

OFANSİF VE DEFANSİF SİBER GÜVENLİK

İLKER ERTUĞRUL

İÇİNDEKİLER

BÖLÜM 1: SİBER GÜVENLİĞE GİRİŞ	1
Siber Güvenlik Nedir?	2
Hacker Nedir?	2
Siyah Şapkalı Hackerlar	2
Beyaz Şapkalı Hackerlar	3
Gri Şapkalı Hackerlar	3
Sızma Testi Nedir?	4
BlacBox (Kara Kutu) Sızma Testi	4
WhiteBox (Beyaz Kutu) Sızma Testi	4
GreyBox (Gri Kutu) Sızma Testi	4
Neler Öğrendik?	4
BÖLÜM 2: GELİŞMİŞ HACKİNG TEST ORTAMINI KURMAK	7
VirtualBox Kurulumu	8
Kali Linux Kurulumu	9
Windows 10 Kurulumu	17
Metasploitable Kurulumu	20
Neler Öğrendik?	22
BÖLÜM 3: TEMEL AĞ BİLGİSİ	23
Network (Ağ) Nedir?	24
LAN (Local Area Network) Nedir?	24
WAN (Wide Area Network) Nedir?	24
MAN (Metropolitan Area Network)	25
Büyükklüklerine Göre Ağlar	25
Ağların Çalışma Prensipleri	25
Broadcast (Yayın)	25
Point To Point (Noktadan Noktaya)	25

IP Adresi Nedir?	25
OSI Modeli ve Katmanları	26
Fiziksel Katman (Physical Layer)	26
Veri Bağlantısı Katmanı (Data Layer)	26
Ağ Katmanı (Network Layer)	27
Ulaşım Katmanı (Transportation Layer)	27
Oturum Katmanı (Session Layer)	27
Sunum Katmanı (Presentation Layer)	27
Uygulama Katmanı (Application Layer)	27
Network Protokolleri	27
TC/P Protokolü	28
DNS Protokolü	28
IVMP Protokolü	28
SMTP Protokolü	28
SNMP Protokolü	28
FTP Protokolü	28
Neler Öğrendik?	28
BÖLÜM 4: TEMEL LINUX BİLGİSİ	31
Linux Nedir?	32
Dosya Sistemi Yapısı	32
Linux Komut Satırına Giriş	33
Root Hakları ve Linux'ta Kullanıcı Hesapları	34
Root (Kök) Kullanıcısı Nedir?	34
Root (Kök) Hakları Nasıl Alınır?	35
Root (Kök) Haklarını Kalıcı Olarak Almak	36
Dosya ve Dizin İşlemleri	37
cd Komutu	37

pwd Komutu	38
ls Komutu	38
touch Komutu	39
rm Komutu	39
cat Komutu	40
rmdir Komutu	40
mkdir Komutu	40
cp Komutu	41
mv Komutu	41
Dosya ve Dizinlerin Erişim İzinlerini Değiştirmek	42
Dosya ve Dizinlerin Erişim İzinleri	42
Program Kurmak-Kaldırmak ve Güncelleme İşlemleri	43
Apt-Get ile Program Kurmak ve Kaldırmak	43
Sistemimizi Güncellemek	45
Nano Editörü ve Leafpad	45
Network Komutları	47
ifconfig Komutu	47
route Komutu	48
İnternet Hizmetini Yeniden Başlatma	48
Neler Öğrendik?	48
BÖLÜM 5: KABLOSUZ AĞLAR VE TEMEL BİLGİLER	51
Kablosuz Ağlar Nedir?	52
kablosuz Ağların Çalışma Şekilleri	52
SSID (Ağ Adı)	52
Kablosuz Ağlarda Şifreleme Modelleri	52
WEP Şifreleme Modeli	53
WPA Şifreleme Modeli	53

WPA2 Şifreleme Modeli	53
WPA3 Şifreleme Modeli	53
Monitor Mod ve Managed Mod	54
Monitor Mod Nedir?	54
WPS Nedir?	54
Managed Mod	55
Handshake Nedir?	55
MAC Adresi Nedir?	55
Neler Öğrendik?	55

BÖLÜM 6: KABLOSUZ AĞ SALDIRILARI İÇİN ORTAMIMIZI HAZIRLAMAK 57

Giriş	58
Kali Linux'u USB'ye Kurmak	59
Kali Linux'u USB'den Çalıştırmak	60
Neler Öğrendik?	63

BÖLÜM 7: KABLOSUZ AĞ SALDIRILARI 65

Kablosuz Ağlara Yönelik Kaba Kuvvet Saldırısı	66
Cihazımızı Saldırlara Hazır Hale Getirme ve Kablosuz Ağlara Yönelik Bilgi Toplama	67
Tek Bir Kablosuz Ağa Yönelik Bilgi Toplama	68
Handshake Yakalamak ve Yetkisizlendirme Saldırısı	69
Kaba Kuvvet Yöntemiyle Kablosuz Ağın Şifresini Kırma	72
WPS Atağı ile Kablosuz Ağ Saldırısı	74
Şeytani İkiz Saldırısı	75
Neler Öğrendik?	83

