



Practical Penetration Testing

Siber Güvenlik Kariyerinizin Başlangıç Noktası.

Practical Penetration Testing Eğitimi Hakkında	11
1. Eğitim Hakkında	11
1.1. Eğitimin Hedefi / Amacı	11
1.2. Eğitim Materyalleri	12
1.3. Lab Erişimi	12
1.4. Öğrenci Formu	12
1.5. Canlı Destek	13
1.6. Sertifika Sınavı Hakkında	13
2. Eğitim Stratejisi ve Eğitim Açıklamaları	14
2.1. Eğitim Hakkında E-Postalar	14
2.2. Eğitim Materyalleri	14
2.3. Eğitim Egzersizleri	14
2.4. LAB	15
3. Destek Hakkında	16
4. Sızma Testleri Hakkında	16
5. Yasal Çerçeve	17
6. LAB Hakkında Detaylı Bilgiler	18
6.1. LAB Uyarıları	18
6.2. Kontrol Paneli	18
Bilgi Güvenliği Temelleri	21
1. Bilgi Güvenliği Temelleri	21
2. Bilgi Güvenliği Alanındaki Karakterler	24
3. Siber Güvenlik Kısaltmaları	25
4. Siber Güvenlik Terimleri (Sözlük)	28
Kriptografi Temelleri	32
1. Kriptografi	32
2. Simetrik Şifreleme	35
3. Asimetrik Şifreleme	36
4. Asimetrik ve Simetrik Şifreleme Farkları	37
4.1. Simetrik Şifreleme Anahtarı	37
4.2. Asimetrik Şifreleme Anahtarı	37
5. Hashing	38
6. Encoding	39
Temel Ağ (Network) Bilgisi	41
1. Wireshark	41
2. Network Temelleri	57

3.	TCP/IP Mimarisi	59
4.	OSI Modeli	61
5.	Önemli Ağ Protokolleri	66
5.1.	HTTP (Hyper-Text Transfer Protocol)	66
5.2.	FTP (File Transfer Protokol).....	67
5.3.	SMTP (Simple Mail Transfer Protokol).....	71
5.4.	DNS (Domain Name Server)	78
5.5.	Telnet (Telecommunication Network).....	80
5.6.	SSH (Secure Shell).....	81
5.7.	NFS (Network File System).....	84
5.8.	SMB (Server Message Block).....	85
5.9.	DHCP (Dynamic Host Configuration Protocol)	86
5.10.	TCP (Transmission Control Protocol/Internet Protocol)	90
5.11.	UDP (User Datagram Protocol)	100
5.12.	IP (Internet Protocol).....	101
5.13.	NAT (Network Address Translation).....	110
5.14.	ICMP (Internet Control Message Protocol)	111
5.15.	ARP (Address Resolution Protocol)	114
6.	Önemli Ağ Cihazları	117
Sanal Makineler.....		120
1.	VirtualBox ve Önemli Ayarlar	121
2.	VMware ve Önemli Ayarlar.....	139
Temel Linux		153
1.	Linux'a Giriş	153
2.	Temel Linux Komutları.....	153
3.	Linux Kullanıcı ve Grup Yönetimi	178
4.	Linux Sistemlerde Önemli Dosya ve Dizinler	183
5.	Linux Sistemlerde Dosya/Dizin Yetkilendirmeleri.....	191
6.	Metin Editörleri	198
7.	Linux Sistemlerde Process Yönetimi	203
8.	Linux Sistemlerde Paket Yönetimi	207
9.	Servis Yönetimi.....	217
10.	Linux Sistemlerde Ağ İşlemleri	221
Temel Windows		228
11.	Windows Sistemlere Giriş.....	228
12.	Temel Windows Komutları.....	229
13.	Windows Sistemlerde Kullanıcı İşlemleri.....	232

