

WEB UYGULAMA GÜVENLİĞİ VE HACKING YÖNTEMLERİ

ERHAN SAYGILI

İÇİNDEKİLER

BÖLÜM 1: Giriş	1
Sektörden Temel Bilgiler	2
Hacker	2
Siyah Şapkalı Hacker	3
Gri Şapkalı Hacker	3
Beyaz Şapkalı Hacker	3
Hacktivist	3
Vulnerability (Güvenlik Açığı)	3
Penetrasyon Testi	4
Penetrasyon Test Çeşitleri	4
White Box	4
Black Box	4
Gray Box	4
Penetrasyon Test Türleri	4
Ağ Penetrasyon Testi	4
Web Uygulama Penetrasyon Testi	5
Mobil Uygulama Penetrasyon Testi	5
Sosyal Mühendislik Penetrasyon Testi	5
Fiziksel Penetrasyon Testi	5
Penetrasyon Test Adımları	5
Bilgi Toplama	6
Ağ Haritasının Çıkartılması	6
Zafiyet Tarama	6
Sisteme Sızma	6
Yetki Yükseltme	7
Başka Ağlara Sızma	7

Erişimi Koruma/Kalıcı Hale Getirme	7
İzleri Temizleme	7
Raporlama	7
Neler Öğrendik?	7
BÖLÜM 2: TEMEL PROGRAMLAR VE İŞLETİM SİSTEMİ KURULUMU	9
VirtualBox	10
VirtualBox Kurulum Aşamaları	10
Parrot Security OS	11
Parrot Security OS Kurulum Aşamaları	12
WampServer	22
WampServer Kurulum Aşamaları	22
WampServer'da Farklı Bir Port Kullanmak	27
WampServer ile Local Ağda Yayın Yapmak	28
Neler Öğrendik?	29
BÖLÜM 3: TEMEL LINUX KOMUTLARI	31
Linux	32
\$	32
#	32
~	33
Linux Dosya/Dizin Hiyerarşisi	33
Genel Amaçlı Komutlar	39
man Komutu	39
apropos Komutu	39
halt Komutu	40
reboot Komutu	40
help, h Komutu	41
type Komutu	41

exit Komutu	42
su Komutu	42
pwd Komutu	43
history Komutu	43
Dosya Komutları	44
ls Komutu	44
cd Komutu	45
sort Komutu	46
mkdir Komutu	48
rm Komutu	48
cp Komutu	49
mv Komutu	49
wc Komutu	50
ln Komutu	50
touch Komutu	51
cat Komutu	52
echo Komutu	54
more Komutu	54
head Komutu	55
tail Komutu	55
chmod Komutu	56
gzip Komutu	57
gunzip Komutu	57
alias Komutu	58
Sistem Komutları	58
date Komutu	58
uptime Komutu	59
cal Komutu	59

df Komutu	60
du Komutu	61
free Komutu	61
whereis Komutu	62
which Komutu	62
uname Komutu	62
w Komutu	64
whoami Komutu	64
hostname Komutu	65
time Komutu	65
who Komutu	66
lsmod Komutu	66
cat /proc/cpuinfo Komutu	67
cat /proc/meminfo Komutu	67
Proses Yönetimi Komutları	68
ps Komutu	68
top Komutu	69
kill Komutu	70
pidof Komutu	70
pgrep Komutu	70
pstree Komutu	71
write Komutu	72
last Komutu	72
Arama Komutları	73
grep Komutu	73
find Komutu	74
Network Komutları	74
ping Komutu	74
traceroute Komutu	75

dig Komutu	76
wget Komutu	76
ifconfig Komutu	77
host Komutu	78
Paket Kurulum Komutları	78
dpkg Komutu	78
apt-get Komutu	79
Neler Öğrendik?	80

BÖLÜM 4: AKTİF VE PASİF BİLGİ TOPLAMA TEKNİKLERİ **83**

Hedef Sistem Hakkında Bilgi Toplama Yöntemleri	84
whois	84
ping	85
thearvester Aracının Kullanımı	86
Dmitry Aracının Kullanımı	88
Fierce Aracının Kullanımı	90
URLcrazy Aracının Kullanımı	92
wafw00n Aracının Kullanımı	92
WhatWeb Aracının Kullanımı	94
IPS-IDS Tespiti	94
Nmap ile Firewall Kontrolü	95
Hedef Sistem Hakkında İnternet Ortamında Bilgi Toplama	96
robtex.com	96
bing.com	96
serversniff.net	97
centralops.net	97
web.archive.org	97
netcraft.com	97
pipl.com	97

sitedigger	97
whois.net	97
ripe.net ve arin.net	97
mxtoolbox.com	97
Google Hacking	98
Bazı Arama Operatörleri ve Kullanım Şekilleri	98
site Operatörü	98
filetype Operatörü	98
" " Operatörü	98
- Operatörü	99
.. Operatörü	99
+ (And) Operatörü	99
(Or) Operatörü	99
link Operatörü	99
related Operatörü	100
info Operatörü	100
allintitle Operatörü	100
intitle Operatörü	100
allinurl Operatörü	101
inurl Operatörü	101
cache Operatörü	102
intext Operatörü	102
mail Operatörü	102
Neler Öğrendik?	102

