

Kibertəhlükəsizlik

Red Team

Hücum təhlükəsizliyi və pentest

Kali Linux | Nmap | Burp Suite | Metasploit | BloodHound

Səviyyə	Proqram	Format	Dərs növü
Sıfırdan	8 modul	Onlayn	Qrup və ya fərdi

Kurs haqqında

Sistemi qorumaq üçün onu hücumçunun gözü ilə görmək lazımdır. Şəbəkə təməlindən başlayıb real hədəf üzərində tam pentest dövrünü – kəşfiyyatdan hesabata qədər – özün aparırsan.

Bu kurs kimin üçündür

01 **Sıfırdan başlayanlar**
Texniki bilik tələb olunmur. İlk modul şəbəkə, Linux və Windows təməlindən başlayır.

02 **IT mütəxəssisləri**
Sistem administratoru, şəbəkə mühəndisi və ya proqramçısansa – bildiklərin üzərinə hücum tərəfini qurursan.

03 **Tələbələr**
Diplomdan əvvəl portfoliona real pentest hesabatları və həll etdiyin laboratoriyalar düşür.

Bir həftə necə keçir

01
Onlayn dərs
Mentor mövzunu real vaxtda izah edir, sualını dərsdəcə verirsən.

02
Laboratoriya
Eyni mövzunu brauzerdə açılan laboratoriyada öz əlinlə təkrarlayırsan.

03
Həftəlik tapşırıq
Real ssenariyə əsaslanan tapşırıqla bildiyini yoxlayırsan.

04
Mentor rəyi
Mentor işini yoxlayır, səhvini göstərir, növbəti addımı deyir.

Bu, video kurs deyil: dərslər onlayndır, mentorla real vaxtda. Qrupda maksimum 5 nəfər və ya fərdi: mentor hər kəsin işini görür.

Tədris proqramı

8 modul – təməldən peşəyə

Hər modul onlayn dərs, laboratoriya və həftəlik tapşırıqla bağlanır. Növbəti modula əvvəlkini praktikada mənimsədikdən sonra keçirsən.

01

Təməl: şəbəkə, Linux və Windows

Hücumun dili: paket necə gedir, sistem necə qurulub.

OSI və TCP/IP · Linux terminal · Windows daxili quruluşu · Bash və Python skriptləri

02

Kəşfiyyat və OSINT

Hədəfə toxunmadan və toxunaraq onu tanımaq.

Passiv və aktiv recon · Nmap · Subdomain axtarışı · Servis enumeration

03

Web tətbiq hücumları

Ən çox rast gəlinən hədəf – web tətbiqləri.

OWASP Top 10 · Burp Suite · SQL injection · XSS · SSRF · Autentifikasiya xətaları

04

Şəbəkə və servis istismarı

Açıq portdan ilk girişə qədər.

Metasploit · İctimai exploitlər · Parol hücumları · Reverse shell

05

Hüquqların yüksəldilməsi

Adi istifadəçidən root və SYSTEM-ə.

Linux privilege escalation · Windows privilege escalation · Yanlış konfiqurasiyalar

06

Active Directory hücumları

Korporativ şəbəkənin ürəyi – domen.

Kerberoasting · BloodHound · Pass-the-hash · Lateral movement

07

Post-exploitation

Girişi saxlamaq və şəbəkədə irəliləmək.

Persistence · Pivoting · Tunelləmə · C2 əsasları

08

Pentest hesabatı və karyera

Tapıntını müştərinin anlayacağı dilə çevirmək.

Hesabat strukturu · Risk qiymətləndirməsi · Portfolio · Müsahibəyə hazırlıq

Kursun sonunda bacaracaqsan

- Hədəf sistem üzərində tam pentest dövrünü müstəqil aparmaq
- Web tətbiqlərdə OWASP Top 10 zəifliklərini tapıb sübut etmək
- Linux və Windows-da hüquqları yüksəltmək
- Active Directory mühitində hücum zəncirini qurmaq
- Müştəriyə təqdim olunacaq peşəkar pentest hesabatı yazmaq
- HackTheBox və TryHackMe maşınlarını köməksiz həll etmək

İşlədəcəyin alətlər

Kali Linux · Nmap · Burp Suite · Metasploit · BloodHound · Impacket · Hydra · Gobuster · Wireshark · Python

Məzunlarımızın çalışdığı qurumlar

Kapital Bank · Rabitəbank · birmarket · R.I.S.K. COMPANY · BMU Bakı Mühəndislik Universiteti · AZTU

Növbəti addım

Pulsuz onlayn sınaq dərsinə qoşul – mentorla tanış ol, sonra qərar ver.

Qrup və ya fərdi format – seçim sənindir. Qiymət, cədvəl və növbəti qrupun başlama tarixini WhatsApp-da yazırıq.

WhatsApp və zəng	+994 70 639 33 09
Sayt	compstyle.tech/kurslar/red-team
Instagram	@compstyle.az
Telegram	@compstylekanal
YouTube	@Compstyle

Compstyle TECHNOLOGY

Özün öyrən, özün yarat.

© Compstyle Technology