Scans: multiple scanners probe the same host or network



15

Recall: Some common NMAP scan options

- Scan a single target with default options (basic scan):


```
nmap 144.16.192.57
nmap www.someserver.com
```
- Scan multiple hosts at the same time:


```
nmap 144.16.192.25 144.16.192.70 10.2.75.38
```
- Scan a range of IP addresses:


```
nmap 144.16.192.100-150
```
- Scan an entire subnet:


```
nmap 144.16.192.0/24
```



16

- Scan a list of targets (IP addresses or host names stored in a file):
`nmap -iL scanlist.txt`
- Scan a specified number of random internet hosts:
`nmap -iR 5`
- Exclude targets from a scan
`nmap 144.16.192.0/24 --exclude 144.16.192.60-70`
`nmap 144.16.192.0/24 --excludefile xfile.txt`
- Perform an aggressive scan (use most commonly used options):
`nmap -A 10.3.100.65`



17

This slide features a large blue triangle on the left containing a photograph of a white building with a flag, identified as the Indian Institute of Technology Bombay. To the right of the triangle is a yellow section containing the NPTEL logo (a book with a gear and the text "NPTEL FREE ONLINE EDUCATION swayam स्वैयम् भारत, उन्नति भारत") and the text "NPTEL ONLINE CERTIFICATION COURSES". Below this is a large, stylized blue "Thank you!" message. The entire slide has a blue footer bar.

18



NPTEL ONLINE CERTIFICATION COURSES

Course Name: Ethical Hacking

Faculty Name: Prof. Indranil Sen Gupta

Department : Computer Science and Engineering

Topic

Lecture 59: Network Analysis using Wireshark

CONCEPTS COVERED

- About Wireshark
- Various menu options in Wireshark
- Packet capturing examples



Introduction

- What is network analysis or Sniffing?
 - It is a process of analyzing network activity by capturing network traffic.
 - Sniffer is a program that monitors the data travelling around the network.
 - Example tools: Wireshark, Solarwinds, Kismet and many others.
- Features of a network analyzer
 - Support for multiple protocols.
 - Graphical user interface.
 - Statistical report generation.



3

What is Wireshark?

- It is an open source tool for profiling network traffic and analyzing packets.
 - Often referred to as a network analyzer, network protocol analyzer or sniffer.
 - <http://www.wireshark.org>
- What does it do?
 - Captures network data and displays them in a readable format.
 - Logs network traffic for forensics and evidence.
 - Analyzes network traffic generated by various applications.



4

How Packet Sniffer works?

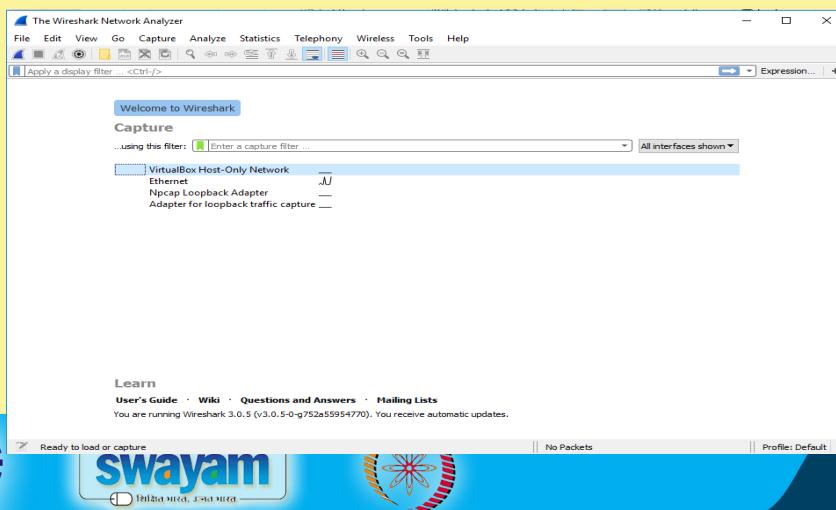
- Ethernet is the most widely used protocol used in a LAN.
 - At the data-link layer level.
- While running Wireshark the machine's network interface card (NIC) is put in ***promiscuous mode***.
 - In this mode, the sniffer can read all traffic on the network segment to which the NIC is connected (irrespective of the sender and the receiver).
 - Requires root privilege to set the NIC to promiscuous mode.
 - If the LAN uses a switch, then packets from other network segments cannot be captured.



5

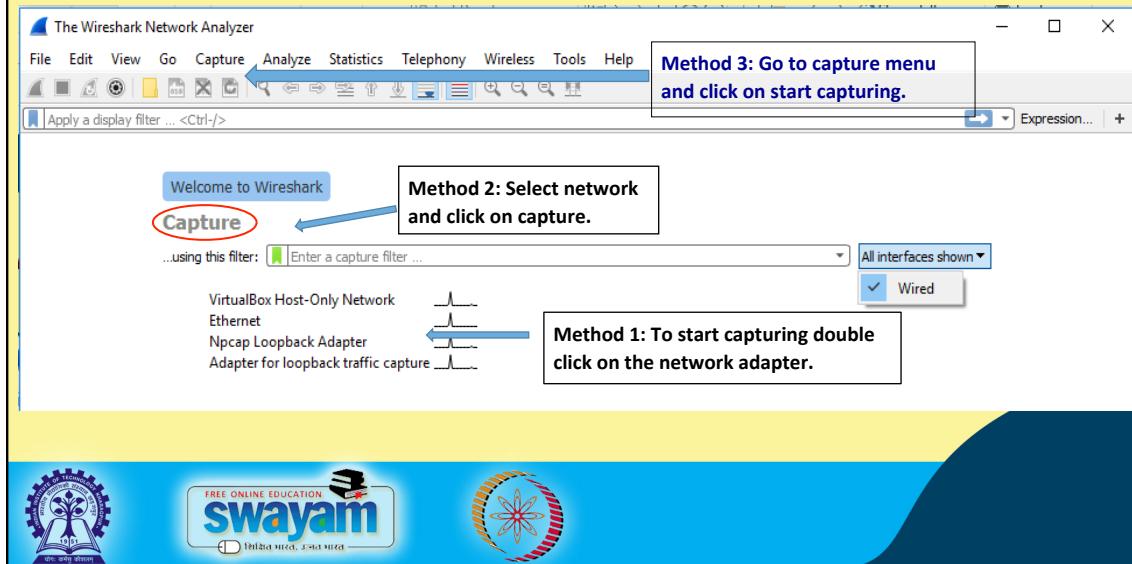
Wireshark

- Can be downloaded from: <http://www.wireshark.org>



6

Packet Capture using Wireshark



7

Packet Capturing Starts

The screenshot shows the Wireshark interface during a live capture session. A callout highlights the "Protocol Window" which displays the following information:

Packet summary

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	Cisco-C814B#	Spanning-tree...	STP	64	RST, Root = 28672/0/94:3fc:2:02:e1:c6 Cost = 60000 Port = 0x8033
2	0.376578	Cisco-C918B#	PVST+	STP	64	Conf. Root = 32768/1301/40:55:39:c9:88:c0 Cost = 0 Port = 0x8011
3	1.635372	10.5.23.2	10.5.0.5	OSPF	90	Hello Packet
4	1.635372	Cisco-C918B#	10.5.23.2	OSPF	90	LSR ID: 32768/1301/40:55:39:c9:88:c0
5	1.766771	Cisco-C918B#	PVST+	STP	64	Conf. Root = 32768/1301/40:55:39:c9:88:c0 Cost = 0 Port = 0x8033
6	3.674808	10.5.23.209	10.5.23.255	NBNS	64	Name query NB WPAD\00>
7	3.675393	fe80::4593::ff92:11:3	LLNMR	84	Standard query 0xb990 A wpad	
8	3.675561	10.5.23.209	224.0.0.252	LLNMR	16	Standard query 0xb990 A wpad
9	3.675571	10.5.18.84	10.5.23.209	ICMP	14	Port unreachable)
10	3.675582	10.5.18.88	10.5.23.209	ICMP	14	Port unreachable)
11	3.675985	fe80::4593::ff92:11:3	LLNMR	64	Standard query 0xbfa4 AAAA wpad	
12	3.676163	10.5.23.209	224.0.0.252	LLNMR	64	RST, Root = 28672/0/94:3fc:2:02:e1:c6 Cost = 60000 Port = 0x8033
13	5.999999	Cisco-C814B#	Spanning-tree...	STP	64	RST, Root = 28672/0/94:3fc:2:02:e1:c6 Cost = 60000 Port = 0x8033

Protocol Window

Data Window

Data in Hexadecimal

Data in ASCII

Packet Information

- No:** Frame number
- Time:** Time in second
- Source:** source address
- Destination:** Destination address
- Protocol:** Protocol that is used for communication
- Length:** Length of packet in bytes
- Info:** Info of the packet (Type version etc.)

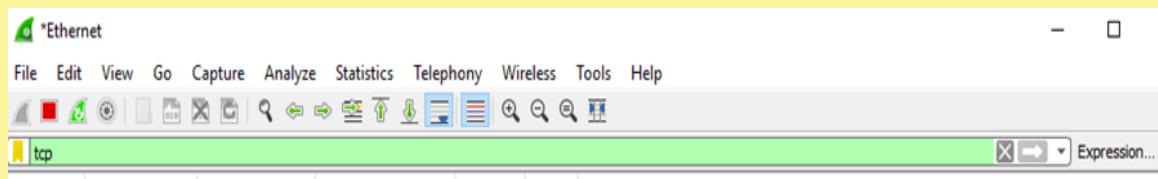
8

Applying Filter

9

Filtering different type of packets

- To filter packets put filter name in filter bar and press <enter> or the arrow.
 - Restrict the packets that are displayed in summary window.
 - For correct filter, bar will convert from white to green and for wrong filter it will be shown as red.



10



TCP Filter: Summary Window

*Ethernet

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp

No.	Time	Source	Destination	Protocol	Length	Info
1907	309.416691	10.5.23.209	172.16.2.30	TCP	2424	53391 → 8080 [PSH, ACK] Seq=23701 Ack=12409 Win=256 Len=2370
1908	309.417306	172.16.2.30	10.5.23.209	TCP	60	8080 → 53391 [ACK] Seq=12409 Ack=26071 Win=32440 Len=0
1909	309.417307	172.16.2.30	10.5.23.209	TCP	60	[TCP Window Update] 8080 → 53391 [ACK] Seq=12409 Ack=26071 Win=328...
1910	309.860548	172.16.2.30	10.5.23.209	TCP	574	8080 → 53391 [PSH, ACK] Seq=12409 Ack=26071 Win=32850 Len=520
1911	309.860794	172.16.2.30	10.5.23.209	TCP	614	8080 → 53391 [PSH, ACK] Seq=12929 Ack=26071 Win=32850 Len=560
1912	309.860861	10.5.23.209	172.16.2.30	TCP	54	53391 → 8080 [ACK] Seq=26071 Ack=13489 Win=252 Len=0
1913	309.860962	172.16.2.30	10.5.23.209	TCP	88	8080 → 53391 [PSH, ACK] Seq=13489 Ack=26071 Win=32850 Len=34
1914	309.921617	10.5.23.209	172.16.2.30	TCP	54	53391 → 8080 [ACK] Seq=26071 Ack=13523 Win=252 Len=0
1918	310.255954	10.5.23.209	40.90.137.127	TCP	66	54470 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
1920	310.524645	10.5.23.209	52.109.120.2	TCP	66	54471 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
1924	311.066332	10.5.23.209	13.107.254.128	TCP	66	54472 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
1930	313.270227	10.5.23.209	40.90.137.127	TCP	66	[TCP Retransmission] 54470 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=14...
1931	313.535564	10.5.23.209	52.109.120.2	TCP	66	[TCP Retransmission] 54471 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=146...



11

TCP Packet Header Details

- When you double click on any of the packets the respective protocol will highlight, and you can see header details.

