

# Day 2: Networking Fundamentals + Nmap for Ethical Hacking

## 1. नेटवर्किंग क्या है?

नेटवर्किंग का मतलब है दो या ज़्यादा डिवाइसेज़ को जोड़ना ताकि वे डेटा शेयर कर सकें।

हैकिंग में उपयोग:

- नेटवर्क स्कैनिंग
- सर्विस पहचानना
- टारगेट डिवाइस का एनालिसिस

टाइप	मतलब
LAN	Local Area Network (जैसे: घर या ऑफिस)
WAN	Wide Area Network (जैसे: इंटरनेट)
WLAN	Wireless LAN (WiFi network)

## 2. Network Components & Terminology

Term	मतलब	Hacking में उपयोग
IP Address	हर डिवाइस का यूनिक एड्रेस	टारगेट की पहचान के लिए
MAC Address	हार्डवेयर का यूनिक ID	MAC spoofing
Subnet	IPs का ग्रुप	नेटवर्क स्कोप समझना
Gateway	Default रास्ता	ट्रैफिक रेडायरेक्शन
DNS	नाम से IP मिलता है	DNS spoofing
Port	हर सर्विस का एक दरवाज़ा	Open पोर्ट्स पर अटैक
Router	इंटरनेट से जुड़ने वाला डिवाइस	-

## 3. IP Address (IPv4 और IPv6)

- **IPv4:** 192.168.1.10
- **IPv6:** 2001:0db8:85a3::8a2e:0370:7334

Reserved IPs:

- 127.0.0.1 = Localhost
- 192.168.x.x = Private IP
- 8.8.8.8 = Google DNS

---

## 4. MAC Address

हर नेटवर्क डिवाइस का यूनिक हार्डवेयर एड्रेस होता है —

Example: 00:1A:2B:3C:4D:5E

### Hacking में उपयोग:

- MAC Spoofing: अपनी पहचान छिपाना
- 

## 5. Subnetting

- Subnet mask: 255.255.255.0
  - यह तय करता है कि कौन-कौन से IP एक ही नेटवर्क में हैं।
- 

## 6. DNS (Domain Name System)

नाम को IP में बदलता है — जैसे google.com → 142.250.183.206

### Hacking में:

- DNS Spoofing
  - DNS Hijacking
- 

## 7. Gateway और Routing

- **Gateway:** Default router IP
  - **Routing:** डेटा को सही डेस्टिनेशन तक भेजना
- 

## 8. Ports & Protocols


Port	Protocol	उपयोग
20/21	FTP	फाइल ट्रांसफर
22	SSH	Secure Shell
23	Telnet	Remote Terminal
25	SMTP	Email भेजना
53	DNS	डोमेन नेम सर्विस
80	HTTP	वेब ट्रैफिक
443	HTTPS	सिक्योर वेब ट्रैफिक

☒ Ethical hackers अक्सर Open Ports स्कैन करते हैं ताकि vulnerable सर्विसेस को ढूँढा जा सके।

---

## 9. OSI Model (7 Layers)

Layer	काम
7. Application	यूज़र एप्लिकेशन (ब्राउज़र)
6. Presentation	डेटा एन्कोड/डिकोड
5. Session	सेशन कंट्रोल
4. Transport	TCP/UDP (डेटा ट्रांसफर)
3. Network	IP Routing
2. Data Link	MAC Address, Ethernet
1. Physical	Cables, Signals, WiFi

 Hackers Layer 3 और Layer 4 पर काम करते हैं —  
जैसे Port Scanning (L4), IP Spoofing (L3)

## 10. Network Tools for Hacking

Tool	काम
ping	कनेक्टिविटी चेक
tracert	रूट ट्रेस
netstat	पोर्ट्स और connections देखना
nmap	पोर्ट स्कैनिंग
wireshark	पैकेट स्निफर
tcpdump	CLI पैकेट कैप्चर
arp	नेटवर्क में MAC पता करें

## 11. Attacks Related to Networking

अटैक	मतलब
ARP Spoofing	नेटवर्क ट्रैफिक चुराना
MAC Spoofing	पहचान छिपाना
IP Spoofing	नकली IP से अटैक
DNS Spoofing	गलत साइट पर redirect करना
MITM (Man-in-Middle)	बीच में ट्रैफिक चुराना

## Hacking के Use Case Examples

---

## Find Target:

```
nmap -sn 192.168.1.0/24 # नेटवर्क में सभी डिवाइसेज दिखाएगा
```

## Check Open Ports:

```
nmap -sS 192.168.1.10
```

## Capture Passwords:

Wireshark से HTTP login डेटा पकड़ सकते हो (अगर encrypt नहीं है)