BÖLÜM 5: WEB TABANLI UYGULAMALAR VE TEMEL BİLGİLER	105
Web Tabanlı Uygulama	106
Web Tabanlı Uygulama Örnekleri	106
Web Tabanlı Uygulamalarının Çalışma Prensipleri	106
Web Tabanlı Uygulama Geliştirme	107
Web Uygulama Güvenliği	107
HTTP ve HTTPS	107
HTTP ile HTTPS Arasındaki Farklar	108
HTTP Başlıkları	108
HTTP Başlık Analizi	109
HTTP Request	113
HTTP Response	114
HTTP Metotları	115
GET	115
POST	116
HEAD	117
TRACE	118
OPTIONS	119
PUT	120
DELETE	120
CONNECT	120
HTTP Durum Kodları	120
En Sık Karşılaşılan Durum Kodları	121
200 OK	121
206 Partial Content (Kısmi İçerik)	121
302 (or 307) Moved Temporarily & 301 Moved Permanently	121
401 Unauthorized (Yetkisiz)	122
403 Forbidden (Yasak)	122

404 Not Found	122
500 Internal Server Error (Dahili Sunucu Hatası)	123
HTTP İsteklerindeki Genel HTTP Başlık Parametreleri	123
Host	123
User-Agent	123
Accept	123
Accept-Language	124
Accept-Encoding	124
If-Modified-Since	124
Cookie	125
Referer	125
Authorization	125
HTTP Yanıtlarında Bulunan HTTP Başlık Parametreleri	127
Cache-Control	127
Content-Type	128
Content-Length	129
Etag	130
Last-Modified	130
Location	130
Set-Cookie	132
www-Authenticate	134
Content-Encoding	136
Server	136
Date	136
Keep-Alive	136
Connection	136
URL	137
URL Encoding	137
Neler Öğrendik?	139

BÖLÜM 6: VERİTABANI 141

SQL	142
SQL Deyimleri	144
Create	144
Use	148
Insert Into	148
Select	149
Where	150
Delete	151
Update	151
Alter Table	151
And/Or	152
Limit	153
In	154
Between	155
Like	155
Order By	157
Union	158
Drop	158
Join	159
Neler Öğrendik?	159

BÖLÜM 7: WEB GÜVENLİK ZAFİYETLERİNDE KULLANILAN PROGRAM VE ARAÇLAR161

Burp Suite	162
Firefox'u BurpSuite ile Çalışacak Şekilde Yapılandırma	162
Tarayıcı Proxy Yapılandırmasını Denetleme	164
Firefox'a Burp Suite CA Sertifikasını Yükleme	165

Burp Suite Menüleri	166
Target	167
Proxy	167
Spider	168
Scanner	168
Intruder	169
Repeater	169
Sequencer	170
Decoder	170
Comparer	170
Extender	171
Project Options	171
Alerts	171
Burp Suite ile Brute Force Saldırısı	172
Sqlmap	177
Windows'a Sqlmap Kurulumu	177
Python Kurulumu	177
Sqlmap Kurulumu	179
Sqlmap Parametreleri	181
Options	182
Target	183
Request	184
Optimization	190
Injection	191
Detection	193
Techniques	195
Fingerprint	196
Enumeration	196

Brute Force	202
User-Defined Function Injection	203
File System Access	203
Operation System Access	204
Windows Registry Access	205
General	206
Miscellaneous	209
Sqlmap Kullanımı	211
Crunch Aracının Kullanımı	219
hash-identifier Aracının Kullanımı	223
Findmyhash Aracının Kullanımı	224
Nikto Aracının Kullanımı	224
Dirbuster Aracının Kullanımı	226
Wapiti Aracının Kullanımı	227
Uniscan Aracının Kullanımı	227
Neler Öğrendik?	229
BÖLÜM 8: OWASP, WAF VE BAZI WEB GÜVENLİK ZAFİYETLERİ	231
OWASP	232
WAF	232
Command Injection	233
SQL Injection	237
Veri Giriş Alanlarının Belirlenmesi	238
Veri Akışı	240
SQL Injection Tespiti	241
SQL Injection'ü Sonlandırma	241
Dize Birleştirme	243
SQL Injection Sırasında Veri Akışı	244

