

Bilgi Toplama

Necmettin ÇARKACI – Ahmet Alperen BULUT

Biz kimiz

İstihbarat Çeşitleri

Pasif Bilgi Toplama

- Hedef sistemden bağımsız

Aktif Bilgi Toplama

- Hedef sistemle doğrudan iletişime geçerek

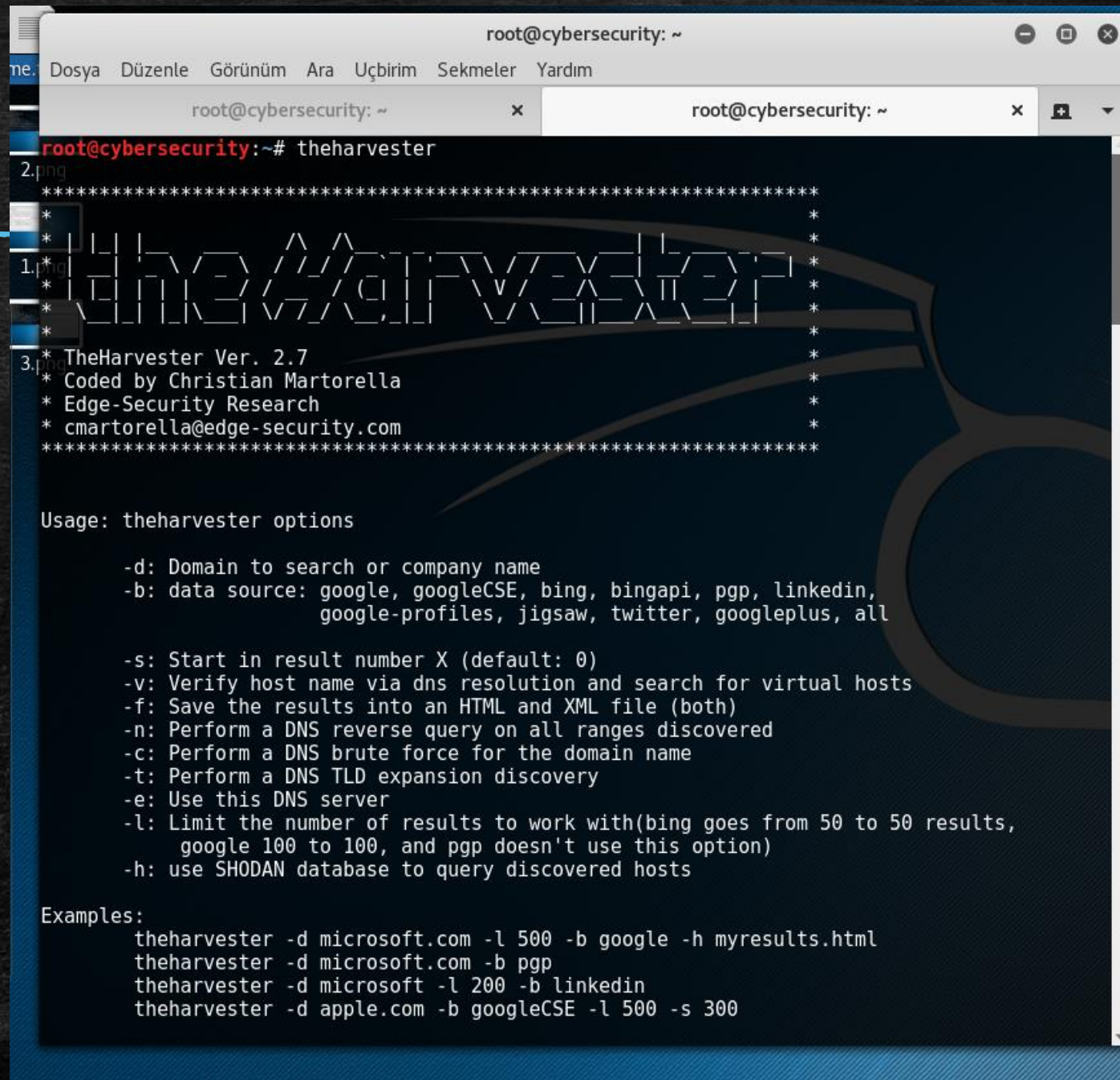
Aktif Bilgi Toplama

theharvester

- ⌚ TheHarvester aracı, hedef sistem/etki alanı üzerinden aktif ve pasif olarak bilgi toplamaya yarayan ve sızma testlerinde de kullanılan bir araçtır. Bu yazıda TheHarvester tarafından sunulan temel hizmetler incelenecektir.
- ⌚ TheHarvester aracı ile pasif olarak Google, Bing,... gibi arama motorlarından, LinkedIn, Shodan gibi platformlardan kullanıcı profilleri, mail adresleri, sanal hostlar,... tespit edilebilir. Aktif olarak da DNS adlarını ve alt etki alanlarını bulmaya yönelik kaba kuvvet saldırıları gerçekleştirilebilir.

Theharvester kullanımı

- ① "-d microsoft.com". microsoft.com etki alanı hakkında bilgi edinilir.
- ① "-b all". Google, Bing, PGP, LinkedIn, Jigsaw, Twitter,... gibi veri kaynaklarından bilgi toplanır.
- ① "-s o". Arama motorlarının sayfalarının kaçınıcı indeksinden itibaren arama yapılacağı belirtilir.
- ① "-l 400". Arama yapılacağı sonuç sayısını belirtir.
- ① "-v". DNS çözümlemesi ile Host isimleri doğrulanır ve sanal Host araması yapılır.
- ① "-h". Tespit edilen sistemler için Shodan veritabanından bilgi elde edilir.
- ① "-t". Üst alan adları için arama yapılır.
- ① "-n". Tespit edilen IP aralıkları için ters DNS sorguları gerçekleştirilerek daha fazla ve ilişkili sonuç elde edilir.
- ① "-f /root/Desktop/sonuclar". Tarama sonucu belirtilen dosyaya HTML ve XML formatında kaydedilir.





root@cybersecurity: ~



[+] Emails found:

365@gtu.edu.tr
afari@gtu.edu.tr
b.sezen@gtu.edu.tr
bashalk@gtu.edu.tr
bim@gtu.edu.tr
boral@gtu.edu.tr
cyigit@gtu.edu.tr
datilla@gtu.edu.tr
egumus@gtu.edu.tr
fdumoulin@gtu.edu.tr
girisimcilik@gtu.edu.tr
girisimcilikzirvesi@gtu.edu.tr
gorgun@gtu.edu.tr
gozturk@gtu.edu.tr
gtuburslar@gtu.edu.tr
halimkazan@gtu.edu.tr
kavzoglu@gtu.edu.tr
kuram@gtu.edu.tr
mgurol@gtu.edu.tr
mozturk@gtu.edu.tr
nkaya@gtu.edu.tr
oesen@gtu.edu.tr
ogrenci@gtu.edu.tr
rezanakova@gtu.edu.tr
saes@gtu.edu.tr
scakalogullari@gtu.edu.tr
sedakol@gtu.edu.tr
sem@gtu.edu.tr
serkovan@gtu.edu.tr
sztopal@gtu.edu.tr
tcakir@gtu.edu.tr
tsalihoglu@gtu.edu.tr
tto@gtu.edu.tr
venilmez@gtu.edu.tr

root@cybersecurity: ~

root@cybersecurity: ~

root@cybersecurity: ~

Profil adı: [isimsiz]

Profil Kimliği: b1dcc9dd-5262-4d8d-a863-997e6d979b9

İlk uçbirim boyutu: 80 - + sütun 2 - + satır Sıfırla

İmleç şekli: Blok

☒ Uçbirim zili

Metin Görünümü

☒ Kalın metne izin ver

☒ Yeniden boyutlandırma yeniden sar

☒ Custom font: Monosp Regular 15

Yardım

Profil adı: [isimsiz]

Profil Kimliği: b1dcc9dd-5262-4d8d-a863-997e6d979b9

İlk uçbirim boyutu: 80 - + sütun 2 - + satır Sıfırla

İmleç şekli: Blok

☒ Uçbirim zili

Metin Görünümü

☒ Kalın metne izin ver

☒ Yeniden boyutlandırma yeniden sar

☒ Custom font: Monosp Regular 15

Kapat

Uygulamalar Yerler Uçbirim Çrş 11:02 1 tr

root@cybersecurity: ~

me.tx Dosya Düzenle Görünüm Ara Uçbirim Sekmeler Yardım

root@cybersecurity: ~

root@cybersecurity: ~

2.pn [+] Hosts found in search engines:

1.pn [-] Resolving hostnames IPs...
192.168.50.77:Akademik.gtu.edu.tr
192.168.50.6:abl.gtu.edu.tr
192.168.50.77:akademik.gtu.edu.tr
3.pn 10.1.2.21:aks.gtu.edu.tr
192.168.50.3:anibal.gtu.edu.tr
192.168.50.77:basvuru.gtu.edu.tr
heharv 192.168.50.150:bilmuh.gtu.edu.tr
r1.pn 192.168.50.69:bte.gtu.edu.tr
192.168.50.81:burslar.gtu.edu.tr
PNG 31.222.147.144:ekutuphane.gtu.edu.tr
theharve 192.168.50.30:irisimcilik.gtu.edu.tr
r2.png 192.168.50.5:ismc.gtu.edu.tr
192.168.50.64:kariyer.gtu.edu.tr
192.168.60.10:kutuphane.gtu.edu.tr
192.168.50.77:ogrenci.gtu.edu.tr
192.168.50.6:passchange.gtu.edu.tr
192.168.50.5:portal.gtu.edu.tr
159.253.39.27:sem.gtu.edu.tr
192.168.50.56:tto.gtu.edu.tr
192.168.50.50:web.gtu.edu.tr
192.168.50.5:www.gtu.edu.tr
[+] Virtual hosts:
=====
31.222.147.144 www.gop-elibrary.com
31.222.147.144 www.marmara-elibrary.com
31.222.147.144 www.kirikkale-elibrary.com
31.222.147.144 elibrary.beykent.edu.tr
31.222.147.144 ekutuphane.yyu.edu.tr
31.222.147.144 ekutuphane.sakarya.edu.tr
31.222.147.144 elibrary.medipol.edu.tr
31.222.147.144 elibrary.aku.edu.tr
31.222.147.144 www.okan-elibrary.com

Yardımluk

Profil adı: İsimli

Profil Kimliği: b1dcc9dd-5262-4d8d-a863-97e6d979b9

Uçbirim boyutu: 80 sütun 2 satır Sıfırla

İmleç şekli: Blok

☒ Uçbirim zili

Metin Görünümü

☒ Kalın metne izin ver

☒ Yeniden boyutlandırma yeniden sar

☒ Custom font: Monosp Regular 15

Yardımluk

Kapat

Traceroute

- ⌚ Traceroute bir paketin istediği adrese gidene kadar hangi hostlar ve yönlendirmelerden geçtiğini gösteren programdır.

Dig

- ⌚ Detaylı DNS sorgulaması yapan gelişmiş bir araçtır.

Dirbuster

⌚ dirbuster hedef bir websitenin alt dizinlerini bulmak için kullanılan gelişmiş güzel bir araçtır. Kalide kurulu olarak gelmekte terminale dirbuster yazdığımız programın GUI si bulunmakta ve o açılmakta. Bir wordlist belirterek aradığınız dizinlere ve daha fazlasına ulaşabilirsiniz.

OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing

FileOptionsAboutHelp

Target URL (eg http://example.com:80/)

Buraya sitenin adresini

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

buraya wordlisti

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

buraya dosya uzantisi

URL to fuzz - /test.html?url={dir}.asp

Exit

Start

Please complete the test details

OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing

File Options About Help

Target URL (eg http://example.com:80/)

https://bilmuh.gtu.edu.tr/moodle:80/

Work Method

☐ Use GET requests only ☒ Auto Switch (HEAD and GET)

Number Of Threads



200 Thre...

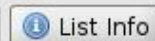
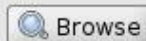
☒ Go Faster

Select scanning type:

☒ List based brute force ☐ Pure Brute Force

File with list of dirs/files

/root/Masaüstü/me.txt



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

/moodle/

☒ Brute Force Files

☐ Use Blank Extension

File extension

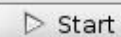
php

URL to fuzz - /test.html?url={dir}.asp

/moodle/



Exit



Start

DirBuster Stopped


```
root@cybersecurity: ~
me: Dosya Düzenle Görünüm Ara Uçbirim Yardım
Dir found: /moodle/ - 200
Dir found: / - 403
Dir found: /moodle/login/ - 200
File found: /moodle/login/index.php - 200
File found: /moodle/user/profile.php - 303
File found: /moodle/user/view.php - 303
Dir found: /moodle/mod/ - 200
Dir found: /moodle/mod/forum/ - 200
Dir found: /moodle/course/ - 200
File found: /moodle/course/index.php - 200
File found: /moodle/calendar/view.php - 200
Dir found: /moodle/calendar/ - 303
Dir found: /moodle/pluginfile.php/5/user/icon/ - 200
File found: /moodle/pluginfile.php/5/user/icon/clean/f2 - 200
Dir found: /moodle/theme/ - 303
File found: /moodle/theme/image.php/clean/forum/1489570996/icon - 200
File found: /moodle/theme/image.php/clean/core/1489570996/moodlelogo - 200
Dir found: /moodle/lib/ - 200
File found: /moodle/lib/javascript.php/1489570996/lib/javascript-static.js - 200
File found: /moodle/lib/javascript.php/1489570996/lib/requirejs/require.min.js - 200
File found: /moodle/theme/javascript.php/clean/1489570996/footer - 200
DirBuster Stopped
□
```

OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing

File Options About Help

https://bilmuh.gtu.edu.tr:443/moodle/

Scan Information Results - List View: Dirs: 9 Files: 11 Results - Tree View Errors: 0

Type	Found	Response	Size
Dir	/moodle/	200	35883
Dir	/	403	481
Dir	/moodle/login/	200	502
File	/moodle/login/index.php	200	502
File	/moodle/user/profile.php	303	931
File	/moodle/user/view.php	303	931
Dir	/moodle/mod/	200	289
Dir	/moodle/mod/forum/	200	502
Dir	/moodle/course/	200	502
File	/moodle/course/index.php	200	502
File	/moodle/calendar/view.php	200	502
Dir	/moodle/calendar/	303	935
Dir	/moodle/pluginfile.php/5/user/icon/	200	8865
File	/moodle/pluginfile.php/5/user/icon/clean/f2	200	2321

Current speed: 0 requests/sec (Select and right click for more options)

Average speed: (T) 3, (C) 1 requests/sec

Parse Queue Size: 0

Total Requests: 92/86

Time To Finish: 00:00:0-6

Current number of running threads: 200

Back Pause Stop Change Report

DirBuster Stopped


```
root@cybersecurity: ~  
me Dosya Düzenle Görünüm Ara Uçbirim Yardım  
Dir found: / - 403  
Dir found: /moodle/login/ - 200  
File found: /moodle/user/profile.php - 303  
2. File found: /moodle/login/index.php - 200  
File found: /moodle/user/view.php - 303  
Dir found: /moodle/mod/ - 200  
Dir found: /moodle/mod/forum/ - 200  
1. Dir found: /moodle/course/ - 200  
File found: /moodle/course/index.php - 200  
Dir found: /moodle/calendar/ - 303  
File found: /moodle/calendar/view.php - 200  
Dir found: /moodle/pluginfile.php/5/user/icon/ - 200  
File found: /moodle/pluginfile.php/5/user/icon/clean/f2 - 200  
Dir found: /moodle/theme/ - 303  
File found: /moodle/theme/image.php/clean/forum/1489570996/icon - 200  
File found: /moodle/theme/image.php/clean/core/1489570996/moodlelogo - 200  
Dir found: /moodle/lib/ - 200  
File found: /moodle/lib/javascript.php/1489570996/lib/javascript-static.js - 200  
File found: /moodle/lib/javascript.php/1489570996/lib/requirejs/require.min.js - 200  
File found: /moodle/theme/javascript.php/clean/1489570996/footer - 200  
DirBuster Stopped  
URL from tree item: https://bilmuh.gtu.edu.tr/moodle/login/index.php  
□
```

OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing

File Options About Help

https://bilmuh.gtu.edu.tr:443/moodle/

Scan Information Results - List View: Dirs: 9 Files: 11 Results - Tree View Errors: 0

Directory Structure	Response Code	Response Size
└─ moodle	403	481
└─ login	200	35952
└─ user	???	502
└─ mod	200	289
└─ course	200	502
└─ calendar	303	935
└─ pluginfile.php	???	???
└─ theme	303	931
└─ lib	200	291
└─ javascript.php	???	???
└─ 1489570996	???	???

Current speed: 0 requests/sec

(Select and right click for more options)

Average speed: (T) 2, (C) 2 requests/sec

Parse Queue Size: 0

Total Requests: 104/96

Current number of running threads: 200

Time To Finish: 00:00:0-4

Back

Pause

Stop

Report

DirBuster Stopped

Nmap

- ⌚ Nmap, bilgisayar ağları uzmanı Gordon Lyon (Fyodor) tarafından C/C++ ve Python programlama dilleri kullanılarak geliştirilmiş bir güvenlik tarayıcısıdır. Taranan ağın haritasını çıkarabilir ve ağ makinalarında çalışan servislerin durumlarını, işletim sistemlerini, portların durumlarını gözlemleyebilir.
- ⌚ Hatta NSE (Nmap Scripting Engine) ler kullanarak bazı açıklıklar tespit edilebilir, brute force saldırıları gerçekleştirilebilir.

⌚ Nmap kullanarak ağıba bağılı herhangi bir bilgisayarın işletim sistemi, çalışan fiziksel aygıt tipleri, çalışma süresi, yazılımların hangi servisleri kullandığı, yazılımların sürüm numaraları, bilgisayarın ateşduvarına sahip olup olmadığı, ağ kartının üreticisinin adı gibi bilgiler öğrenilebilmektedir. GUI şeklinde olanı Zenmap

Kullanım alanları

- ⌚ Nmap kullanım alanları .
- ⌚ Herhangi bir ağ hazırlanırken gerekli ayarların test edilmesinde.
- ⌚ Ağ envanteri tutulması, haritalaması, bakımında ve yönetiminde.
- ⌚ Bilinmeyen yeni sunucuları tanımlayarak, güvenlik denetimlerinin yapılması.

Örnek

- ⌚ #nmap -A -T4 192.168.1.2
- ⌚ -A, OS ve versiyon bulma, script taraması ve traceroute özelliğini çalıştırır.
- ⌚ -T4, daha hızlı bir şekilde tarama yapar (To - T5 arası seçim yapılabilir).

Nmap Hedef Belirtme Özelliği

- ⌚ Nmap taramalarında hedef belirlemek için birçok farklı özellik kullanılabilir. Hedef belirtilirken, DNS ismi, IP, Subnet gibi seçenekler kullanılabileceği gibi farklı özelliklerde kullanılabilir.
- ⌚ Hedef belirtme özellikleri .
- ⌚ -iL <dosya_ismi> . Hostların veya networklerin belirtildiği dosyadan bilgileri alarak tarama yapar.
- ⌚ -iR <host sayısı> . Rastgele hedef seçer. Host sayısı ile kaç hedefin taranılması istenildiği belirtilir.
- ⌚ - -exclude <host1[,host2][,host3],...> . Taranılması istenilmeyen hostların veya networklerin belirtilmesi için kullanılır.
- ⌚ - -excludefile <exclude_file> . Taranılması istenilmeyen hostların veya networklerin bir dosya içerisinde alınarak hedefler belirtilir.

Hedef belirtme seçenekleri .

- ⌚ 192.168.1.10
- ⌚ 192.168.1.10/24 .192.168.1.0 – 192.168.1.255 aralığında bulunan subneti tarar.
- ⌚ 192.168.1-2.* . 192.168.1.0 – 192.168.2.255 aralığındaki herşeyi tarar.
- ⌚ 192.168.1,2.0-255 . 192.168.1.0 – 192.168.2.255 aralığındaki herşeyi tarar.
- ⌚ *.*.1.5 . 1.0.1.5 – 255.255.1.5 aralığındaki herşeyi tarar.

-
- ⌚ `nmap -sV -iL hosts.txt` . Taranılacak olan hostları, hosts.txt dosyasından alır
 - ⌚ `nmap -p 443 -iR 10` . HTTPS servisini kullanan rastgele 10 tane hostu bulmak için kullanılır.
 - ⌚ `nmap -sP - - exclude web.xyz.com,dns.xyz.com,mail.xyz.com 192.168.1.0/24 . 192.168.1.0 192.168.1.255` subnetinde belirtilen adresler dışındaki herşeyi tarar.
 - ⌚ `nmap - -excludefile riskli.txt 192.168.0.0/16 . 192.168.0.0 - 192.168.255.255` subnetinde belirtilen dosyadaki adresler dışındaki herşeyi tarar.

Sunucuları/İstemcileri Keşfetme

- ⌚ Organizasyon içerisindeki hostları bulmak için çok önemli bir yöntemdir. Keşfetme işlemi için birçok seçenek kullanılabilir. En basit yolu bir ping scan gerçekleştirmektir
- ⌚ `#nmap -sP 192.168.2.0/24`
- ⌚ Ping scan belirtilen hedef veya hedeflerin 80. portuna ICMP echo request ve TCP ACK (root veya Administrator değilse SYN) paketleri gönderir. Hedef veya hedeflerden dönen tepkilere göre bilgiler çıkartılır. Hedef/hedefler Nmap ile aynı yerel ağda bulunuyorsa, Nmap hedef/hedeflerin MAC adreslerini ve ilgili üreticiye ait bilgileri (OUI) sunar. Bunun sebebi, Nmap varsayılan olarak ARP taraması, -PR, yapar. Bu özelliği iptal etmek için - - send-ip seçeneği kullanılabilir. Ping scan portları taramaz yada başka tarama tekniklerini gerçekleştirmez. Ping scan network envanteri vb. işlemler için idealdir.

Keşfetme işlemleri için bazı seçenekler aşağıda sunulmuştur .

- ⌚ -sL. List Scan – Hedefleri ve DNS isimlerinin bir listesini çıkarır.
- ⌚ -sn. Ping Scan - Port scan seçeneğini iptal eder.
- ⌚ -Pn. Host discovery yapılmaz, bütün hostlar ayakta gözükür.
- ⌚ -n/-R. Asla DNS Çözümlemesi yapılmaz/Herzaman DNS çözümlemesi yapılır [varsayılan. bazen]
- ⌚ --dns-servers <serv1[,serv2],...>. Özel DNS serverleri belirtmek için kullanılır.
- ⌚ --system-dns. OS e ait DNS çözümleyici kullanılır.
- ⌚ --traceroute. Traceroute özelliğini aktif hale getirir. TCP Connect ve Idle Scan dışındaki tarama türleri ile yapılmaz.

- ⌚ -p . port veya port aralıklarını belirtmek için kullanılır. -p22; -p1-65535; -p U.53,111,137,T.2125,80,139,8080,S.9
- ⌚ -F. Fast mode, varsayılan taramalarda belirlenen portlardan biraz daha azı kullanılır.
- ⌚ -r. Portları sırayla tarar. Rastgele tarama kullanılmaz.
- ⌚ --top-ports <sayı>. <sayı> ile belirtilen ortak portları taranır.
- ⌚ p--port-ratio <oran>. Belirtilen <oran> üzerinden ortak portlar taranır.
- ⌚ - -randomize_hosts, -rH . Listede belirtilen taranılacak hostları rastgele bir şekilde seçer.
- ⌚ - -source_port, -g . Taramayı yapacak olan makinanın kaynak portunu belirlemek amacıyla kullanılır.
- ⌚ -S <IP> . Kaynak IP yi belirlemek amacıyla kullanılır.
- ⌚ -e . Network arayüzünü belirlemek amacıyla kullanılır.

Tarama

- ⌚ Nmap herhangi bir client veya serverı birçok farklı şekilde tarama yeteneğine sahiptir. Nmapin asıl gücü farklı tarama tekniklerinden gelir. Protokol bazlı (Tcp, Udp vb.) tarayabileceğiniz gibi, belirli aralıklardaki ipler, subnetler ve üzerlerinde çalışan port ve servisleride taranabilir.

Portların Taramalara Verebileceği Cevaplar

- ⌚ Open . Portlar açık ve aktif olarak TCP veya UDP bağlantısı kabul eder.
- ⌚ Closed . Portlar kapalı ancak erişilebilir. Üzerlerinde dinlenen aktif bir bağlantı yoktur.
- ⌚ Filtered . Dönen tepkiler bir paket filtreleme mekanizması tarafından engellenir. Nmap portun açık olduğuna karar veremez.
- ⌚ Unfiltered . portlar erişilebilir ancak Nmap portların açık veya kapalı olduğuna karar veremez. (Sadece ACK scan için)
- ⌚ Open|filtered . Nmap portların açık veya filtrelenmiş olduğuna karar veremez. (UDP, IP Proto, FIN, Null, Xmas Scan için)
- ⌚ Closed|filtered . Nmap portların kapalı yada filtreli olduğuna karar veremez. (Sadece Idle Scan için)

-
- ⌚ Taramalar esnasında Nmapin performansının düşmemesi ve çıktıların daha düzenli olmasıyla amacıyla `-v` yada `-vv` seçenekleri kullanılabilir.
 - ⌚ Bu seçenekler vasıtasıyla Nmap bize sunacağı çıktıları limitler. `-vv` kullanılırsa, Nmap'e ait istatistikler görülmez ve en sade çıktı alınır.

