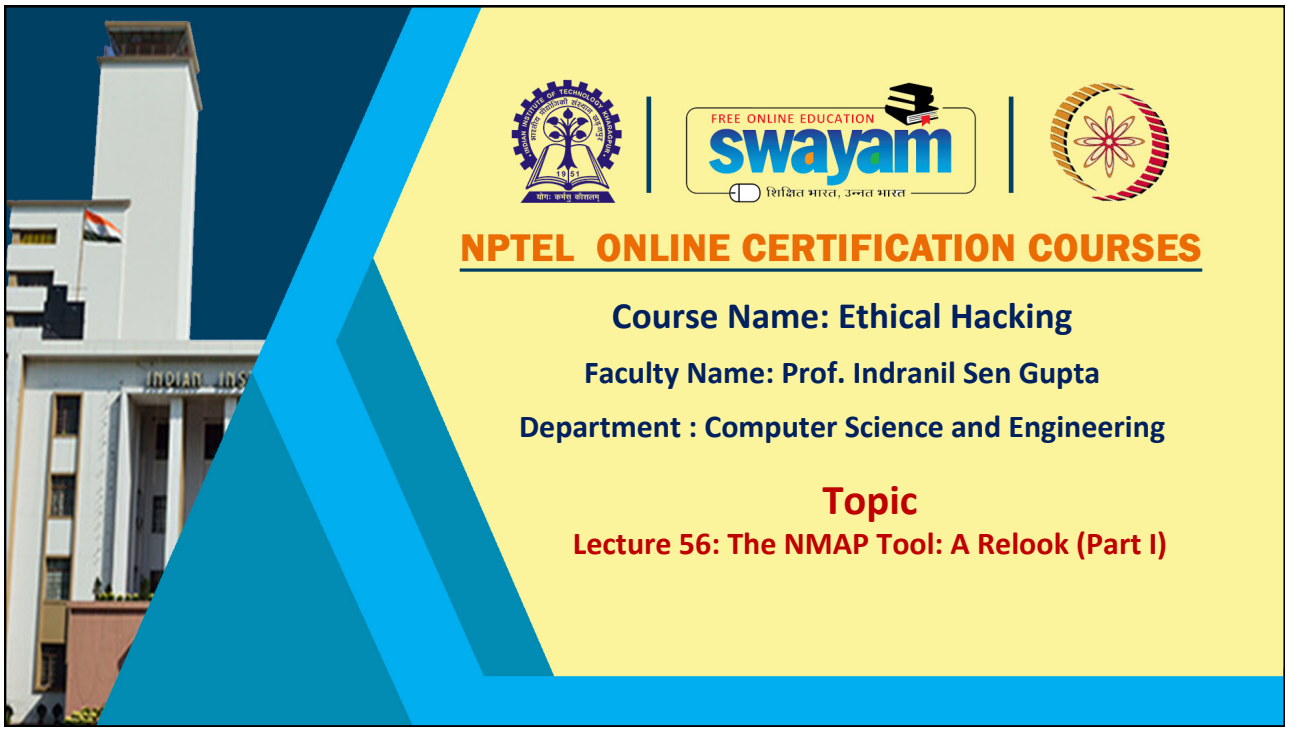
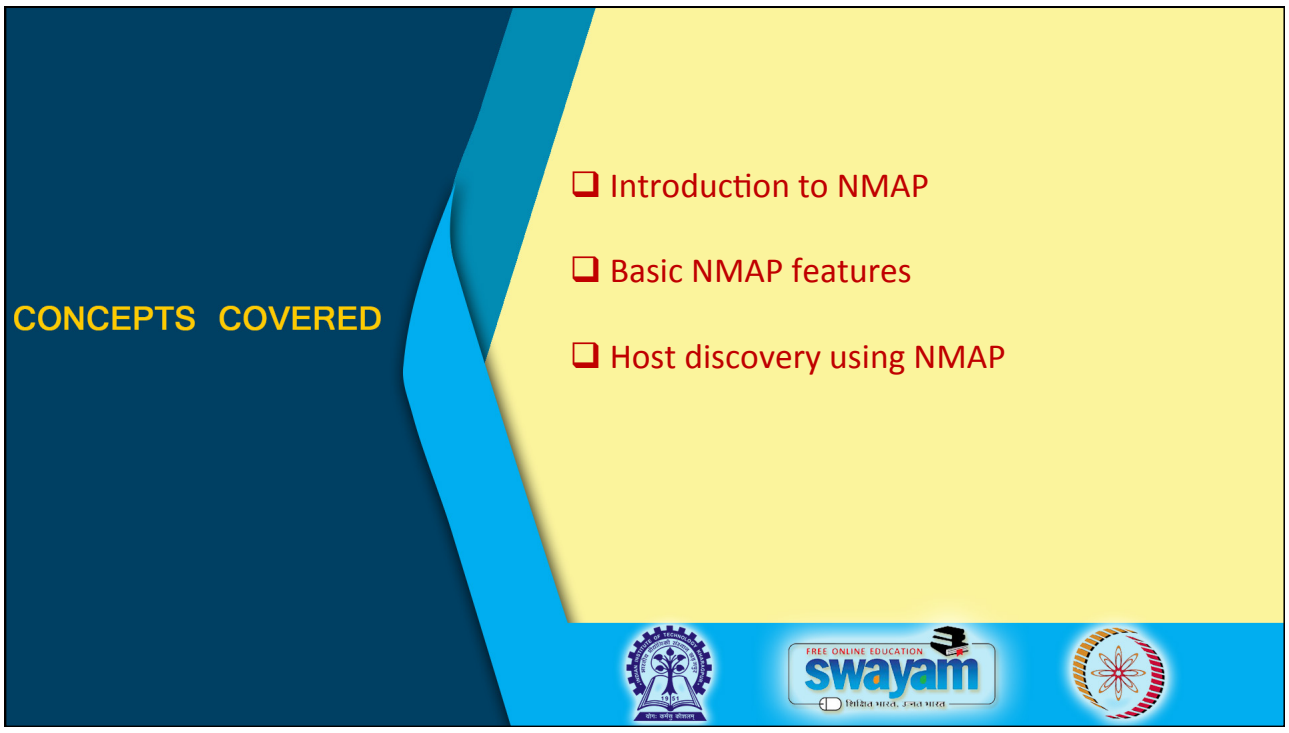

FREE ONLINE EDUCATION
swayam
शिक्षित भारत, उन्नत भारत
NPTEL ONLINE CERTIFICATION COURSES
Course Name: Ethical Hacking
Faculty Name: Prof. Indranil Sen Gupta
Department : Computer Science and Engineering
Topic
Lecture 56: The NMAP Tool: A Relook (Part I)


CONCEPTS COVERED
Introduction to NMAP
Basic NMAP features
Host discovery using NMAP
FREE ONLINE EDUCATION
swayam
शिक्षित भारत, उन्नत भारत

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?

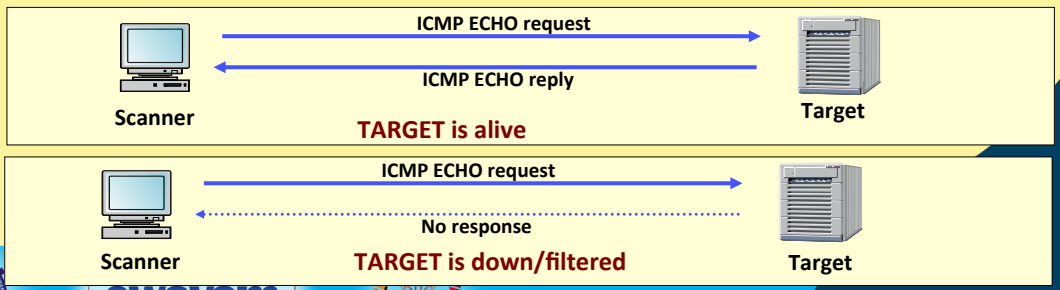
- The most basic step in network mapping.
  - Multiple hosts are queried (called ***ping sweep*** operation)
- Various host scan techniques are supported by NMAP:
  a) ICMP sweep
  b) Broadcast ICMP
  c) Non-Echo ICMP
  d) TCP sweep
  e) UDP sweep


7

(a) Host discovery using ICMP Sweep

- Easy to implement
- Rather slow
- Easy to block

- 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***




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.