SQL Injection Türleri	245
Error-based SQL Injection	245
Union-based SQL Injection	246
Kolon Sayısının Tespiti	247
MySQL Versiyonunun Tespiti	251
Veritabanında Bulunan Tablo Adlarının Tespiti	252
Veritabanında Bulunan Bir Tabloya Ait Kolonlarının Tespiti	254
Tablo ve Kolon İsimleri Tespit Edilen Veri Tabanından Veri Çekme	256
Blind SQL Injection	258
Boolean-Based (Content-Based) Blind SQL Injection	258
MySQL Versiyon Tespiti	260
Veri Tabanı İsmi'nin Uzunluğunun Tespiti	261
Veritabanı İsmi'nin Tespiti	262
Tablo İsimlerinin Tespiti	267
Kolon İsimlerinin Tespiti	274
Tablo ve Kolon İsmi Tespit Edilen Veritabanından Veri Çekme	279
Time-Based Blind SQL Injection	283
MySQL Versiyon Tespiti	285
Veritabanı İsmi'nin Tespiti	285
Tablo İsimlerinin Tespiti	286
Kolon İsimlerinin Tespiti	287
Tablo ve Kolon İsmi Tespit Edilen Veritabanından Veri Çekme	291
Zamana Dayalı Saldırıların Avantaj ve Dezavantajları	293
XSS (Cross Site Scripting)	293
Kullanıcıdan Alınan Verilerin Bazı Kullanım Alanları	295
XSS Zafiyetinin Verebileceği Zararlar	295
Çerez hırsızlığı	295
Kimlik Hırsızlığı	296
Keylogger Ekleme	296

XSS Türleri	296
Stored XSS	296
Reflected XSS	298
DOM XSS	301
CSRF (Cross Site Request Forgery)	303
CSRF Zafiyetine Karşı Alınabilecek Önlemler	306
File Upload	307
File Inclusion	312
Local File Inclusion	312
Remote File Inclusion	312
File Inclusion Zafiyeti Nasıl Oluşur?	313
File Inclusion Zafiyetine Karşı Alınabilecek Güvenlik Önlemi	314
php.ini ile Web Shell Script'lerinin Etkisizleştirilmesi	315
Neler Öğrendik?	315
Dizin	317



Kitap içerisinde anlatılan konular; sadece meraklılarına ve bu alanda uzmanlaşmak isteyen kişilere bilgi vermek amacıyla hazırlanmıştır. Anlatılan konular ve yöntemler ile kişilerin, başkalarına zarar verebilecek davranışlarından dolayı yazar kesinlikle yasal bir sorumluluk kabul etmemektedir...

1

GİRİŞ

BU BÖLÜMDE

Sektörden Temel Bilgiler	2
Penetrasyon Testi	4
Neler Öğrendik?	7

Bu bölümde Hacker, Hacker Tipleri, Penetrasyon Testi, Penetrasyon Test Çeşitleri gibi sektörde önemli yer tutan temel tanımlar hakkında bilgiler verilerek bu sektör hakkında bazı temel bilgilere sahip olmanız sağlanacaktır.

İnternet, günümüzde aklınıza gelebilecek hemen hemen her yerde yer almaktadır. Bugün milyonlarca web uygulaması hayatımızı daha kolay ve ilginç kılmak için internet sayesinde hizmet verebilmektedir. Bu uygulamalar sayesinde çevrimiçi alveriş yapabilir, fatura ödeyebilir, maillerinize bakabilir, haber okuyabilir, sevdiğinizle veya sevmediklerinizle sohbet edebilir ve daha bir çok şeyi gerçekleştirebilirsiniz.



Yayınlanan web site sayısı her geçen gün giderek artmaktadır. Bu artışın en önemli nedeni ise internet sitesi kurmanın kolay olmasından kaynaklanıyor. Sayısı milyarları bulunan web siteleri ve web tabanlı uygulamalar, teknolojinin gelişmesiyle beraber bir takım sorunları da beraberinde getirmiştir. Bu sorunların en başında da güvenlik gelmektedir.

Kitabın ilerleyen bölümlerinde bu güvenlik sorunlarının bazılarını değinilecek ve alınabilecek güvenlik önlemlerinden bahsedilecektir. Bazı otomatize araçlarda hedef uygulamalarda ki güvenlik zafiyetlerinin tespiti anlatılarak, zafiyet tespitinde zaman kazanılması sağlanacaktır.

SEKTÖRDEN TEMEL BİLGİLER

Siber Güvenlik ile ilgili çalışma yapan, yapmak isteyen kişilerin temel terimleri bilmesi gerekmektedir. Bu terimlerden bazıları şunlardır;

HACKER

Türk Dil Kurumu'na göre Hacker, bilgisayar ve haberleşme teknolojileri konusunda bilgi sahibi olan, bilgisayar programlama alanında standartın üzerinde beceriye sahip olan ve böylece ileri düzeyde yazılımlar geliştiren ve onları kullanabilen kimse olarak tanımlaması yapılmıştır. Siyah, gri ve beyaz şapkalı olmak üzere 3 tip hacker çeşidi vardır.



Siyah Şapkalı Hacker

İnternet ağına bağlı bilgisayarlara ve sistemlere zarar vermek amacıyla bu cihazlara izinsiz yollarla giriş yapan, amaçları tamamen zarar vermek olan kişilere denir.

Gri Şapkalı Hacker

Sistemlere izinsiz giriş yapan, genellikle amaçları zarar vermek değil de güvenlik açıklarını kapatmak veya sistem sahiplerine açıklarla ilgili bilgi vererek sisteme fayda sağlamayı amaçlayan kişilere denir.

