**Ay 1–2: Temel Sistem ve Ağ Bilgisi**

**Amaç:** Linux kullanımı ve ağ temellerini öğrenmek

**Hafta 1**

* Kali Linux veya Ubuntu kur (VMware / VirtualBox ile sanal makine olarak)
* Temel terminal komutları öğren: ls, cd, pwd, mkdir, cp, mv, rm, cat, nano, chmod, chown
* Kaynak: Linux Journey (Beginner Level) - https://linuxjourney.com/

**Hafta 2**

* Kullanıcı yönetimi: useradd, passwd, usermod
* Dosya izinleri (rwx mantığı)
* Basit ağ komutları: ping, ifconfig/ip, netstat, traceroute

**Hafta 3**

* Ağ katmanlarını öğren (OSI modeli)
* TCP/IP, DNS, HTTP, HTTPS mantığı
* Kaynak: “Computer Networking Crash Course” (YouTube, 1 saatlik)

**Hafta 4**

* Wireshark kur ve paket yakalamayı dene
* Basit trafik analizi: HTTP isteklerini gör, IP adreslerini tespit et
* Küçük görev: Kendi bilgisayarından Google’a ping at, paketi Wireshark’ta yakala.

**Ay 3–4: Temel Siber Güvenlik Araçları**

**Amaç:** Penetrasyon testi araçlarını tanımak

**Hafta 5**

* Nmap ile ağ taraması yapmayı öğren
* Görev: Yerel ağında açık portları bul

**Hafta 6**

* Metasploit Framework’e giriş
* Yerel ağda test amaçlı bir zafiyetli makine (Metasploitable 2) kur

**Hafta 7**

* Burp Suite ile HTTP isteklerini yakalamayı öğren
* Basit login formu üzerinden kullanıcı giriş trafiğini izle

**Hafta 8**

* TryHackMe hesabı aç
* “Pre Security” öğrenme yolunu başlat (haftada 2-3 modül bitir)

**Ay 5–6: Web Güvenliği ve Mini Projeler**

**Amaç:** Web uygulama açıklarını anlamak

**Hafta 9**

* OWASP Top 10 açıklarını öğren (SQL Injection, XSS, CSRF vb.)
* Kaynak: OWASP Cheat Sheet Series

**Hafta 10**

* SQL Injection mantığını öğren (test ortamında)
* Damn Vulnerable Web Application (DVWA) kur ve dene

**Hafta 11**

* XSS (Cross Site Scripting) mantığını öğren
* DVWA üzerinde pratik yap

**Hafta 12**

* Mini proje:
  + 2–3 basit zafiyeti olan web uygulamasında açıkları bul ve rapor hazırla
  + Rapor formatı: Açık adı, nasıl bulundu, çözüm önerisi

**Hafta 13–14**

* TryHackMe’de “Web Fundamentals” ve “OWASP Top 10” odalarını bitir

**Hafta 15–16**

* Final mini proje:
  + Zafiyetli bir sanal makineyi (ör. VulnHub’tan) indir
  + Açıkları bul, not al, raporla

**1. Temel Linux ve Ağ Bilgisi**

* **Linux Journey** → https://linuxjourney.com/  
  Adım adım Linux komutlarını ve mantığını öğretir.
* **OverTheWire - Bandit** → https://overthewire.org/wargames/bandit/  
  Eğlenceli bir şekilde terminal pratiği yapmanı sağlar.
* **Computer Networking Crash Course** (YouTube) → “Computer Networking Full Course” yazarak 1–2 saatlik temel anlatımları bulabilirsin.
* **Wireshark University** → https://www.wireshark.org/docs/  
  Paket analizi örnekleri.

**2. Siber Güvenlik Temelleri**

* **TryHackMe – Pre Security Path** → https://tryhackme.com/path/outline/presecurity  
  Yeni başlayanlar için en iyi başlangıç.
* **Cybrary – Introduction to IT & Cybersecurity** → https://www.cybrary.it/course/introduction-to-it-and-cybersecurity/  
  Alanın genel mantığını anlatır.
* **HackTheBox – Starting Point** → https://app.hackthebox.com/starting-point  
  Kolay makinelerle başlarsın.

**3. Web Güvenliği**

* **OWASP Top 10 Cheat Sheet** → https://cheatsheetseries.owasp.org/  
  Web açıklarının kısa özeti.
* **PortSwigger Web Security Academy** → https://portswigger.net/web-security  
  Burp Suite ile pratik yapabileceğin interaktif eğitimler.

**4. Pratik Ortamlar**

* **VulnHub** → https://www.vulnhub.com/  
  Zafiyetli sanal makineler.
* **DVWA (Damn Vulnerable Web Application)** → http://www.dvwa.co.uk/  
  Kendi bilgisayarında web açıklarını test edebileceğin ortam.