

Bilgi Toplama

İstihbarat Çeşitleri

Pasif Bilgi Toplama

- Hedef sistemden bağımsız

Aktif Bilgi Toplama

- Hedef sistemle doğrudan iletişime geçerek

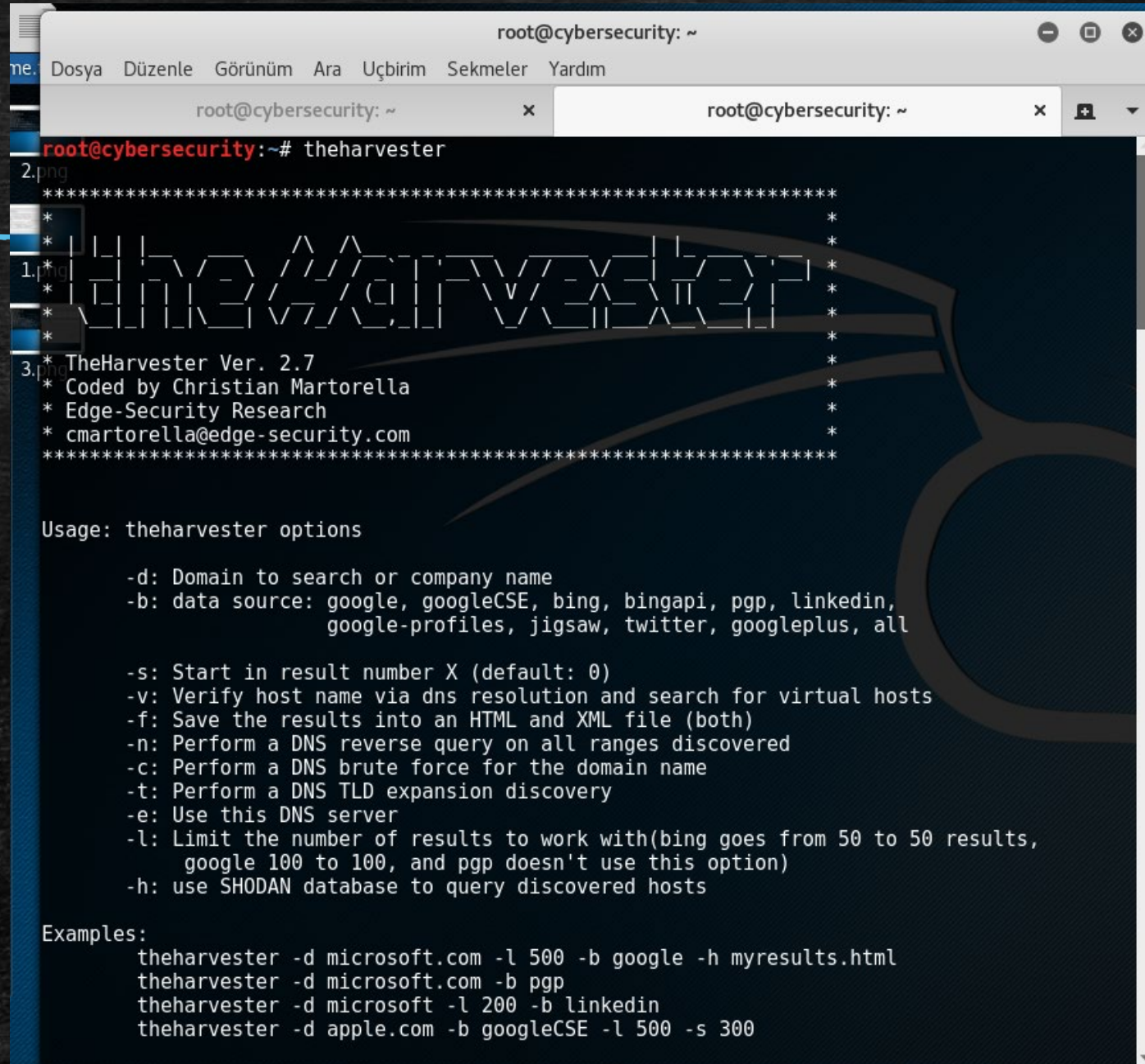
Aktif Bilgi Toplama

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.

thearvester 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
sares@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: ~

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

Kapat

eniyor

```
root@cybersecurity: ~
```

© 2006 The Authors
Journal compilation © 2006 Blackwell Publishing Ltd

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

File Options About Help

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

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 /moodle/

☒ Brute Force Files

☐ Use Blank Extension

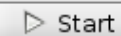
File extension php

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 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	200	502
mod	200	289
course	200	502
calendar	303	935
pluginfile.php	200	502
theme	303	931
lib	200	291
javascript.php	200	291
1489570996	200	291

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

- Nmap kullanarak ağa bağlı 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

- 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.

Hedef belirtme seçenekleri .

- `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

- -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 gözüktür.
- -n/-R. Asla DNS Çözümlemesi yapılmaz/Herzaman DNS çözümlemesi yapılır [varsayılan. bazen]
- --dns-servers <serv1[,serv2],...>. Özel DNS serverları 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)

Portların Taramaları

- 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.