Beyaz Şapkalı Hacker

Bu tür bir hacker sık sık bir güvenlik uzmanı veya güvenlik araştırmacısı olarak anılır. Beyaz şapkalı hacker'lar görev yaptıkları kuruluşların siber saldırıya uğramasını engellemek ya da siber saldırılardan en az zararla kurtulmasını sağlamak için hem saldırı yöntemlerini hem de bu saldırılardan korunma yöntemlerini bilmek zorundadır.

HACKTIVIST

Bir amaç için bilgisayar sistemlerine giren hacker'lar olarak tanımlanır. Amaç siyasi kazanç, konuşma özgürlüğü, insan hakları vb. olabilir.

VULNERABILITY (GÜVENLİK AÇIĞI)

Hedef içinde yetkisiz erişime neden olabilecek bir kusur veya zayıflık olarak tanımlanır. Güvenlik açığı hedefin başarılı bir şekilde ele geçirilmesi, veri işleme, yetki yükseltilmesi gibi kritik durumlara nedenler olabilir.

2

TEMEL PROGRAMLAR VE İŞLETİM SİSTEMİ KURULUMU

BU BÖLÜMDE

VirtualBox	10
Parrot Security OS	11
WampServer	22
Neler Öğrendik?	29

Bu bölümde,

Web Güvenlik Zafiyetlerine giriş yapmadan önce örnek uygulamaları çalıştırıp test etmek için gerekli sanal bilgisayarın, örnek zafiyet barındıran uygulamaları çalıştırmak için gerekli web server'ın ve sızma testlerinde kullanılan işletim sisteminin kullanıma hazır hale getirilebilmesi için için izlenecek adımlar anlatılacaktır.

VIRTUALBOX

VirtualBox, masaüstü sanallaştırma yazılımıdır. Yeni bir işletim sistemi denemek istediğinizde bunu bilgisayarınıza kurmadan sanal bir bilgisayar oluşturup üzerine bu işletim sistemini kurarak deneyebilirsiniz. İşte burada bahsi geçen sanal bilgisayarı **VirtualBox** sayesinde oluşturacağız. VirtualBox sadece işletim sistemi kurup denemek için değil diğer yazılım ve program kurulumlarında oluşturulan sanal bilgisayar üzerinde yapabilirsiniz. İnternette indirmek istediğiniz şüpheli programları oluşturmuş olduğunuz sanal makine üzerinde çalışan işletim sisteminiz vasıtasıyla indirip kontrol edebilirsiniz.

VIRTUALBOX KURULUM AŞAMALARI

VirtualBox programını indirmek için <https://www.virtualbox.org/> sitesine giriniz ve sol taraftaki menüden **Download**'a tıklayınız.

The screenshot shows the VirtualBox website homepage. The main heading is "VirtualBox" with a sub-heading "Welcome to VirtualBox.org!". Below this, there is a large "Download 5.2" button. The page also features a "Hot picks" section with links to pre-built virtual machines and a "Recent Flash" section with a list of recent releases and updates.

VirtualBox

Welcome to VirtualBox.org!

VirtualBox is a powerful x86 and AMD64/Intel® virtualization product for enterprise as well as home use. Not only is VirtualBox an extremely feature rich, high performance product for enterprise customers, it is also the only professional solution that is freely available as Open Source Software under the terms of the GNU General Public License (GPL) version 2. See "About VirtualBox" for an introduction.

Presently, VirtualBox runs on Windows, Linux, Macintosh, and Solaris hosts and supports a large number of guest operating systems including but not limited to Windows (NT 4.0, 2000, XP, Server 2003, Vista, Windows 7, Windows 8, Windows 10), DOS/Windows 3.x, Linux (2.4, 2.6, 3.x and 4.x), Solaris and OpenSolaris, OS/2, and openBSD.

VirtualBox is being actively developed with frequent releases and has an ever growing list of features, supported guest operating systems and platforms it runs on. VirtualBox is a community effort backed by a dedicated company: everyone is encouraged to contribute while Oracle ensures the product always meets professional quality criteria.

Download 5.2

Hot picks:

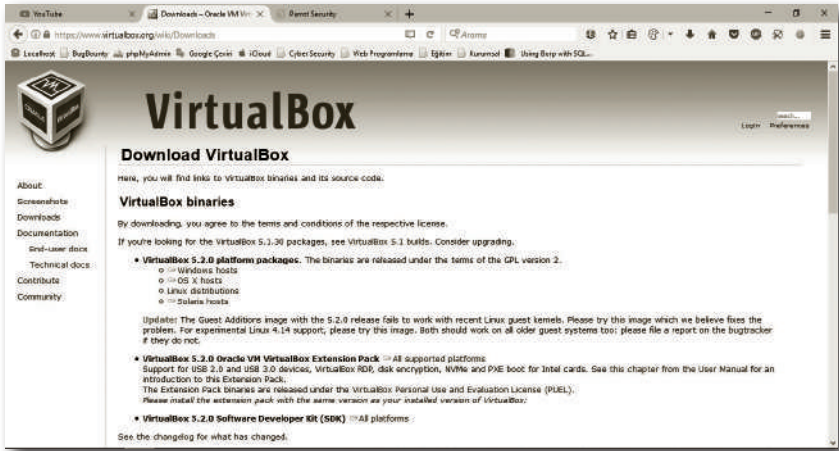
- Pre-built virtual machines for developers at Oracle Tech Network
- Howto: Clone your VirtualBox VMs to a new VM