---

## Summary (Revision Table)

Concept	Relevance to Hacking
IP Address	Target को पहचानना
Ports	Vulnerable services ढूँढना
MAC Address	Spoofing से identity छिपाना
DNS	Fake site या spoofing करना
Tools	Reconnaissance और Attack tools
OSI Layer	Layer specific attacks (ARP = Layer 2)

---

## Extra Resource Options:

- PDF Notes (हिंदी/इंग्लिश)
  - Diagram (OSI, TCP Handshake, ARP Table)
  - Practicals: Nmap, ARP spoofing, MITM lab
- 

## 3. Private IP vs Public IP

- **Private IP:** Internal (e.g. 192.168.1.5)
- **Public IP:** Internet-visible (e.g. 49.205.22.1)

 आप <https://whatismyip.com> से पब्लिक IP देख सकते हैं

---

## 4. Common Network Services & Ports


Port	Protocol	Service
21	FTP	File Transfer
22	SSH	Remote Login
23	Telnet	Insecure Remote Login
25	SMTP	Email Sending
53	DNS	Name Resolution
80	HTTP	Web
443	HTTPS	Secure Web

☒ Hacker के रूप में आपको पता होना चाहिए कि कौन सा पोर्ट कौन सी सर्विस को चला रहा है।

## 5. Basic Networking Tools (Linux में)

Command	काम
ping	कनेक्टिविटी चेक
tracert	रूट ट्रैक करना
ifconfig / ip a	नेटवर्क इंटरफेस देखना
netstat -tuln	रनिंग पोर्ट्स देखना
arp -a	नेटवर्क में डिवाइसेज़
hostname -I	अपना IP देखना
netstat -tuln	Open Ports & Services

## 6. Nmap: Network Scanning Tool

 Nmap क्या करता है?

Nmap (Network Mapper): एक powerful स्कैनिंग टूल है जिससे आप कर सकते हैं:

- Port Scan
- OS Detection
- Service Version पता करना
- Vulnerability Scripts चलाना

### Basic Nmap Commands

Command	काम	Example
nmap	Basic Scan	nmap 192.168.1.1

Command	काम	Example
nmap -p-	सभी 65535 पोर्ट स्कैन	nmap -p- 192.168.1.1
nmap -sS	Stealth SYN स्कैन	nmap -sS 192.168.1.1
nmap -sV	सर्विस वर्जन डिटेक्ट	nmap -sV 192.168.1.1
nmap -O	OS डिटेक्शन	nmap -O 192.168.1.1
nmap -A	Advanced: OS, script, traceroute	nmap -A 192.168.1.1
nmap -F	Fast Scan (100 पोर्ट्स)	nmap -F 192.168.1.1
nmap -sU	UDP पोर्ट स्कैन	nmap -sU 192.168.1.1

## Practical Examples

```
# 1. Fast scan
nmap -F 192.168.1.1

# 2. Scan all ports
nmap -p- 192.168.1.1

# 3. Scan multiple IPs
nmap 192.168.1.1 192.168.1.2

# 4. Scan a range
nmap 192.168.1.1-10

# 5. Scan entire subnet
nmap 192.168.1.0/24

# 6. Save result to file
nmap -oN result.txt 192.168.1.1
```

## 7. Nmap NSE Scripts (Advanced Scans)

```
# HTTP enum
nmap --script http-enum 192.168.1.1

# Vulnerability scan
nmap --script vuln 192.168.1.1

# SMB Enumeration
nmap --script smb-os-discovery 192.168.1.1
```

## 8. Real Life Ethical Hacking Examples

Scenario	Command
नेटवर्क में सारे सिस्टम	nmap -sn 192.168.1.0/24
एक सिस्टम के open ports	nmap -sS 192.168.1.10
कौन सी सर्विस चल रही	nmap -sV 192.168.1.10
OS और version पता करना	nmap -O 192.168.1.10

### Day 2 Summary

टॉपिक	आपने क्या सीखा
Networking Basics	IP, Subnet, DNS, Gateway
Tools	Ping, ifconfig, traceroute
Nmap	Port Scanning, OS Detection
NSE Scripts	Vulnerability Scan, Enum
Real Hacking Use	Network Recon & Mapping

### Extra Learning:

- Try on your home WiFi (ethically)
- Install Wireshark for packet sniffing
- Create a local network and try Nmap on multiple devices