BÖLÜM 8: KABLOSUZ AĞLARDA GÜVENLİK 85

Modem Arayüzüne Erişmek	86
SSID Değiştirmek	86
WPS Seçeneğini Kapatmak	87

Kablosuz Ağlar için Şifreleme Seçme ve Oluşturma Yolları 87

Kablosuz Ağların Güvenliğini MAC Filtrelemesi ile Arttırma 89

MAC Filtreleme Aşılabilir Mi? 91

Neler Öğrendik? 91

BÖLÜM 9: NETDISCOVER VE NMAP 93

Netdicover-IP ve MAC Adreslerini Tespit Etmek 94

NMAP ile Ağ Keşfi 95

NMAP ile Port Keşfi 96

NMAP Nedir? 96

NMAP ile İşletim Sistemi Keşfi 96

NMAP ile Çalışan Servis Sürümlerinin Belirlenmesi 98

NMAP Raporlama Yapmak 99

Zenmap Kurulumu (Kali Sisteminde Yüklü Olmayanlar İçin) 99

Zenmap 102

Neler Öğrendik? 103

BÖLÜM 10: YEREL AĞ SALDIRILARI 105

man-in-the-middle attack (Ortadaki Adam Saldırısı) 106

ARP Spoofing-ARP Zehirleme Saldırısı 112

DNS Spoofing-DNS Zehirleme Saldırısı 114

Drifnet ile Ağdaki Cihazların Ekran Görüntülerini Ele Geçirmek 122

Bettercap ile Yerel Ağ Saldırıları 125

SSL (Secure Sockets Layer) Sertifikası Nedir? 125

Neden Bettercap? 126

Bettercap ile ARP Spoof Saldırısı 126

Neler Öğrendik? 130

BÖLÜM 11: YEREL AĞ SALDIRILARINDAN KORUNMA YÖNTEMLERİ 133

Ortakdaki Adam Saldırısı Korunma ve Tespiti	134
DNS Spoofing Saldırılarından Korunmak	136
Her SSL Sertifikası Olan Site Güvenli Midir?	137
Tek Güveneceğiniz Adres URL Satırı	137
Neler Öğrendik?	137

BÖLÜM 12: AKTİF VE PASİF BİLGİ TOPLAMAK 139

Aktif ve Pasif Bilgi Toplama Nedir?	140
Whois Kayıtları	140
archive.org	141
Netcraft	142
IP Adresi Sorgulama	143
WhatWeb	144
DNSenum Subdomain Tespiti	144
DNSmap	145
Dmitry	145
Hedef Kişi Hakkında Bilgi Toplama	147
PeekYou	147
TheHarvester ile Aktif ve Pasif Bilgi Toplamak	149
Neler Öğrendik?	151

BÖLÜM 13: NESSUS İLE ZAFİYET TARAMALARI 153

Nessus Kurulumu	154
Nessus Panelini Tanımak ve Tarama Çeşitleri	158
Nessus ile Hedef Sistemde Zafiyet Taraması Gerçekleştirmek	159
Neler Öğrendik?	161

BÖLÜM 14: METASPLOİT İLE GÜVENLİK ZAFİYETLERİNİ SÖMÜRMEK 163

Temel Kavramlar	164
Exploit Nedir?	164
Metasploit Modülleri	165
Metasploit ile Güvenlik Zafiyetini Sömürmek-1	165
Metasploit ile Güvenlik Zafiyetini Sömürmek-2	167
Metasploit ile Güvenlik Zafiyetini Sömürmek-3	171
Neler Öğrendik?	172

BÖLÜM 15: ARMITAGE İLE SIZMA TESTLERİ 175

Armitage Nedir?	176
Armitage Kurulumu	176
Armitage ile Güvenlik Zafiyetlerini Sömürmek	178
Neler Öğrendik?	181

BÖLÜM 16: BACKDOOR (ARKA KAPI) OLUŞTURMAK 183

Backdoor Nedir?	184
Veil Framework Nedir?	185
Veil Framework Kurulumu	185
Backdoor Oluşturmadan Önce Bilinmesi Gerekenler	189
Yerel Ağ ve Dış Ağ	189
IP Sabitleme ve Modemden Port Açma İşlemini Neden Gerçekleştiriyoruz?	190
IP Sabitleme ve Modemden Port Açma İşlemi	190
Veil-Framework ile Backdoor Oluşturma	195
Backdoor Anti Virüs Testi	197
Backdoor'u Dinlemeye Almak ve Test Etmek	199
Uygulamalar Arasına Zararlı Yazılım Gizlemek	201
Neler Öğrendik?	205

BÖLÜM 17: BACKDOOR SONRASI İŞLEMLER	207
Meterpreter Nedir?	208
Ekran Görüntüsü Almak	208
Sistem Özelliklerini Öğrenmek	209
Dosya İşlemleri	209
Kameradan Görüntü Ve Kayıt Almak	210
Browserdan Veri Çekmek	212
Ses Kaydı Almak	212
Keylogger	213
İzleri Silmek	214
Backdoor'un Kalıcılığını Sağlama	214
Hedefle İlişkiyi Keskem	215
Neler Öğrendik?	215
BÖLÜM 18: ZARARLI YAZILIMLAR VE BİLGİSAYAR GÜVENLİĞİ	217
Zararlı Yazılımlar Nedir?	218
Bilgisayar Virüsleri	218
Malware	219
Solucan	219
Casus Yazılımlar (Spyware)	219
Truva Atı (Trojen)	220
Adware (Reklam Yazılımı)	220
Keylogger	221
Zararlı Yazılım Nasıl Yazılır?	221
Bilgisayar Güvenliği	221
Güncel İşletim Sistemi Şart!	221
Güncellemeler Mutlaka Yapılmalı!	222
Anti Virüs Programı Kullanımı	222