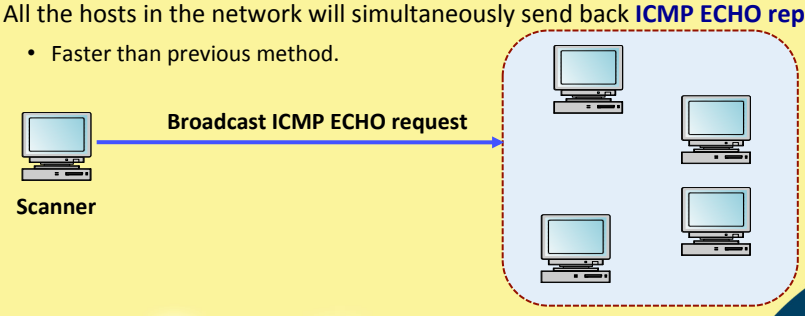
```
root@root:~# nmap -PE 10.5.23.209 --packet-trace --disable-arp-ping
Starting Nmap 7.70 ( https://nmap.org ) at 2019-09-26 08:47 EDT
SENT (0.0664s) ICMP [10.5.23.251 > 10.5.23.209 Echo request (type=8/c
ode=0) id=9047 seq=0] IP [ttl=41 id=15635 iplen=28 ]
RCVD (0.0666s) ICMP [10.5.23.209 > 10.5.23.251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

9

(b) Host discovery using Broadcast ICMP

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

- 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.



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)


- 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 (typ
e=13/code=0) id=25777 seq=0 orig=0 recv=0 trans=0] IP [ttl=59 id=2138
2 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 ]
```


```
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 prob
es, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 2.04 seconds
root@root:~#
```


(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.

- 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`**


(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-p
ing
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)
```


(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**


- 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 ]
```


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.



```
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:~#
```


```
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=5
3664 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=25
327 iplen=40  seq=0 win=1024
SENT (0.0019s) ICMP [10.5.23.251 > 10.5.23.209 Timestamp request (ty
pe=13/code=0) id=11069 seq=0 orig=0 recv=0 trans=0] IP [ttl=39 id=43
055 iplen=40 ]
RCVD (0.0018s) ICMP [10.5.23.209 > 10.5.23.251 Echo reply (type=0/co
de=0) id=48998 seq=0] IP [ttl=128 id=31703 iplen=28 ]
NSOCK INFO [0.0020s] nsock_iod_new2(): nsock_iod_new (IOD #1)
```

All type of sweep options are used with –sn except UDP.

"`--packet-trace`" gives the details.


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)


```
File  Edit  View  Search  Terminal  Help
root@root:~# nmap -PN 10.5.23.209-235
Starting Nmap 7.70 ( 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.

25

```
File  Edit  View  Search  Terminal  Help
root@root:~# nmap -sn 10.5.23.209-230
Starting Nmap 7.70 ( 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 range)

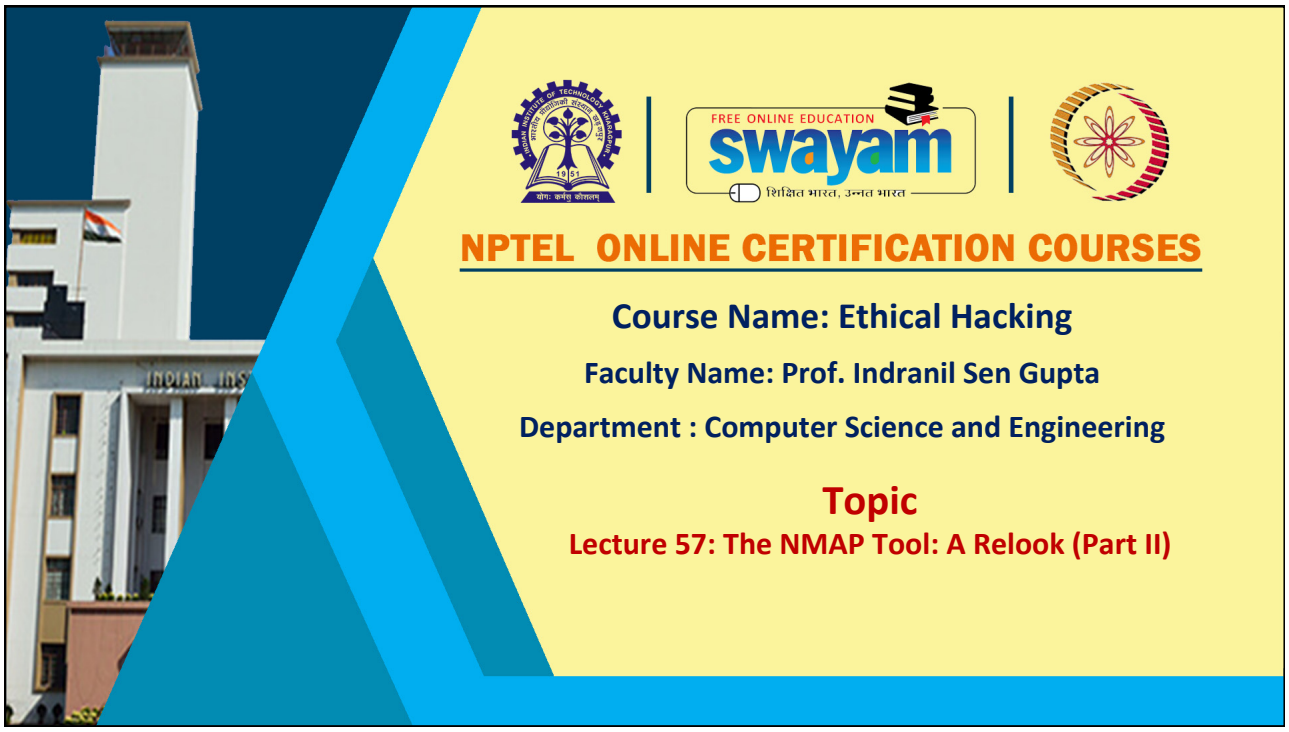
Multiple host discovery (by specifying list)

```
File  Edit  View  Search  Terminal  Help
root@root:~# nmap -sn 10.5.23.209,203
Starting Nmap 7.70 ( 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:~#
```

26

NMAP Command Options for Host Discovery

- **`sL:`** 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



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

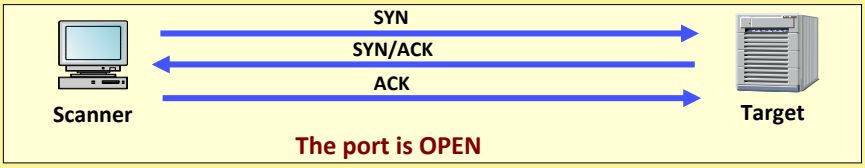
Introduction

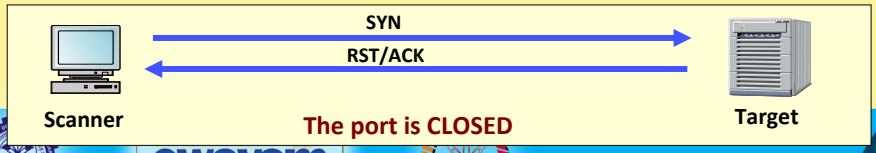
- To determine what services are running or LISTENing.
  - Each running TCP service is associated with a port number, which ***listens*** for incoming connections.
  - Each running UDP service is associated with a port number.
- Various port scanning techniques in NMAP:
  a) TCP Connect scan
  b) TCP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

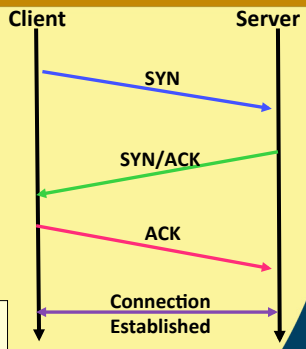

4

(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.