Recent Flash:

- October 18th, 2017**
VirtualBox 5.2 released! Oracle today shipped a new minor release, VirtualBox 5.2. See the announcement for details.
- October 16th, 2017**
VirtualBox 5.1.20 released! Oracle today released a 5.1 maintenance release which improves stability and fixes regressions. See the ChangeLog for details.
- December 2nd, 2016**
We're hiring! Looking for a new challenge? We're looking for a System administrator (Germany).
- July 28th, 2016**
VirtualBox 5.1 released! Many enhancements and improvements. Read more in the announcement.

More information...

Açılan sayfadan **VirtualBox 5.2.0 platform packages** altında bulunan sistemimize uygun olan sürümü indirmek için bağlantıya tıklayınız. Windows üzerine kurulum yapıp kullanacaksanız **Windows host'u** seçerek indirme işlemini başlatabilirsiniz. İndirme tamamlandıktan sonra programa çift tıklayıp çalıştırınız.



Açılan pencerelelerde **Next, Next** butonlarını kullanarak kurulumu tamamlayabiliriz.



PARROT SECURITY OS

Debian temelli ve varsayılan olarak Mate masaüstü kullanan Parrot Security OS pentest, bilgisayar güvenliği, tersine mühendislik ve kriptografi alanında bir çok aracı üzerinde bulundurmaktadır. **FrozenBox Network** tarafından geliştirilen dağıtım çok düşük sistem gereksinimlerinde dahi hızlı bir şekilde çalışabilmektedir. Kitabın ilerleyen bölümlerinde Parrot Security OS'da yüklü gelen bazı araçlar kullanılacaktır. Dilerseniz siz Kali Linux, Black Arch gibi işletim sistemleri kurup kullanabilirsiniz.

3

TEMEL LINUX KOMUTLARI

BU BÖLÜMDE

Linux	32
Genel Amaçlı Komutlar	39
Dosya Komutları	44
Sistem Komutları	58
Proses Yönetimi Komutları	68
Arama Komutları	73
Network Komutları	74
Paket Kurulum Komutları	78
Neler Öğrendik?	80

Bu bölümde, Linux komutlarının ne işe yaradığı, nasıl kullanıldığı hakkında bazı temel bilgilere sahip olmanız sağlanacaktır.

LINUX

Linux, İnternet üzerinde ilgili ve meraklı birçok kişi tarafından ortak olarak geliştirilmekte olan, kişisel bilgisayarlar olmak üzere birçok platformda çalışabilen ve herhangi bir maliyeti olmayan açık kaynak kodlu özgür bir işletim sistemidir.

Linux çekirdeği 1991 yılında **Linus Torvalds** tarafından geliştirilerek piyasaya sürülmüştür. Bu çekirdek ilerleyen zamanda birçok işletim sisteminin temelini oluşturmuştur. Bir önceki bölümde sanal makine oluşturarak kurulumunu yaptığımız **Parrot Security OS Linux** çekirdeği üzerine yapılandırılmış bir çok işletim sisteminden sadece birisidir.

Bu bölümde linux kullanıcıların bilmeleri gereken temel linux komutları;

- » Genel Amaçlı Komutlar
- » Dosya Komutları
- » Sistem Komutları
- » Proses Yönetim Komutları
- » Arama Komutları
- » Network Komutları
- » Paket Yükleme Komutları

olmak üzere akılda kalması açısından 7 farklı bölümde kategorilendirilerek açıklama ve örnek kullanımları ile birlikte anlatılacaktır.

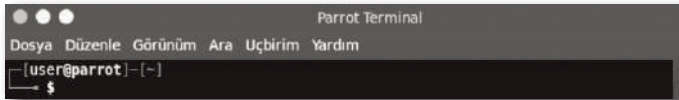
DİKKAT

Bu kategorilendirmenin bir standart olmadığına belirtmek isterim. Sizin gibi yeni kullanıcıların daha kolay öğrenebilmesi ve akılda kalıcılığı arttırmak adına böyle bir kategorilendirme oluşturulmuştur. Sizde kendinize göre bir sınıflandırma oluşturarak kitapta bahsetmediğimiz diğer Linux komutlarını öğrenebilir, ileride hatırlamak adına dönüp bakacağınız bir doküman oluşturabilirsiniz.

Terminal ile ilgili bazı ufak bilgiler;

\$

Terminalde user modunda olduğunuzu belirtir.

