📘 Ethical Hacking Course – Lecture 5 Notes

---

1) TCP 3-Way Handshake

What it is

The TCP handshake is the standard process used to create a reliable connection between a client and a server before data is exchanged.

Step-by-step (with sequence/ack numbers)

1. **Client → Server:** SYN (synchronize) with sequence = x
    - Client says: "I want to start a connection; my initial sequence number is x."
2. **Server → Client:** SYN + ACK (synchronize + acknowledge) with SYN = q, ACK = x + 1
    - Server replies with its own sequence q and acknowledges client's SYN by setting ACK = x+1.
3. **Client → Server:** ACK with SEQ = x+1 (or client's next seq y+1) and ACK = q+1
    - Client acknowledges server's SYN. After this, the connection is established and both sides can send data.

Why it's used

- Ensures both sides agree on initial sequence numbers and are ready to communicate reliably.
- Enables features like ordered delivery, retransmission, flow control.

Attacks & defenses

- **SYN flood:** attacker sends many SYNs and never completes handshake → server allocates resources and can be exhausted.
    - Defenses: SYN cookies, connection backlog tuning, rate limiting, stateful firewalls.
- **Session hijacking:** stealing sequence/ACK info to inject packets. Use TLS and strong session controls to defend.

2) Firewall — How They Work & Generations

Basic concept

A firewall examines traffic between zones (e.g., Internet ↔ PC) and applies rules to **allow, block, or modify** traffic based on criteria (IP, port, protocol, application).

Typical packet path

PC ↔ Firewall ↔ Internet
The firewall checks **source port → destination port**, source/destination IP, and rulebook (inbound/outbound) to permit or deny traffic.

Generation 1 — Packet-filtering firewall (stateless)

- **What:** Checks IP header fields (source/destination IP, source/destination port, protocol).
- **How:** Simple rule table.
- **Limitation:** No context of connection state; can be bypassed with some attacks.

Generation 2 — Stateful firewall

- **What:** Tracks connection state (e.g., TCP handshake info, sequence/ack numbers).
- **How:** Keeps a connection table and only allows packets that match an established session.
- **Benefits:** Blocks unsolicited packets that don't match a session.

Next-Generation Firewall (NGFW)

- **What:** Combines stateful firewalling with application awareness and integrated security services.
- **Common features:**
    - **Application identification & control** (can block specific web/apps).
    - **Intrusion Detection/Prevention (IDS/IPS)** — detects/blocks malicious packets/events.
    - **Antivirus/antimalware scanning** of traffic.

    - **URL filtering, content inspection**, SSL/TLS inspection (if configured).
    - **Threat intelligence / signature updates** — uses signature/hash/digital sign values to identify malware.
- **Why used:** Provides deep inspection and better protection against modern threats (ransomware, APTs).

How IDS vs IPS differ

- **IDS (detect):** Monitors and alerts on suspicious activity.
- **IPS (prevent):** Actively blocks or drops malicious traffic.

Operational notes

- **Inbound rules** control traffic entering your network (e.g., remote desktop).
- **Outbound rules** control traffic leaving your network (e.g., block exfiltration).
- **Reputed IP / IP reputation**: Many firewalls/IDS consult IP reputation feeds to block known bad IPs.

---

3) Useful Threat/Intelligence Resources (study & practice)

- Sites like **SafetyDetectives** (example blog: “most dangerous new malware and security threats”) are useful to read regularly to keep up with ransomware and malware families and their indicators (hashes, behaviors).
- **IP reputation services** (example: ipqualityscore.com) let you check whether an IP has been flagged for abuse — useful for investigating suspicious traffic.

Note: always cross-verify threat intel from multiple trusted sources and avoid downloading “cracked” tools or suspicious payloads for testing on production machines.

---

4) VPN (Virtual Private Network)

What a VPN does (high level)

- Creates an **encrypted tunnel** between a client and a VPN server (or between sites), protecting the confidentiality and sometimes the integrity of traffic, and often hiding the client's public IP from the destination.

Typical components (client perspective)

User device → VPN client → ISP → VPN server → Internet

- With VPN: the destination sees the **VPN server's IP**, not the user's real public IP.

Why people use VPNs

- **Privacy** (mask IP address), **security** on untrusted networks (public Wi-Fi), **access** (bypass geo-restrictions), and **remote access** to corporate networks.