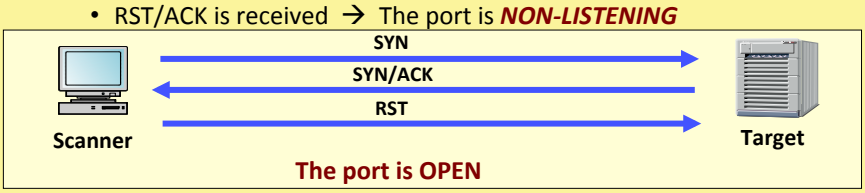


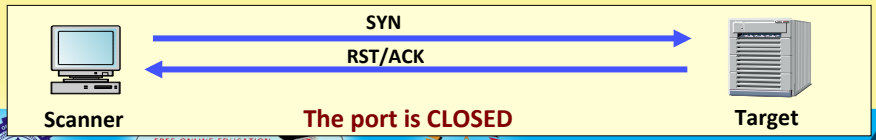


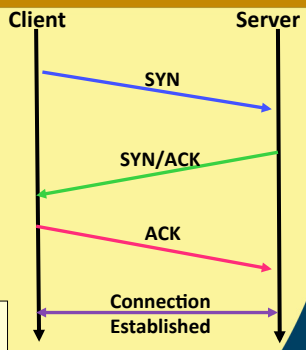
5

(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:~#
```


7

File Edit View Search Terminal Help

```
root@root:~# nmap -sT -p22 10.5.23.209 --packet-trace --disable-arp-p
ing
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/c
ode=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=22
375 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=560
71 iplen=40  seq=0 win=1024
CONN (0.0356s) TCP localhost > 10.5.23.209:22 => Operation now in pro
gress
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).

PORT   STATE  SERVICE
22/tcp closed ssh
```

-sT packet trace for closed port


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/c
ode=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=17
007 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=510
78 iplen=40  seq=0 win=1024
CONN (0.0354s) TCP localhost > 10.5.23.209:135 => Operation now in pr
ogress
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

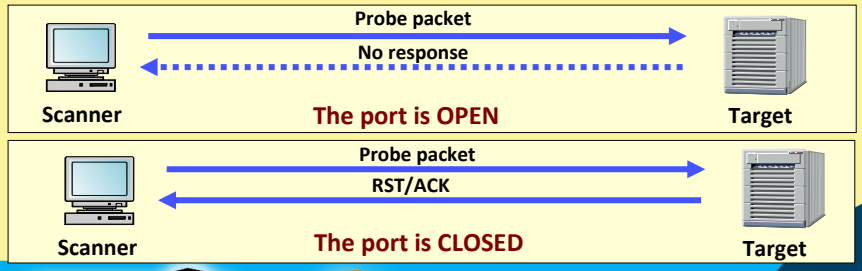

9

(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.

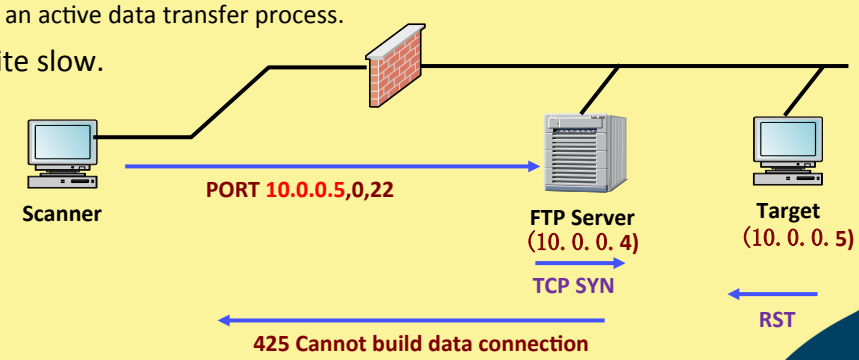

10

- 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.



(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.



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 that 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

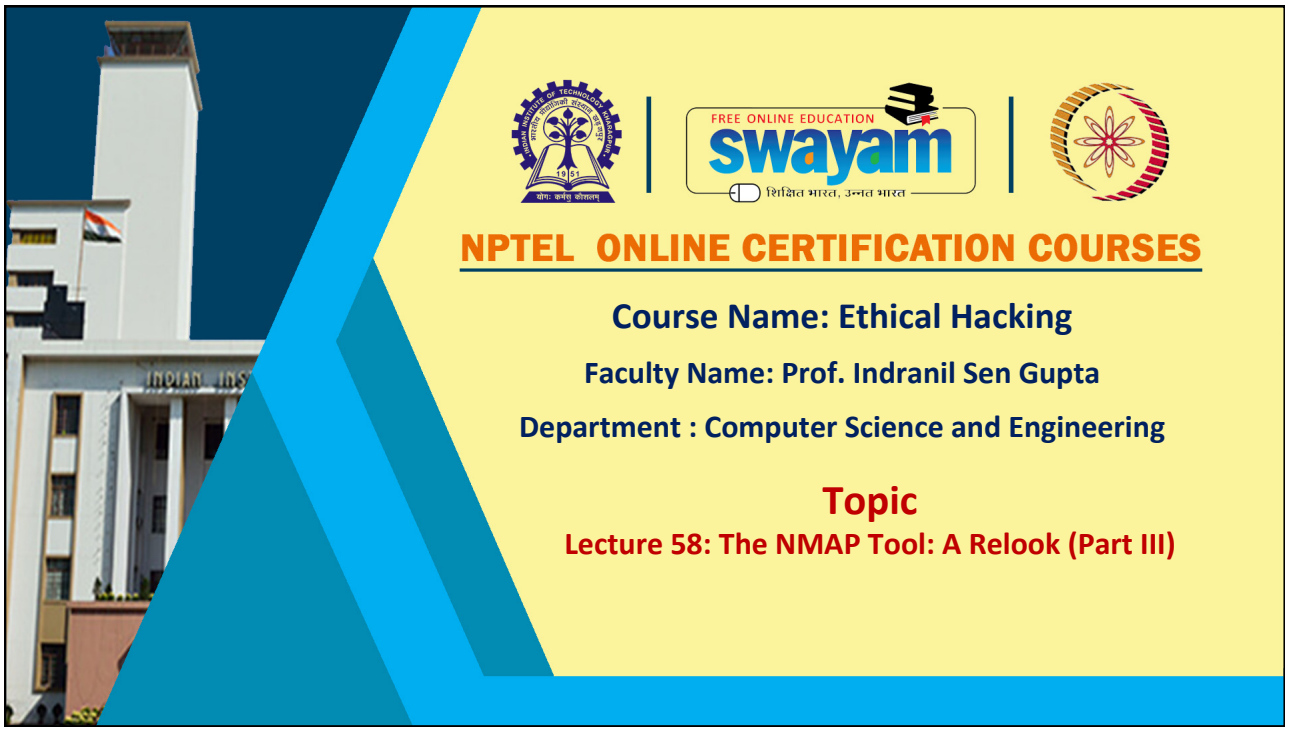
16

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

18



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

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

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.


```
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
Show Applications
```

OS detection using the **-O** option

```
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 (wo
rkgroup: 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:microso
ft:windows

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

Version detection using the `-sV` option

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

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 there 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  wsdapi
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


```
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:window
s

Service detection performed. Please report any incorrect results at https://nm
ap.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