203 4.711825 10.5.23.209 52.109.124.4 TCP 62 61870 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 SACK_PERM=1

Source: 10.5.23.209
Destination: 52.109.124.4

Transmission Control Protocol, Src Port: 61870, Dst Port: 80, Seq: 0, Len: 0

Source Port: 61870
Destination Port: 80
[Stream index: 14]
[TCP Segment Len: 0]
Sequence number: 0 (relative sequence number)
Next sequence number: 0 (relative sequence number)
Acknowledgment number: 0
0111 = Header Length: 28 bytes (7)

Flags: 0x002 (SYN)
Window size value: 8192
[Calculated window size: 8192]
Checksum: 0xd269 [unverified]
[Checksum Status: Unverified]
Urgent pointer: 0
Options: (8 bytes), Maximum segment size, No-Operation (NOP), No-Operation (NOP), SACK permitted
[Timestamps]



12

IP Filter Summary Window

*Ethernet

No.	Time	Source	Destination	Protocol	Lengt	Info
2	0.173997	10.5.23.209	10.5.23.255	NBNS	92	Name query NB WPAD<00>
3	0.174867	10.5.18.84	10.5.23.209	ICMP	120	Destination unreachable (Port unreachable)
4	0.175126	10.5.18.80	10.5.23.209	ICMP	120	Destination unreachable (Port unreachable)
5	1.111743	10.5.23.2	224.0.0.5	OSPF	90	Hello Packet
7	1.736689	10.5.23.209	239.255.255.255	SSDP	179	M-SEARCH * HTTP/1.1
9	2.242863	10.5.23.209	20.189.72.2	TCP	66	61873 → 443 [SYN] Seq=0 Win=8192 MSS=1460 WS=256 SACK_PERM=1
10	2.703911	10.5.23.209	172.16.2.30	TCP	278	61849 → 8080 [PSH, ACK] Seq=1 Ack=1 Win=252 Len=224
11	2.704030	10.5.23.209	172.16.2.30	TCP	93	61849 → 8080 [PSH, ACK] Seq=225 Ack=21 Win=252 Len=39
12	2.706032	172.16.2.30	10.5.23.209	TCP	60	8080 → 61849 [ACK] Seq=1 Ack=225 Win=32730 Len=0
13	2.706033	172.16.2.30	10.5.23.209	TCP	60	8080 → 61849 [ACK] Seq=1 Ack=264 Win=32725 Len=39
14	2.757709	172.16.2.30	10.5.23.209	TCP	93	8080 → 61849 [PSH, ACK] Seq=1 Ack=264 Win=32725 Len=39
15	2.816121	10.5.23.209	172.16.2.30	TCP	54	61849 → 8080 [ACK] Seq=264 Ack=40 Win=252 Len=0
16	2.868148	172.16.2.30	10.5.23.209	TCP	488	8080 → 61849 [PSH, ACK] Seq=40 Ack=264 Win=32725 Len=434
17	2.868864	10.5.23.209	172.16.2.30	TCP	93	61849 → 8080 [PSH, ACK] Seq=264 Ack=474 Win=251 Len=39
18	2.876859	172.16.2.30	10.5.23.209	TCP	60	8080 → 61849 [ACK] Seq=474 Ack=303 Win=32720 Len=0
20	3.514887	10.5.23.209	172.16.2.30	TCP	66	61874 → 8080 [SYN] Seq=0 Win=8192 MSS=1460 WS=256 SACK_PERM=1
21	3.515881	10.5.23.209	172.16.2.30	TCP	66	61875 → 8080 [SYN] Seq=0 Win=8192 MSS=1460 WS=256 SACK_PERM=1
22	3.516112	10.5.23.209	172.16.2.30	TCP	66	61876 → 8080 [SYN] Seq=0 Win=8192 MSS=1460 WS=256 SACK_PERM=1
23	3.516293	172.16.2.30	10.5.23.209	TCP	66	8080 → 61874 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=8 SACK_PERM=1
24	3.516293	172.16.2.30	10.5.23.209	TCP	66	8080 → 61875 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=8 SACK_PERM=1

> Frame 4: 120 bytes on wire (960 bits), 120 bytes captured (960 bits) on interface 0
> Ethernet II, Src: Cisco_c9:88:ff (40:55:39:c9:88:ff), Dst: Dell_d7:2b:77 (f8:b1:56:d7:2b:77)
> Internet Protocol Version 4, Src: 10.5.18.80, Dst: 10.5.23.209
> Internet Control Message Protocol



13

IP Packet Header Detail

*Ethernet

No.	Time	Source	Destination	Protocol	Lengt	Info
2	0.173997	10.5.23.209	10.5.23.255	NBNS	92	Name query NB WPAD<00>
3	0.174867	10.5.18.84	10.5.23.209	ICMP	120	Destination unreachable (Port unreachable)
4	0.175126	10.5.18.80	10.5.23.209	ICMP	120	Destination unreachable (Port unreachable)

> Frame 4: 120 bytes on wire (960 bits), 120 bytes captured (960 bits) on interface 0
> Ethernet II, Src: Cisco_c9:88:ff (40:55:39:c9:88:ff), Dst: Dell_d7:2b:77 (f8:b1:56:d7:2b:77)
> Internet Protocol Version 4, Src: 10.5.18.80, Dst: 10.5.23.209

```

0100 ... = Version: 4
... 0101 = Header Length: 20 bytes (5)
> Differentiated Services Field: 0xc0 (DSCP: CS6, ECN: Not-ECT)
Total Length: 106
Identification: 0xc383 (50051)
> Flags: 0x0000
Time to live: 63
Protocol: ICMP (1)
Header checksum: 0x7925 [validation disabled]
[Header checksum status: Unverified]
Source: 10.5.18.80
Destination: 10.5.23.209
> Internet Control Message Protocol
0000 f8 b1 56 d7 2b 77 40 55 39 c9 88 ff 08 00 45 c0 ..V+@U 9 ...E.
0010 00 6a c3 83 00 00 3f 01 79 25 00 05 12 50 0a 05 .j...?y$...P...
0020 17 d1 03 03 73 00 00 00 45 00 00 4e 1f ca ..;s... E-N...
0030 00 66 00 11 dd aa 00 00 00 00 00 00 00 00 00 00 ..: ... P...
0040 00 00 00 00 45 f9 0f 01 10 00 00 00 00 00 00 ..: ?...
0050 00 20 46 48 46 41 45 42 45 45 43 41 43 41 43 FHFAC BEECACAC
0060 41 43 41 43 41 43 41 43 41 43 41 43 41 43 ACACACAC ACACACAC
0070 41 41 41 00 00 20 00 01 AAA ...