VPN protocols & examples

- **PPTP:** old, insecure — avoid.
- **L2TP/IPsec:** more secure (tunnel + encryption).
- **IPsec:** standard for site-to-site VPNs.
- **OpenVPN:** widely used, secure, configurable.
- **WireGuard:** modern, fast, simpler codebase.

VPN architecture variants

- **Remote-access VPN:** Individual users connect into corporate network (use RDP, fileshares).
- **Site-to-site VPN:** Connects two networks (office ↔ branch) with a persistent tunnel.

With vs Without VPN (flow)

- **Without VPN:** User device → ISP → Internet (destination sees user's public IP).

- **With VPN:** User device → VPN client (encrypted) → ISP → VPN server (decrypt) → Internet (requests originate from VPN server IP).

Risks & caveats

- **Cracked software** sites (e.g., getintopc.com or similar) often bundle malware; they may collect your public IP and create logs on their servers — downloading cracked software is dangerous (malware, backdoors, data exfiltration).
- **VPN leaks:** Misconfigured VPNs can leak DNS, WebRTC, or IPv6 info revealing your real IP. Use VPNs that pass leak tests and implement robust DNS handling.
- **Compromised VPN providers**: If a VPN server is hacked or logs are kept, privacy is compromised.

Best practices

- Use reputable VPN providers, enable killswitch, check for DNS/IP leaks, prefer strong protocols (WireGuard/OpenVPN/IPsec), and avoid downloading cracked software.

---

5) Types of VPN & Use Cases

1. **Site-to-Site VPN (Tunnel):**
    - Connects two networks (branch offices). Transparent for users.
    - Often built with IPsec tunnels between routers/firewalls.
2. **Remote-Access VPN:**
    - Individual users connect into a network to access internal resources (RDP, file servers).
    - Common for teleworking.

---

6) Proxy Servers

What is a proxy?

- A **proxy** is an intermediary that forwards client requests to the destination and returns responses. The destination sees the proxy's IP (not the client's).

Types of proxies

- **Forward proxy:** Clients configure it — hides client IP; used for privacy or content filtering.
- **Reverse proxy:** Placed in front of web servers; hides backend servers, provides load balancing, caching, WAF features (e.g., Cloudflare).
- **Transparent proxy:** Intercepts traffic without client config (often used by ISPs).
- **Anonymous / elite proxy:** Varying degrees of anonymity (elite hides proxy header entirely).

Use cases

- **Privacy & anonymity**, **caching** to speed up responses, **content filtering**, **load balancing**, and **security** (reverse proxy + WAF protects backend servers).

Security notes

- Proxies can log requests; trustworthiness matters.
- Combining proxy + VPN may provide layered privacy, but both must be trusted providers.
- Attackers can use proxies to obfuscate origin.

---

7) Specific Practical Warnings (from your notes)

Cracked software (e.g., getintopc)

- Cracked software often contains malware/backdoors and may:
    - **Log** machine info (IPs, ports used, installed apps) and send it to attacker servers.
    - Facilitate **social engineering** or targeted follow-up attacks.
- **Never** use cracked software on production or personal machines if you care about security and privacy.

IP & server logging

- When you access a website or download files, the remote server logs:
    - Requesting IP address, timestamp, requested resource, and sometimes user-agent and ports.
- These logs can be used to trace requests, so hiding IPs via VPN/proxy is a privacy measure — but a compromised or malicious VPN/proxy provider can abuse logs.

---

8) Why change default ports (RDP, SMB, etc.)

- Default ports (RDP 3389, SMB 139/445) are widely scanned and targeted. Changing ports:
    - Reduces automated scanning hits (security by obscurity — not a substitute for real security).
    - Requires updating firewall rules and documentation.

---

9) Quick practical defensive checklist

- Use stateful or NGFWs with IDS/IPS and updated threat feeds.
- Block unnecessary inbound ports; enforce least privilege and MFA for remote access.
- Monitor IP reputation and block known bad IPs.

- Avoid cracked software; test malware only in isolated VMs with no host/Internet links.
- Use reputable VPNs; verify they don’t leak DNS/IP addresses.
- Regularly review scheduled tasks, autoruns, and logs for persistence.