```
File  Edit  View  Search  Terminal  Tabs  Help
root@root: ~                    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



```
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)


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

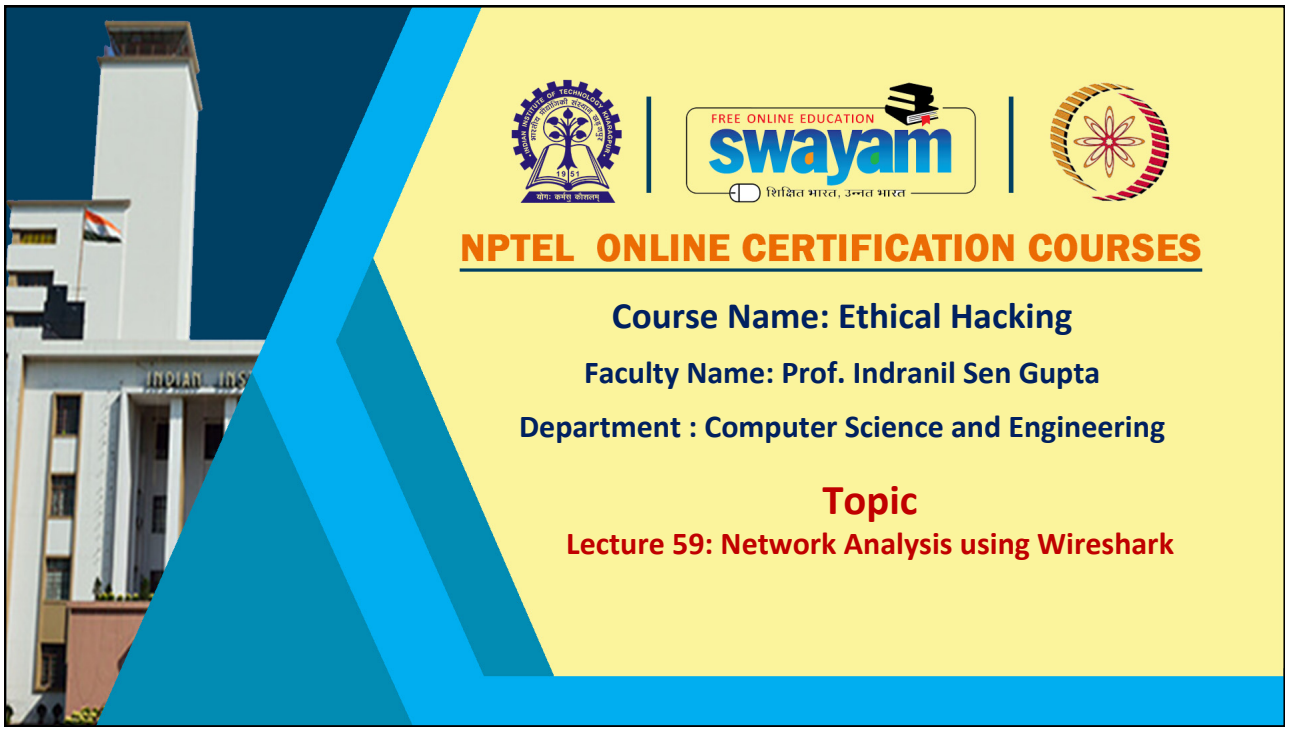
```
nmap 144.16.192.0/24 --exclude 144.16.192.60-70
nmap 144.16.192.0/24 --excludefile xfile.txt
```

- Perform an aggressive scan (use most commonly used options):