14.	Önemli Klasör ve Dosyalar	235
15.	Dosya ve Klasör Arama İşlemleri	238
16.	Process İşlemleri	240
17.	Network (Ağ) İşlemleri	243
18.	Windows Sistemlerde Dosya İndirme İşlemleri.....	249
19.	Windows Sistemlerde Zamanlanmış Görevler.....	255
20.	Windows Sistemlerde Servis Yönetimi.....	266
Netcat ve Türevleri.....		272
1.	Netcat	272
2.	Ncat	277
3.	Powercat.....	280
Tünelleme.....		284
1.	SSH Tünelleme	284
Programlama		286
1.	Python.....	286
1.1.	Python Temelleri	288
1.2.	Sızma Testi Süreçleri İçin Örnek Uygulamalar	305
2.	Komut Satırı Betikleri Oluşturma	309
2.1.	Bash Ortamı.....	309
2.1.1.	Çevresel Değişkenler.....	309
2.2.	Çıktıları Yönlendirme (Piping)	311
2.2.1.	Piping	311
2.2.2.	Yeni Bir Dosyaya Yönlendirme	311
2.2.3.	Bir Dosyadan İçeriği Yönlendirme	312
2.3.	Metin Arama İşlemleri ve Manipülasyon.....	313
2.3.1.	Grep.....	313
2.3.2.	Awk	314
2.3.3.	Sort	315
2.3.4.	Find.....	316
2.4.	Komut ve Dosya İzleme	317
2.4.1.	Watch	317
2.4.2.	Tail	318
2.5.	Terminal Özelleştirme ve Özel Terminaller.....	319
2.5.1.	Tmux	319
2.5.2.	Alias	322
3.	Bash Script Geliştirme	323
3.1.	Bash Script Temelleri.....	325

3.2.	Kullanıcıdan Girdi Alma	328
3.3.	if, else, elif	329
3.4.	Lojik (Mantıksal) Operatörler	330
3.5.	Döngüler	331
3.6.	Fonksiyonlar	332
Pratik Sızma Testleri		334
1.	Sızma Testine Başlamadan Önce Müşteri ile İlişkiler	334
2.	Pasif Bilgi Toplama Teknikleri	335
3.	Yerel Ağ Sızma Testleri	351
3.1.	Temel Yaklaşım	351
3.2.	Pratik Pentest Araçları	354
3.2.1.	Metasploit	354
3.2.2.	SoftPerfect Network Scanner	365
3.2.3.	Nmap	371
3.2.4.	Zenmap	373
3.2.5.	Medusa	379
3.2.6.	Hydra	382
3.2.7.	Crowbar	383
3.2.8.	Nessus	385
3.2.9.	JohnTheRipper	391
3.3.	Pasif Bilgi Toplama	393
3.3.1.	Browser Protokol Analizi	393
3.4.	Aktif Bilgi Toplama	394
3.4.1.	Port Tarama Teknikleri	394
3.5.	Protokol Analizleri	395
3.5.1.	SMB Protokol Analizi	395
3.5.2.	VNC Protokol Analizi	405
3.5.3.	FTP Protokol Analizi	413
3.5.4.	SMTP Protokol Analizi	420
3.5.5.	HTTP Protokol Analizi	425
3.5.6.	SSH Protokol Analizi	432
3.5.7.	NFS Protokol Analizi	434
3.6.	Zafiyet Taraması ve Analizi	439
3.6.1.	Nmap ile Zafiyet Tarama	439
3.6.2.	Metasploit ile Zafiyet Tarama	441
3.6.3.	Nikto ile Zafiyet Tarama	446
3.6.4.	Nessus ile Zafiyet Tarama	450