---

10) Summary — One-line definitions

- **TCP Handshake:** SYN → SYN+ACK → ACK to establish a reliable TCP connection.
- **Firewall (1st→NG):** Packet filter → stateful (session tracking) → NGFW (app awareness + IDS/IPS + AV).
- **VPN:** Encrypted tunnel that hides client IP and secures traffic (remote-access or site-to-site).
- **Proxy:** Middleman that forwards client requests; can be for privacy, caching, or load balancing.
- **Cracked software risk:** Often contains malware; avoid.

✅ CHAPTER SUMMARY

This chapter explains the fundamentals of networking security components used in ethical hacking, including the TCP 3-way handshake, firewall generations, VPN architectures, proxy servers, threat intelligence sources, and practical security tips.

It begins with how TCP connections are formed using a SYN → SYN/ACK → ACK sequence, why the handshake prevents packet loss, and how attackers abuse it via SYN floods or session hijacking.

Next, it explains firewall evolution from packet-filtering (stateless) to stateful firewalls (connection-aware) to today's NGFWs that provide application control, IDS/IPS, malware scanning, and URL filtering.

VPNs are covered with emphasis on encryption, anonymity, remote access, site-to-site tunnels, and vulnerabilities such as DNS/WebRTC leaks or untrustworthy VPN providers. Proxy servers are explained including forward, reverse, transparent, and elite proxies.

The chapter also includes essential warnings about cracked software—how it often contains malware, spyware, backdoors, and logs user information. It explains why organizations change default ports like RDP/SMB and ends with a practical defensive checklist.

Overall, the chapter provides foundational networking security knowledge necessary for ethical hacking and interviews.

✅ CONCLUSION

This chapter builds a solid understanding of how network communication, security controls, and privacy tools work together. A proper understanding of TCP handshakes, firewalls, VPNs, and proxies is essential for both attackers and defenders. Modern cybersecurity relies not only on technical configurations but also on safe practices, updated systems, and avoiding risky sources such as cracked software. Mastery of these topics allows a cybersecurity professional to analyze, secure, and monitor network traffic effectively while identifying threats and preventing intrusions.

✅ TEXT-BASED MINDMAP (DETAILED)

ETHICAL HACKING – LECTURE 5

1. TCP 3-Way Handshake

- Steps
  - SYN → Client to Server (seq = x)
  - SYN+ACK → Server to Client (seq = q, ack = x+1)
  - ACK → Client to Server (ack = q+1)
- Purpose
  - Reliable connection
  - Sequence number agreement
  - Ordered + error-free delivery
- Attacks
  - SYN Flood
  - Session Hijacking
- Defenses
  - SYN Cookies
  - Firewalls
  - Rate limiting
  - TLS

2. Firewalls

- Generation 1 – Packet Filtering (Stateless)
  - Checks IP, port, protocol
  - No connection tracking
- Generation 2 – Stateful Firewall

- ├— Tracks sessions
- └— Blocks unsolicited packets
- ├— Next-Generation Firewall
- ├— Application identification
- ├— IDS/IPS
- ├— Antivirus engine
- ├— SSL inspection
- └— Threat intelligence
- └— Rules
  - ├— Inbound
  - └— Outbound

3. Threat Intelligence Resources
   - ├— Blogs on malware
   - ├— IP reputation sites
   - └— Cross-verification of intel

4. VPN
   - ├— What it does
     - ├— Encrypts traffic
     - ├— Hides IP
     - └— Protects from untrusted networks
   - ├— Protocols
     - ├— PPTP (weak)
     - ├— L2TP/IPsec
     - ├— OpenVPN

- └── WireGuard
- ├── Types
  - ├── Remote-access
  - └── Site-to-site
- ├── Risks
  - ├── DNS leaks
  - ├── VPN logging
  - └── Fake/cracked VPN apps

5. Proxy
   - ├── Forward Proxy
   - ├── Reverse Proxy (Cloudflare)
   - ├── Transparent Proxy
   - ├── Anonymous/Elite Proxy
   - └── Uses: anonymity, load balancing, caching

6. Cracked Software Risks
   - ├── Malware/backdoors
   - ├── IP logging
   - ├── Data theft
   - └── Persistence mechanisms

7. Port Changing
   - ├── Avoid default scanned ports
   - └── Reduce brute force attempts

8. Defensive Checklist

├— NGFW + IDS/IPS

├— Block unused ports

├— MFA + least privilege

├— Avoid cracked software

├— Check VPN leaks

└— Monitor logs

✅ INTERVIEW QUESTIONS + PERFECT SIMPLE ANSWERS

🔹 TCP 3-WAY HANDSHAKE – Interview Q&A

1. What is the TCP 3-way handshake?

It is the process TCP uses to create a reliable connection between client and server using SYN → SYN+ACK → ACK.