```
nmap -A 10.3.100.65
```

17

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 is does really?
  - Captures network data and displays them to readable format.
  - Log network traffic for forensics and evidence.
  - Analyze network traffic generated by various applications.


4

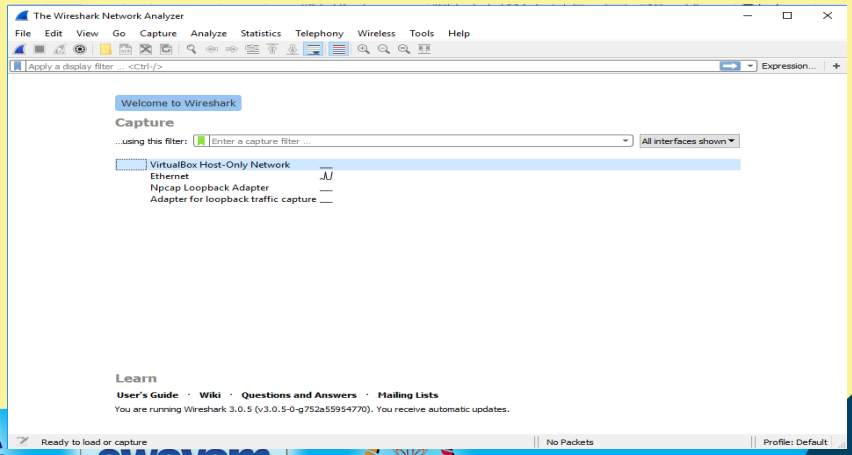
How Packet Sniffer works?

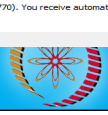
- Ethernet is the most widely used protocol used in a LAN.
  - At the data-link layer level.
- While running Wireshark the machine's network interface card (NIC) is put in ***promiscuous mode***.
  - In this mode, the sniffer can read all traffic on the network segment to which the NIC is connected (irrespective 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

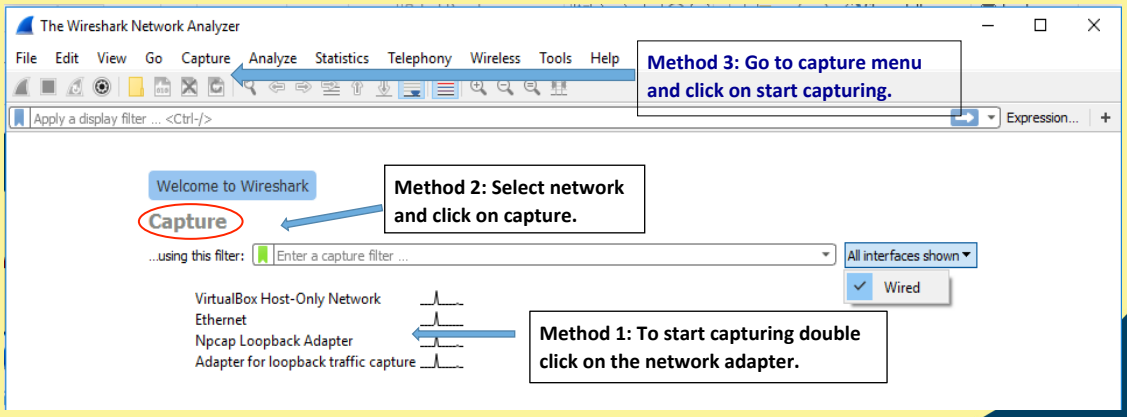
- Can be downloaded from: **http://www.wireshark.org**



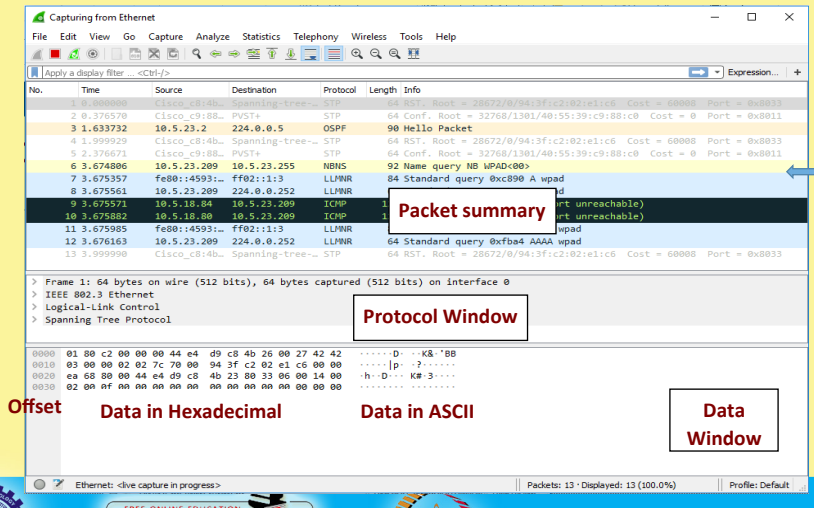



6

Packet Capture using Wireshark



Packet Capturing Starts



Packet Information

No: Frame number

Time: Time in second

Source: source address

Destination: Destination address

Protocol: Protocol that is used for communication

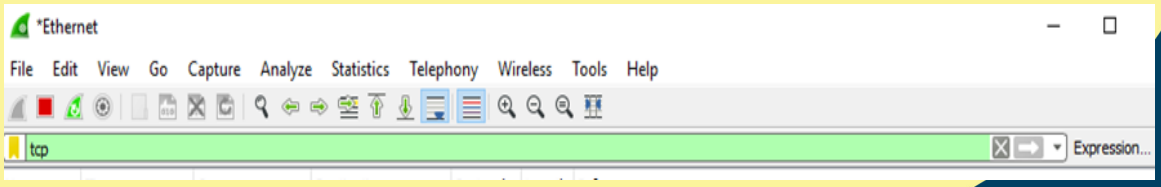
Length: Length of packet in bytes

Info: Info of the packet (Type version etc.)

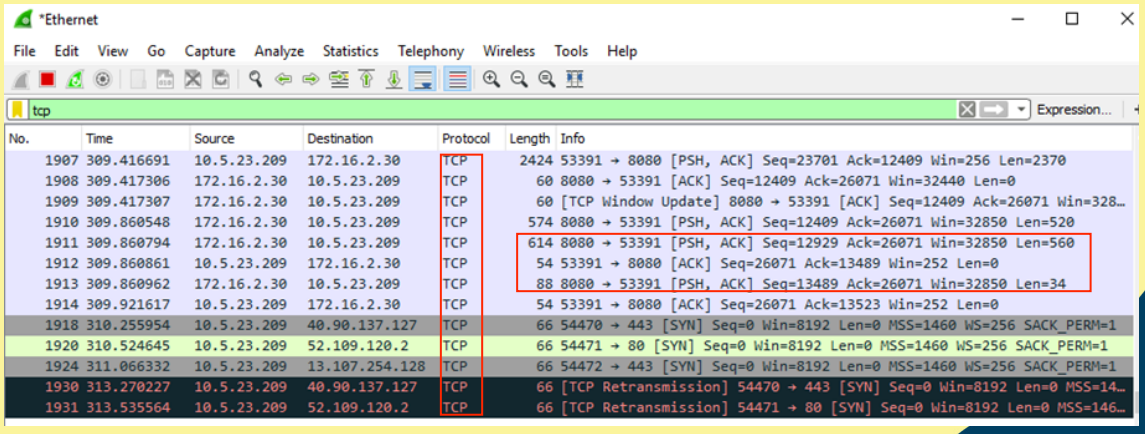
Applying Filter

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.

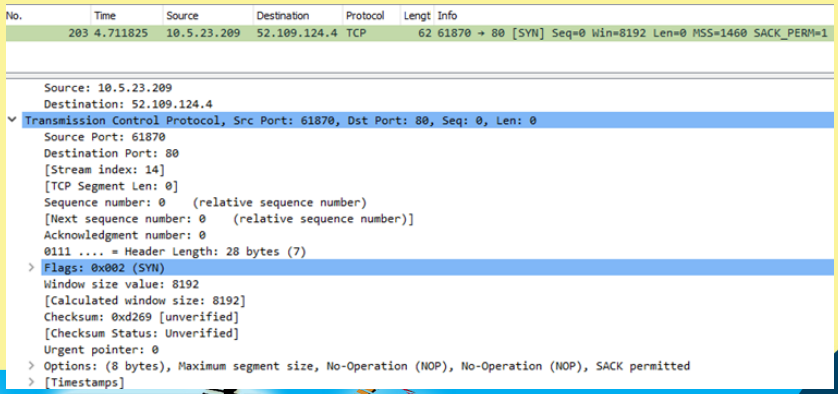


TCP Filter: Summary Window

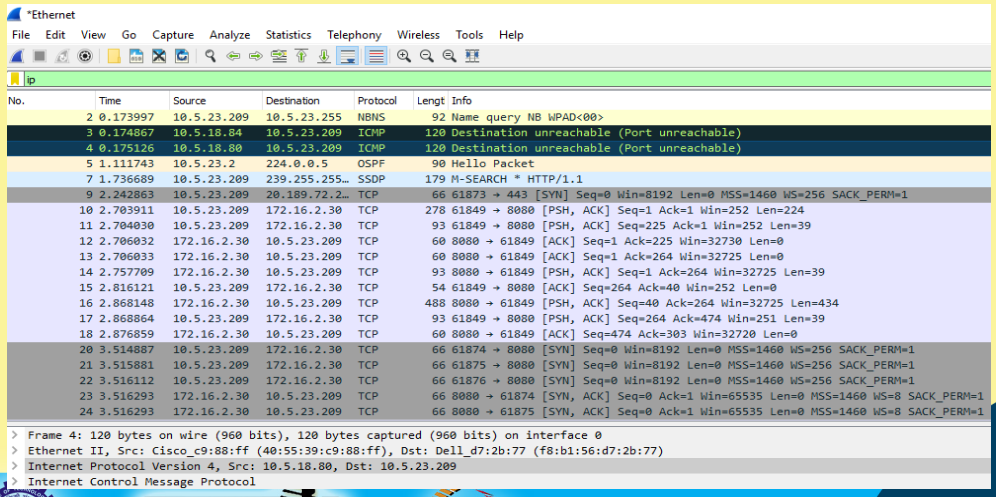



TCP Packet Header Details

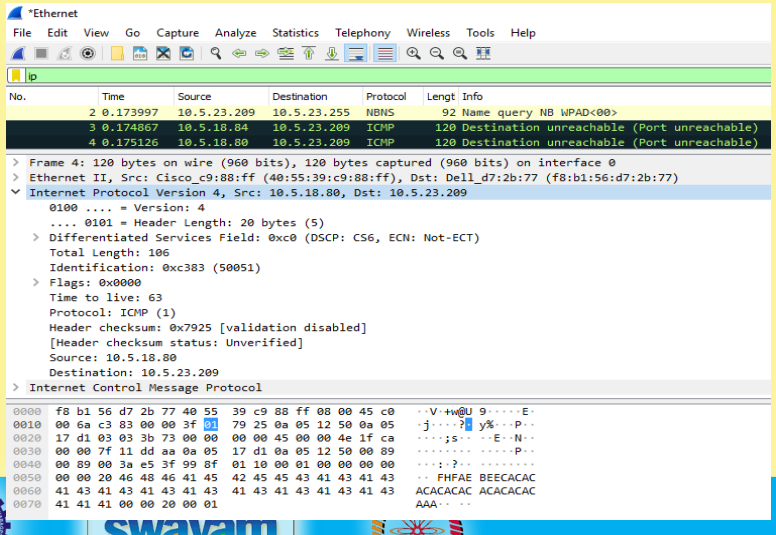
- When you double click on any of the packets the respective protocol will highlight, and you can see header details.