Güvenlik Duvarı	222
Güvenilir Kaynaklardan İndirme Yapın!	222
Önemli Dosyalarını Şifreleyin ve Yedekleyin	223
Neler Öğrendik?	223
BÖLÜM 19: ANDROID CİHAZLARA YÖNELİK SALDIRILAR	225
Android Cihazlar için Backdoor Oluşturmak	226
Backdoor'u Dinlemeye Almak ve Test Etmek	227
Backdoor Sonrası İşlemler	228
SMS Kayıtlarını Almak	229
Android Cihazın Kamerasından Yayın ve Görüntü Almak	229
Cihazın Arama Kayıtlarına Ulaşmak	231
Ses Kaydı Almak	231
Backdoor'u Hedef Cihazda Gizleme	232
Backdoor'u Kalıcı Hale Getirme	232
Daha Fazla İşlem	234
Mobil Cihazların Güvenliği	234
Güncellemelere Önem Verin!	234
Bilinmeyen Kaynaklardan Uygulama İndirirken Dikkat Edin!	235
Uygulamayı Kurarken İzinlere Bakın!	235
Güvenlik Uygulamaları Kullanın	235
Cihazlarınızın Kaybolması ve Çalınması Durumu için Önlem Alın!	235
Önemli Verilerinizi ve Bilgilerinizi Taşıyın	236
Bulut Uygulama Kullanırken Dikkat Edin!	236
Güvenli Şifreleme Modelini Seçin	236
Neler Öğrendik?	236

BÖLÜM 20: SOSYAL MÜHENDİSLİK VE PHISHİNG	239
Sosyal Mühendislik Nedir?	240
Phishing Nedir?	240
Sosyal Mühendislik Teknikleri	241
Bilgi Toplamadan Asla!	241
Saldırı Planını Oluştur!	242
Hedefini Doğru Seç!	242
Saldırı Senaryosunu Belirle	243
Örnek Saldırı Senaryosu	244
Sosyal Mühendislik Saldırılarında Kullanılmak Üzere Geliştirilen Donanımlar	246
Arkadaşlarıma Yaptığım Sosyal Mühendislik Saldırısı	246
Sosyal Mühendislik Saldırıları	248
Metasploit ile Şirket ve Kurumlara Ait E-Posta Hesaplarını Bulma	248
Sosyal Mühendislik Araç Seti (S.E.T)	249
Fake Mail Göndermek Sahte E-Posta	252
Ghost Phisher Aracı ile Sosyal Mühendislik Saldırıları	254
Sosyal Medya Hesaplarına Phishing Saldırısı Gerçekleştirmek	256
Sosyal Mühendislik ve Phishing Saldırılarından Korunmak	260
Yetkili Kişilerle Dahil Şifrenizi Paylaşmayın	260
Her Gelen Mesaja İtibar Etmeyin	260
Spama Düşen Maileri Kayda Almayın	260
Fake Maillere Dikkat!-Sahte Mail Tespiti	260
Hediye Vaatlerine Kanmayın!	260
Farklı Yetkililer İle Görüşün	261
Yakınlarınız dan Gelen Mesajlara Hemen Aldanmayın	261
Neler Öğrendik?	261

BÖLÜM 21: GİZLİLİK VE ANONİMLİK	263
İnternette Anonim Olmak Mümkün mü?	264
Hackerlar Nasıl Yakalanmıyor?	264
Log Tutmayan VPN Servisleri	265
Tor Ağı Güvenli mi?	265
Off Shore Mail Servisleri	266
Linux da VPN Kullanımı IP Adresini Değiştirmek	267
VPN Nedir?	267
VPN Kullanımı IP Adresini Değiştirmek	268
DNS Değiştirmek	271
MAC Adresini Değiştirmek	271
Anonim Mail Hesabı Açmak	272
Gösterilen Teknikler ile Gizlilik Mümkün Mü?	272
Neler Öğrendik?	272
BÖLÜM 22: DEEP WEB/DARK WEB İNTERNETİN KARANLIK YÜZÜ	275
Deep Web Nedir?	276
İnternet Katmanları	277
0. Seviye Common Web	277
1. Seviye Surface Web	277
2. Seviye Bergie Web	277
3. Seviye Deep Web	277
4. Seviye Charter Web	278
5. Seviye Marianas Web	278
6. Seviye	278
7. Seviye The Fog/Virus Soup	278
8. Seviye The Primarch System	278

Deep Web'e Girmek Suç Teşkil Eder mi?	279
Deep Web'e Nasıl Girilir?	279
Peki, Dark Web Nedir?	279
Tor Browser Kurulumu	279
Deep Web Linkleri Bulmak	284
Deep Web'e Girmek	285
Neler Öğrendik?	285

BÖLÜM 23: BİLİŞİM SUÇLARI **287**

5651 Sayılı Kanun	288
Bilişim Suçları	288
Bilişim Suçları Nelerdir?	288
Neler Öğrendik?	289

BÖLÜM 24: DoS/DDoS ATTACK VE BOTNET **291**

DoS/DDoS Attack Nedir?	292
SYN Flood	293
UDP Flood	293
Ping Flood	294
Botnet Nedir?	294
DoS/DDoS Saldırısı Gerçekleştirmek	294
Metasploit ile DoS Attack Saldırısı Gerçekleştirmek	295
DoS/DDoS Saldırılarından Korunmak	296
Neler Öğrendik?	297

BÖLÜM 25: KRİPTOLOJİ **299**

Kriptoloji Nedir?	300
Sezar Şifreleme Algoritması	300
Hash Algoritmaları	301

Simetrik ve Asimetrik Şifreleme	302
Steganografi	302
Neler Öğrendik?	303

BÖLÜM 26: PAROLA SALDIRILARI **305**

Parola Nedir?	306
Brute-Force Nedir?	306
Wordlist Oluşturmak	306
Wordlist Nedir?	306
Crunch Aracı ile Wordlist Oluşturmak	306
Hydra ile Parola Saldırıları	307
Medusa ile Parola Saldırıları	308
Hydra ile Parola Kıрма Saldırısı	308
rar ve zip Dosyalarının Parolasını Kırmak	309
Instagram Hesaplarına Yönelik Brute Force Saldırısı	312
Hash Algoritmaları ile Şifreleme Yapmak	313
Hash Algoritmalarının Türünü Öğrenme-Şifreleme Türünü Tespit Etme	314
Hash Algoritmaları Kullanılarak Şifrelenen Şifreleri Kırmak	315
Güvenli Parola Oluşturmanın Yolları	316
İki Adımlı Doğrulamayı Aktif Edin!	316
Parolanızı txt Dosyası Olarak Saklamayın!	317
Tüm Hesaplarınız'da Aynı Parolayı Kullanmayın!	317
Parolanızı Sitelerden Oluşturmayın	317
Neler Öğrendik?	317