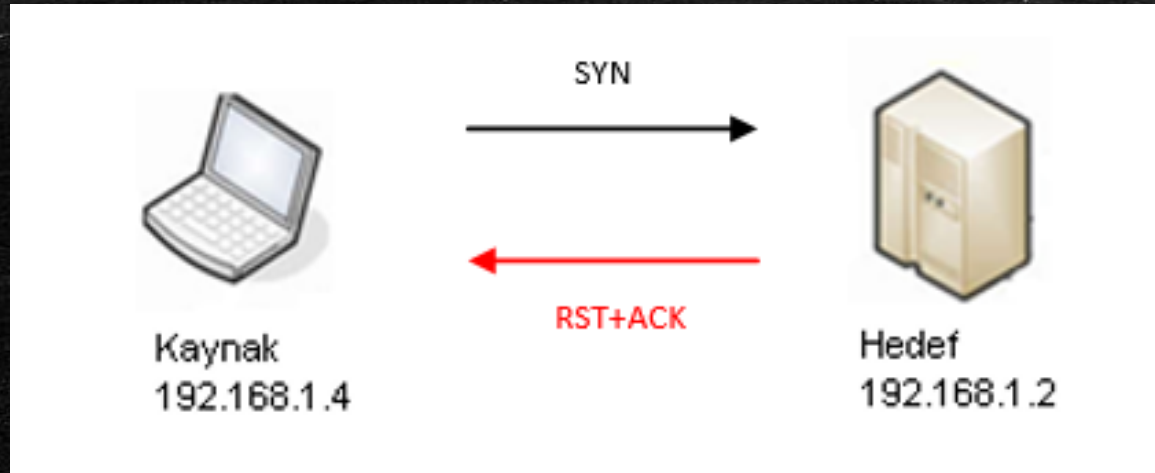
Tarama Türleri

🕒 nmap - -scanflags <TCP_Bayrağı> [Hedef_IP]

Nmap Scan	Command Syntax	Requires Privileged Access	Identifies TCP Ports	Identifies UDP Ports
TCP SYN Scan	-sS	YES	YES	NO
TCP connect() Scan	-sT	NO	YES	NO
FIN Scan	-sF	YES	YES	NO
Xmas Tree Scan	-sX	YES	YES	NO
Null Scan	-sN	YES	YES	NO
Ping Scan	-sP	NO	NO	NO
Version Detection	-sV	NO	NO	NO
UDP Scan	-sU	YES	NO	YES
IP Protocol Scan	-sO	YES	NO	NO
ACK Scan	-sA	YES	YES	NO
Window Scan	-sW	YES	YES	NO
RPC Scan	-sR	NO	NO	NO
List Scan	-sL	NO	NO	NO
Idlescan	-sI	YES	YES	NO
FTP Bounce Attack	-b	NO	YES	NO

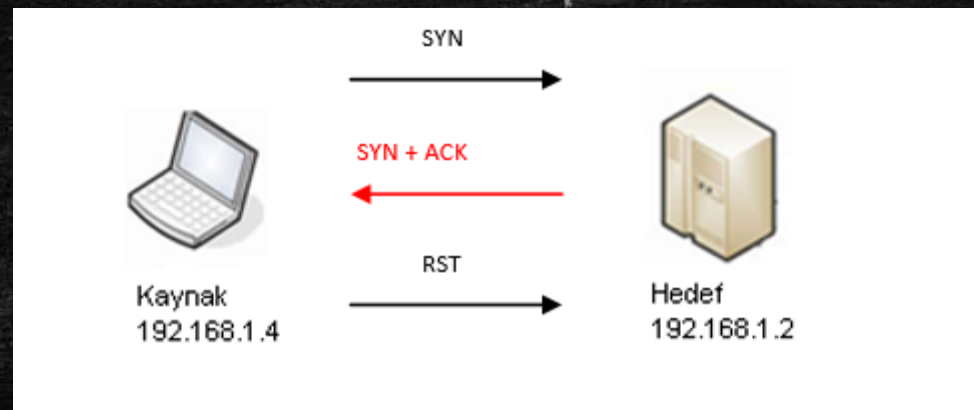
TCP Syn Scan

- ⌚ Kaynak makinanın hedef makinaya TCP SYN bayraklı paket göndererek başlattığı bu tarama türünde, tarama esnasında muhtemelen portların çoğu kapalı olacaktır. Kapalı olduğu durumlarda hedef makina RST + ACK bayraklı paket döndürür.



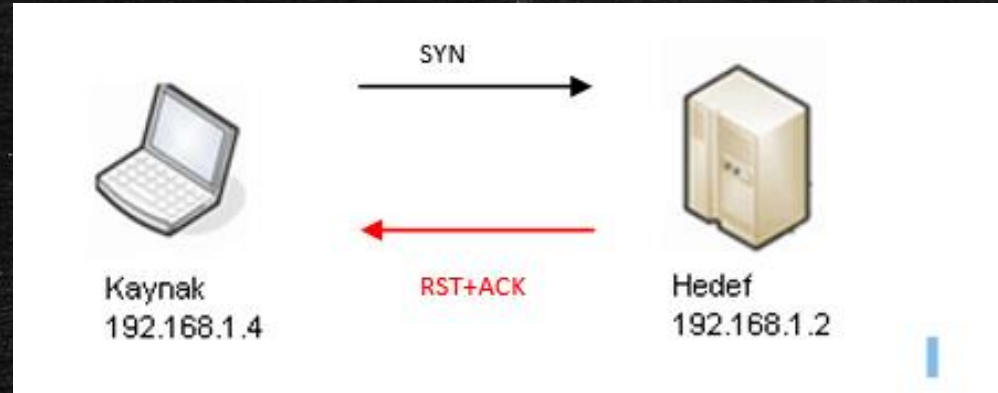
TCP Syn Scan

- ⌚ Açık olduğu durumda SYN + ACK bayraklı paket dönecektir. Kaynak makinada RST bayraklı paket göndererek bağlantıyı koparır ve böylelikle üçlü el sıkışma tamamlanmaz.
- ⌚ Bu taramayı gerçekleştirmek için aşağıdaki komut kullanılmalıdır
- ⌚ `#nmap -sS -v 192.168.1.2`



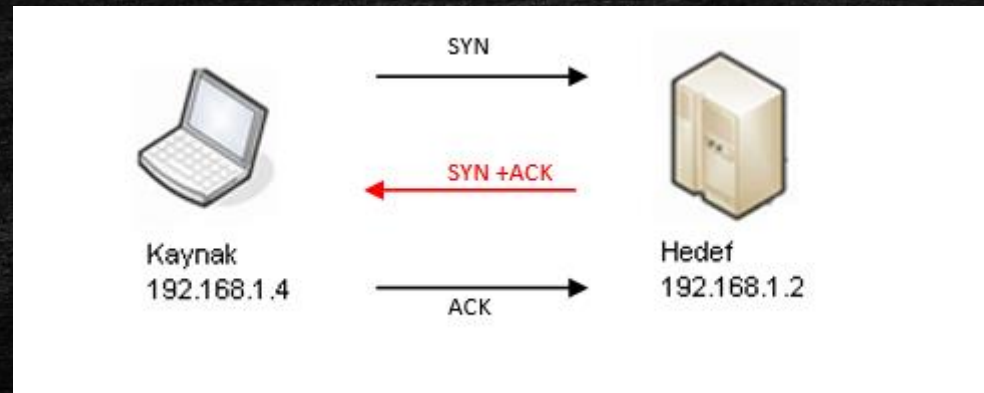
TCP Connect Scan

- ⌚ Kaynak makinanın gerçekleştireceği TCP Connect Scan, kapalı portlara yapıldığı zaman dönecek cevaplar TCP SYN Scan gibi olacaktır, RST + ACK bayraklı paket dönecektir .



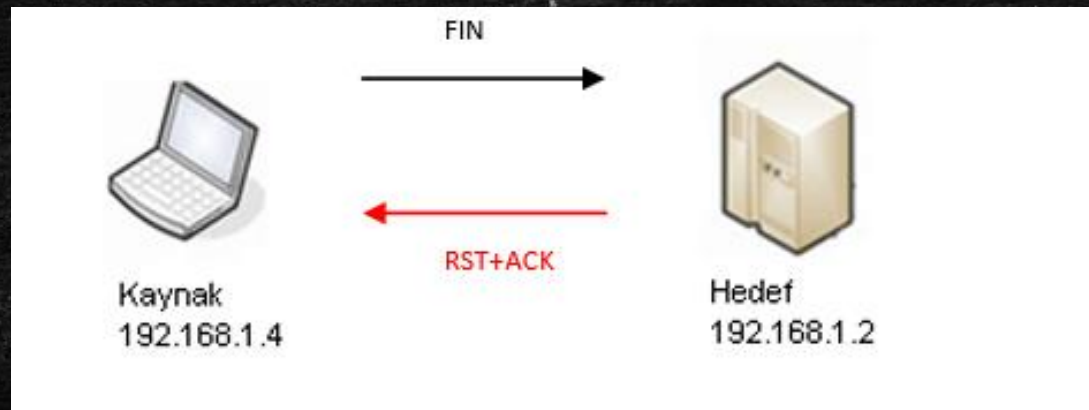
TCP Connect Scan

- ⌚ Ancak açık olduğu durumlarda TCP SYN Scan tersine, hedef makinanın göndereceği SYN + ACK bayraklı paketi, kaynak makina ACK bayraklı paket göndererek cevaplar ve üçlü el sıkışmayı tamamlar.
- ⌚ Bu taramayı gerçekleştirmek için aşağıdaki komut kullanılmalıdır
- ⌚ `#nmap -sT -v 192.168.1.2`



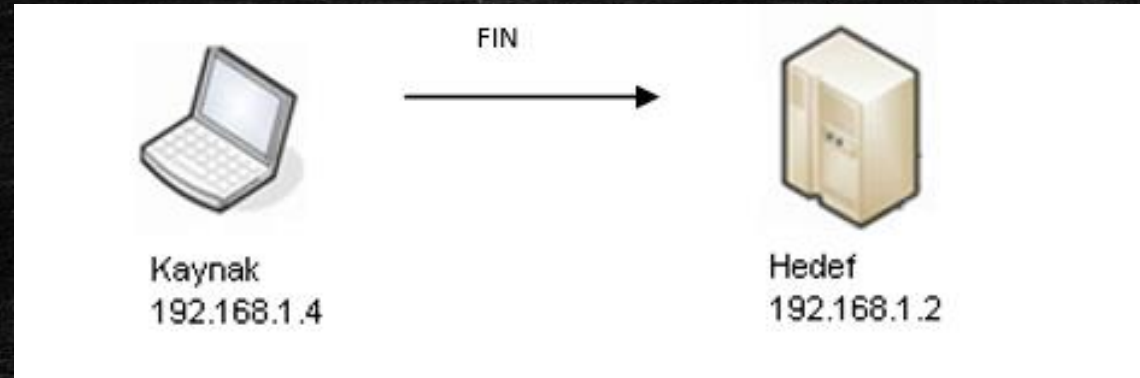
FIN Scan

- ⌚ FIN Scan ilişkin “saklı” frameler olağandışıdır çünkü hedef makinaya ilk TCP el sıkışması olmadan gönderilirler.
- ⌚ Kaynak makinanın göndereceği FIN bayraklı paket, hedef makinanın kapalı bir portuna gelirse hedef makina RST + ACK bayraklı paket döndürecektir .



