6 Aylıq Təlim Proqramı (Red Team)

İlk 1 ay İT biliklərini möhkəmləndirmək üçün İT Foundation dərsləri üzərinə aparılır. Növbəti aylarda isə sillabus aşağıdakı kimidir.

Kibertəhlükəsizlik və Penetrasiya Testinə Giriş

1. Kibertəhlükəsizliyə Giriş
• Kibertəhlükəsizlik anlayışı və məqsədləri
• Kibertəhlükəsizlik mütəxəssisi olmaq üçün tələb olunan bilik və bacarıqlar
• Kibertəhlükəsizlik sahəsində rollar və karyera istiqamətləri

---

2. Şəbəkə Əsasları

• Şəbəkə anlayışı və şəbəkəyə giriş
• OSI və TCP/IP modelləri
• Şəbəkə cihazları (Router, Switch, Firewall və s.)
• Subnetting və IP ünvanlama
• NAT, VPN, VLAN və Routing anlayışları
• Digər əsas şəbəkə konseptləri
Və digərləri

---

3. Əməliyyat Sistemləri və Linux Əsasları

• Linux Distributionları (Kali Linux və s.)
• Kali Linux-un qurulması və konfiqurasiyası
• Linux əsas komandaları
• Fayl oxuma və emal alətləri: cat, less, cut, sort
• Mətn emalı alətləri: regex, awk, sed
• İstifadəçilər və qruplar
• Fayl və sistem yetkiləri (permissions)

---

4. Kriptoqrafiya Əsasları

• Əsas anlayışlar və kriptoqrafik konseptlər
• Encryption və Decryption mexanizmləri
• Hash alqoritmləri və istifadəsi
• Digər kriptoqrafik mexanizmlər

---

5. Penetrasiya Testinə Giriş

• Penetrasiya testi anlayışı və məqsədi
• Etik hacking prinsipləri
• Cyber Kill Chain modeli və mərhələləri

---

6. Kəşfiyyat və İnformasiya Toplama

• İnformasiya toplama (Information Gathering)
• Enumeration anlayışı
• Footprinting protokolları
• Sosial Mühəndislik əsasları
• Nmap alətindən istifadə

---

7. İstismar və İlkin Giriş Texnikaları

• Metasploit Framework istifadəsi
• Müxtəlif servislərə qarşı hücumlar
• Zərərli yazılımlar və Initial Compromise anlayışı
⚠️ Təlim məqsədli, etik və laboratoriya mühitində

---

8. Təhlükəsizlik Mexanizmlərinin Bypass Edilməsi

• Antivirus və təhlükəsizlik kontrollarının bypass edilməsi •
Detection və Prevention mexanizmlərinin ümumi icmalı

9. Post-Exploitation Texnikaları

• Post-Exploitation anlayışı
• Sistem daxilində lateral hərəkət
• Məlumat toplanması və davamlılıq (Persistence)
• Müxtəlif Post-Exploitation hücum vektorları

10. Linux İmtiyaz Yüksəltmə

•Linux privilege escalation anlayışı
•SUID/SGID səhv konfiqurasiyaları
•Kernel və konfiqurasiya əsaslı imtiyaz yüksəltmə

QEYD:Sillabusdan kənar digər zəifliklər.

Web Application Penetration Testing

Fundamental Web -Frontend+backend – Fundamental səviyyə
Hosting +cpanel ilə tanışlıq real mühitin qurulması

1. Web Penetrasiya Testinə Giriş
• Web tətbiqlərin işləmə prinsipləri (HTTP/HTTPS, request–response modeli və s.)
• Penetrasiya testinin məqsədi, əhatə dairəsi və məhdudiyyətləri
• OWASP Top 10 anlayışı və risk qiymətləndirmə modeli

2. Web Pentest Alətləri
• Burp Suite (Proxy, Repeater, Intruder, Decoder, Scanner və s.)
• Avtomatlaşdırılmış Web Scanner proqramları
• SQLMap aləti və istifadə qaydaları

3. Kəşfiyyat və Enumeration
• Directory və file enumeration (Dirbusting)
• Parametr, endpoint və API aşkarlanması
• Texnologiya və framework identifikasiyası

4. Autentifikasiya və Sessiya Zəifliklər
• Login bruteforce və password attack texnikaları
• Broken Authentication
• Session management zəifliklər

5. Input Validation Zəifliklər
• SQL Injection (manual və SQLMap ilə)
• Command Injection
• Cross-Site Scripting (XSS – Self, Reflected, Stored, DOM)
• HTML Injection
• XML External Entities (XXE)

6. Fayl və Yol Zəifliklər
• Local File Inclusion (LFI)
• Remote File Inclusion (RFI)
• Directory Traversal

• File Upload zəifliklər

---

7. Access Control və Biznes Məntiqi Zəifliklər

• Broken Access Control
• Insecure Direct Object Reference (IDOR)
• Web səviyyəsində Privilege Escalation

---

8. Server-Side Hücumlar və Konfiqurasiya Zəifliklər

• Server-Side Request Forgery (SSRF)
• Cross-Site Request Forgery (CSRF)
• Sensitive Data Exposure
• Security Misconfiguration

---

9. Digər Web Zəifliklər

• İnformasiya sızmaları
• Error handling zəifliklər
• Digər aşkarlanan web zəifliklər və s.