BÖLÜM 27: BEEF XSS FRAMEWORK **319**

BeEF XSS Framework Nedir?	320
Beef Kurulumu	320
Hedefi Hook'lamak	324

BeEF ile Hedef Hakkında Bilgi Toplamak	329
BeEF XSS Framework ile Google Phishing Saldırısı	329
BeEF ile Sosyal Medya Hesaplarına Saldırısı Yapmak	331
Ekran Görüntülerini Ele Geçirmek	332
BeEF XSS Saldırılarından Korunmak	333
Neler Öğrendik?	333

BÖLÜM 28: WEB UYGULAMA GÜVENLİĞİ **335**

Web Güvenliği için Gerekli Pentest Ortamını Hazırlamak	336
Web Sitelere Yönelik Brute Force Saldırısı Gerçekleştirmek	337
Komut Yürütme Saldırısı	344
Siteler Arası İstek Sahteciliği Açığı (CSRF)	347
Dosya Çağırma Açığı	351
Dosya Yükleme Açığı	353
SQL Injection-Veritabanı Açığı	356
SQL Injection Açığını Manuel Yolla Sömürmek	357
SQLmap ile SQL Injection Saldırıları	361
XSS (Cross Site Scripting) Açığı	365
Reflected XSS Açığı	365
Stored XSS Açığı	366
Beef XSS Framework İle XSS Saldırıları	367
Neler Öğrendik?	369

BÖLÜM 29: ÖNEMLİ TAVSİYELER VE MERAK EDİLEN SORULAR	371
Siber Güvenlik Dünyasında Sertifikaların Yeri	372
Hangi Programlama Dilini Öğrenmeliyim?	373
İngilizcenin Önemi	374
Linux'un Önemi	375
Capture The Flag (CTF)	375
İnternette Güvenilir Alışveriş Yapmanın Yolları	376
Banka Hesabınızın Güvenliğini Sağlama	377
Kitabı Bitirdim Şimdi Ne Yapmalıyım?	377
Son Söz	378

1

SİBER GÜVENLİĞE GİRİŞ

BU BÖLÜMDE

Siber Güvenlik Nedir? 2

Hacker Nedir? 2

Sızma Testi Nedir? 4

Neler Öğrendik? 4

Kitabımızın eğitim bölümlerine geçmeden önce bazı kavramları bilmeniz yararınıza olacağını düşünüyorum. Bu kavramları bilenler bu bölümü atlayabilirler.

Bu bölümde, sızma testi nedir? Hacker çeşitleri vb. kavramların açıklaması yapılacaktır.

Kavramlar için doğru bildiğiniz yanlışlar olabilir bu yüzden bu bölümü atlamadan birkaç dakikanızı ayırarak okumanızı tavsiye ederim.

SİBER GÜVENLİK NEDİR?

Siber güvenlik, günümüz bilişim çağında elektronik cihazların, dijital ortamdaki verilerin siber saldırılara karşı korunması ve gerekli güvenlik önlemlerinin alınmasıdır. Kısa bir tanım yaparsak bu yorum yeterlidir. Siber güvenlik kavramı ayrıca çok geniş bir kavramdır.



HACKER NEDİR?

Hacker nedir? sorusunun cevabını vermeden önce **HACK** kavramını açıklamak daha doğru olacaktır. Hack kavramı, bir sistemin açıklarını yani zaaflarını bulmak, belirli kişilerin dosya ve sistemlerine izinsiz giriş yapmaktır. Hacker kavramı ise belirli teknik ve yöntemleri bilerek hack yapan kişidir. Hackerlar kendi prensiplerine göre çeşitli kategorilere ayrılırlar.

SİYAH ŞAPKALI HACKERLAR

Hackerların kendi prensiplerine göre çeşitli kategorilere ayrıldığını bir önceki paragrafımızda yazmıştım. Hackerlar kendi prensiplerine göre 3 kategoriye ayrılırlar. Bu kısımda siyah şapkalı hacker kavramı nedir onu açıklayacağım.

Siyah şapkalı hackerlar, kötü niyetli kişilerdir. Bildikleri yöntem ve teknikleri acımasızca kullanırlar. Genelde çıkarları doğrultusunda hareket ederler. Sistemlere ve kişilere izinsiz ve acımasızca saldırıp genelde ele geçirdikleri veriler için para talep ederler. Günümüzde sanal para teknoloji bitcoin çıktığından beri siyah şapkalı hackerların hareket alanı da artmıştır. Sanal para teknolojisinin devletler ve güvenlik ekipleri tarafından izlenememesi nedeniyle siyah şapkalı hackerlar genelde şifreledikleri veriler için bitcoin talep etmektedir. Sanal paranın iyi yanları olduğu gibi olumsuz yanı da para merkezli siyah şapkalı hackerların siber saldırılarını arttırmış olmasıdır.

Örnek bir saldırıdan bahsederek siyah şapkalı hackerların ne kadar tehlikeli olduklarını anlamanızı istiyorum.