2. Why is the handshake needed?

To agree on sequence numbers, synchronize both ends, and ensure reliable, ordered data transmission.

3. Explain SYN, ACK, and sequence numbers.

- **SYN:** A request to start a connection.
- **ACK:** Acknowledges received packets.
- **Sequence numbers:** Track data order and prevent duplication.

4. What is a SYN flood attack?

An attacker sends many SYN packets without completing the handshake, causing the server to waste resources and potentially crash.

5. How do you prevent SYN flood attacks?

SYN cookies, rate limiting, firewalls, and increasing connection backlog.

6. What is session hijacking?

Taking over an existing TCP session by guessing or stealing sequence and ACK numbers.

🔹 **FIREWALLS – Interview Q&A**

7. What is a firewall?

A security device/software that controls inbound and outbound traffic based on rules.

8. Difference between stateless and stateful firewalls.

- **Stateless:** Checks only IPs/ports, no session tracking.
- **Stateful:** Tracks connection states (SYN/ACK) and blocks invalid packets.

9. What is an NGFW?

A Next-Generation Firewall that includes application control, IDS/IPS, URL filtering, malware detection, and SSL inspection.

10. How does IDS differ from IPS?

- **IDS:** Detects & alerts.
- **IPS:** Detects & blocks in real time.

11. What is IP reputation?

A security score of an IP based on past malicious activity.

🔹 **THREAT INTELLIGENCE – Interview Q&A**

12. What is threat intelligence?

Information about malware, attackers, vulnerabilities, and suspicious IPs collected from various security sources.

13. Why cross-check threat intelligence?

Single sources may give false positives; verifying ensures accuracy.

🔹 VPN – Interview Q&A

14. What is a VPN?

A Virtual Private Network that creates an encrypted tunnel and hides your real IP.

15. What are the two types of VPN?

- **Remote Access VPN:** User connects to company network.
- **Site-to-Site VPN:** Two networks are connected securely.

16. Explain how VPN hides your identity.

Traffic goes through the VPN server, so websites see the VPN's IP instead of yours.

17. Common VPN protocols?

PPTP (weak), L2TP/IPsec, OpenVPN, WireGuard.

18. What are VPN leaks?

DNS, WebRTC, or IPv6 leaks that expose your real IP even when using VPN.

19. Why are free or cracked VPN apps dangerous?

They often log data, inject ads/malware, or sell browsing history.

🔹 PROXY – Interview Q&A

20. What is a proxy server?

A server that forwards client requests to another server.

21. Difference between forward and reverse proxy?

- **Forward proxy:** Used by clients for anonymity.
- **Reverse proxy:** Protects servers and load balances traffic.

22. What is a transparent proxy?

A proxy that intercepts traffic without client configuration.

23. Why use a reverse proxy like Cloudflare?

DDoS protection, load balancing, caching, and hiding backend IPs.

🔹 **CRACKED SOFTWARE – Interview Q&A**

24. Why should cracked software be avoided?

It often contains malware, spyware, keyloggers, and backdoors.

25. How do cracked software sites track users?

By logging IP addresses, browser details, and download activity.

🔹 **CHANGING DEFAULT PORTS – Interview Q&A**

26. Why should we change default ports like RDP 3389?

Attackers automatically scan known ports; changing reduces brute-force attempts.

27. Is changing ports a security solution?

No — it is only **security by obscurity**. Proper security still needs MFA, firewall rules, and monitoring.

🔹 **SECURITY BEST PRACTICES – Interview Q&A**

28. What is least privilege?

Giving users only the permissions they absolutely need.

29. What is the purpose of MFA?

To add a second authentication factor for stronger security.

30. Why monitor logs regularly?

Logs reveal suspicious login attempts, malware activity, or unauthorized access.

31. Why isolate malware testing in a VM?

To prevent malware from infecting the host or leaking data.