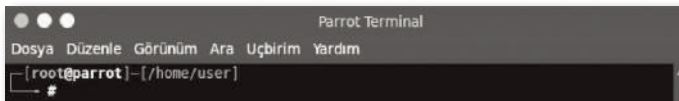


```

Parrot Terminal
Dosya Düzenle Görünüm Ara Uçbirim Yardım
[user@parrot]~$
  
```

#

Terminalde root modunda olduğunuzu belirtir.



```

Parrot Terminal
Dosya Düzenle Görünüm Ara Uçbirim Yardım
[root@parrot]~/home/user#
  
```

~

Terminalde home dizininde bulunduğunuzu belirtir.

```

Parrot Terminal
Dosya Düzenle Görünüm Ara Uçbirim Yardım
[user@parrot] ~
└─$ pwd
/home/user
[user@parrot] ~
└─$

```

LINUX DOSYA/DİZİN HİYERARŞİSİ

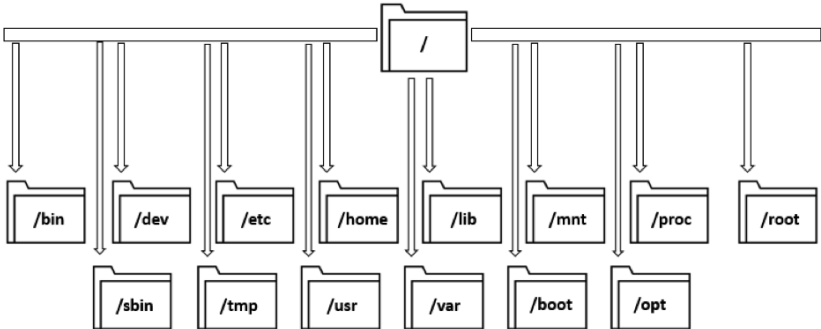
Dosya/dizin sistemi, işletim sisteminin bir disk veya bölüm üzerindeki dosyaları/dizinleri takip edebilmesi için oluşturulmuş yöntemdir. Linux'da her şey / simgesiyle ifade edilen kök dizinden başlayarak dallanıp budaklanarak devam eder. Kök dizin altındaki dizinler, geçmişte Linux Dosya Sistem Hiyerarşisi denilen bir standart ile belirlenmiş klasörlerdir. Günümüzde Linux dağıtımlarının büyük çoğunluğunun bu standartta belirlenmiş klasörlerin dışında kök dizine bir iki klasör daha ekledikleri ya da bu yapıdan bir klasörü çıkardıkları görülmektedir.

Herhangi bir dizin ya da dosyanın sistemdeki adresi öncelikle kök dizinden başlar sonra o dosya ya da dizine ulaşmak için geçilmesi gereken tüm dizinler arasında yine / yazılarak elde edilir.

Örneğin; /etc/python yolu, kök dizininde, etc isimli dizin içindeki python dizinin konumunu belirtir. Bu ifadede en baştaki / işareti kök dizini belirtmektedir.

NOT

Aşağıda bahsi geçen bu dizinlerin neler olduğu, Parrot Security OS üzerinden bu dizinlerin altında bulunun dosya ve klasörler listelenerek ekran görüntüleri eklenmiştir. Bazı dizin altındaki dosya ve klasör sayısının fazlalığı nedeniyle bir bölümünün ekran görüntüsü alınmıştır.



4

AKTİF VE PASİF BİLGİ TOPLAMA TEKNİKLERİ

BU BÖLÜMDE

Hedef Sistem Hakkında Bilgi Toplama Yöntemleri	84
Hedef Sistem Hakkında İnternet Ortamında Bilgi Toplama	96
Google Hacking	98
Neler Öğrendik?	102

Bu bölümde, hedef sistem hakkında aktif ve pasif bilgi toplamanın ne olduğu, hedef sistem hakkında nasıl bilgi toplanılacağı, bilgi toplama aşamasında hangi araçların kullanılacağına dair genel bilgiler verilecektir.

Hedef sistem hakkında bilgi toplama;

- » Pasif Bilgi Toplama
- » Aktif Bilgi Toplama olmak üzere 2 şekilde yapılabilir.

Pasif Bilgi Toplama; Hedef sisteme doğrudan bir erişim ya da tarama yapılmadan internet üzerindeki servislerden veya web siteleri kullanarak hedef hakkında bilgi toplama yoludur.

Aktif Bilgi Toplama; Hedef sisteme doğrudan erişim ya da tarama ile yapılan bilgi toplama tekniğidir. Sistem ile etkileşim içerisinde olan bir bilgi toplama yöntemi olduğu için hedef sistemin güvenlik duvarı vs. cihazların log'larına düşme ihtimali yüksektir. Bu tarz bilgi toplanırken dikkatli olunmalıdır.

Aktif ve Pasif Bilgi Toplama aşaması sızma testlerinin ilk ve en önemli adımıdır. Sızma testinde hedef sistem üzerinde daha fazla etkili olabilmek için hedef sistem hakkında yeterince bilgi sahibi olmak gerekir. Sistem hakkında ne kadar çok bilgi toplanırsa daha sonraki testlerde hangi yolların izleneceği nelerin test edileceği rahatlıkla belirlenmiş olur. Toplanılan tüm bilgiler kategorilendirilmeli, gerekli veya gereksiz diye ayırım yapılmamalıdır. Sızma testinin ilerleyen aşamalarında elde edilen bilgilerin hangilerinin bizim için yararlı olacağı hemen tespit edilemeyebilir.