Bir şirketin patronu bir gün çalışanlarının evde internet ortamından da işlerini yapabilmeleri fikrini düşünür ve hayata geçirir. Bu doğrultuda çalışanlara yazılım verilir. Şirkette çalışanlardan biri kendi şifresini basit bir şekilde koyar. Her ne olduysa bu basit şifreden sonra olur. Kötü niyetli bilgisayar korsanları yani siyah şapkalı hackerlar yazılımda yer alan verileri şifrelerler. Sonrasında ise bitcoin talep ederler ve bu bitcoinin ödenmesiyle yazılımdaki şifrelenmiş verileri sunarlar. Aynen okuduğunuz gibi basit bir şifre koymanın bile nelere mal olacağını kestiremezsiniz.

Her gün bu ve bu tarz siber saldırıları duyuyoruz bu yüzden gerekli güvenlik önlemlerini almalı sistemimizdeki güvenlik açıklarını minimuma indirmeliyiz. Siyah şapkalı hackerlar gerçekten tehlikelidirler.

BEYAZ ŞAPKALI HACKERLAR

Beyaz şapkalı hackerlar, siyah şapkalı hackerların tam tersidir. Beyaz şapkalı hackerlar genelde bu sektörde çalışan kişilerdir. Şirketleri, kurumları, devletleri siber saldırılara karşı korurlar. Tabii her beyaz şapkalı hacker bu sektörde çalışan değildir bu işi hobi olarak yapan beyaz şapkalı hackerlar da vardır.

Beyaz şapkalı hackerlar, siyah şapkalı hackerların sahip olduğu teknik ve yöntemleri bilen sistemleri ve kişileri siber saldırılara, kötü niyetli bilgisayar korsanlarına karşı koruyan kişilerdir. İzinsiz bir şekilde sistemlere ve kişilere kesinlikle saldırmazlar. Bilgi bakımından beyaz şapkalı hackerlar ve siyah şapkalı hackerlar arasında bir fark yoktur. Sadece amaç doğrultusunda ayrılırlar.

GRI ŞAPKALI HACKERLAR

Gri şapkalı hackerlar için siyah ve beyaz şapkalı hacker karışımı hackerlar diyebiliriz. Bir sisteme izinsiz giriş yaparlar fakat zarar vermek yerine bunu sistem yöneticisine iletirler. Fakat günümüz bilişim yasalarında bir sisteme zarar vermeyecek olsanız da öncesinden gerekli izinleri almadan sisteme giriş yapmak suç teşkil etmektedir. Bu nedenden ötürü çoğu kişi gri şapkalı hacker kavramını kabul etmez. Bir sisteme izinsiz erişildiğinde hacker zarar vermeyecek olsa da bilişim yasalarına göre suç işlediğinden gri şapkalı hackerları, siyah şapkalı hackerlar olarak nitelendiren kişilerde vardır.

3

TEMEL AĖ BİLGİSİ

BU BÖLÜMDE

Netwok (AĖ) Nedir?	24
Büyükliklerine Göre AĖlar	25
AĖların Çalışma Prensipleri	25
IP Adresi Nedir?	25
OSI Modeli ve Katmanları	26
Network Protokolleri	27
Neler Öğrendik?	28

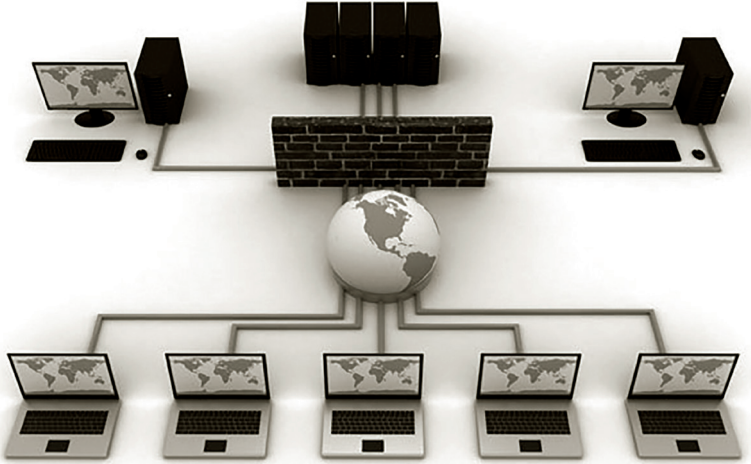
Network alanında bilgi sahibi olmak çok önemli. Gerek sızma testlerinde gerekse siber saldırılarda kullanılan yöntemlerde network bilginize ihtiyaç duyacaksınız.

Bu bölümde, temel seviyede aĖ kavramlarını açıklayacağım. Kitap bir aĖ kitabı olmadığı için aĖ ile alakalı tüm kavramları açıklamam mümkün değil maalesef.

Kitabı bitirdikten sonra network bilginizi ileriye taşımanızı tavsiye ederim.

NETWOK (AĞ) NEDİR?

En az iki bilgisayarın birbirleriyle iletişim halinde olmasıdır. Bu iki bilgisayar birbirlerinden farklı uzaklıklarda olabilirler. Eğer bu iki bilgisayar aynı ortamdaysa yani aynı Ağ üzerindeyse LAN (Local Area Network) olarak adlandırılır. LAN dışında birçok Network daha vardır. Ancak ben kitapta LAN ağı dahil iki ağ çeşidine yer vereceğim. Bunlar Wide Area Network ve Metropolitan Area Network'dur.



LAN (LOCAL AREA NETWORK) NEDİR?

LAN ağlarına örnek vermek gerekirse internet kafeler gösterilebilir. İnternet kafelerde yer alan bilgisayarlar çoğunlukla aynı ağda bulunurlar. İnternet kafede arkadaşlarınız ile oynadığınız multiplayer oyunları LAN ağı sayesinde oynamaktasınız. İnternet kafelerde bulunan bilgisayarlar aynı ağda yer aldıkları için arkadaşınız ve siz multiplayer oyunlarda iki bilgisayarın birbirleriyle iletişim kurmasıyla oyunu oynamaktasınız. Lan (Local Area Network) kavramını Türkçeye çevirecek olursak **Yerel Alan Ağı** diyebiliriz. Lan ağlarında bilgisayarlar ethernet kartları ve kablolar ile aynı ağa bağlanırlar.