IP Filter Summary Window



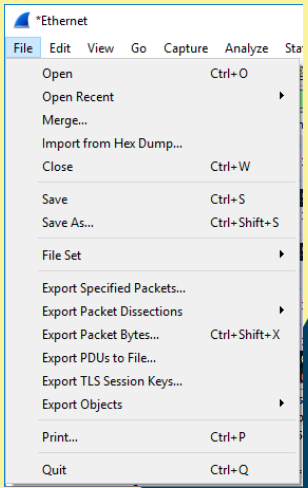
IP Packet Header Detail



Exploring the Menu

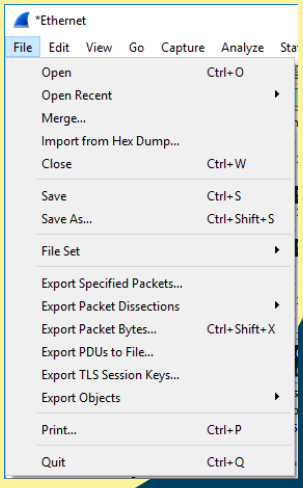
File Menu

- 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).



File Menu

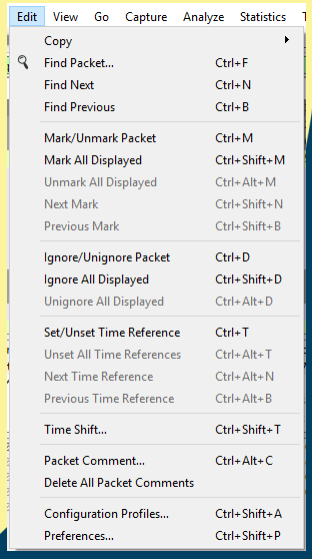
- **Export :**
  - **File Set:** navigate the directory where file will be stored.
  - **Various Exports Options:** allow to save report in different format such as CSV, C array, XML, JSON etc., it also allows to save data for selected packet or range of packets.
  - **Print:** to print report as a plain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



17

Edit Menu

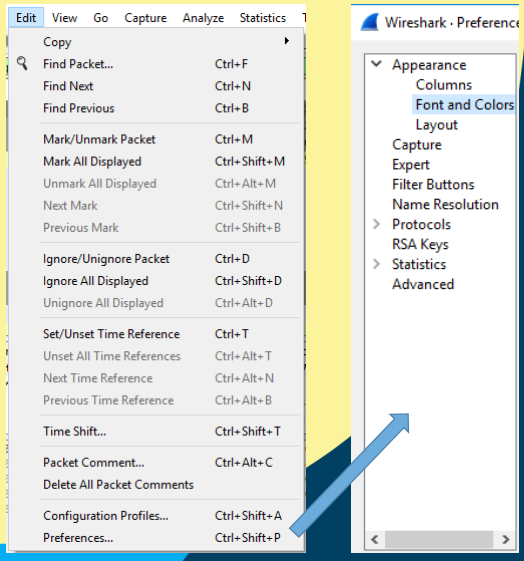
- Edit menu can also be divided into 5 sections:
- **Find:**
  - Used to search packets by matching hexadecimal string, and to search for next and previous packets as per requirement.
- **Mark:**
  - Mark options are used for marking the packets that are displayed in summary window.



18

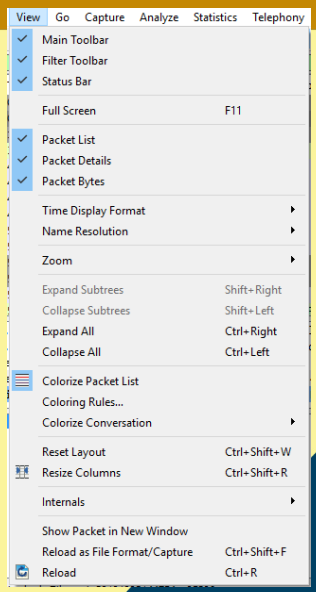
Edit Menu

- **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.).



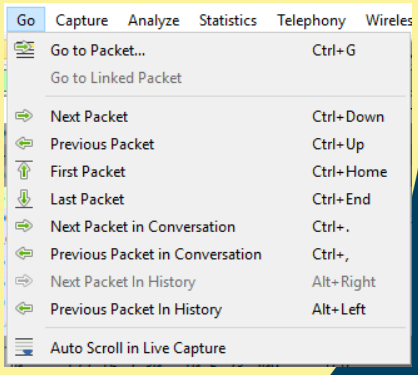
View Menu

- 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.



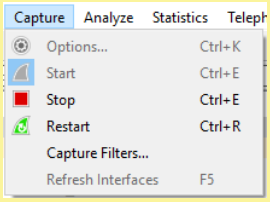
Go Menu

- Go menu is used to switch between packets.

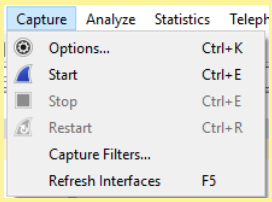



Capture Menu

- 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.



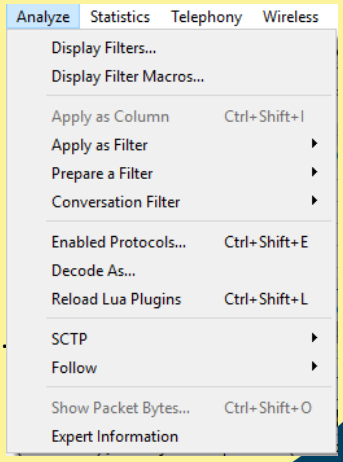
Capturing



Capture stopped


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.



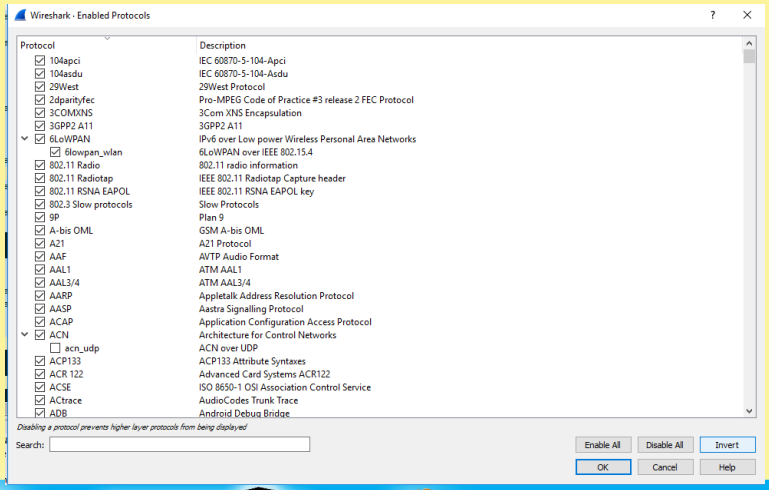
Analyze Menu: Display Filter