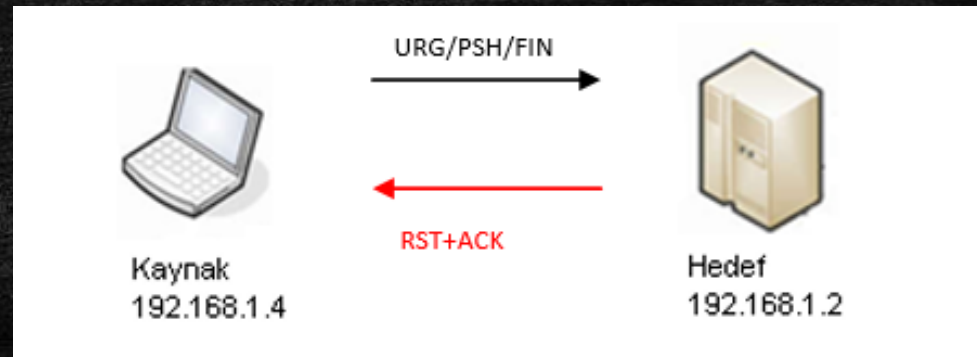
FIN Scan

- ⌚ Eğer port açık olursa hedef makinadan herhangi bir tepki dönmeyecektir .
- ⌚ Bu taramayı gerçekleştirmek için aşağıdaki komut kullanılmalıdır .
- ⌚ `#nmap -sF -v 192.168.1.2`



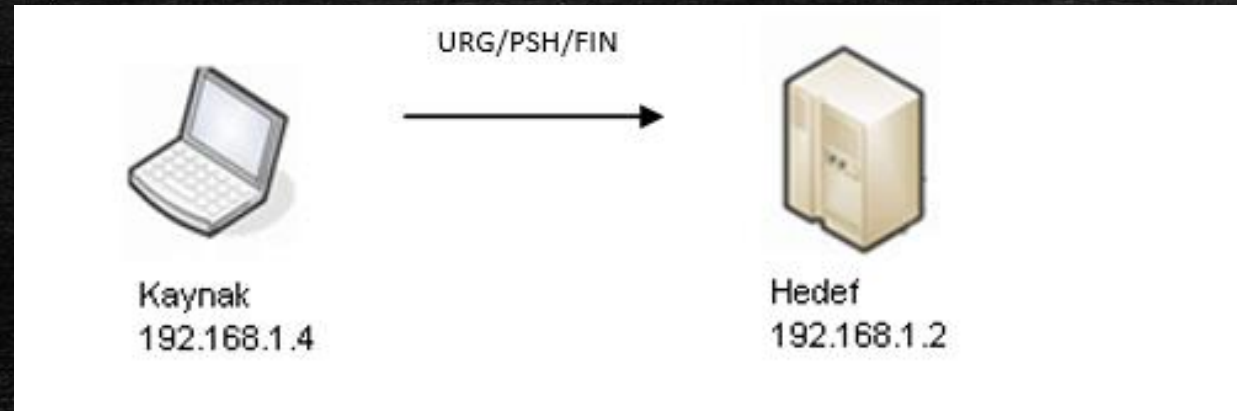
XMas Tree Scan

- ① Kaynak makinanın TCP frame içine URG, PSH ve FIN bayraklarını set edeceği paket hedef makinaya gönderilir. Hedef makinanın döndüreceği cevaplar FIN Scan ile aynıdır.
- ① Kaynak makinanın göndereceği URG,PSH ve FIN bayraklı paket, hedef makinanın kapalı bir portuna gelirse hedef makina RST + ACK bayraklı paket döndürecektir .



XMas Tree Scan

- ⌚ Eğer port açık olursa hedef makinadan herhangi bir tepki dönmeyecektir .
- ⌚ Bu taramayı gerçekleştirmek için aşağıdaki komut kullanılmalıdır .
- ⌚ `#nmap -sX -v 192.168.1.2`



Null Scan

- ⌚ Hiçbir bayrağın bulunmayacağı bu tarama türü, gerçek hayatta karşımıza çıkmayan bir durumdur. kaynak makinanın göndereceği bayraksız paketler karşısında hedef makinanın vereceği tepkiler FIN Scan ile aynıdır.
- ⌚ Kaynak makinanın göndereceği bayraksız paket, hedef makinanın kapalı bir portuna gelirse hedef makina RST + ACK bayraklı paket döndürecektir.
- ⌚ Eğer port açık olursa hedef makinadan herhangi bir tepki dönmeyecektir .
- ⌚ Bu taramayı gerçekleştirmek için aşağıdaki komut kullanılmalıdır.
- ⌚ `#nmap -sN -v 192.168.1.2`

Ping Scan

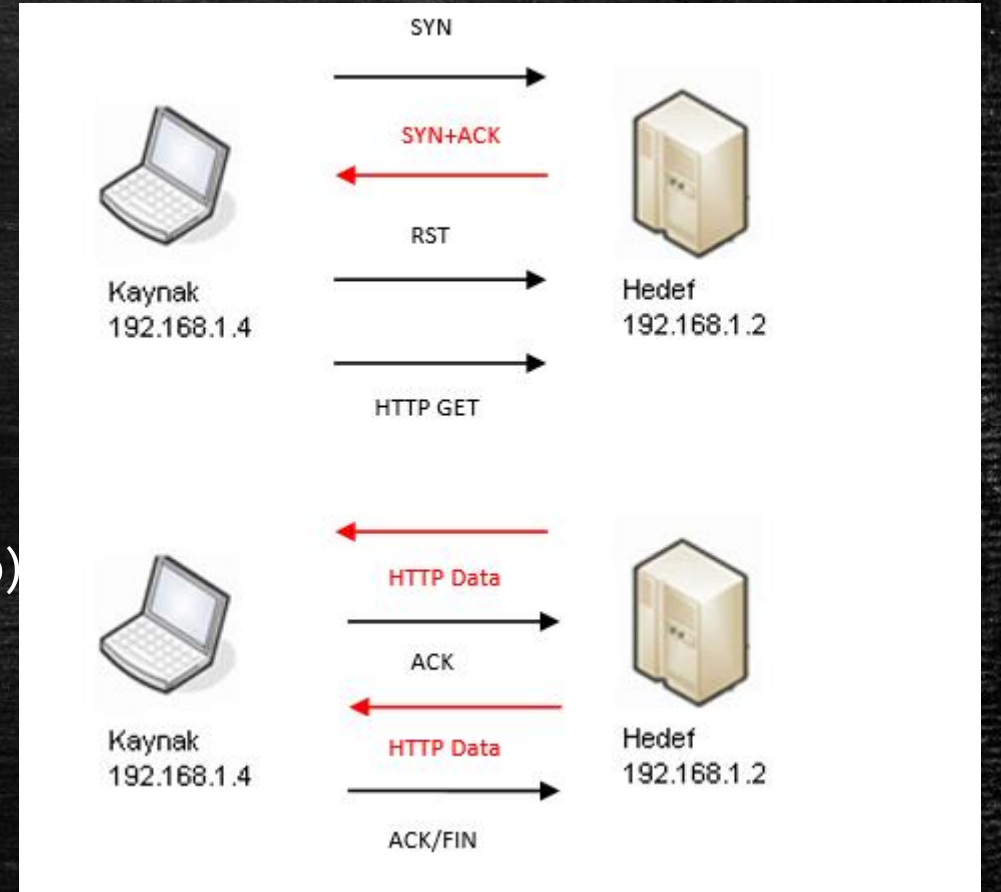
- ⌚ Kaynak makinanın hedef makinaya tek bir ICMP Echo istek paketi göndereceği bu tarama türünde, IP adresi erişilebilir ve ICMP filtreleme bulunmadığı sürece, hedef makina ICMP Echo cevabı döndürecektir.
- ⌚ Eğer hedef makina erişilebilir değilse veya paket filtreliyiçi ICMP paketlerini filtreliyorsa, hedef makinadan herhangi bir cevap dönmeyecektir .
- ⌚ Bu taramayı gerçekleştirmek için aşağıdaki komut kullanılmalıdır .
- ⌚ `#nmap -sP -v 192.168.1.2`

Version Detection

- ⌚ Version Detection, bütün portların bilgilerini bulabilecek herhangi bir tarama türü ile beraber çalışır. Eğer herhangi bir tarama türü belirtilmezse yetkili kullanıcılar (root, admin) için TCP SYN, yetkisiz kullanıcılar için TCP Connect Scan çalıştırılır.
- ⌚ Eğer açık port bulunursa, Version Detection Scan hedef makina üzerinde araştırma sürecini başlatır. Hedef makinanın uygulamalarıyla direkt olarak iletişime geçerek elde edebileceği kadar bilgiyi almaya çalışır.
- ⌚ Başlangıçta varsayılan olarak TCP SYN Scan yapıldığı ve cevaplarının döndüğünü kabul edersek, 80. Port üzerinde çalışan HTTP hakkında bilgi toplayacak olan Version Detection Scan gerçekleştireceği tarama işlemleri aşağıdaki gibidir .

Version Detection

- ⌚ Farklı port ve uygulamalarda işlem farklı olacaktır.
- ⌚ Bu taramayı gerçekleştirmek için aşağıdaki komut kullanılmalıdır.
- ⌚ `#nmap -sV -v 192.168.1.2`
- ⌚ PORT STATE SERVICE VERSION
- ⌚ 22/tcp open ssh OpenSSH 5.2 (protocol 2.0)
- ⌚ 53/tcp open domain dnsmasq 2.48
- ⌚ 80/tcp open http Apache httpd 2.2.13 ((Fedora))



UDP Scan

- ⌚ Kaynak makinanın göndereceği UDP paketine ICMP Port Unreachable cevabı döndüren hedef makina kapalı kabul edilecektir.
- ⌚ Herhangi bir tepki döndürmeyen hedef makina open | filtered (Bknz. Portların Taramalara Verebileceği Cevaplar) kabul edilecektir.
- ⌚ UDP paketiyle cevap döndüren hedef makinaya ait port açık kabul edilecektir.
- ⌚ Bu taramayı gerçekleştirmek için aşağıdaki komut kullanılmalıdır .
- ⌚ `#nmap -sU -v 192.168.1.2`

IP Protocol Scan

- ⌚ IP paketleriyle gerçekleştirilen bu taramada, erişilemeyen bir IP taramaya cevap vermeyecektir.
- ⌚ Erişilebilen bir IP ise protokol tipine mahsus olacak şekilde RST bayraklı paket döndürecektir .
- ⌚ Bu taramayı gerçekleştirmek için aşağıdaki komut kullanılmalıdır .
- ⌚ `#nmap -sO -v 192.168.1.2`

ACK Scan

- ⌚ Kaynak makinanın hedef makinaya TCP ACK bayraklı paket göndereceği bu tarama türünde, hedef makina tarafından ICMP Destination Unreachable mesajı dönerse yada herhangi bir tepki oluşmazsa port “filtered” olarak kabul edilir.
- ⌚ Eğer hedef makina RST bayraklı paket döndürürse port “unfiltered” kabul edilir.
- ⌚ Bu taramayı gerçekleştirmek için aşağıdaki komut kullanılmalıdır.
- ⌚ `#nmap -sA -v 192.168.1.2 -p 80`

Window Scan

- ⌚ -Window Scan, ACK Scan türüne benzer ancak bir önemli farkı vardır. Window Scan portların açık olma durumlarını yani "open" durumlarını gösterebilir. Bu taramanın ismi TCP Windowing işleminden gelmektedir. Bazı TCP yığınları, RST bayraklı paketlere cevap döndüreceği zaman, kendilerine mahsus window boyutları sağlarlar.
- ⌚ Hedef makineye ait kapalı bir porttan dönen RST frame ait window boyutu sıfırdır (0) .
- ⌚ Hedef makineye ait açık bir porttan dönen RST frame ait window boyutu sıfırdan farklı olur .
- ⌚ Bu taramayı gerçekleştirmek için aşağıdaki komut kullanılmalıdır
- ⌚ `#nmap -sW -v 192.168.1.2`