WAN (WIDE AREA NETWORK) NEDİR?

WAN ağları, LAN ağlarından farklı olarak coğrafi uzaklıktaki iki veya ikiden fazla bilgisayarın birbirine bağlanmasıdır. Şehirler arası, kıtalar arası bilgisayarların ve Networklerin birbiri ile bağlanması ve iletişim kurması diyebiliriz. Türkçeye çevirdiğimizde **Geniş Alan Ağı** olarak geçer.

11

YEREL AĞ SALDIRILARINDAN KORUNMA YÖNTEMLERİ

BU BÖLÜMDE

Ortakdaki Adam Saldırısı Korunma ve Tespiti	134
DNS Spoofing Saldırılarından Korunmak	136
Her SSL Sertifikası Olan Site Güvenli Midir?	137
Neler Öğrendik?	137

Bu bölümde yerel ağ saldırılarından korunma yöntemlerini işleyeceğiz.

Yerel ağ saldırılarına karşı gerekli güvenlik önlemlerini almak ve saldırılara karşı dikkatli olmak çok önemlidir.

ORTADAKİ ADAM SALDIRISI KORUNMA VE TESPİTİ

Ortakdaki adam saldırısını zaten işlemiştik. Yerel ağlara yönelik en çok yapılan saldırılardan biri olan ortakdaki adam saldırısına karşı nasıl korunur bunu öğreneceğiz. Aynı zamanda olası bir ortakdaki adam saldırısını nasıl tespit edebiliriz öğrenmiş olacağız. Ortadaki adam ve benzeri yerel ağ saldırılarında korunmanın en iyi yolu bağlı bulunduğunuz ağı korumaktan geçer. Bulduğunuz ağda gerekli önlemleri almalı ve yabancı cihazların ağınıza bağlanmasını engellemelisiniz. Olurda bir yabancı cihaz ağınıza bağlanır ve bu saldırıyı yaparsa dikkatli olmalı ve saldırıyı tespit etmelisiniz.

İlk olarak ortakdaki adam saldırısından korunmak için yapmanız gereken kesinlikle gitmek istediğiniz sitelerin adres satırını incelemeniz gerekmektedir. Facebook, twitter gibi sosyal medya adreslerine giriş yaparken veya internet bankacılığı kullanırken gideceğiniz sitenin adres satırına bakarak https kullandığından emin olun. Http kullanan SSL sertifikası kullanmayan sitelerde bilgileriniz saldırganların eline geçeceği için bu tarz http kullanan sitelere oturum açmayın, giriş yapmayın.

En azından bu şekilde hesap bilgileriniz saldırganların eline geçmemiş olacaktır, fakat http kullanan sitelere giriş yaptığınızda saldırganlar gezindiğiniz siteleri görecektir. Ortadaki adam saldırısını tespit edip gerekli önlemleri alarak gezindiğiniz sitelerin saldırganlar tarafından görülmesini engelleyebilirsiniz.

Ortakdaki adam saldırısını nasıl tespit edebileceğinizi öğrenelim. Sanal makineye kurduğumuz Windows makinemizi açalım.

Ortakdaki adam saldırısının olup olmadığını görebilmek için ARP tablosuna bakmamız gerekiyor. Windows bir cihazda ARP tablosunu görebilmek için komut satırını açmamız gerekiyor. Komut satırını açabilmek için Windows cihazda arama kutusuna komut istemi yazınız. Bu şekilde komut satırını açın.

```
Komut İstemi
Microsoft Windows [Version 10.0.17763.615]
(c) 2018 Microsoft Corporation. Tüm hakları saklıdır.
C:\Users\İlker>
```

Görüldüğü üzere komut istemi açıldı. ARP Tablolarını görebilmek için arp -a komutunu komut satırına girelim.

```
C:\Users\İlker>arp -a
Interface: 192.168.1.110 --- 0x3
Internet Address      Physical Address      Type
192.168.1.1          30-b5-c2-8c-f3-fa    dynamic
192.168.1.255        ff-ff-ff-ff-ff-ff    static
224.0.0.22           01-00-5e-00-00-16    static
224.0.0.251          01-00-5e-00-00-fb    static
224.0.0.252          01-00-5e-00-00-fc    static
239.255.255.250     01-00-5e-7f-ff-fa    static
255.255.255.255     ff-ff-ff-ff-ff-ff    static
C:\Users\İlker>
```

Resimde olduğu gibi ARP tablolarını görebildik. Ortadaki adama saldırısı olup olmadığını görebilmek için ARP tablolarına göz atmamız yeterlidir. Görseli inceleyecek olursak ARP tablosunda ortadaki adam saldırısı olmadığı görülüyor. Şimdiki aşamada ise Kali bilgisayarımızdan şu anki Windows makineye ortadaki adam saldırısını gerçekleştirelim. Bakalım ARP tablolarında ne gibi değişiklikler olacak.

```
Interface: 192.168.1.110 --- 0x3
Internet Address      Physical Address      Type
192.168.1.1          08-00-27-93-cc-e0    dynamic
192.168.1.106        08-00-27-93-cc-e0    dynamic
192.168.1.107        08-00-27-93-cc-e0    dynamic
192.168.1.109        08-00-27-93-cc-e0    dynamic
192.168.1.111        08-00-27-93-cc-e0    dynamic
192.168.1.255        ff-ff-ff-ff-ff-ff    static
224.0.0.22           01-00-5e-00-00-16    static
224.0.0.251          01-00-5e-00-00-fb    static
224.0.0.252          01-00-5e-00-00-fc    static
239.255.255.250     01-00-5e-7f-ff-fa    static
255.255.255.255     ff-ff-ff-ff-ff-ff    static
C:\Users\İlker>
```