4.	Kablosuz Ağ Sızma Testleri.....	459
4.1.	Terimler.....	460
4.2.	Metodoloji.....	463
4.3.	Pratik WiFi Pentest Araçları.....	468
4.4.	Temel İletişim.....	477
4.5.	Önemli Kablosuz Ağ Paketleri.....	478
4.6.	Yapılandırma.....	482
4.7.	Bilgi Toplama.....	490
4.7.1.	Linux Sistemlerde Bilgi Toplama.....	490
4.7.2.	Windows Sistemlerde Bilgi Toplama.....	500
4.8.	Yetkilendirme Saldırıları.....	502
4.8.1.	WPA-PSK Destekli Kablosuz Ağların Ele Geçirilmesi.....	502
4.8.2.	WPA2 (802.1x) Destekli Kablosuz Ağların Ele Geçirilmesi.....	510
4.9.	Güvenlik Tavsiyeleri.....	521
5.	Web Uygulama Sızma Testi.....	522
5.1.	Web Uygulama Teknolojileri.....	522
5.1.1.	URL Sözdizimi.....	522
5.1.2.	HTTP Protokolü.....	524
5.1.3.	HTTP Request ve HTTP Response Yapısı.....	525
5.1.4.	HTTP Metodları.....	527
5.1.5.	HTTP Başlık Bilgileri.....	528
5.1.6.	Cookies.....	534
5.1.7.	HTTP Yetkilendirmeleri.....	535
5.1.8.	HTTP Durum Kodları.....	535
5.2.	Pratik Pentest Araçları.....	537
5.2.1.	Burp Suite.....	537
5.2.2.	ZAPProxy.....	560
5.2.3.	Wfuzz.....	575
5.2.4.	Dirb.....	577
5.2.5.	Sqlmap.....	579
5.2.6.	WPScan.....	581
5.2.7.	Nikto.....	582
5.2.8.	Firefox Eklentileri.....	584
5.3.	Bir Web Uygulamasının Analiz Edilme Süreci.....	590
5.3.1.	İçerik ve Fonksiyonların Haritalandırılması.....	590
5.3.2.	Uygulamanın Analiz Edilmesi.....	591
5.3.3.	Uygulamanın Kullandığı Teknolojilerin Analiz Edilmesi.....	592

5.4.	XSS Zafiyetinin Sömürülmesi	596
5.4.1.	Javascript Hakkında Temel Bilgiler	596
5.4.2.	XSS Zafiyeti Nedir?	598
5.4.3.	XSS Zafiyeti Nasıl Aranmalıdır?	602
5.4.4.	XSS Zafiyetinin Sömürülmesi	603
5.5.	SQL Injection Zafiyetinin Sömürülmesi	609
5.5.1.	SQL Injection Zafiyeti Nedir?	609
5.5.2.	SQL Injection Zafiyeti Neyden Kaynaklanmaktadır?	620
5.5.3.	SQL Injection Zafiyeti Nasıl Aranmalıdır?	622
5.5.4.	SQL Injection Zafiyetinin Sömürülmesi	623
5.6.	IDOR Zafiyetinin Sömürülmesi	632
5.6.1.	IDOR Nedir?	632
5.6.2.	IDOR Zafiyeti Neyden Kaynaklanmaktadır?	632
5.6.3.	IDOR Zafiyeti Nasıl Aranmalıdır?	633
5.6.4.	IDOR Zafiyetinin Sömürülmesi?	635
5.7.	LFI Zafiyetinin Sömürülmesi	638
5.7.1.	LFI Nedir?	638
5.7.2.	LFI Zafiyeti Neyden Kaynaklanmaktadır?	639
5.7.3.	LFI Zafiyeti Nasıl Aranmalıdır?	639
5.7.4.	LFI Zafiyetinin Sömürülmesi	640
5.8.	Dosya Yükleme Zafiyetinin Sömürülmesi	646
5.8.1.	Dosya Yükleme Zafiyeti Nedir?	646
5.8.2.	Dosya Yükleme Zafiyeti Neyden Kaynaklanmaktadır?	646
5.8.3.	Dosya Yükleme Zafiyeti Nasıl Aranmalıdır?	649
5.8.4.	Dosya Yükleme Zafiyetinin Sömürülmesi	650
5.9.	Apache Tomcat Manager	656
5.9.1.	Uygulamanın Tespit Edilmesi	656
5.9.2.	Uygulamaya Erişim Sağlanması	658
5.9.3.	Uygulama Fonksiyonlarının Analizi	660
5.9.4.	Uygulamanın Sömürülmesi	661
5.10.	Wordpress Uygulama Analizi	664
5.10.1.	Uygulamanın Tespit Edilmesi	664
5.10.2.	Uygulamanın Sömürü Noktalarının Analizi	666
5.10.3.	Uygulamanın Sömürülmesi	670
6.	Mobil Uygulama Sızma Testleri	677
6.1.	Android Uygulama Bileşenleri	677
6.2.	Bir APK Dosyasının Anatomisi	678