HEDEF SİSTEM HAKKINDA BİLGİ TOPLAMA YÖNTEMLERİ

WHOIS

Hedef domain hakkında name server bilgileri, admin iletişim bilgileri, teknik iletişim bilgileri, tescil ettiren kişi/kuruluş bilgileri gibi önemli bilgiler elde edilebilir.

Kullanım şekli

```
#whois DOMAIN_ADI
```

```
#whois IP_ADRESİ
```

Alabileceği parametreleri görmek için terminalde `man whois` komutunu kullanabilirsiniz.

Örnek kullanım

```
#whois 3rh4n.com
```

```
Parrot Terminal
Dosya Düzenle Görünüm Ara Uçbirim Yardım
[user@parrot]~$ whois 3rh4n.com
Domain Name: 3RH4N.COM
Registry Domain ID: 2115440043_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.nicproxy.com
Registrar URL: http://www.nicproxy.com
Updated Date: 2017-04-18T12:26:19Z
Creation Date: 2017-04-18T12:26:19Z
Registry Expiry Date: 2018-04-18T12:26:19Z
Registrar: Nics Telekomunikasyon Tic Ltd. Sti.
Registrar IANA ID: 1454
Registrar Abuse Contact Email:
Registrar Abuse Contact Phone:
Domain Status: ok https://icann.org/epp#ok
Name Server: NS1.NATROHOST.COM
Name Server: NS2.NATROHOST.COM
DNSSEC: unsigned
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2017-12-20T22:52:28Z <<<

For more information on Whois status codes, please visit https://icann.org/epp

NOTICE: The expiration date displayed in this record is the date the
registrar's sponsorship of the domain name registration in the registry is
currently set to expire. This date does not necessarily reflect the expiration
date of the domain name registrant's agreement with the sponsoring
registrar. Users may consult the sponsoring registrar's Whois database to
view the registrar's reported date of expiration for this registration.
```

Online whois sorgulama yapılabilecek site: <http://www.who.is/>

PING

Hedef domainin IP adresini öğrenmek için kullanılabilir. (ping hakkında merak ettiklerinizi bir önceki bölümden daha detaylıca öğrenebilirsiniz.)

Kullanım şekli

```
#ping DOMAIN_ADI
```

Örnek kullanım

```
Parrot Terminal
Dosya Düzenle Görünüm Ara Uçbirim Yardım
[root@parrot]~/home/user$ #ping www.3rh4n.com
PING 3rh4n.com (94.73.158.26) 56(84) bytes of data.
```

8

OWASP, WAF VE BAZI WEB GÜVENLİK ZAFİYETLERİ

BU BÖLÜMDE

OWASP	232
WAF	232
Command Injection	233
SQL Injection	237
SQL Injection Türleri	245
XSS (Cross Site Scripting)	293
Kullanıcıdan Alınan Verilerin Bazı	
Kullanım Alanları	295
XSS Zafiyetinin Verebileceği Zararlar	295
XSS Türleri	296
CSRF (Cross Site Request Forgery)	303
File Upload	307
File Inclusion	312
Neler Öğrendik?	315
Dizin	317

Bu bölümde Command Injection, SQL Injection, XSS gibi önemli güvenlik zafiyetleri hakkında detaylı bilgiler verilerek bu gibi zafiyetleri kullanarak örnek uygulamalar üzerinden hedef sistemlere nasıl sızılabilceği, nasıl veri elde edilebileceği hakkında bilgiler verilecektir.

OWASP

OWASP, Open Web Application Security Project'in kısaltmasıdır. Açık Web Uygulama Güvenliği Projesi anlamına gelen OWASP, güvensiz yazılımların oluşturduğu problemlere karşı mücadele etmek için kurulmuş uluslararası, kâr amacı gütmeyen bir kuruluştur.

OWASP Top 10, en kritik 10 güvenlik açığının OWASP tarafından düzenli olarak yayınlandığı listedir. Kitabın yayınlandığı tarihlerde en kritik 10 güvenlik açığı aşağıdaki şekildedir. Kitabı okuduğunuz tarihte belki bu sıralama değişmiş olabilir. Gelişmeleri <https://www.owasp.org> adresinden takip edebilirsiniz.

- » A1 - Injection
- » A2 - Broken Authentication
- » A3 - Sensitive Data Exposure
- » A4 - XML External Entities (XXE)
- » A5 - Broken Access Control
- » A6 - Security Misconfiguration
- » A7 - Cross-Site Scripting (XSS)
- » A8 - Insecure Deserialization
- » A9: - Using Components with Known Vulnerabilities
- » A10: - Insufficient Logging & Monitoring

WAF

Web Application Firewall'ın kısaltması olan **WAF**, bir istemci ve web uygulaması arasındaki HTTP trafiğini inceleyen, filtreleyen ve gerekli durumlarda (bilinen güvenlik açığı ve saldırganlara karşı korumak için) engelleyen bir çevrimiçi güvenlik çözümdür. WAF genelde ağ tabanlı, ana bilgisayar veya bulut tabanlı olabilir. Genellikle bir veya daha fazla web uygulamasının önüne yerleştirilir.