Yukarıdaki resimde görüldüğü üzere ortadaki adam saldırısını gerçekleştirdikten sonra ARP tablolarında değişiklikler oldu. ARP tablolarına ilk baktığımızda 192.168.1.1 yani modemın MAC adresi gözükürken saldırıdan sonra modemın MAC adresi 08 ile başlayan MAC adresi ile değiştiğini görüyoruz. Sadece modemın MAC adresi değil birçok IP adresinin de MAC adresinin 08 ile başlayan MAC adresi ile değiştiğini görüyoruz. Şimdiki aşamada ise ortadaki adama saldırısını sonlandıralım ve ARP tablolarına tekrar göz atalım.

```
C:\Users\İlker>arp -a
Interface: 192.168.1.110 --- 0x3
Internet Address      Physical Address      Type
192.168.1.1          30-b5-c2-8c-f3-fa    dynamic
192.168.1.106        5c-1d-d9-14-1a-21    dynamic
192.168.1.107        00-26-18-b5-81-2c    dynamic
192.168.1.109        68-07-15-83-77-1e    dynamic
192.168.1.111        08-00-27-93-cc-e0    dynamic
192.168.1.255        ff-ff-ff-ff-ff-ff    static
224.0.0.22           01-00-5e-00-00-16    static
224.0.0.251          01-00-5e-00-00-fb    static
224.0.0.252          01-00-5e-00-00-fc    static
239.255.255.250     01-00-5e-7f-ff-fa    static
255.255.255.255     ff-ff-ff-ff-ff-ff    static
C:\Users\İlker>
```


13

NESSUS İLE ZAFİYET TARAMALARI

BU BÖLÜMDE

Nessus Kurulumu	154
Nessus Panelini Tanımak ve Tarama Çeşitleri	158
Nessus ile Hedef Sistemde Zafiyet Taraması Gerçekleştirmek	159
Neler Öğrendik?	161

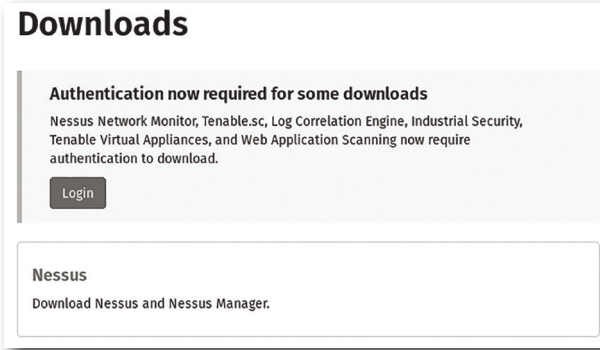
Bu bölümde Nessus ile zafiyet taramaları nasıl yapılır bunu öğreneceğiz.

Bir sistemde yer alan açıkları ve zaafaları bulmak, tespit etmek gereklidir. Nessus kapsamlı bir güvenlik açığı tarama yazılımıdır.

NESSUS KURULUMU

Nessus kurulu olarak gelmemektedir. Nessus'u kullanabilmek için sistemimize kurmamız gereklidir. Nessus'un farklı sürümleri bulunmakta olup, ücretli sürümü daha çok ticari amaçlar için kullanılmaktadır.

Nessus Tenable firması tarafından geliştirilmektedir. Nessus kurulumu için Kali makinemizde arama motorunun URL kısmına <https://www.tenable.com/downloads> adresini yazalım.



Siteye eriştikten sonra görselde görünen Nessus download Nessus and Nessus Manager kısmına tıklayalım.

Name	Description
Nessus-8.5.1-Win32.msi	Windows 7, 8, 10 (32-bit)
Nessus-8.5.1-amzn.x86_64.rpm	Amazon Linux 2015.03, 2015.09, 2017.09
Nessus-8.5.1-debian6_amd64.deb	Debian 6, 7, 8, 9 / Kali Linux 1, 2017.3 AMD64
Nessus-8.5.1-debian6_i386.deb	Debian 6, 7, 8, 9 / Kali Linux 1, 2017.3 i386(32-bit)
Nessus-8.5.1.dmg	macOS (10.8 - 10.14)
Nessus-8.5.1-es6.i386.rpm	Red Hat ES 6 i386(32-bit) / CentOS 6 / Oracle Linux 6 (i386)
Nessus-8.5.1-fc20.x86_64.rpm	Fedora 20, 21, 25, 26, 27 (64-bit)
Nessus-8.5.1-es6.x86_64.rpm	Red Hat ES 6 (64-bit) / CentOS 6 / Oracle Linux 6 (x86_64)
Nessus-8.5.1-suse11.x86_64.rpm	SUSE 11 Enterprise (64-bit)
Nessus-8.5.1-es7.x86_64.rpm	Red Hat ES 7 (64-bit) / CentOS 7 / Oracle Linux 7 (x86_64)

Görüldüğü üzere belirttiğim kutucuğa tıkladıktan sonra indirme sayfası açılacak. İndirme sayfasında sistemimize uygun olan kurulum dosyasını seçmeliyiz. İndirme sayfasında da görüldüğü üzere Linux dışında Windows ve macOS cihazlarda da Nessus kullanabiliyoruz.

İndirme sayfasında indirmemiz gereken dosya eğer Kali sistemini 64 bit olarak kurduysanız **Nessus-8.5.1-debian6_amd64.deb** dosyası olacaktır. Kali sistemini 32 bit olarak kurarsanız **Nessus-8.5.1-debian6_i386.deb** dosyasını indirecektir. Siz bu satırları okuduğunuz vakit Nessus'un yeni bir sürümü çıkmış olabilir. En yeni sürüm zaten indirme sayfasında yer alacaktır.