🔟 Web Pentest Hesabatlandırma

• Aşkarlanmış zəifliklərin riskə görə qiymətləndirilməsi
• Proof of Concept (PoC) hazırlanması
• Tövsiyələr və remediation planı
• Peşəkar Web Penetrasiya Testi Hesabatının yazılması

🔬 Praktiki Laboratoriya:

• OWASP Top 10 əsaslı real laboratoriya mühiti
• Manual və tool-based test yanaşmaları
• Burp Suite və SQLMap ilə praktiki istismar

A1 – Injection

• HTML Injection (Reflected / Stored)
• iFrame Injection
• LDAP Injection
• OS Command Injection (Blind daxil olmaqla)
• PHP Code Injection
• SSI Injection
• SQL Injection (GET, POST, AJAX, JSON, Login, Blind, Stored, SQLite, Drupal)
• XML / XPath Injection

A2 – Broken Authentication & Session Management

• CAPTCHA Bypass
• Weak Passwords
• Password Attacks
• Insecure Login Forms
• Session ID zəifliklər
• Cookie (HTTPOnly / Secure) problemləri

A3 – Cross-Site Scripting (XSS)

• Reflected XSS (GET, POST, JSON, Headers və s.)
• Stored XSS (Blog, Cookies, User-Agent və s.)
• DOM-Based XSS

A4 – Insecure Direct Object References (IDOR)
• Object manipulation
• Unauthorized data access
• Business logic bypass

A5 – Security Misconfiguration

• Insecure services (FTP, SNMP, NTP, VNC və s.)
• CORS & Cross-Domain zəifliklər
• Old/Backup files
• Robots.txt disclosure
• DoS ssenariləri

A6 – Sensitive Data Exposure

• Clear-text credentials
• SSL/TLS zəifliklər (Heartbleed, POODLE və s.)
• Host Header Attacks
• HTML5 Storage məlumat sızmaları

A7 – Missing Functional Level Access Control

• Directory Traversal
• LFI / RFI
• SSRF
• XXE
• Restriction bypass ssenariləri

A8 – Cross-Site Request Forgery (CSRF)

• State-changing əməliyyatların istismarı
• Token bypass ssenariləri

A9 – Using Known Vulnerable Components

• Drupalgeddon
• Shellshock
• PHP CGI RCE
• Vulnerable third-party komponentlər

A10 – Unvalidated Redirects & Forwards

• Open Redirect istismarı
• Phishing ssenariləri

Other & Advanced Bugs

• Clickjacking
• HTTP Parameter Pollution
• HTTP Verb Tampering
• Information Disclosure
• Unrestricted File Upload

🏆 Bug Bounty Yanaşması

• Bug Bounty platformalarına giriş (HackerOne, Bugcrowd və s.)
• Scope analizi və qaydaların oxunması
• Real-world target-lərdə zəiflik axtarışı
• Duplicate və false-positive riskləri
• Responsible Disclosure və report yazılması

QEYD:Sillabusdan kənar digər zəifliklər.

APİ Pentest

DevSecops Fundamental

QEYD:Sillabusdan kənar digər zəifliklər.

Active Directory Penetrasiya Testi üzrə Sillabus

1. Penetrasiya testinə ümumi baxış, onun məhdudiyyətləri və pentest müdaxiləsinin həyata keçirilməsi zamanı nəzərə alınmalı olan əsas logistika məsələləri.
2. Active Directory (AD) arxitekturası və əsas anlayışlarının mənimsənilməsi.
3. Təhlükəsiz mühitdə hücum ssenarilərinin icrası üçün Active Directory laboratoriya mühitinin qurulması.
4. Daxili Active Directory nüfuzetmə test prosesinin bir hissəsi kimi xarici OSINT mənbələrindən istifadənin öyrənilməsi.
5. Dig, Nslookup, NetExec, BloodHound və oxşar alətlərdən istifadə etməklə həm əl ilə, həm də yarı-avtomatik şəkildə Şəbəkə və Domen Enumeration texnikalarının tətbiqi.
6. Kerberos əsaslı Şifrə Spreyi (Password Spraying), NTLM Relay, NBNS/LLMNR protokol sui-istifadəsi, AS-REP Roasting və digər İlkin Giriş (Initial Access) texnikalarının öyrənilməsi.
7. Kerberos protokolundan sui-istifadə etməklə Kerberos hücumları, Kerberos Delegation mexanizmləri vasitəsilə Domen İmtiyazlarının Eskalasiyası və Yanal Hərəkət texnikalarının tətbiqi.
8. Yanlış konfiqurasiya edilmiş Active Directory Giriş Nəzarət Siyahılarından (ACL) sui-istifadə etməklə Domen İmtiyazlarının Eskalasiyası və Yanal Hərəkət (Lateral Movement) texnikalarının öyrənilməsi.
9. Səhv konfiqurasiya edilmiş Active Directory Sertifikat Xidmətlərindən (AD CS) sui-istifadə etməklə imtiyaz eskalasiyası və domen dominantlığının əldə edilməsi.
10. Ümumi səhv konfiqurasiyalar və zəif Active Directory istifadəçi vərdişlərindən sui-istifadə etməklə domen səviyyəsində imtiyaz eskalasiyası və lateral hərəkət ssenarilərinin öyrənilməsi.
11. SID Filtrləmə bypassı və digər qabaqcıl metodlar daxil olmaqla Cross-Domain və Cross-Forest hücumlarının araşdırılması.
12. Qızıl Bilet (Golden Ticket), Gümüş Bilet (Silver Ticket), Brilyant Bilet (Diamond Ticket), Sapfir Bileti (Sapphire Ticket) kimi Domen Davamlılığı (Persistence) texnikalarının öyrənilməsi.
13. Windows Active Directory nüfuzetmə testləri zamanı Active Directory Kill Chain mərhələlərinin nəzərdən keçirilməsi.
14. Aşkar edilmiş hücum vektorlarını və zəifliklər prioritetləşdirən, onların aradan qaldırılması üçün tövsiyələr təqdim edən peşəkar Nüfuzetmə Testi Hesabatının hazırlanması.
15. QEYD:Sillabusdan kənar digər zəifliklər.