Network Firewall, IDS ve IPS ağ düzeyinde güvenliği sağlamak için kullanılırken, WAF ise sunucuya gelen HTTP isteklerinin incelenmesi ve tehditlerin engellenmesi için kullanılır. Bu tehditler SQL Injection, XSS ve web uygulamalarında bulunan diğer güvenlik açıklarından kaynaklanabilmektedir. WAF, web uygulamalarını hedefleyen saldırıları önlemede etkili ancak kesin çözüm sunmamaktadır. Genellikle birden fazla web güvenlik çözümü kullanmak güvenliğinizi biraz daha arttıracaktır.

WAF'ın çalışma sistemine kısaca değinecek olursak, web sunucusuna gelen tüm http istekler WAF tarafından kesilerek bileşenlerine ayrılır. Bileşenlerine ayrılan http isteklerindeki veriler normalleştirilerek (URL decode, base64 gibi) gerekli filtrelemeler yapılır. WAF, yapılandırmasına bağlı olarak trafiği engelleyebilir, ziyaretçinin bir CAPTCHA girmesini zorlayabilir. Engelleme ve zorlayıcı seçenekler, herhangi bir istenmeyen trafiğin web sunucusuna ulaşmasını engeller.

COMMAND INJECTION

Bir saldırganın zafiyet barındıran bir uygulama üzerinden hedef sistemde dilediği komutları çalıştırabilmesine yarayan güvenlik açığıdır. Bu saldırı türünde saldırgan tarafından girilen işletim sistemi komutları genellikle savunmasız uygulamaya ayrıcalıkları/yetkileri ile çalıştırılır.

Command Injection saldırıları büyük ölçüde kullanıcı tarafından girilen verilerin denetlenmemesi nedeniyle ortaya çıkar. Bu tür uygulamalarda kullanıcı girdisi denetlemeye tabi tutulmamışsa komut satırı bilginizi kullanarak girdi kısmına ekstra kodlar ekleyip çalıştırabilirsiniz.

Eğer shell (komut satırı) hakkında biraz bilginiz varsa &&, | ya da || gibi operatörler, ayrıca ; gibi sonlandırıcı operatörlerin shell komutlarını birbirlerinden ayıran ya da birbirlerine bağlayan özelliğe sahip olduğunu bilirsiniz. Bu operatörler yardımıyla mevcut komutun sonuna yeni bir komut ekleyebilir ve hedef sistem üzerinde çalıştırabilirsiniz.

Aşağıda zafiyet barındıran örnek bir kod bloğu bulunmaktadır.

```
<?php
if(isset($_POST[ 'giris' ])){
    $hedef = $_POST["domain"];
    if( strstr( php_uname( 's' ), 'Windows NT' ) ){
        $cmd = shell_exec( 'ping ' . $hedef );
    }
    else{
        $cmd = shell_exec( 'ping -c 4 ' . $hedef );
    }
    echo $cmd;
}
?>
```

NOT

`php_uname()` fonksiyonu PHP'nin üzerinde çalıştığı işletim sistemi hakkında bilgi döndürür.
`striStr()` fonksiyonu bir yazı içinde kelime aramak için kullanılır. Aranana kelimedeki büyük/küçük harf olması fark etmeden aradığınızı bulur.

Yukarıda zafiyet barındıran kod bloğu incelendiğinde kullanıcıdan alınan girdinin hiçbir filtreleme işleminden geçirilmeden direk kullanıldığı görülmektedir. Bu durum güvenlik zafiyetine yol açmaktadır.

Bu bölüm için hazırladığımız **Command Injection** uygulamasını www.3RH4N.com/wug/ci.zip adresinden indirebilirsiniz. Bu uygulamayı daha önce kurulumunu yapmış olduğunuz WampServer'a kurduktan sonra adres çubuğuna <http://localhost/ci/> yazdığınızda hazırlamış olduğumuz uygulamaya ulaşarak vermiş olduğumuz örnekleri deneyebilirsiniz. WampServerınıza Command Injection uygulamasını ekledikten sonra <http://localhost/ci/> adresini ziyaret ettiğinizde sizi aşağıdaki gibi bir ekran karşılayacaktır.



Hazırlamış olduğumuz uygulamanın inputuna aşağıdaki değeri girdiğinizde;

```
192.168.1.1 && echo "<font color=green><center><h1>Hacked By 3RH4N </h1></center></font><br>" > login.php
```

Localhost içerisinde bulunan Command Injection uygulaması içerisinde yer alan `login.php` isimli dosya içerisine `<center><h1>Hacked By 3RH4N </h1></center>
` değerinin yazıldığını göreceksiniz.

NOT

Yukarıdaki kod parçasındaki `echo` komutu argüman olarak aldığı string'i `login.php` dosyasının içine yazmaya yarar.

Tarayıcınızdan <http://localhost/ci/login.php> adresine giriş yapmaya çalıştığınızda aşağıdaki gibi bir ekranla karşılaşacaksınız.