```



14

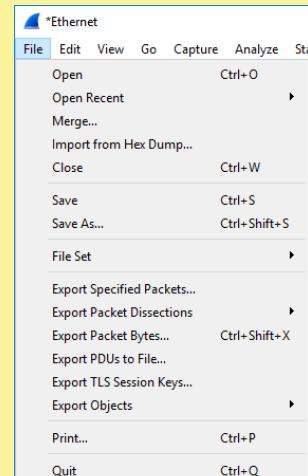
Exploring the Menu



15

File Menu

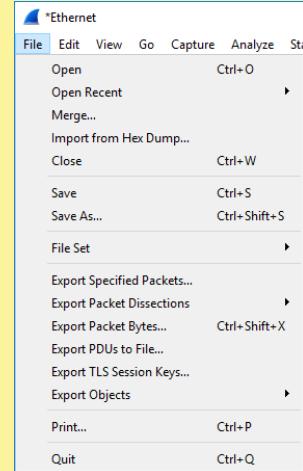
- We can divide File Menu into 3 major sections as per their functionality.
- **Import :**
 - **Open:** open captured file.
 - **Open recent:** open recently captured file.
 - **Merge:** merge current capture with other captured file.
 - **Import from hex dump:** Import from hexadecimal file.
- **Save:**
 - **Save:** save in .pcapng (wireshark format)
 - **Save as:** Save in different format such that it can be imported to other network analyzer (.txt, .dmp, .5vw, .erf etc).



16

File Menu

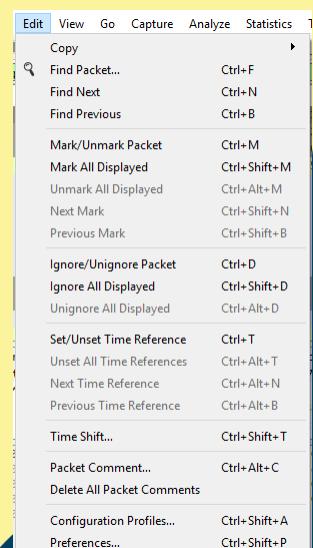
- **Export :**
 - **File Set:** navigate the directory where file will be stored.
 - **Various Exports Options:** allow to save report in different format such as CSV, C array, XML, JSON etc., it also allows to save data for selected packet or range of packets.
 - **Print:** to print report as a plain text.
- **Close and Quit** are used to turn off capturing, and exit from application.



17

Edit Menu

- Edit menu can also be divided into 5 sections:
- **Find:**
 - Used to search packets by matching hexadecimal string, and to search for next and previous packets as per requirement.
- **Mark:**
 - Mark options are used for marking the packets that are displayed in summary window.



18

Edit Menu

- Preferences:** Used to set:-
 - How many packets you want to show at once?
 - Font and color for packets.
 - Fields to be displayed (no, time, source, dest. etc.).

Callout arrow pointing to the "Preferences..." option in the Edit menu.

19

View Menu

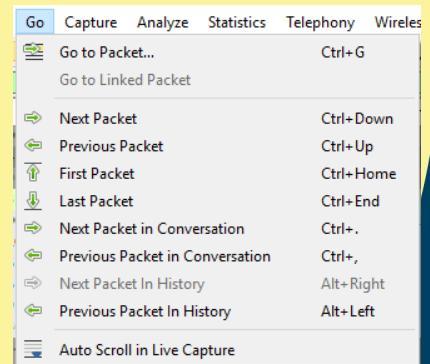
- View menu is used to manage the look of the windows.
- Expand and collapse options are used to expand/collapse the detail of header file in protocol window.
- You can handle coloring of packets from view menu as well.

Callout arrow pointing to the "Colorize Packet List" option in the View menu.

20

Go Menu

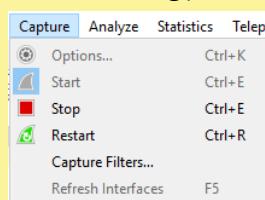
- Go menu is used to switch between packets.



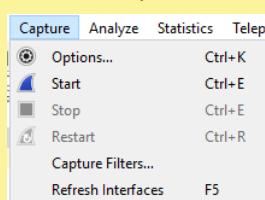
21

Capture Menu

- Capture menu is used to start/stop capturing as well as to set capture options (preferred network interface, Wi-Fi, etc.).
- It can also provide filtering(ARP/TCP/IP/ICMP etc.) when capturing is running.



Capturing



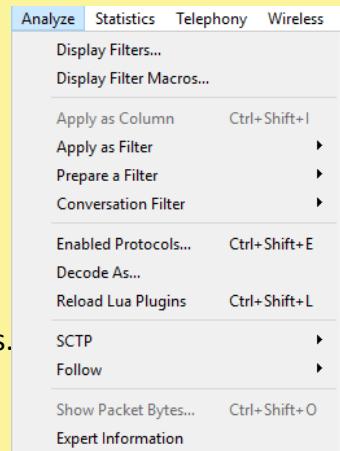
Capture stopped



22

Analyze Menu

- This is the most important menu in Wireshark.
- This is used to analyze the packets and manage different filtering options.
- **Display Filters:** To see what commands needs to be given in filter bar to filter those type of packets.



23

Analyze Menu: Display Filter

Wireshark - Display Filters	
Name	Filter
Non-HTTP and non-SMTP to/from 192.0.2.1	ip.addr == 192.0.2.1 and not tcp.port in {80 25}
No ARP and no DNS	not arp and !(udp.port == 53)
HTTP	http
TCP or UDP port is 80 (HTTP)	tcp.port == 80 udp.port == 80
Non-DNS	!(udp.port == 53 tcp.port == 53)
UDP only	udp
TCP only	tcp
IPv6 address 2001:db8::1	ipv6.addr == 2001:db8::1
IPv6 only	ipv6
IPv4 address isn't 192.0.2.1 (don't use != for this!)	!(ip.addr == 192.0.2.1)
IPv4 address 192.0.2.1	ip.addr == 192.0.2.1
IPv4 only	ip
No ARP	not arp
Ethernet broadcast	eth.addr == ff:ff:ff:ff:ff:ff
Ethernet type 0x0806 (ARP)	eth.type == 0x0806
Ethernet address 00:00:5e:00:53:00	eth.addr == 00:00:5e:00:53:00

- To filter packets we need to give a specific filter name.



24

Analyze Menu: Enable protocol

• We can enable or disable protocol.

• If we don't want to see icmp packets, then uncheck icmp protocol.

Analyze Menu: Conversion Filter

Basically this option directly applies a filter and shows the output.