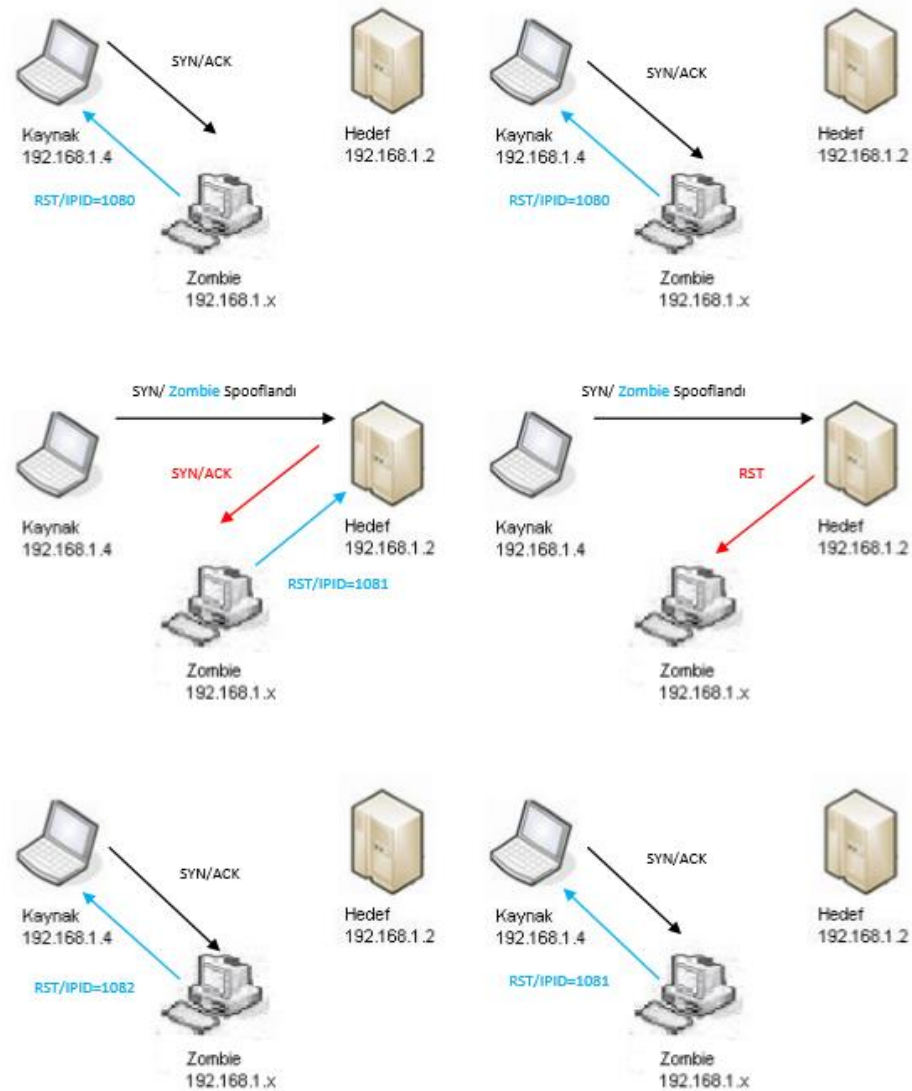
RPC Scan

- ⌚ RPC Scan, hedef makina üzerinde kořan RPC uygulamalarını keřfeder. Bařka bir tarama tőrü ile aık portlar keřfedildikten sonra, RPC Scan hedef makinanın aık portlarına RPC null gōndererek, eęer alıřan bir RPC uygulaması varsa, RPC uygulamasını harekete geirir. RPC Scan, Version Detection Scan iřlemi esnasında otomatik olarak alıřtırılır.
- ⌚ Bu taramayı gerekleřtirmek iin ařaęıdaki komut kullanılmalıdır :
- ⌚ `#nmap -sR -v 192.168.1.2`

IdleScan

- ⌚ Kaynak makinanın hedef makinayı tarama esnasında aktif olarak rol almadığı bir türdür. Kaynak makina “zombie” olarak nitelendirilen makinalar üzerinden hedef makinayı tarayarak bilgi toplar .
- ⌚ Bu taramayı gerçekleştirmek için aşağıdaki komut kullanılmalıdır .
- ⌚ `nmap -sl -v [Zombie_IP] [Hedef_IP]`

IdleScan



FTP Bounce Scan

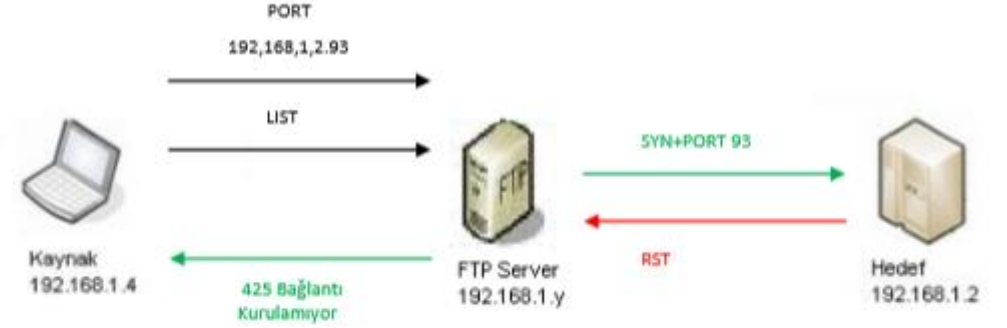
- ⌚ FTP Bounce Scan, FTP Serverlerinin pasif olarak çalışması ile gerçekleştirilir. Pasif moddaki FTPde, komut bağlantıları ile veriler tamamen ayrıdır. FTP Serverlar dışarıya veri bağlantıları kurduğu için FW ile uyumlu çalışması gerekir. Bunun dışında, herhangi bir kullanıcı bir veriyi tamamen farklı bir hedefe gönderebilir.
- ⌚ Nmapin taramayı gerçekleştirebilmesi için, aradaki adam olacak olan FTP Serverla bağlantı kurması gerekir. Bağlantı kurulduktan sonra Nmap verileri taranacak olan hedef IP ve porta yönlendirir.
- ⌚ Yönlendirme işleminden sonra FTP üzerinde taramayı gerçekleştirebilmek için öncelikle PORT komutu, daha sonra verileri aktarabilmek için LIST komutu çalıştırılır.
- ⌚ Kapalı portta bağlantı sağlanamazken, açık portta sağlanır .

FTP Bounce Scan

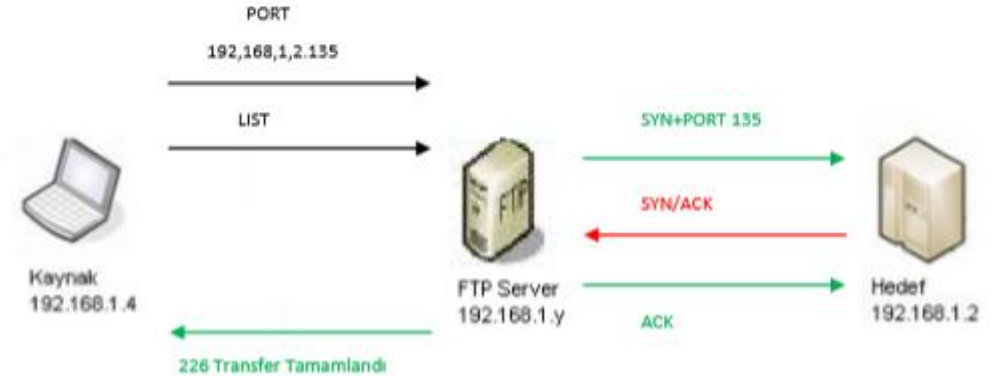
⌚ Bu taramayı gerçekleştirmek için aşağıdaki komut kullanılmalıdır :

⌚ `nmap -b -v [user@ftpserver] [Hedef_IP]`

HEDEF KAPALI DURUMDA



HEDEF AÇIK DURUMDA



Nmap Ping Seçenekleri

- ① Nmap taramaya başlamadan önce hedef makinayı mutlaka pingler. Ping işlemi, ICMP Echo isteği ve ardından 80. Porta TCP ACK bayraklı paketin gönderilmesinden oluşur. Eğer hedef makina ping işlemine cevap vermezse, Nmap diğer hedefe geçer. Eğer başka hedef yoksa tarama biter.
- ① Network dünyasında bilinen ping işlemi, ICMP Echo isteği gönderilir ve ICMP Echo cevabı döndürülerek gerçekleşir. Ancak Nmapin ping işlemi biraz daha kendine özgüdür. Nmap dünyasındaki pingi hedef makinanın cevap döndürebileceği herhangi bir istek olarak nitelendirilebilir.

Nmap Ping Seçenekleri

- ICMP Echo Request ve TCP ACK Ping
 - Kaynak makina hedef makinaya aynı anda ICMP Echo isteği ve TCP ACK bayraklı paket gönderir ve aşağıdakilerin dönmesi bekler :
 - TCP RST ve ICMP Echo Reply
 - `nmap -PB [Hedef_IP]`
- ICMP Echo Request Ping
 - Kaynak makina hedef makinaya ICMP Echo isteği gönderir. Eğer herhangi bir cevap dönmezse makina kapalıdır veya "filtered" olarak kabul edilir.
 - `nmap -PE [Hedef_IP]`

Nmap Ping Seçenekleri

- TCP ACK Ping
 - Kaynak makinanın hedef makinaya göndereceği TCP ACK bayraklı pakete gelen cevap RST bayraklı paket olursa hedef makina açıktır. Herhangi bir cevap dönmezse makina kapalıdır. TCP ACK ping ile TCP ACK Scan sonuçları birbirine benzer çıkabilir.
 - `nmap -PA [Hedef_IP]`
- TCP SYN Ping
 - TCP SYN Scan ile benzerlik taşıyan bu seçenekte, kaynak makina hedef makinaya TCP SYN bayraklı paket gönderir. Eğer hedef makina açıksa SYN + ACK bayraklı paket, kapalıysa RST bayraklı paket döndürecektir.
 - `nmap -PS [Hedef_IP]`

Nmap Ping Seçenekleri

- UDP Ping
 - Kaynak makinanın hedef makinaya tek bir UDP paketi göndereceği bu seçenekte, eğer hedef makina açıksa ICMP Port Unreachable mesajı geri dönecektir.
 - Eğer herhangi bir cevap dönmezse hedef makina erişilebilir değildir denilebilir, ancak çoğu UDP uygulamaları herhangi bir cevap döndürmediğinden, bu sonuç doğru olmayabilir. Bu yüzden kapalı olduğu bilinen bir porta bu işlem uygulanarak test edilmelidir
 - `nmap -PU [Hedef_IP]`

Nmap Ping Seçenekleri

- Don't Ping Before Scanning
 - Bu seçenekler Nmap taramalardan önceki “ping” işlemini gerçekleştirmez ve direkt tarama işlemini gerçekleştirir. Yinede reverse DNS sorgusu aktif halde bulunur.
 - `nmap -PO [Hedef_IP]`
- Require Reverse DNS
 - Bu seçenekle, Nmap IP-Hostname eşleşmesi sürecini gerçekleştirmez ve direkt olarak tarama işlemine geçer. Bu şekilde daha fazla zaman kazanılır.
 - `nmap -n [Hedef_IP]`

Nmap Ping Seçenekleri

- Ping Scan (Disable Port Scan)
 - Bu seçenek ile Nmap sadece ping işlemi gerçekleştirir ve hedef makinanın açık olup olmadığını bildirir. Tarama işlemi gerçekleştirilmez.
 - `nmap -sn [Hedef_IP]`
- Treat all hosts as online
 - Bu seçenek ile filtered olarak görülen bütün portlar open konumunda ele alınacaktır.
 - `nmap -Pn [Hedef_IP]`

OS İzi Belirleme

- OS izi belirleme işlemi başlamadan önce, Nmap sırasıyla ping ve scan işlemlerini gerçekleştirir. Nmap tarama esnasında hedef makinanın portlarını open, closed, filtered olarak kategorize eder.
- Bu işlem OS izi belirlemede çok önemlidir çünkü sorgular esnasında hem kapalı hemde açık portlar ele alınarak bir sonuç belirlenir.
- Açık ve kapalı portlar belirlendikten sonra, OS izi belirleme işlemine geçilir. Bu işlem OS araştırması, TCP el sıkışma serileri ile devam eder. El sıkışma serileri ile TCP uptime, TCP sequence ve IPID tahminleri gerçekleştirilir.
- Gönderilen herhangi bayraklı paketlere verilen cevaplar, ttl değerleri ve yukarıda bahsedilen seçenekler sonucunda Nmap OS izi ile ilgili bir tahminde bulunacaktır.
- `#nmap -O 192.168.1.2`

Os İzi Belirleme Seçenekleri

- `--osscan-limit` : En az bir açık ve bir kapalı portu bulunan hedeflerin OS izini belirlemeye çalışır.
- `--osscan-guess` : Daha agresif bir şekilde belirleme yapar.
- `--max-retries <sayı>` : Belirtilen <sayı> miktarında OS izi belirleme denemesi yapar.

Nmap Script Motoru

(Nmap Scripting Engine – NSE)

- NSE, varolan Nmap yeteneklerini geliştirmek ve Nmap dahilindeki formatlarla çıktı alabilmek için kullanılan bir yapıdır. NSE scriptlerinin içerdiği bazı örnekler aşağıdaki gibidir.
- Geliştirilmiş Ağ Keşfi : Whois lookup istekleri ve ek protokol sorguları gerçekleştirir. Ayrıca erişilebilir network paylaşımları gibi dinlenen servislerden bilgi toplamak amacıyla istemci gibi davranır.
- Geliştirilmiş Versiyon Keşfi : Karmaşık versiyon araştırmaları yapar ve servislere brute force saldırısı düzenler.
- Zafiyet Keşfi : Özel zafiyetlerin kontrolü amacıyla araştırma yapar.
- Zararlı Yazılım Keşfi : Virus, worm ve trojan gibi zararlı yazılımların bulunması amacıyla araştırmalar yapar.
- Zafiyeti Kullanmak : Bulunan zafiyetleri kullanmak amacıyla scriptleri çalıştırır.

