🔐 নেটওয়ার্ক পোর্টস এবং সাইবার সিকিউরিটির দৃষ্টিকোণে তাদের গুরুত্ব (বাংলায় সম্পূর্ণ গাইড)

🧠 ভূমিকা:

নেটওয়ার্ক পোর্ট হল একটি লজিক্যাল চ্যানেল যেটা দিয়ে ডেটা এক সিস্টেম থেকে অন্য সিস্টেমে ট্রান্সফার হয়। প্রতিটি নেটওয়ার্ক সার্ভিস (যেমন HTTP, FTP, DNS) নির্দিষ্ট একটি পোর্ট ব্যবহার করে। একজন SOC Analyst বা Security Professional হিসেবে, আপনাকে অবশ্যই জানতে হবে কোন সার্ভিস কোন পোর্টে চলে, এবং সেই পোর্ট কীভাবে নিরাপত্তা হুমকির কারণ হতে পারে।

🎯 পোর্টের ক্যাটাগরি (Port Categories):

ধরন	পরিসীমা	ব্যাখ্যা
Well-known Ports	0 – 1023	গুরুত্বপূর্ণ সার্ভিস যেমন HTTP, FTP, DNS
Registered Ports	1024 – 49151	কিছু অ্যাপ্লিকেশন ও সার্ভিস
Dynamic/Private Ports	49152 – 65535	Client-side communication বা temporary communication

---

🔥 ইন্টারভিউ ও SOC কাজে সবচেয়ে গুরুত্বপূর্ণ পোর্টসমূহ:

1️⃣ Port 80 – HTTP

- প্রটোকল: TCP
- ব্যাখ্যা: ওয়েবসাইটের জন্য ডিফল্ট HTTP পোর্ট।
- হুমকি: Data sniffing, malware delivery
- SOC বিষয়: Web traffic monitoring, Phishing analysis

2️⃣ Port 443 – HTTPS

- প্রটোকল: TCP
- ব্যাখ্যা: Encrypted web traffic (SSL/TLS)
- হুমকি: Encrypted C2 communication
- SOC বিষয়: SSL traffic analysis, certificate inspection

3️⃣ Port 53 – DNS

- প্রটোকল: UDP/TCP
- ব্যাখ্যা: Domain Name Resolution
- হুমকি: DNS tunneling, spoofing
- SOC বিষয়: Suspicious DNS queries, data exfiltration

4️⃣ Port 21 – FTP (Control)

- প্রটোকল: TCP
- ব্যাখ্যা: ফাইল ট্রান্সফারের জন্য কমান্ড পাঠানো।
- হুমকি: Cleartext credentials, brute-force attacks
- SOC বিষয়: FTP traffic alert, unauthorized login detection

5️⃣ Port 20 – FTP (Data Transfer)

- প্রটোকল: TCP
- ব্যাখ্যা: মূল ফাইল পাঠানোর জন্য ব্যবহৃত পোর্ট।
- SOC বিষয়: Suspicious file transfer monitoring

6️⃣ Port 22 – SSH

- প্রটোকল: TCP
- ব্যাখ্যা: Secure remote login
- হুমকি: Brute-force login, unauthorized access
- SOC বিষয়: SSH login alert, honeypot detection

7️⃣ Port 23 – Telnet

- প্রটোকল: TCP
- ব্যাখ্যা: Remote login (unencrypted)
- হুমকি: Credential sniffing, legacy vulnerability
- SOC বিষয়: Telnet usage alert (risk!)

8️⃣ Port 25 – SMTP

- প্রটোকল: TCP
- ব্যাখ্যা: ইমেইল প্রেরণের জন্য ব্যবহার হয়।
- হুমকি: Spam, phishing, spoofing
- SOC বিষয়: Outbound SMTP block policy, spam detection

9️⃣ Port 110 – POP3

- প্রটোকল: TCP
- ব্যাখ্যা: ইমেইল রিসিভ করার প্রটোকল।
- SOC বিষয়: POP3 over insecure channel alert

🔟 Port 143 – IMAP

- প্রটোকল: TCP
- ব্যাখ্যা: ইমেইল access (multiple-device sync)
- হুমকি: IMAP hijacking
- SOC বিষয়: Email exfiltration detection

1️⃣1️⃣ Port 3389 – RDP

- প্রটোকল: TCP
- ব্যাখ্যা: Remote Desktop Protocol
- হুমকি: RDP brute-force, lateral movement

- SOC বিষয়: Remote access monitoring, geolocation mismatch alert

---

12️⃣ Port 445 – SMB (Windows File Sharing)

- প্রটোকল: TCP
- হুমকি: WannaCry, EternalBlue exploit
- SOC বিষয়: Internal lateral movement, file share exploit detection

---

13️⃣ Port 67/68 – DHCP

- প্রটোকল: UDP
- ব্যাখ্যা: IP assignment to client
- হুমকি: Rogue DHCP server
- SOC বিষয়: DHCP starvation, rogue IP allocation detection

14️⃣ Port 137-139 – NetBIOS

- ব্যাখ্যা: Windows systems communication (legacy)
- হুমকি: NetBIOS name spoofing
- SOC বিষয়: LLMNR/NBT-NS poisoning detection

15️⃣ Port 8080 – Alternate HTTP

- ব্যাখ্যা: Custom HTTP, admin panel, proxy
- হুমকি: Custom malware panel, exposed dashboard
- SOC বিষয়: Unexpected HTTP services

16️⃣ Port 3306 – MySQL

- হুমকি: DB dump, SQLi exploitation
- SOC বিষয়: Database access alert, DB brute force detection

1️⃣7️⃣ Port 1433 – MS SQL Server

- হুমকি: Brute-force attacks
- SOC বিষয়: SQL server enumeration, credential guessing

🛡️ SOC ও Security Point of View থেকে প্রয়োজনীয় কাজ:

বিষয়	SOC Analyst কী করবেন?
Suspicious port scanning	Detect using IDS (Snort/Suricata), firewall logs
Unauthorized access attempt	Alert tuning in SIEM
Brute-force on port 22, 3389	Geo-based login monitoring
DNS tunneling on port 53	Deep packet inspection
Malware C2 on port 8080/443	Encrypted traffic analysis

📜 টুলস এবং লজ উৎস:

টুলস	ব্যবহার
Wireshark	পোর্টভিত্তিক ট্রাফিক বিশ্লেষণ
SIEM (Splunk, LogRhythm)	Suspicious port traffic alerting
Nessus/Qualys	Vulnerability detection on open ports
Firewall logs	Port-level access tracking
Netstat/lsof (Linux)	Live port and process mapping

📘 ইন্টারভিউতে সম্ভাব্য প্রশ্ন:

1. **DHCP ও DNS এর মধ্যে পার্থক্য কী? কোন পোর্টে চলে?**
2. **FTP কেন দুইটা পোর্ট ব্যবহার করে?**
3. **RDP port এ brute force detection কীভাবে করবেন?**
4. **Port 53 দিয়ে data exfiltration detect করবেন কীভাবে?**
5. **HTTPS traffic এনালাইসিস কীভাবে করবেন যদি SSL Inspection না থাকে?**

🧠 শেষ কথা:

একজন দক্ষ SOC Analyst বা Security Engineer-এর উচিত:

- Common ও uncommon port চেনা
- Port exploitation technique জানা
- SIEM ও firewall-এ এসব পোর্টের ট্রাফিক মনিটরিং করা
- Threat intel দিয়ে পোর্টের ট্রেন্ড বিশ্লেষণ করা