Analyze Menu: Follow

The screenshot shows the Wireshark interface with a blue header bar. Below it, a yellow section contains the title 'Analyze Menu: Follow'. A dark blue section at the bottom contains the Wireshark logo and the text 'swayam'.

Using this option we can see the complete detail of the packets.

Wireshark window details:

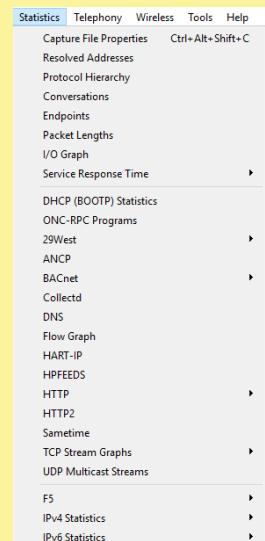
- HTTP/1.1 304 Not Modified
- Date: Fri, 08 Oct 2019 12:53:59 GMT
- Etag: "4dcda04d4-15ea"
- Connection: keep-alive
- Server: ATS/5.3.1
- POST http://testphp.vulnweb.com/userinfo.php HTTP/1.1
- Host: testphp.vulnweb.com
- Proxy-Connection: keep-alive
- Content-Length: 25
- Cache-Control: max-age=0
- Origin: http://testphp.vulnweb.com
- Upgrade-Insecure-Requests: 1
- Content-Type: application/x-www-form-urlencoded
- User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/77.0.3865.90 Safari/537.36
- Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/png,*/*;q=0.8,application/signed-exchange;v=b3
- Referer: http://testphp.vulnweb.com/login.php
- Accept-Encoding: gzip, deflate
- Accept-Language: en-US,en;q=0.9
- uname=nptel&pass=password
- HTTP/1.1 302 Found
- Server: ATS/5.3.1
- Date: Fri, 24 Apr 1970 06:09:32 GMT
- Content-Type: text/html
- X-Powered-By: PHP/5.3.10-1~lucid+2uwsq12
- Location: login.php
- Age: 1560321875
- Transfer-Encoding: chunked
- Connection: keep-alive

Bottom status bar: 4 client pkts, 9 server pkts, 7 tums. Entire conversation (8388 bytes) Show and save data as ASCII Stream 3

27

Statistics Menu

- This is used to check the statistics of the capturing, like property of the network, number of packets sent and received, etc.



28

Statistics Menu: Capture File Properties

File

Name: C:\Users\user\AppData\Local\Temp\wireshark_Ethernet_20191003190446_a01600.pcapng
Length: 58 kB
Hash: bf0abfe4ac58ba50db4ea2297c06faff485f297c1c07816274bc3fbefbf656d0
(Sha256): 90cdcc113606bad766907d2d5ef1bb3b9602678
Hash (SHA1): 11ab84e25ce29502345723f0320bc8dfc02e91d2
Format: Wireshark/... - pcapng
Encapsulation: Ethernet

Time

First packet: 2019-10-03 19:04:46
Last packet: 2019-10-03 19:05:35
Elapsed: 00:00:48

Capture

Hardware: Intel(R) Core(TM) i5-4570 CPU @ 3.20GHz (with SSE4.2)
OS: 64-bit Windows 10 (1511), build 10586
Application: Dumpcap (Wireshark) 3.0.5 (v3.0.5-0-g752a55954770)

Interfaces

Interface	Dropped packets	Capture filter	Link type	Packet size limit
Ethernet	0 (0 %)	none	Ethernet	262144 bytes

Statistics

Measurement	Captured	Displayed	Marked
Packets	214	214 (100.0%)	—
Time span, s	48.256	48.256	—
Average pps	4.4	4.4	—
Average packet size, B	240	240	—
Bytes	51425	51425 (100.0%)	0
Average bytes/s	1065	1065	—
Average bits/s	8525	8525	—

It shows the full system detail of the capturing machine.





29

Statistics Menu: Protocol Hierarchy

Wireshark - Protocol Hierarchy Statistics - Ethernet

Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets	End Bytes	End Bits/s
Frame	100.0	214	100.0	51425	4925	0	0	0
Ethernet	100.0	214	5.8	2996	496	0	0	0
Logical-Link Control	23.4	50	4.5	2323	385	0	0	0
Spanning Tree Protocol	22.9	49	3.7	1908	316	49	1908	316
Cisco Discovery Protocol	0.5	1	0.3	140	23	1	140	23
Link Layer Discovery Protocol	0.5	1	0.1	50	8	1	50	8
Internet Protocol Version 6	4.2	9	0.7	360	59	0	0	0
User Datagram Protocol	4.2	9	0.1	72	11	0	0	0
Link-local Multicast Name Resolution	1.9	4	0.2	88	14	4	88	14
DHCPv6	2.3	5	0.9	475	78	5	475	78
Internet Protocol Version 4	69.6	149	5.8	2980	494	0	0	0
User Datagram Protocol	14.5	31	0.5	248	41	0	0	0
Simple Service Discovery Protocol	6.1	13	4.4	2237	370	13	2237	370
NetBIOS Name Service	1.4	3	0.3	150	24	3	150	24
Link-local Multicast Name Resolution	1.9	4	0.2	88	14	4	88	14
Domain Name System	1.9	4	1.6	822	136	4	822	136
Data	3.3	7	8.9	4592	761	7	4592	761
Transmission Control Protocol	50.0	107	63.3	32553	5396	83	22235	3686
Hypertext Transfer Protocol	11.7	25	41.7	21431	3552	4	740	122
Transport Layer Security	9.8	21	40.2	20691	3430	20	20353	3374
Open Shortest Path First	2.3	5	0.5	280	46	5	280	46
Internet Control Message Protocol	2.8	6	1.0	516	85	6	516	85
Data	2.3	5	0.4	194	32	5	194	32

It will display statistics about packets as per protocols





30

Statistics Menu: Destination and Ports

This will give information about connections, ports, and number of packets to that destination.