Nmap Script Motoru (Nmap Scripting Engine – NSE)

- ⌚ Varsayılan olarak, Version Scanning (-sV) versiyon kategorisinde bulunan bütün NSE scriptlerini çalıştırır. -A özelliği ise, -sC (güvenli ve izinsiz giriş kategorileri) seçeneğini çalıştırır.
- ⌚ NSE scriptleri Lua script dilinde yazılır ve .nse uzantısına sahiptir ve Nmap ana dizinin altında "scripts" dizininde saklanırlar. Bununla birlikte "script.db" Nmap ana dizinin altında bulunur ve bütün scriptleri kategorileriyle (Güvenli, Zorla Giriş, Zararlı Yazılım, Arka Kapı, Versiyon, Keşif, Zafiyet) saklar. NSE, scripti çalıştırmadan önce hedefteki makinanın, Nmap çıktılarına dayanarak, gerekli kriterleri karşılayıp karşılamadığını araştırır. Bu araştırmadan sonra scriptin çalışmasına karar verir.
- ⌚ NSE kullanmanın en çabuk yolu aşağıdaki gibidir.
- ⌚ `nmap -sC 192.168.1.0/24`

Nmap Script Motoru

(Nmap Scripting Engine – NSE)

- Yukarıdaki seçenek vasıtasıyla NSE bütün Güvenli ve Zorla Giriş scriptlerinin çalıştıracaktır. Eğer daha özel bir scriptin çalıştırılması istenirse - - script seçeneği kullanılarak istenilen bir kategoriye ait scriptler çalıştırılabilir :
 - `nmap --script=vulnerability 192.168.1.34`
- Sadece tek bir script çalıştırılmak istenirse aşağıdaki seçenek kullanılmalıdır
 - `nmap --script=promiscuous.nse 192.168.1.0/24`
- Belirli bir dizinin altındaki scriptleri çalıştırmak istenirse aşağıdaki seçenek kullanılmalıdır :
 - `nmap --script=/my-scripts 192.168.1.0/24`
- Bütün scriptlerin çalışması istenirse aşağıdaki seçenek kullanılmalıdır :
 - `nmap --script=all 192.168.1.55`

NSE Seçenekleri

- `--script-args=<n1=v1*,n2=v2,...+>` : Varolan script değerlerinin yerine belirlenen yeni değerler atanır.
- `--script-trace` : Scripte ait bütün iç ve dış iletişimin çıktısını gösterir.
- `--script-updatedb` : Scriptlerin bulunduğu veritabanını günceller.

Güvenlik Ürünleri ve Nmap

- Nmap, taranılacak olan hedeflerin önünde bulunan güvenlik ürünlerinin kısıtlaması nedeniyle, istenilen şekilde tam olarak çalışamayabilir.
- Günümüzdeki güvenlik ürünleri Nmap ve taramalarını rahatlıkla yakalayabiliyor. Ancak Nmap kendi bünyesinde bulunan bazı seçenekler vasıtasıyla bu güvenlik ürünlerini atlatabilir.
- Fragmentasyon, spoofing ve packet manipulating seçenekleri vasıtasıyla Nmap güvenlik ürünlerini atlatıp, taramalarını daha rahat bir şekilde gerçekleştirebilir.

Fragmentation

- Nmap ile fragmantasyon yapılmak istenirse, -f, -f -f veya - -mtu seçenekleri kullanılmalıdır. Eğer parçalanmak istenilen paketin maksimum boyutu, IP başlık bilgisinden sonra, 8 byte olması isteniyorsa aşağıdaki komut kullanılmalıdır :
 - `nmap -f [Hedef_IP]`
- Eğer parçalanmak istenilen paketin maksimum boyutu, IP başlık bilgisinden sonra, 16 byte olması isteniyorsa aşağıdaki komut kullanılmalıdır :
 - `nmap -f -f [Hedef_IP]`
- Eğer parçalanmak istenilen paketin maksimum boyutu, IP başlık bilgisinden sonra, el ile girilerek belirlenmek isteniyorsa aşağıdaki komut kullanılmalıdır :
 - `nmap - -mtu <Sayı> [Hedef_IP]`

Spoofing

- Fragmentasyon seçeneğinin güvenlik ürünleri tarafından yüksek oranla yakalanması yüzünden diğer bir atlatma türü olan spoofing tercih edilebilir.
- Nmap Decoy Scan (-D), tercih edilen Nmap taramasının bir makinadan değil, belirtilecek olan makinalardan da yapılmış gibi göstererek yakalanma riskini düşürür. Belirtilecek olan makinaların IP'leri taramanın yapılacağı ortamla uyumlu olması çok önemlidir.
- Private IP kullanılan LAN ortamın Reel IP ile tarama yapılması pek akıllıca olmayacaktır. Eğer IP'ler belirtilmezse Nmap rastgele olarak IP'ler seçecektir.
- Ancak bu IP'lerin Reel IP olma olasılığı var ve yukarıda bahsedilen durumun aynısı oluşabilir. Spoofing işleminin yapılması için kullanılması gereken komut aşağıdaki gibidir :
- `nmap -D < [Spooflanan_IP] > [Hedef_IP]`

Spoofing

- Eğer geleneksel spoof yöntemi kullanılmak istenirse aşağıdaki komut kullanılmalıdır. Ancak geleneksel yöntemle gönderilen paketlerin cevapları taramanın yapıldığı makinaya geri dönmeyecektir. Aynı zamanda bu yöntemi Nmapin ethernet kart arayüzünün IP adresini bulamadığı durumlarda -e parametresi ile beraber kullanarak IP adresi atanabilir. Buradaki -e parametresi interface ismini belirtir.
- `nmap -S <[Spooflanan_IP]> [Hedef_IP]`
- `nmap -S <[Spooflanan_IP]> -e [interface] [Hedef_IP]`

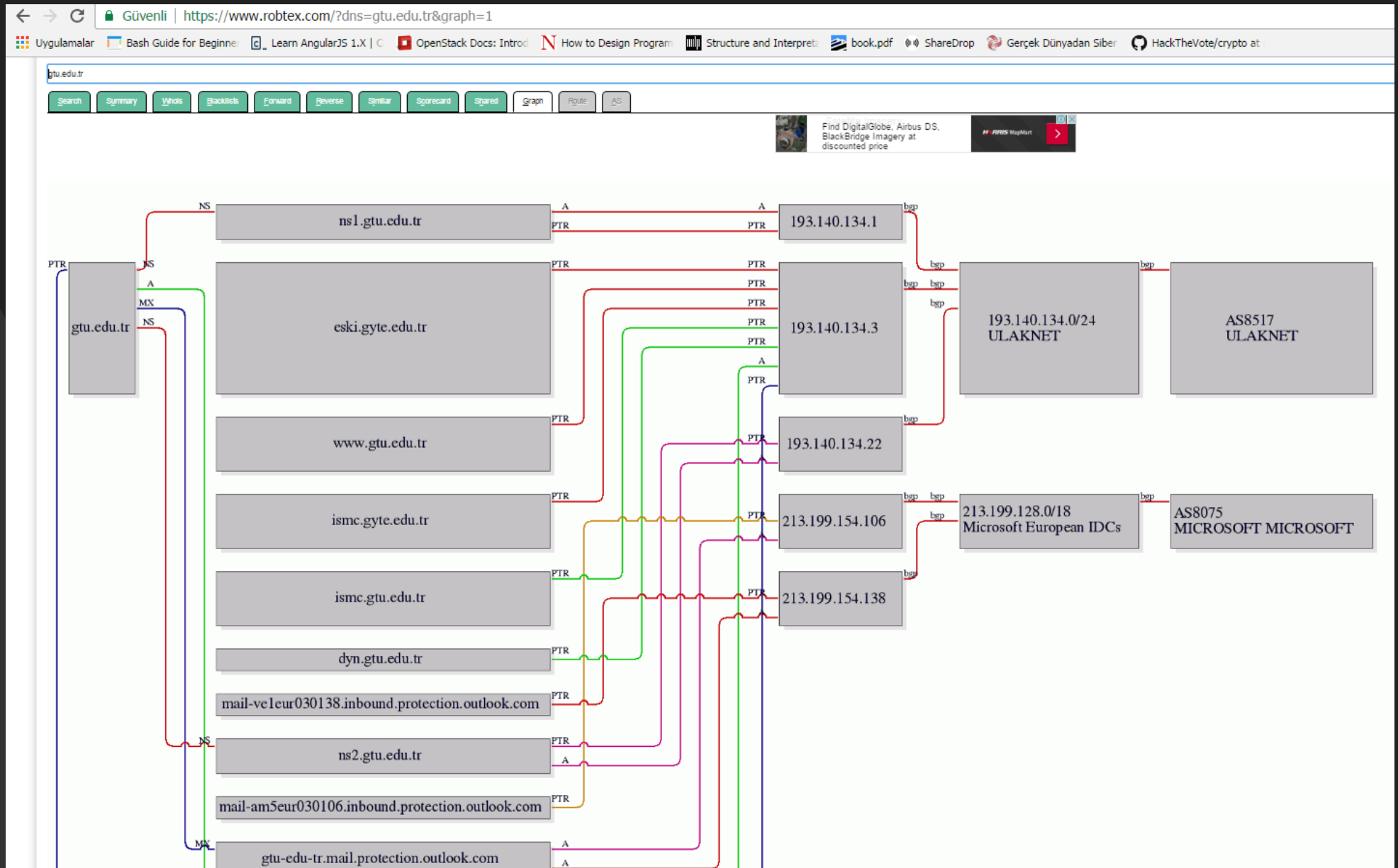
Spoofing

- Diğer bir spoofing yöntemi ise MAC adresleri. Nmap paketlerinin içerisinde farklı MAC adresleri bulunması sağlanabilir. Bütün bir MAC adresi girilebileceği gibi bir vendor ismi veya vendor prefixi de girilebilir. Eğer () şeklinde yazılırsa Nmap MAC adresini kendisi belirler. MAC spoofing için aşağıdaki komutlar kullanılmalıdır :
 - `nmap --spoof-mac 11:22:33:44:55:66 192.168.1.0/24`
 - `nmap --spoof-mac 000D93 192.168.1.0/24`
 - `nmap --spoof-mac D-Link 192.168.1.0/24`
- Son olarak kaynak port için spoofing kullanılabilir. Bu işlem için aşağıdaki komut kullanılmalıdır :
 - `nmap -g 53 192.168.1.0/24`
 - `nmap --source-port 53 192.168.1.0/24`

Packet Manipulating

- Güvenlik ürünlerini atlatmak için, Nmap çok fazla sayıda packet manipulating özelliği barındırır. Aşağıda bu özellikler ve açıklamaları bulunmaktadır :
 - `--data-length <sayı>` : Paket boyutunun olacağı uzunluğu <sayı> belirtir.
 - `--ip-options <R|T|U|S *IP IP2...+ |L *IP IP2 ...+ >` yada `--ip-options <hex string>` : Paketler içerisindeki IP özelliklerini belirtir.
 - `--ttl <değer>` : Paketin kaç routerda yönlendirilmesi isteniyorsa girilir.
 - `--randomize-hosts` : Listede belirtilen taranılacak hostları rastgele bir şekilde seçer.
 - `--badsum` : Yanlış checksuma sahip TCP veya UDP paketleri gönderir.

Robtex



Wireshark

Ralink Technology Inc. (Microsoft's Packet Scheduler) : Capturing - Wireshark

File Edit View Go Capture Analyze Statistics Help

Filter:

Current Wireless Interface: None 802.11 Channel: FC5 Filter: Decryption Mode: Wireless Settings... Decryption Keys...