Kurulum dosyasını sisteminize göre uygun olanını seçerek indirelim. İndirme için Lisans sözleşmelerini kabul ediniz. İndirme tamamlandıktan sonra komut satırından İndirilenler dizinine geliyoruz.

```

root@ilker: ~/Downloads
Dosya Düzenle Görünüm Ara Uçbirim Yardım
root@ilker:~# cd Downloads
root@ilker:~/Downloads# ls
Nessus-8.5.1-debian6_amd64.deb
root@ilker:~/Downloads#

```

Görüldüğü üzere kurulum dosyamız indirilenler dizininde bulunuyor. Kurulumu başlatmak için `dpkg -i Nessus-8.5.1-debian6_amd64.deb` komutunu giriyoruz. `dpkg -i` komutundan sonra kurulum dosyasının adını komut satırından kopyalayıp doğrudan yapıştırabilirsiniz.

Kurulumu başlattıktan sonra kurulumun tamamlanmasını bekleyelim. Bu süre zarfında komut satırını kapatmayın!

```

- You can start Nessus Scanner by typing /etc/init.d/nessusd start
- Then go to https://ilker:8834/ to configure your scanner
Setup Chrome://global/content/bindings/notification.xml?4
Tetikleyiciler işleniyor: systemd (241-7) ...
root@ilker:~/Downloads#

```

Nessus kurulumu başarıyla tamamlandı. Nessus'u başlatmamız gerekli. Nessus'u başlatmak için komut satırına `/etc/init.d/nessusd start` komutunu girerseniz yeterlidir. Bu komutu girdikten sonra komut satırında `Starting Nessus` yazısını görürseniz Nessus başarıyla başlatılmış demektir.

Nessus'u tarayıcımızdan kullanıyoruz. Bir web paneli var. Bu panele ulaşmak için <https://ilker:8834/> URL adresine gitmem yeterli. Zaten yukarıdaki görselde görüldüğü üzere panele ulaşmak için yazmanız gereken URL adresini söylüyor. Sizin gireceğiniz URL adresi Kali'yi kurduğunuz vakit belirlediğiniz isim. Ben kendi adıma vermiştim. Nessus kurulumu tamamlandıktan sonra URL adresini söyleyecektir. URL adresini tarayıcımıza girerek panele ulaşalım.

14

METASPLOIT İLE GÜVENLİK ZAFİYETLERİNİ SÖMÜRMEK

BU BÖLÜMDE

Temel Kavramlar	164
Metasploit ile Güvenlik Zafiyetini Sömürmek-1	165
Metasploit ile Güvenlik Zafiyetini Sömürmek-2	167
Metasploit ile Güvenlik Zafiyetini Sömürmek-3	171
Neler Öğrendik?	172

Metasploit güvenlik zafiyetlerini sömürmek için kullanılan en iyi araçlardan biridir. Sadece güvenlik zafiyetlerini sömürmek için kullanılmaz. Kitabın ilerleyen bölümlerinde Metasploit ile bilgi toplama işlemi bile gerçekleştireceğiz.

Metasploit bir siber saldırı ve analiz aracıdır. Ruby dili ile kodlanmıştır. İçerisinde exploit, auxiliary, payload, nop ve encoder modüllerini bulundurur.

İlk olarak bazı temel kavramları öğreneceğiz. Sonrasında Metasploit içerisinde kullanabileceğimiz önemli komutları tanıyacağız. Son olarak Metasploit ile hedef sistemde yer alan zaafırları sömüreceğiz.

TEMEL KAVRAMLAR

Metasploit framework kullanırken bazı kavramlar ile oldukça haşır neşir olacağız. Bu kavramları bilmemiz anlam karmaşasının önüne geçecektir.

EXPLOİT NEDİR?

Exploit, sistemde yer alan güvenlik zaafalarını sömürmek için geliştirilmiş, bir bilgisayar programı veya scrip'tir. Perl, Ruby, C, Python gibi programlama dilleri ile yazılmaktadırlar. Exploit yazmak oldukça zordur. Exploit'ler iki türlü yayımlanır. Ücretli ve ücretsiz olarak yayımlanırlar.

Metasploit framework içerisinde exploit modülü mevcuttur. Biz uygulamamızı gerçekleştirirken ücretsiz yayımlanan hazır exploitleri kullanacağız. Başlangıç aşaması için hazır exploitleri kullanmak ve bu exploitler ile hedefi sömürmek iyi bir başlangıçtır. Kim bilebilir ilerde belki bir gün kendi exploitinizi yazacak seviyeye bile gelebilirsiniz.



Exploitlerin kendi aralarında farklı çeşitleri bulunmaktadır. Exploit çeşitlerini tanıyalım.

- » **Remote Exploits;** Bu Exploit çeşidinde, uzak sistemlerde bulunan sistemleri sömürmek için kullanırız.
- » **Local Exploits;** Bu Exploit çeşidi, genelde sistemde hak ve rütbe yükseltmek için kullanılır. Linux bir sistemde root kullanıcı olmak istiyorsak ve bir güvenlik zafiyeti keşfettiyssek Local Exploit kullanırız.
- » **Zero-Day Exploits;** Bu Exploit çeşidi, oldukça tehlikelidir. Sistemde yer alan güvenlik zafiyetlerini sömürmek için yazılırlar. Birçok teknoloji sitesinde bir makalede veya haberde bu tarz exploitler ile yapılan siber saldırıları duymuş olabilirsiniz. Çoğunlukla ücretli satılırlar.
- » **Client Side Exploit;** Ağ üzerinden sistemle etkileşim kurulur. Tetiklenmesi gerekmektedir. Sosyal mühendislik atağıyla exploit tetiklenir.