Topic / Item	Count	Average	Min val	Max val	Rate (ms)	Percent	Burst rate	Burst start
Destinations and Ports	149				0.0032	100%	0.2000	12.964
52.109.124.4	2				0.0000	1.34%	0.0100	0.447
TCP	2				0.0000	100.00%	0.0100	0.447
80	2				0.0000	100.00%	0.0100	0.447
40.90.23.247	3				0.0001	2.01%	0.0100	25.570
TCP	3				0.0001	100.00%	0.0100	25.570
443	3				0.0001	100.00%	0.0100	25.570
40.90.137.124	3				0.0001	2.01%	0.0100	4.550
TCP	3				0.0001	100.00%	0.0100	4.550
443	3				0.0001	100.00%	0.0100	4.550
239.255.255.250	20				0.0004	13.42%	0.0200	31.891
UDP	20				0.0004	100.00%	0.0200	31.891
3702	7				0.0002	35.00%	0.0100	4.724
1900	13				0.0003	65.00%	0.0200	31.891
224.0.0.5	5				0.0001	3.36%	0.0100	2.334
NONE	5				0.0001	100.00%	0.0100	2.334
0	5				0.0001	100.00%	0.0100	2.334
224.0.0.252	4				0.0001	2.68%	0.0200	16.822
UDP	4				0.0001	100.00%	0.0200	16.822
5355	4				0.0001	100.00%	0.0200	16.822
20.189.74.153	1				0.0000	0.67%	0.0100	46.615

Display filter: Enter a display filter ...

31

Telephony Menu

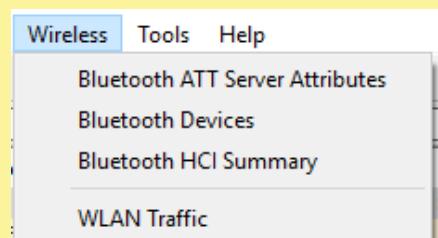
- Provides analysis for telephony and media streaming related network traffic.
- It can track details for VoIP call, i.e. start time, end time, initiator IP, etc.

Telephony	Wireless	Tools	Help
VoIP Calls			
ANSI			
GSM			
IAX2 Stream Analysis			
ISUP Messages			
LTE			
MTP3			
Osmux			
RTP			
RTSP			
SCTP			
SMPP Operations			
UCP Messages			
H.225			
SIP Flows			
SIP Statistics			
WAP-WSP Packet Counter			

32

Wireless Menu

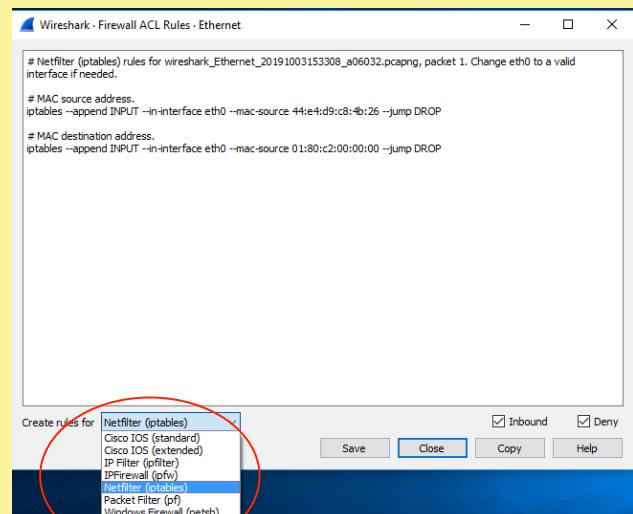
- This option is used when you are using Wireshark to analyze wireless networks.



33

Tools Menu

- This menu is used to select the rules (which type of scanning do you want to do).
- It also provides help for various tools that are used by Wireshark.