No.	Time	Source	Destination *	Protocol	Info
56	6.565943	192.168.1.2	80.93.212.86	TCP	1857 > http [FIN, ACK] Seq=8 Ack=29686 win=63556 Len=0
55	6.527297	192.168.1.2	80.93.212.86	TCP	1857 > http [ACK] Seq=8 Ack=29686 win=63556 Len=0
53	6.521441	192.168.1.2	80.93.212.86	TCP	1857 > http [ACK] Seq=8 Ack=28981 win=64260 Len=0
50	6.498083	192.168.1.2	80.93.212.86	TCP	1857 > http [ACK] Seq=8 Ack=26461 win=64260 Len=0
48	6.486681	192.168.1.2	80.93.212.86	TCP	1857 > http [ACK] Seq=8 Ack=25201 win=64260 Len=0
45	6.463445	192.168.1.2	80.93.212.86	TCP	1857 > http [ACK] Seq=8 Ack=22681 win=64260 Len=0
43	6.452057	192.168.1.2	80.93.212.86	TCP	1857 > http [ACK] Seq=8 Ack=21421 win=64260 Len=0
40	6.428705	192.168.1.2	80.93.212.86	TCP	1857 > http [ACK] Seq=8 Ack=18901 win=64260 Len=0
38	6.416944	192.168.1.2	80.93.212.86	TCP	1857 > http [ACK] Seq=8 Ack=17641 win=64260 Len=0
35	6.393781	192.168.1.2	80.93.212.86	TCP	1857 > http [ACK] Seq=8 Ack=15121 win=64260 Len=0
33	6.382065	192.168.1.2	80.93.212.86	TCP	1857 > http [ACK] Seq=8 Ack=13861 win=64260 Len=0
30	6.359078	192.168.1.2	80.93.212.86	TCP	1857 > http [ACK] Seq=8 Ack=11341 win=64260 Len=0

Genel Protokol Bilgisi

Internet Protocol, Src: 192.168.1.2 (192.168.1.2), Dst: 80.93.212.86 (80.93.212.86)

- Version: 4
- Header length: 20 bytes
- Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
 - 0000 00.. = Differentiated Services Codepoint: Default (0x00)
 - 00.. = ECN-Capable Transport (ECT): 0
 - 00.. = ECN-CE: 0
- Total Length: 40
- Identification: 0x31a2 (12706)
- Flags: 0x04 (Don't Fragment)
 - 0... = Reserved bit: Not set
 - 1... = Don't fragment: Set
 - ..0. = More fragments: Not set
- Fragment offset: 0
- Time to live: 222
- Protocol: TCP (0x06)
- Header checksum: 0x84cf [correct]
 - [Good: True]
 - [Bad: False]
- Source: 192.168.1.2 (192.168.1.2)
- Destination: 80.93.212.86 (80.93.212.86)

Protokol Detayı

Transmission Control Protocol, Src Port: 1857 (1857), Dst Port: http (80), Seq: 8, Ack: 29686, Len: 0

- Source port: 1857 (1857)
- Destination port: http (80)
- Sequence number: 8 (relative sequence number)
- Acknowledgement number: 29686 (relative ack number)
- Header length: 20 bytes
- Flags: 0x11 (FIN, ACK)
 - 0... .. = Congestion window Reduced (CWR): Not set
 - ..0. = ECN-Echo: Not set
 - ..0. = Urgent: Not set
 - ...1 = Acknowledgment: Set
 - 0... .. = Push: Not set

Wireshark: Capture from Ralink Technolo...

Captured Packets	Total	% of total
SCTP	0	0,0%
TCP	57	100,0%
UDP	0	0,0%
ICMP	0	0,0%
ARP	0	0,0%
OSPF	0	0,0%
GRE	0	0,0%
NetBIOS	0	0,0%
IPX	0	0,0%
VINES	0	0,0%
Other	0	0,0%

Running 00:01:20

Help Stop

Don't fragment (ip.flags.df), 1 byte

P: 57 D: 57 M: 0

Capture Filter. Yakalanacak paketlerin türü portu protokol bilgisi önceden belirtilerek hedef odaklı bir paket analizi yapılabilir.

Wireshark

The image displays the Wireshark network protocol analyzer interface. The main window shows a list of captured packets with columns for No., Time, Source, Destination, Protocol, Length, and Info. The first five packets are TCP connections related to an FTP session.

Overlaid on the main window is the "Wireshark: Capture Options" dialog box. This dialog is used to configure the capture process. It includes a table of capture interfaces and several checkboxes for capture settings.

Capture	Interface	Link-layer header	Prom. Mode	Snaplen [B]	Buffer [MB]	Mon. Mode	Capture Filter
<input checked="" type="checkbox"/>	Wi-Fi: en0 fe80::22c9:d0ff:fe86:5691 192.168.2.7	Ethernet	enabled	default	2	disabled	tcp port 21
<input type="checkbox"/>	p2p0	Raw IP	enabled	default	2	n/a	
<input type="checkbox"/>	Loopback: lo0 fe80::1 127.0.0.1	BSD loopback	enabled	default	2	n/a	

Below the table, the following options are visible:

- ☐ Capture on all interfaces
- ☒ Use promiscuous mode on all interfaces
- ☒ Capture Filter: tcp port 21
- ☐ Capture on all interfaces
- ☐ Use promiscuous mode on all interfaces

The "Capture Filter" field is highlighted with a red box, and a red arrow points from the text "Capture Filter" in the main window's filter bar to this field.

At the bottom of the dialog, there are sections for "Capture Files" and "Display Options".

Capture Files:

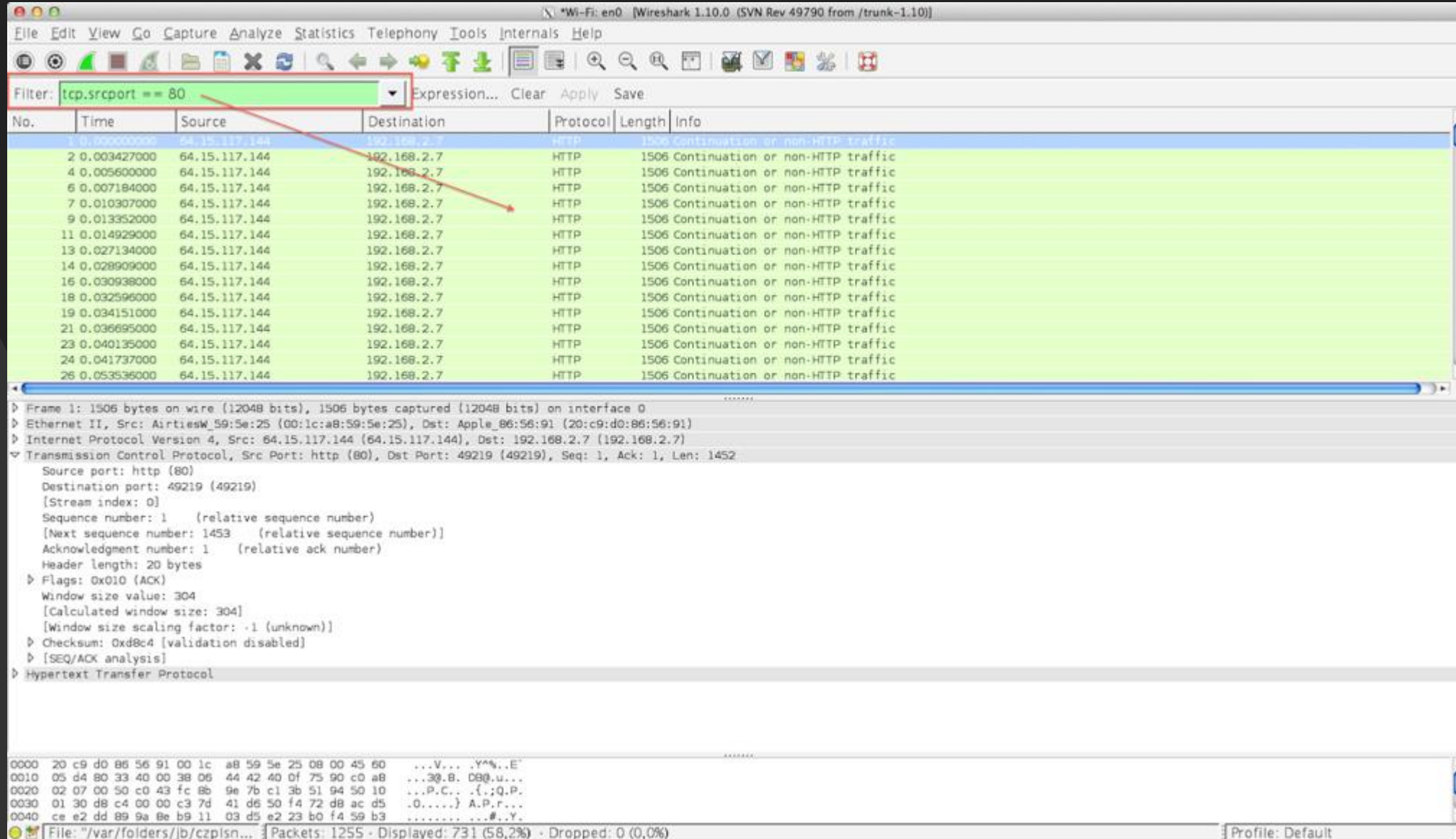
- File: [] Browse...
- ☐ Use multiple files
- ☒ Use pcap-ng format
- ☒ Next file every 1 megabyte(s)
- ☐ Next file every 1 minute(s)
- ☐ Ring buffer with 2 files
- ☐ Stop capture after 1 file(s)
- Stop Capture Automatically After... 1 packet(s)

Display Options:

- ☒ Update list of packets in real time
- ☒ Automatically scroll during live capture
- ☒ Hide capture info dialog
- ☒ Resolve MAC addresses
- ☐ Resolve network-layer names

Display Filter. Yakalanan paketlerin içerisinde istenilen özelliklerdeki paketlerin ayıklanması kısmında kullanılabilir.

Wireshark



The screenshot shows the Wireshark network protocol analyzer interface. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Tools, Internals, and Help. Below the menu is a toolbar with various icons for packet capture and analysis. The filter bar at the top displays the expression `tcp.srcport == 80`, which is highlighted with a red box. A red arrow points from this filter bar to the 'Info' column of the packet list. The packet list table shows 26 captured packets, all of which are HTTP continuation requests from source IP 64.15.117.144 to destination IP 192.168.2.7 on port 80. The selected packet (No. 1) is expanded in the bottom pane, showing the following details:

- Frame 1: 1506 bytes on wire (12048 bits), 1506 bytes captured (12048 bits) on interface 0
- Ethernet II, Src: AirtiesW_59:5e:25 (00:1c:a8:59:5e:25), Dst: Apple_86:56:91 (20:c9:d0:86:56:91)
- Internet Protocol Version 4, Src: 64.15.117.144 (64.15.117.144), Dst: 192.168.2.7 (192.168.2.7)
- Transmission Control Protocol, Src Port: http (80), Dst Port: 49219 (49219), Seq: 1, Ack: 1, Len: 1452
 - Source port: http (80)
 - Destination port: 49219 (49219)
 - [Stream index: 0]
 - Sequence number: 1 (relative sequence number)
 - [Next sequence number: 1453 (relative sequence number)]
 - Acknowledgment number: 1 (relative ack number)
 - Header length: 20 bytes
 - Flags: 0x010 (ACK)
 - Window size value: 304
 - [Calculated window size: 304]
 - [Window size scaling factor: -1 (unknown)]
 - Checksum: 0xd8c4 [validation disabled]
 - [SEQ/ACK analysis]
- Hypertext Transfer Protocol

The bottom status bar indicates the current file is `/var/folders/jb/czplsn...`, with 1255 packets captured, 731 displayed (58.2%), and 0 dropped (0.0%). The profile is set to 'Default'.

Kelime arama . İzlenen trafik içerisinde kelime arama;

Wireshark

The image shows the Wireshark network protocol analyzer interface. The main window displays a list of captured packets. A red arrow points from the word 'berbergokmen' in the search dialog to the same word in the packet list, specifically in the 'Info' column of packet 264.