6.3.	Pratik Pentest Araçları.....	680
6.4.	Lab Kurulumu	697
6.5.	Genel Yaklaşım (Attack Surface Mapping).....	710
6.6.	Jailbreak İşlemi - IOS Cihazlar	712
6.7.	Statik Analiz.....	720
6.7.1.	Android Uygulamaların Statik Analizi	720
6.7.2.	IOS Uygulamaların Statik Analizi	738
6.8.	Dinamik Analiz	739
6.8.1.	Android Uygulamaların Dinamik Analizi.....	739
6.8.2.	IOS Uygulamaların Dinamik Analizi.....	751
7.	Sosyal Mühendislik Testleri.....	768
7.1.	Sosyal Mühendislik Nedir?	768
7.2.	Sosyal Mühendislik Testlerinin Amacı	768
7.3.	Pratik Sosyal Mühendislik Araçları	769
7.4.	Oltama Saldırısı.....	772
7.5.	Makro Geliştirme Teknikleri.....	802
7.6.	Zararlı HTA Dosyası Geliştirmek	813
7.7.	Sosyal Mühendislik Senaryoları.....	818
	Active Directory Sızma Testleri.....	821
1.	Active Directory Hakkında	821
2.	Pratik Sızma Testi Araçları	827
3.	Bilgi Toplama Yöntemleri	843
1.1.	Temel Komutlar İle Bilgi Toplama	843
1.2.	PowerView ile Bilgi Toplama.....	848
1.3.	PowerUpSql ile Bilgi Toplama	853
1.4.	mmc.exe ile Bilgi Toplama	857
4.	Active Directory Aktif Saldırı Yöntemleri.....	862
	Windows Sistemlerde Yetki Yükseltme Saldırıları	881
1.	İşletim Sistemi Hakkında Bilgi Toplama	881
2.	Uygulamalar Hakkında Bilgi Toplama	882
3.	Ağ Bağlantıları Hakkında Bilgi Toplama	885
4.	Hassas Verilerin Araştırılması	889
5.	Kayıtlı Kablosuz Ağ Parola Bilgileri	891
6.	Sistemdeki Kullanıcıların Parola Bilgilerinin Dump Edilmesi	893
7.	Zafiyetli Servis Yapılandırmalarının Tespit Edilmesi	895
8.	AllwaysInstallElevated.....	902
	Linux Sistemlerde Yetki Yükseltme Saldırıları	904

1. İşletim Sistemi Hakkında Bilgi Toplama	905
2. Uygulama ve Servisler Hakkında Bilgi Toplama	906
3. Hassas bilgilerin tespit edilmesi	907
4. Ağ Bağlantıları Hakkında Bilgi Toplama	909
5. Kullanıcılar ve Aktiviteleri Hakkında Bilgi Toplama.....	910
6. Pratik Uygulamalar	911
Sızma Testi Sonuç Raporu	915
1. Müşteri ile İlişkiler	915
2. Raporlama	915
3. Rapor Taslağı	916
4. Üst ve Alt Bilgi Tasarımı	917
5. Kapak Tasarımı	917
6. Doküman Künyesi.....	918
7. Kuruma Hitap.....	919
8. İçindekiler Tablosu.....	920
9. Tablo Listesi.....	922
10. Şekiller Listesi.....	923
11. Yasal Sorumluluklar.....	925
12. Yönetici Özeti	926
13. Bulgu Kartı Hazırlanması.....	927
14. Raporda Bulunması Gerekenler	931
15. Rapor İletim Standardı	933
16. Dört Göz Kuralının İşletilmesi	934