34

Packet Analysis Examples

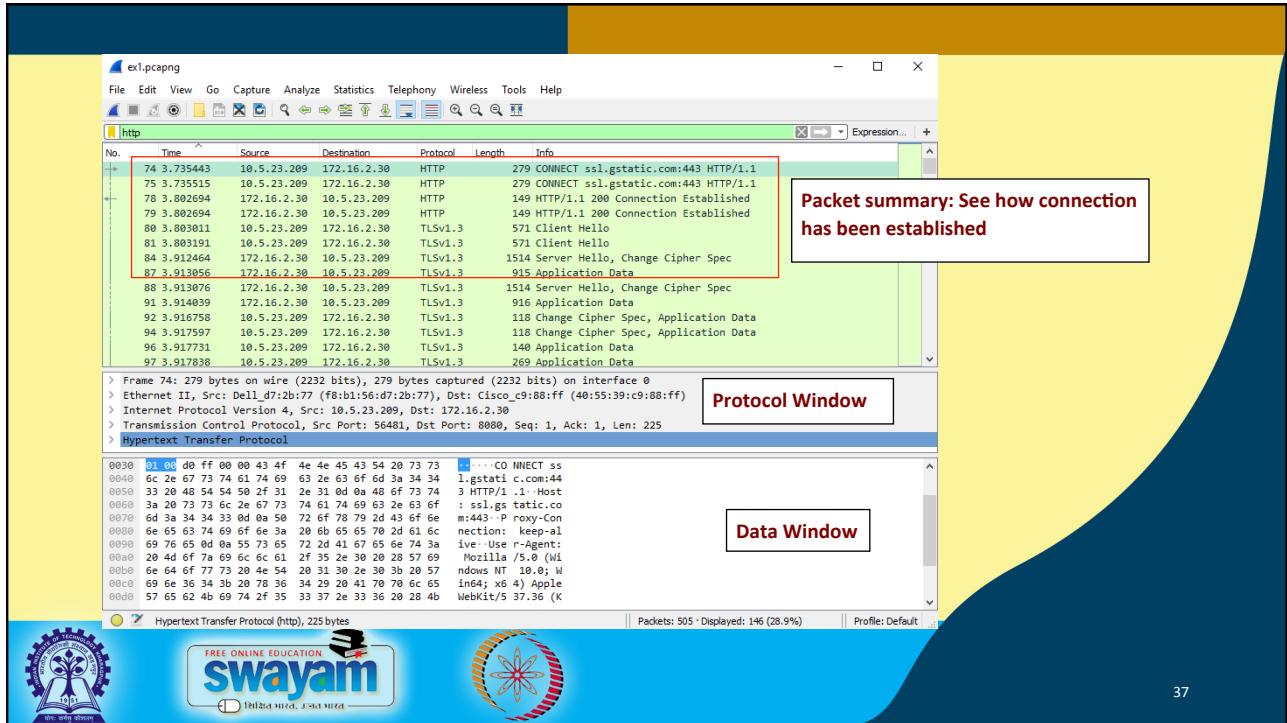


35

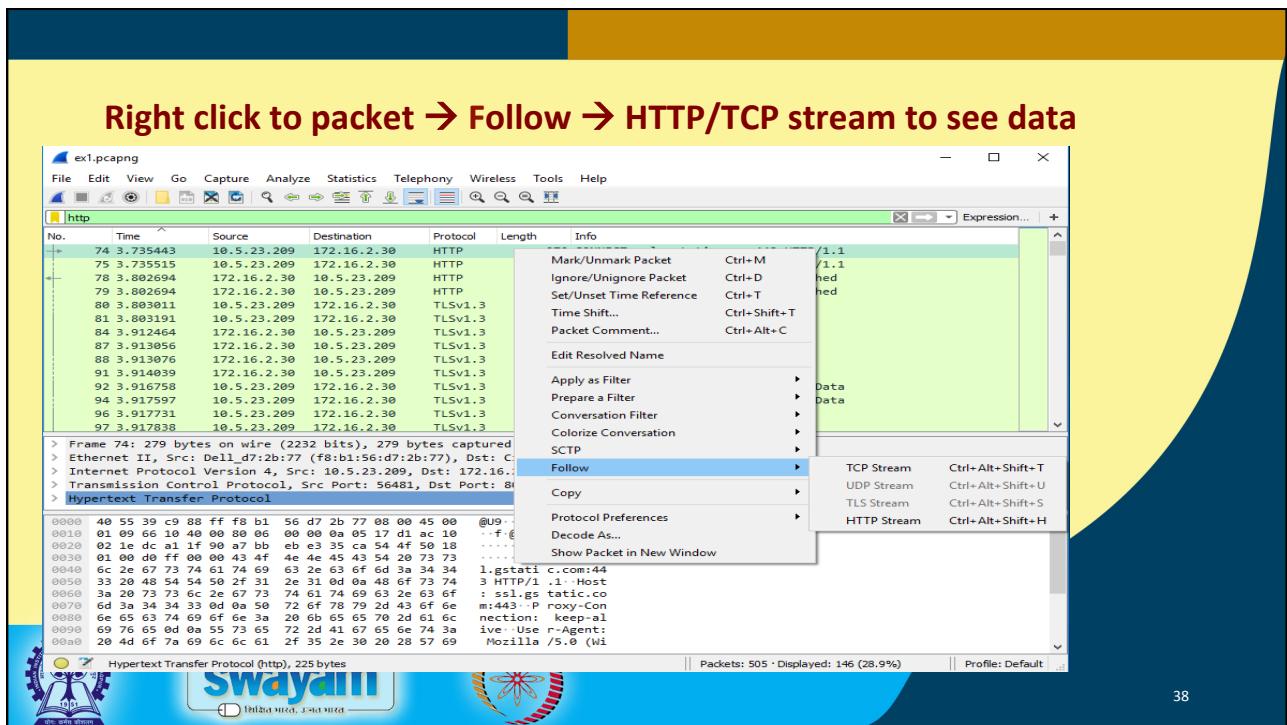
Example:

- Start a capture in wireshark.
- Open browser and type www.google.com and search.
- Save capture and analyze by applying http filter.





37



38

Data Details

CONNECT ssl.gstatic.com:443 HTTP/1.1
Host: ssl.gstatic.com:443
Proxy-Connection: keep-alive
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/77.0.3865.90 Safari/537.36

HTTP/1.1 200 Connection Established
Proxy-Agent: IwSS
Date: Thu, 03 Oct 2019 10:36:08 GMT

.....+..C.Z.B.=
.P(.H.,
.D.,"+.....+/.,0...../S.
.....ssl.gstatic.com.....
.....#.....h2.http/1.1.....
....3.+.).....rC...D.G.y.j....g..
..!6AC...T.B.-....+..
.....
.....z...v...K...^...j)...W
.....-9n\$,...
.P(.H.,
.D.,.....3.\$... .k...QF...0...j
....wSB...j...F"...+.....X...2...0^...K.J&.#q...9.k.h....g.C.T..
(...*...9.u"....R
....TG...S...4...)t...(.hr...E.O...g ...[.X...)...f...k...A...&..
....OTO...".).M...8e.J...g.i.F...".E..."1FP...N...s"....&
....j...q0...".9x.vG...N...V...-Y...\$.3(\$...B.S...-p.#)...{....
[...oW...".>|...ID...D...t{.mX.p@...M...yV4...-...p.D...%...#m
...s"....b...o[n...b...b6...(H...m1wGA...O...-...G.U.|\\J.Q.YW...&w...O...R.
B>...Uv.B...H

8 client pkts, 117 server pkts, 9 turns.
Entire conversation (164 kB)

Show and save data as: **ASCII** Stream 4 Find Next Help

Find: Filter Out This Stream Print Save as... Back ASCII C Arrays EBCDIC Hex Dump UTF-8 UTF-16 YAML Raw

39

Capture Login credentials of unsecured website: vulnweb.com

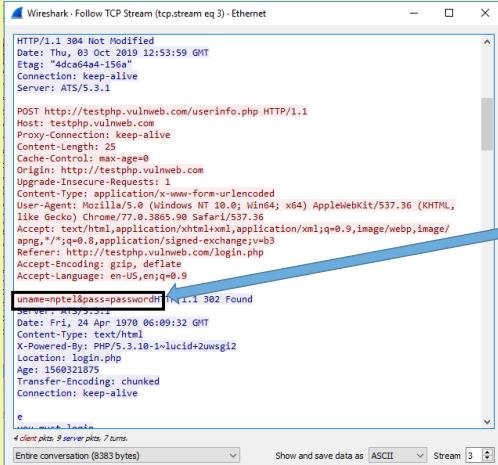
- Click on the frame number 106 (userinfo.php frame) for analysis.

82 6.549036	172.16.2.30	10.5.23.209	HTTP	186 HTTP/1.1 304 Not Modified
83 6.598996	10.5.23.209	172.16.2.30	TCP	54 61385 + 8080 [ACK] Seq=912 Ack=265 Win=65280 Len=0
→ 106 14.107445	10.5.23.209	172.16.2.30	HTTP	722 POST http://testphp.vulnweb.com/userinfo.php HTTP/1.1 (application/x-www-form-urlencoded)
107 14.107816	172.16.2.30	10.5.23.209	TCP	60 8080 + 61385 [ACK] Seq=265 Ack=1580 Win=261216 Len=0
108 14.661990	172.16.2.30	10.5.23.209	TCP	306 8080 + 61385 [PSH, ACK] Seq=265 Ack=1580 Win=262800 Len=252 [TCP segment of a reassembled PDU]

FREE ONLINE EDUCATION **swayam** Prashna Mrid. Jyoti Mrid.