Wireshark: Find Packet

Find By: ☐ Display filter ☐ Hex value ☒ String

Filter: **berbergokmen**

Search In: ☐ Packet list ☐ Packet details ☒ Packet bytes

String Options: ☐ Case sensitive, Character width: **Narrow & wide**

Direction: ☐ Up ☒ Down

Packet List:

No.	Time	Source	Destination	Protocol	Length	Info
257	4.504274000	192.168.2.7	173.194.39.206	TLSv1	107	Encrypted Handshake Message
258	4.504451000	192.168.2.7	173.194.39.206	TLSv1	1203	Application Data
259	4.537153000	173.194.39.206	192.168.2.7	TCP	66	https > 49714 [ACK] Seq=134 Ack=226 Win=42368 Len=0 TSval=1573130431 TSecr=871760693
260	4.590256000	173.194.39.206	192.168.2.7	TCP	66	https > 49714 [ACK] Seq=134 Ack=1363 Win=42304 Len=0 TSval=1573130485 TSecr=871760693
261	4.606608000	173.194.39.206	192.168.2.7	TLSv1	505	Application Data
262	4.606756000	192.168.2.7	173.194.39.206	TCP	66	49714 > https [ACK] Seq=1363 Ack=573 Win=131296 Len=0 TSval=871760794 TSecr=1573130500
263	4.870551000	Apple_86:56:91	Broadcast	ARP	42	Who has 6.6.6.254? Tell 6.6.6.113
264	4.893195000	192.168.2.7	8.8.8.8	DNS	76	Standard query 0xa2a2 A berbergokmen.com
265	5.005994000	8.8.8.8	192.168.2.7	DNS	128	Standard query response 0xa2a2 A 178.210.160.70
266	5.006572000	192.168.2.7	178.210.160.70	TCP	535	Len=0 MSS=1460 WS=16 TSval=871761191 TSecr=0 SACK_PERM=1
267	5.016842000	178.210.160.70	192.168.2.7	TCP	535	Len=0 MSS=1460 WS=16 TSval=871761191 TSecr=0 SACK_PERM=1
268	5.017051000	192.168.2.7	178.210.160.70	TCP	535	Len=0 MSS=1460 WS=16 TSval=871761191 TSecr=0 SACK_PERM=1
269	5.019271000	192.168.2.7	178.210.160.70	TCP	535	Len=0 MSS=1460 WS=16 TSval=871761191 TSecr=0 SACK_PERM=1
270	5.037164000	178.210.160.70	192.168.2.7	TCP	535	Len=0 MSS=1460 WS=16 TSval=871761191 TSecr=0 SACK_PERM=1
271	5.062309000	178.210.160.70	192.168.2.7	TCP	535	Len=0 MSS=1460 WS=16 TSval=871761191 TSecr=0 SACK_PERM=1

Packet Details:

- Frame 264: 76 bytes on wire (608 bits), 76 bytes captured (608 bits) on interface
- Ethernet II, Src: Apple_86:56:91 (20:c9:d0:86:56:91), Dst: Airtim
- Internet Protocol Version 4, Src: 192.168.2.7 (192.168.2.7), Dst:
- User Datagram Protocol, Src Port: 50757 (50757), Dst Port: domain
- Domain Name System (query)
 - [Response in: 265]
 - Transaction ID: 0xa2a2
 - Flags: 0x0100 Standard query
 - Questions: 1
 - Answer RRs: 0
 - Authority RRs: 0
 - Additional RRs: 0
 - Queries
 - berbergokmen.com: type A, class IN
 - Name: berbergokmen.com
 - Type: A (Host address)
 - Class: IN (0x0001)

Packet Bytes:

0010 00 3e 7d 63 00 00 ff 11 6b 8c c0 a8 02 07 08 08 .>|.k.....
0020 08 08 c6 45 00 35 00 2a 60 d5 a2 a2 01 00 00 01 ...E.S.*.....
0030 00 00 00 00 00 00 0c 02 66 22 18 05 02 67 6f 6e ...berbergokmen.com.....
0040 00 00 00 03 63 6f 6d 00 00 01 00 01

Query Name (dns.qry.name),... Packets: 9872 · Displayed: 9872 (100,0%) · Dropped: 0 (0,0%) Profile: Default

Protokol detayı . Protokol detaylarının gösterilmesi. Özellikle DDOS saldırılarında saldırı tipini belirlemek için kullanılır.

Wireshark

The image displays the Wireshark network protocol analyzer interface. The main window shows a list of captured packets with columns for No., Time, Source, Destination, Protocol, Length, and Info. A red box highlights the 'Protocol Hierarchy Statistics' window, which provides a detailed breakdown of the captured traffic by protocol.

Protocol Hierarchy Statistics

Protocol	% Packets	Packets	% Bytes	Bytes	Mbit/s	End Packets	End Bytes	End Mbit/s
Frame	100,00 %	6337	100,00 %	6157061	0,436	0	0	0,000
Ethernet	100,00 %	6337	100,00 %	6157061	0,436	0	0	0,000
Internet Protocol Version 4	99,07 %	6278	99,96 %	6154583	0,435	0	0	0,000
User Datagram Protocol	1,01 %	64	0,12 %	7296	0,001	0	0	0,000
Domain Name Service	0,98 %	62	0,11 %	6730	0,000	62	6730	0,000
Hypertext Transfer Protocol	0,03 %	2	0,01 %	566	0,000	2	566	0,000
Transmission Control Protocol	98,04 %	6213	99,84 %	6147217	0,435	6021	6068695	0,429
Secure Sockets Layer	2,30 %	146	0,70 %	42941	0,003	144	41111	0,003
Secure Sockets Layer	0,03 %	2	0,03 %	1830	0,000	2	1830	0,000
Hypertext Transfer Protocol	0,66 %	42	0,50 %	30937	0,002	24	18724	0,001
Media Type	0,27 %	17	0,18 %	11353	0,001	17	11353	0,001
Line-based text data	0,02 %	1	0,01 %	860	0,000	1	860	0,000
Malformed Packet	0,06 %	4	0,08 %	4644	0,000	4	4644	0,000
Internet Control Message Protocol	0,02 %	1	0,00 %	70	0,000	1	70	0,000
Address Resolution Protocol	0,93 %	59	0,04 %	2478	0,000	59	2478	0,000

The bottom status bar indicates: Text item (text), 31 bytes | Packets: 6337 - Displayed: 6337 (100,0%) - Dropped: 0 (0,0%) | Profile: Default

TCP follow . TCP oturumlarında paket birleştirme, HTTP bağlantısındaki tüm giden gelen paketlerin birleştirilip session hakkında bilgi verilmesi.

Wireshark

Birleştirilmek istenilen protokol paketi üzerinde sağ tıklanır ve "Follow TCP Stream" seçeneği seçilir.

Wireshark 1.10.0 (SVN Rev 49790 from /trunk-1.10.0)

Filter: tcp.stream eq 6

No.	Time	Source	Destination	Protocol	Length	Info
1475	40.454880000	192.168.2.7	64.15.117.173	TCP	60	1162 bytes captured on interface Wi-Fi en0
1476	40.543435000	64.15.117.173	192.168.2.7	TCP	60	1162 bytes captured on interface Wi-Fi en0
1477	41.418220000	64.15.117.173	192.168.2.7	TCP	60	1162 bytes captured on interface Wi-Fi en0
1478	41.418359000	192.168.2.7	64.15.117.173	TCP	60	1162 bytes captured on interface Wi-Fi en0
1479	41.418931000	64.15.117.173	192.168.2.7	TCP	60	1162 bytes captured on interface Wi-Fi en0
1480	41.419598000	64.15.117.173	192.168.2.7	TCP	60	1162 bytes captured on interface Wi-Fi en0
1481	41.419647000	192.168.2.7	64.15.117.173	TCP	60	1162 bytes captured on interface Wi-Fi en0
1482	41.420712000	64.15.117.173	192.168.2.7	TCP	60	1162 bytes captured on interface Wi-Fi en0
1483	41.420837000	192.168.2.7	64.15.117.173	TCP	60	1162 bytes captured on interface Wi-Fi en0
1484	41.421437000	64.15.117.173	192.168.2.7	TCP	60	1162 bytes captured on interface Wi-Fi en0
1485	41.422449000	64.15.117.173	192.168.2.7	TCP	60	1162 bytes captured on interface Wi-Fi en0
1486	41.422503000	192.168.2.7	64.15.117.173	TCP	60	1162 bytes captured on interface Wi-Fi en0
1487	41.423213000	64.15.117.173	192.168.2.7	TCP	60	1162 bytes captured on interface Wi-Fi en0
1488	41.423437000	192.168.2.7	64.15.117.173	TCP	60	1162 bytes captured on interface Wi-Fi en0
1489	41.425061000	64.15.117.173	192.168.2.7	TCP	60	1162 bytes captured on interface Wi-Fi en0
1490	41.426357000	64.15.117.173	192.168.2.7	TCP	60	1162 bytes captured on interface Wi-Fi en0

Frame 1475: 1162 bytes on wire (9296 bits), 1162 bytes captured (9296 bits) on interface Wi-Fi en0

Ethernet II, Src: Apple_08:00:27:00:00:00, Dst: AirtiesW_59:5e:25

Internet Protocol Version 4, Src: 192.168.2.7, Dst: 64.15.117.173

Transmission Control Protocol, Src Port: 50540 (50540), Dst Port: http (80)

Source port: 50540 (50540)

Destination port: http (80)

[Stream index: 6]

Sequence number: 8121 (relative sequence number)

Next sequence number: 9229 (relative sequence number)

Acknowledgment number: 1479767 (relative ack number)

Header length: 20 bytes

Flags: 0x018 (PSH, ACK)

Window size value: 16384

[Calculated window size: 16384]

0000 00 1c a8 59 5e 25 20 c9 d0 86 56 91 08 00 45 00 ...Y% . .V...E.

0010 04 7c d9 1c 00 00 40 06 24 f4 c0 a8 02 07 40 0f .|...@. \$.....@.

0020 75 ad c5 6c 00 50 18 cb 9b ef 40 82 8a e0 50 18 u..l.P.. ..@...P.

0030 40 00 84 b3 00 00 3d 31 33 37 36 33 38 30 32 33 @.....=1 37638023

0040 38 33 32 35 36 20 50 52 45 46 3d 48 49 44 44 45 8325; PR EF=HIDOE

0050 4e 5f 4d 41 53 54 48 45 41 44 5f 49 44 3d 33 4c N_MASTHE AD_ID=3L

0060 79 5f 66 73 46 64 52 45 49 26 61 6c 3d 74 72 2b y_f5f6RE I6a1tr+

0070 65 6e 26 66 76 3d 31 31 2e 37 2e 37 30 30 26 66 en&fv=11 .7.7006f

0080 34 3d 34 30 30 30 30 30 30 26 66 31 3d 35 30 30 4=400000 0&f1=500

0090 30 30 30 30 30 30 30 30 31 56 48 58 2e 72 65 73 00000; W 1VHX.res

00a0 75 6d 65 3d 56 5f 78 45 52 71 46 53 34 34 59 3a une=V_xE RqPS44Y:

00b0 31 31 35 33 2c 30 59 43 41 63 58 69 48 45 64 6b 1153,0YC ACXiHedk

00c0 7a 72 70 78 74 2c 47 66 70 4c 65 61 79 4f 75 72 +20R6.Gf m1ea90ur

Frame (1162 bytes) Reassembled TCP (2308 bytes)

File: /var/folders/jb/czplsn... Packets: 6337 - Displayed: 2630 (41.5%) - Dropped: 0 (0.0%) Profile: Default

İstek sayıları . http istek sayılarının görüntülenmesi.

Wireshark

The image shows the Wireshark network protocol analyzer interface. The main packet list on the left displays a series of captured packets, with packet 337 selected. The packet details pane on the right shows the structure of the selected packet, including Ethernet II, Internet Protocol Version 4, Transmission Control Protocol, and Hypertext Transfer Protocol. A summary window titled 'HTTP/Requests with filter:' is open in the foreground, displaying a table of HTTP requests by host. The table includes columns for Topic / Item, Count, Rate (ms), and Percent. The data is sorted by count in descending order.

Topic / Item	Count	Rate (ms)	Percent
HTTP Requests by HTTP Host	972	0,001136	
res.reklamport.com	15	0,000018	1,54%
www.sahibinden.com	30	0,000035	3,09%
banner2.sahibinden.com	90	0,000105	9,26%
image5.sahibinden.com	40	0,000047	4,12%
b.scorecardresearch.com	55	0,000064	5,66%
pubads.g.doubleclick.net	10	0,000012	1,03%
ad.reklamport.com	10	0,000012	1,03%
gatr.hit.gemius.pl	21	0,000025	2,16%
www.google-analytics.com	32	0,000037	3,29%
csi.gstatic.com	1	0,000001	0,10%
ds.serving-sys.com	1	0,000001	0,10%
kelebekgaleri.hurriyet.com.tr	50	0,000058	5,14%
www.hurriyet.com.tr	21	0,000025	2,16%
api1.hurpass.com	15	0,000018	1,54%
imgkelebek.hurriyet.com.tr	22	0,000026	2,26%
adonline.e-kolay.net	7	0,000008	0,72%
sayac.hurriyet.com.tr	9	0,000011	0,93%
ad.e-kolay.net	19	0,000022	1,95%
www.facebook.com	16	0,000019	1,65%

Uygulama . Paket yakalama

- ⌚ Tcp port 21 (FTP)
- ⌚ Tcp port 21 and tcp port 1982
- ⌚ Tcp port 22 and host bilmuh.gtu.edu.tr
- ⌚ Tcp port 21 (SMTP)

Uygulama . dsniff

Kaynakça

- ⌚ Paket/Protokol Analizi Amaçlı Wireshark Kullanımı,
http://wiki.bgasecurity.com/Paket/Protokol_Analizi_Amaçlı_Wireshark_Kullanımı
- ⌚ BGA, Beyaz şapkalı hacker eğitimi yardımcı ders notları – I
- ⌚ BGA, Nmap Kullanım Kitapçığı