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

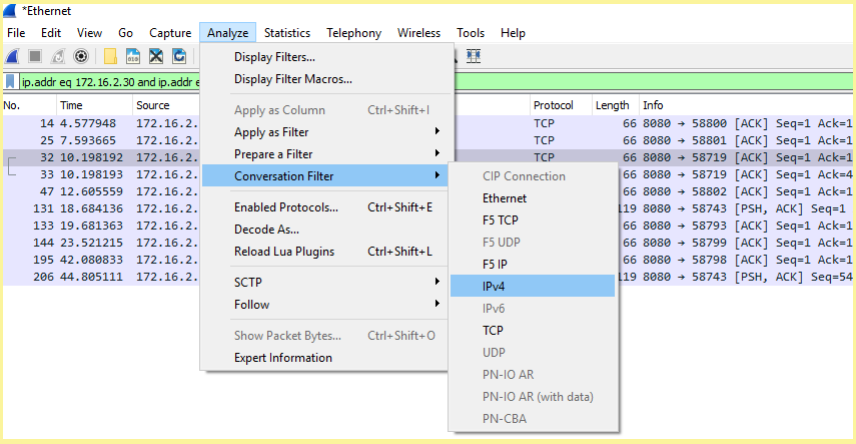
- To filter packets we need to give a specific filter name.

Analyze Menu: Enable protocol



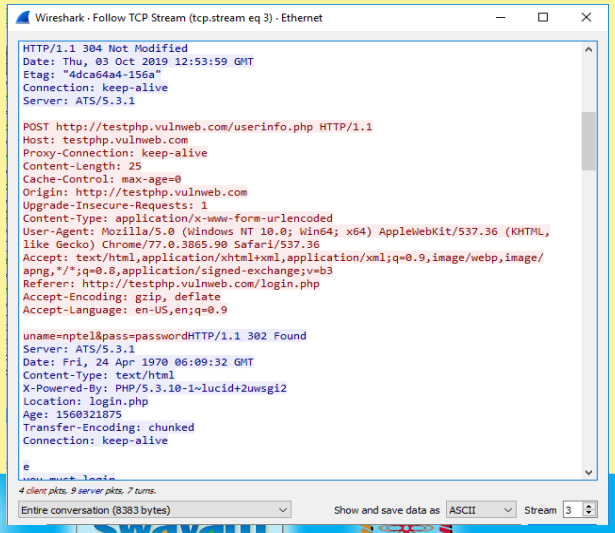
- We can enable or disable protocol.
- If we don't want to see icmp packets, then uncheck icmp protocol.

Analyze Menu: Conversion Filter



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

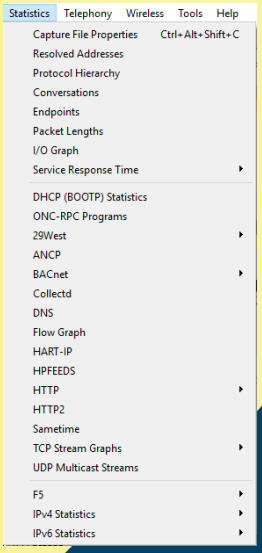
Analyze Menu: Follow



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

Statistics Menu

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



Statistics Menu: Capture File Properties

File

Name: C:\Users\user\AppData\Local\Temp\wireshark_Ethernet_20191003190446_a01600.pcapng
Length: 58 kB
Hash (SHA256): bfeabfe4ac58ba50db4ea2297c06faff485f297c1c0781627 4bc3fbebff656d0
Hash (RIPEMD160): 90cdee113606bad766907d2d5e0f1bb3b9b02678
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 show the full system detail of the capturing machine.

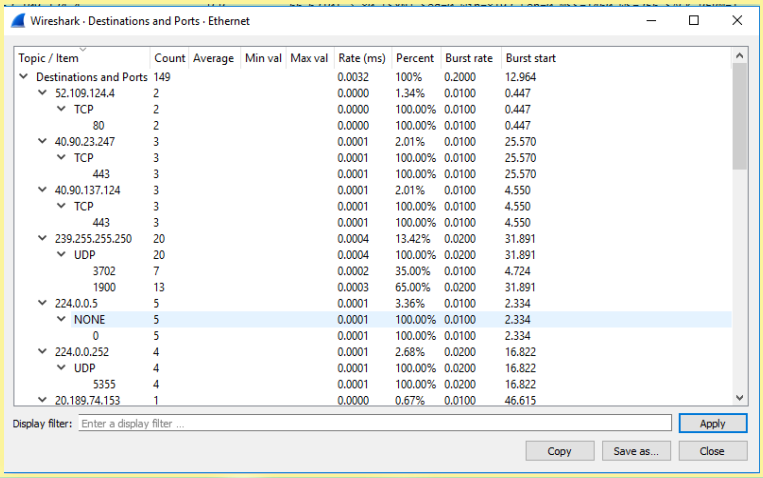
Statistics Menu: Protocol Hierarchy

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	8525	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

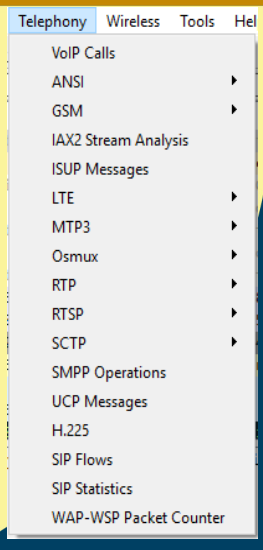
Statistics Menu: Destination and Ports



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

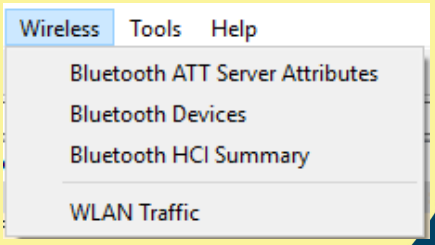
Telephony Menu

- 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.



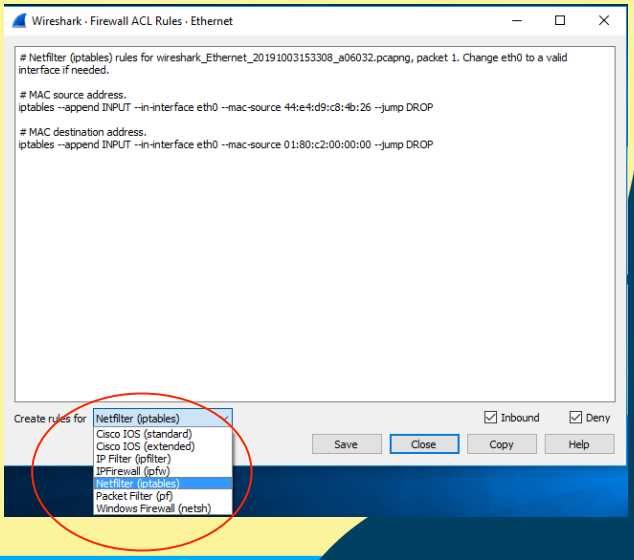
Wireless Menu

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



Tools Menu

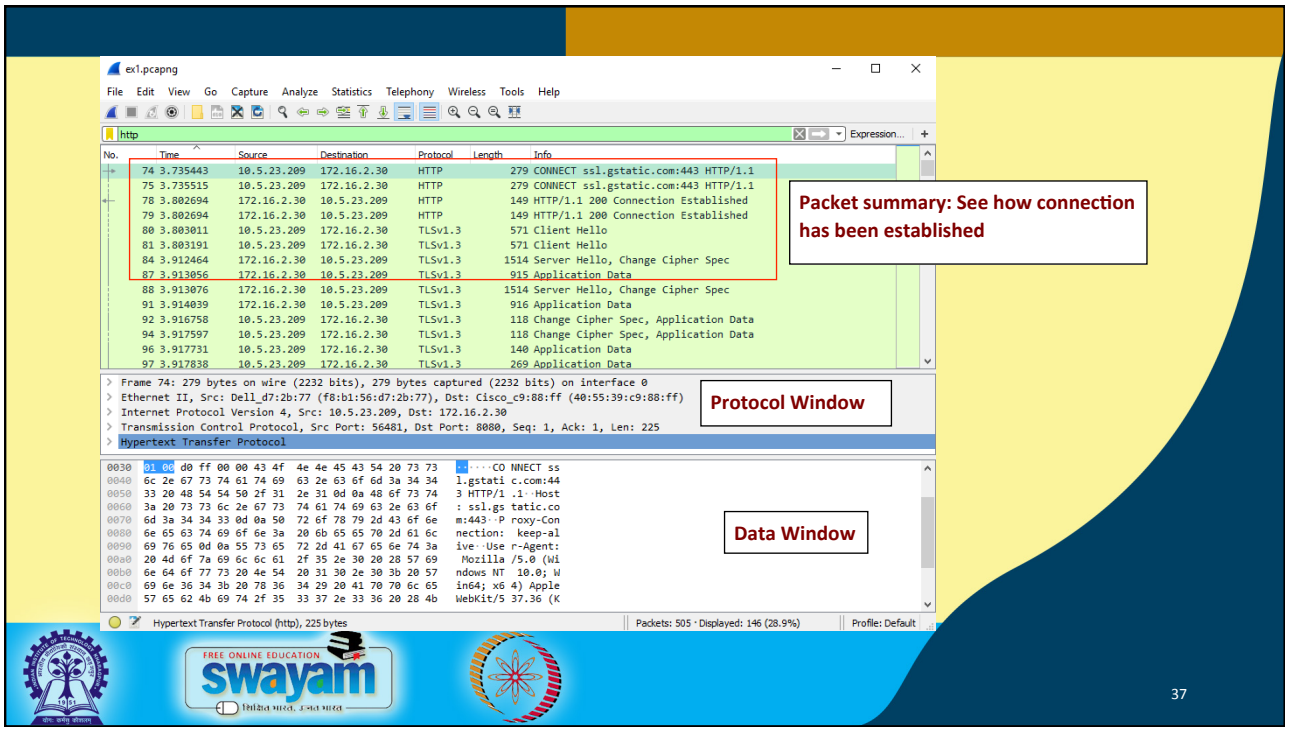
- This menu is used to select the rules (which type of scanning do you want to do).