40

We can even view username and password from http packet



A screenshot of the Wireshark network traffic analyzer. A specific packet is highlighted, showing an HTTP POST request to `http://testphp.vulnweb.com/userinfo.php`. The packet details show the following headers:

```

HTTP/1.1 304 Not Modified
Date: Thu, 03 Oct 2019 12:53:59 GMT
Etag: "4dcfa64a-156a"
Connection: keep-alive
Content-Length: 25
Cache-Control: max-age=0
Origin: http://testphp.vulnweb.com
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/77.0.3865.90 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3
Referer: http://testphp.vulnweb.com/login.php
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9

```

The payload of the POST request contains the user's credentials:

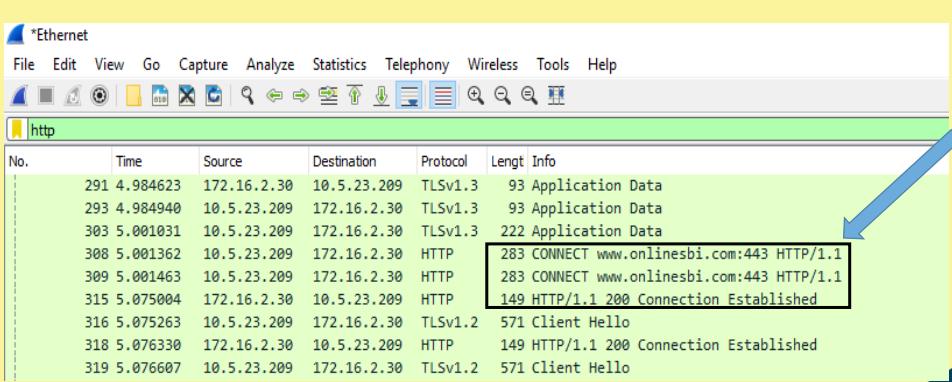
```
uname=ntp1&pass=password
```

The response shows a successful 304 Not Modified status, indicating the credentials were captured.

**See we
captured
username
and password**

41

Packet details for SBI net banking



A screenshot of the Wireshark interface showing a list of network packets. The packet details table highlights several key interactions:

No.	Time	Source	Destination	Protocol	Length	Info
291	4.984623	172.16.2.30	10.5.23.209	TLSv1.3	93	Application Data
293	4.984940	10.5.23.209	172.16.2.30	TLSv1.3	93	Application Data
303	5.001031	10.5.23.209	172.16.2.30	TLSv1.3	222	Application Data
308	5.001362	10.5.23.209	172.16.2.30	HTTP	283	CONNECT www.onlinesbi.com:443 HTTP/1.1
309	5.001463	10.5.23.209	172.16.2.30	HTTP	283	CONNECT www.onlinesbi.com:443 HTTP/1.1
315	5.075004	172.16.2.30	10.5.23.209	HTTP	149	HTTP/1.1 200 Connection Established
316	5.075263	10.5.23.209	172.16.2.30	TLSv1.2	571	Client Hello
318	5.076330	172.16.2.30	10.5.23.209	HTTP	149	HTTP/1.1 200 Connection Established
319	5.076607	10.5.23.209	172.16.2.30	TLSv1.2	571	Client Hello

**Making
secure
connection
with port 443**

42

21

*Ethernet

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

No.	Time	Source	Destination	Protocol	Len/ Info
321	5.111442	172.16.2.30	10.5.23.209	TLSv1.3	268 Application Data
322	5.113657	172.16.2.30	10.5.23.209	TLSv1.3	124 Application Data, Application Data
324	5.113943	10.5.23.209	172.16.2.30	TLSv1.3	93 Application Data
334	5.146640	172.16.2.30	10.5.23.209	TLSv1.2	514 Server Hello
337	5.147245	172.16.2.30	10.5.23.209	TLSv1.2	1386 Certificate, Server Key Exchange, Server Hello Done
338	5.148219	172.16.2.30	10.5.23.209	TLSv1.2	514 Server Hello
341	5.149789	172.16.2.30	10.5.23.209	TLSv1.2	1386 Certificate, Server Key Exchange, Server Hello Done
342	5.152680	10.5.23.209	172.16.2.30	TLSv1.3	218 Application Data
352	5.178274	10.5.23.209	172.16.2.30	HTTP	326 GET http://ocsp.digicert.com/MFEwtzBNMEswSTAjBglDgMCggLABBQ50otx%2Fh0Zt1
355	5.186212	172.16.2.30	10.5.23.209	OCSP	873 Response
356	5.191014	10.5.23.209	172.16.2.30	TLSv1.2	180 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
357	5.192134	10.5.23.209	172.16.2.30	TLSv1.2	180 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
358	5.192321	10.5.23.209	172.16.2.30	TLSv1.2	629 Application Data
363	5.268110	172.16.2.30	10.5.23.209	TLSv1.2	105 Change Cipher Spec, Encrypted Handshake Message
364	5.269753	172.16.2.30	10.5.23.209	TLSv1.2	105 Change Cipher Spec, Encrypted Handshake Message
365	5.272563	172.16.2.30	10.5.23.209	TLSv1.3	138 Application Data
366	5.274500	10.5.23.209	172.16.2.30	TLSv1.3	89 Application Data
368	5.274893	172.16.2.30	10.5.23.209	TLSv1.3	124 Application Data, Application Data
369	5.275003	10.5.23.209	172.16.2.30	TLSv1.3	93 Application Data
373	5.386705	172.16.2.30	10.5.23.209	TLSv1.2	685 Application Data

Key exchange and encrypted handshaking processes between server and client

43

FREE ONLINE EDUCATION
swayam
स्वायम् भारत, उन्नति भारत

INDIAN INSTITUTE OF TECHNOLOGY KHARAGPUR

FREE ONLINE EDUCATION
swayam
स्वायम् भारत, उन्नति भारत

NPTEL ONLINE CERTIFICATION COURSES

Thank you!

44