

# Siber Güvenlik Temel İlerleme

## 1- Siber Güvenliğe Giriş

- CIA triadı: Gizlilik, Bütünlük, Erişilebilirlik
- Saldırı türleri: Malware, Exploit, Zero-Day
- Gerçek örnekler: NSA, WannaCry, Stuxnet
- Hacker türleri: White/Black/Gray Hat
- Red/Blue/Purple Team mantığı

## 2-Linux Temel ve orta seviye

### Dosya Sistemi ve Temel Komutlar

- Dizin yapısı ( `/home` , `/etc` , `/var` vs.)
- `ls` , `cd` , `pwd` , `cat` , `mkdir` , `rm` , `cp` , `mv`

### Kullanıcı, İzin ve Yetki Yönetimi

- `chmod` , `chown` , `sudo` , `su`
- Kullanıcı & grup mantığı, root ayrıcalıkları

### Dosya Arama ve Metin İşleme

- `grep` , `find` , `head` , `tail` , `sort` , `less`
- Log dosyaları ( `/var/log/` )

### Süreç ve Servis Yönetimi

- `ps` , `top` , `kill` , `systemctl` , `service` , `journalctl`

### Ağ Komutları

- `ping` , `ip a` , `netstat` / `ss` , `curl` , `wget` , `ssh` , `scp`

ek olarak: cron, sudo -l

### **3-Network**

- IP, MAC, Port, DNS kavramları
- TCP 3-way handshake
- UDP vs TCP farkı
- Temel protokoller (HTTP, FTP, SSH, DNS)
- Ağ katmanları (OSI & TCP/IP modeli)
- Paket yakalama mantığı
- nmap ile tarama işlemleri
- wireshark ile paket yakalama ve analizi

#### **Sniffing & Spoofing**

1. ARP protokolü ve ARP spoofing
2. DNS spoofing mantığı
3. Man-in-the-Middle (MITM) saldırısı
4. Sniffing araçları (tcpdump, Ettercap)
5. HTTPS vs HTTP farkı (neden şifreleme önemli?)
6. Demo: Basit ağ trafiği manipülasyonu

### **4-Web Güvenliğine Giriş**

- HTTP request/response yapısı
- Header, Cookie, Session kavramı
- GET vs POST farkı
- HTTPS ve SSL/TLS mantığı
- Status kodları (200, 404, 500)
- Temel güvenlik açıkları ile bağlantısı
- BurpSuite kullanımı ve örnek senaryo analizi

Ek olarak:

- OWASP nedir ve TOP 10 web zafiyetleri hakkında bilgilendirme

## **5-OSINT & Sosyal Mühendislik**

1. OSINT nedir, neden önemlidir
2. Domain, IP, kişi araştırma yöntemleri
3. Araçlar: whois, theHarvester, Shodan
4. Sosyal medya OSINT
5. E-posta analiz araçları
6. TryHackMe OSINT pratikleri

### **Sosyal Mühendislik & Phishing**

1. Sosyal mühendislik nedir
2. Phishing e-postaları
3. Spear phishing vs normal phishing
4. Araç: Gophish
5. Gerçek dünyadan phishing örnekleri
6. Önleme yolları (eğitim, 2FA, filtreleme)

Ek olarak:

- metadata analizi, örnek exif

## **6-Kimlik ve Şifreleme**

### **Şifreleme:**

- Hash fonksiyonları (MD5, SHA-1, SHA-256)
- Symmetric encryption (AES, DES)
- Asymmetric encryption (RSA, ECC)

- Digital signature mantığı
- SSL/TLS'de kullanım
- Rainbow table ve salt

### **Parola Kırma:**

1. Hash mantığı ve parola ilişkisi
2. Wordlist ile brute force (rockyou.txt)
3. Dictionary attack
4. Hydra ile servis saldırıları
5. Hashcat ile hash kırma
6. Güçlü parola önemi

### **Devam konular:**

- Tunneling & Pivoting
- owasp top 10
- Port dinleme, reverse ve bind shell
- Windows active directory
- Linux privileges escalation