- It also provides help for various tools that are used by Wireshark.



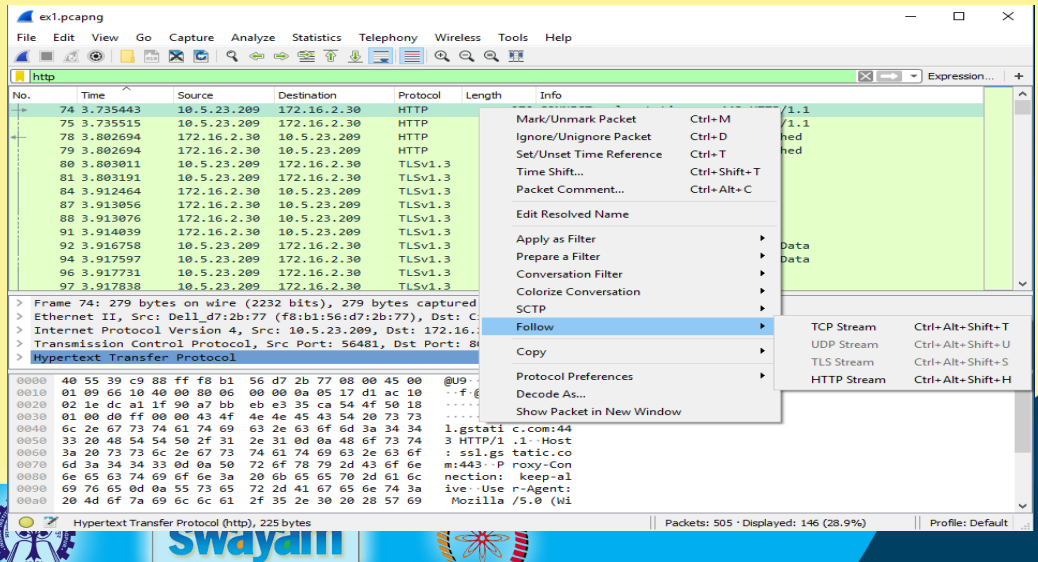
Packet Analysis Examples


Example:

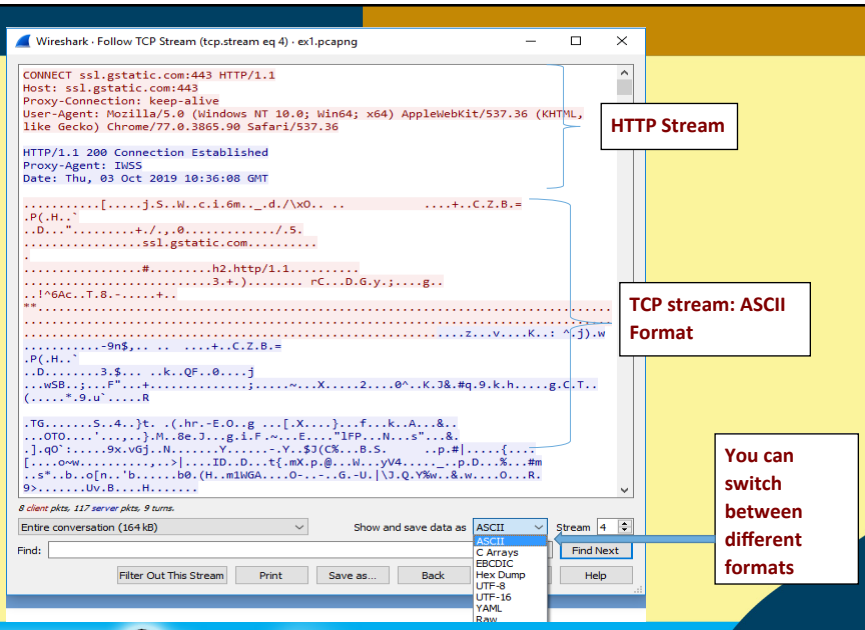
- Start a capture in wireshark.
- Open browser and type www.google.com and search.
- Save capture and analyze by applying http filter.

Right click to packet → Follow → HTTP/TCP stream to see data



Data Details

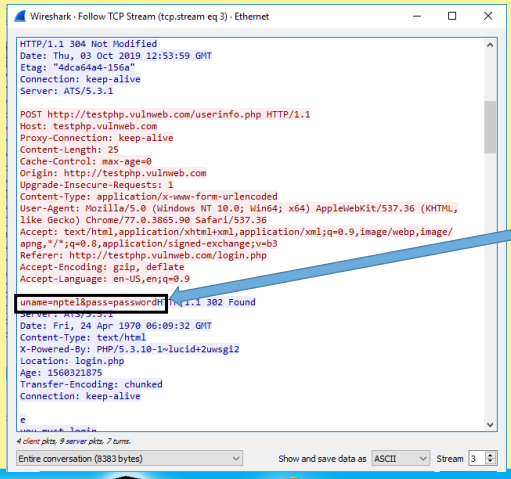


Capture Login credentials of unsecured website: vulnweb.com

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

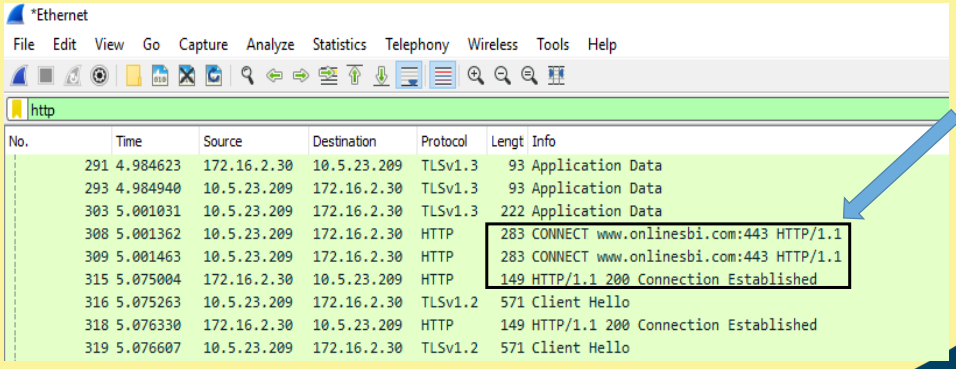
82	6.549036	172.16.2.30	10.5.23.209	HTTP	186 HTTP/1.1 304 Not Modified
83	6.598996	10.5.23.209	172.16.2.30	TCP	54 61385 → 8080 [ACK] Seq=912 Ack=265 Win=65280 Len=0
106	14.107445	10.5.23.209	172.16.2.30	HTTP	722 POST http://testphp.vulnweb.com/userinfo.php HTTP/1.1 (application/x-www-form-urlencoded)
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]

We can even view username and password from http packet

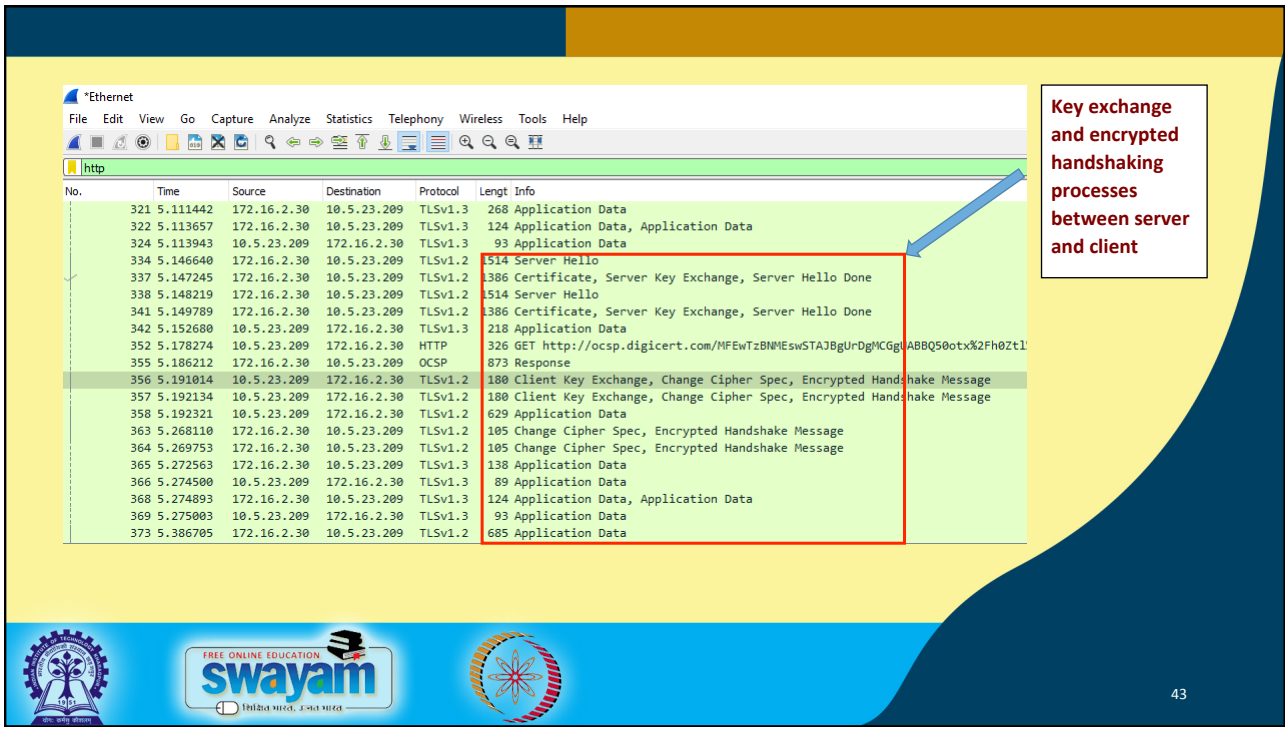


See we captured username and password

Packet details for SBI net banking



Making secure connection with port 443


*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
No. Time Source Destination Protocol Lengt 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 1514 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 1514 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/MFEwTzBNMEswSTAJBgUrDgMCGgUABBQ50otx%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
FREE ONLINE EDUCATION
swayam
43


FREE ONLINE EDUCATION
swayam
NPTEL ONLINE CERTIFICATION COURSES
Thank you!
44