Week 1: Networking & System Security Basics

Understanding OSI & TCP/IP Models in Security

OSI Model Layers & Security Concerns

Layer	Function	Security Concerns & Countermeasures
7. Application	User applications (HTTP, FTP, DNS)	Input validation, encryption (TLS/SSL), Web App Firewalls (WAF)
6. Presentation	Data format, encryption, compression	Secure coding, format validation, TLS security
5. Session	Manages communication sessions	Session hijacking, authentication mechanisms (Kerberos, NTLM)
4. Transport	Ensures data delivery (TCP, UDP)	TCP SYN Flood, DDoS Protection (Rate limiting, firewalls)
3. Network	Routing & IP addressing (IP, ICMP)	Spoofing, DDoS, IPsec for encrypted tunnels
2. Data Link	Frames & MAC addresses (Ethernet, VLANs)	ARP spoofing, VLAN security (802.1X)
1. Physical	Cables, hardware, wireless signals	Physical security, tamper-proofing, electromagnetic shielding

TCP/IP Model & Security Considerations

- **Transport Layer Security:** Prevents session hijacking, uses SSL/TLS encryption
- **Network Security (IPsec, VPNs):** Ensures encrypted, authenticated communication
- **Application Layer Security:** Involves web security (WAFs, Content Security Policies)

Deep Dive into Firewalls, IDS/IPS, and VPNs

Firewalls

- Packet Filtering Firewalls: Control traffic based on IP/port
- Stateful Firewalls: Keep track of active connections
- Application Layer Firewalls (WAFs): Protect web applications

IDS/IPS (Intrusion Detection/Prevention Systems)

- Signature-based IDS: Matches known attack patterns (Snort, Suricata)
- Anomaly-based IDS: Detects abnormal behavior using AI/ML
- Host-based (HIDS) vs. Network-based (NIDS): Protect individual hosts vs. entire networks

VPNs (Virtual Private Networks)

- IPSec VPN: Secure encryption for private communication
- SSL VPN: Web-based VPN for remote access
- WireGuard: Fast, modern VPN protocol

📌 **Windows & Linux Hardening Techniques**

Windows Security Hardening

✅ Disable SMBv1: Set-SmbServerConfiguration - EnableSMB1Protocol $false
✅ Enable Windows Defender & Firewall: Configure rules for blocking unwanted access
✅ Account Lockout Policies: Prevent brute force attacks

Linux Security Hardening

✅ Disable Root Login: Edit /etc/ssh/sshd_config → PermitRootLogin no
✅ Enable Firewall (UFW/IPTables):

bash

CopyEdit

sudo ufw enable

sudo ufw allow ssh

✅ Use AppArmor/SELinux: Constrain process permissions

📌 Active Directory (AD) Security 101

Key AD Concepts & Attacks

- LDAP & Kerberos: AD authentication protocols
- GPO (Group Policy Objects): Controls security settings for users & machines
- NTLM Authentication: Older, vulnerable protocol (use Kerberos instead)
- Pass-the-Hash Attacks: Exploit NTLM hashes for lateral movement

Best Practices for Securing AD

✅ Enable LDAP Signing & Channel Binding
✅ Implement Tiered AD Security (Red Forest Model)
✅ Monitor Event Logs for Unusual Authentication Attempts

🛠️ LABS

1- Configure IDS/IPS with pfSense & Suricata

✅ Install pfSense Firewall in a Virtual Machine
✅ Enable Suricata IDS/IPS to detect malicious traffic
✅ Simulate an attack using nmap and analyze Suricata logs

2- Capture & Analyze Network Traffic with Wireshark

✅ Install Wireshark and capture real-time network packets
✅ Identify security threats such as ARP spoofing or DNS hijacking

You can also try to deep in those concept