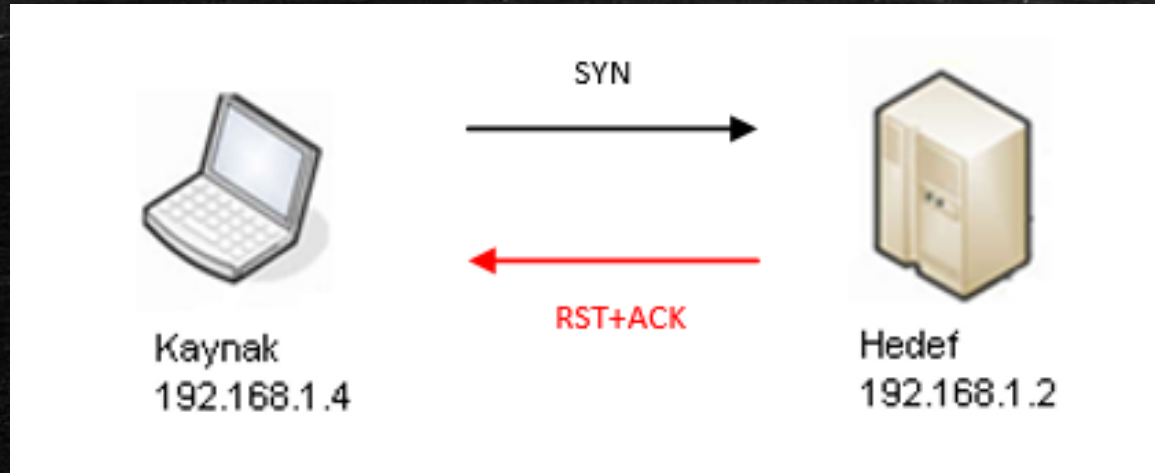
Tarama Türleri

- 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

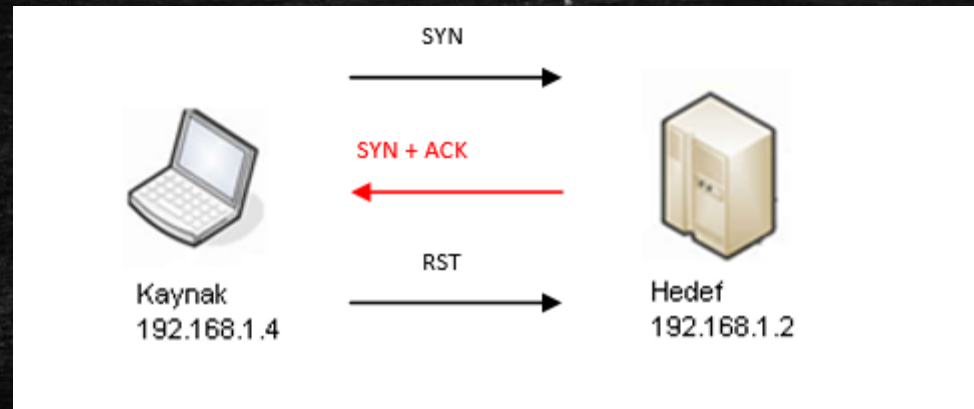
TCP Syn Scan

- 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.



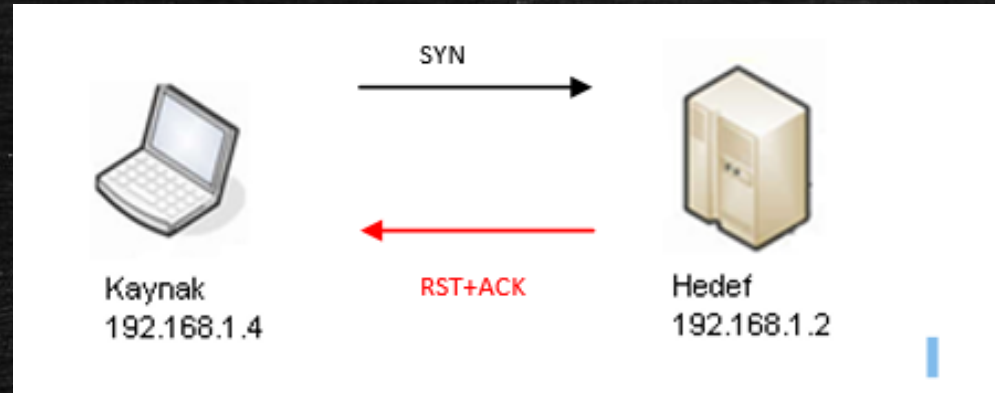
TCP Syn Scan

- Açık olduğu durumda SYN + ACK bayraklı paket dönecektir. Kaynak makinada RST bayraklı paket göndererek bağlantıyı koparır ve böylelikle üçlü el sıkışma tamamlanmaz.
- `#nmap -sS -v 192.168.1.2`



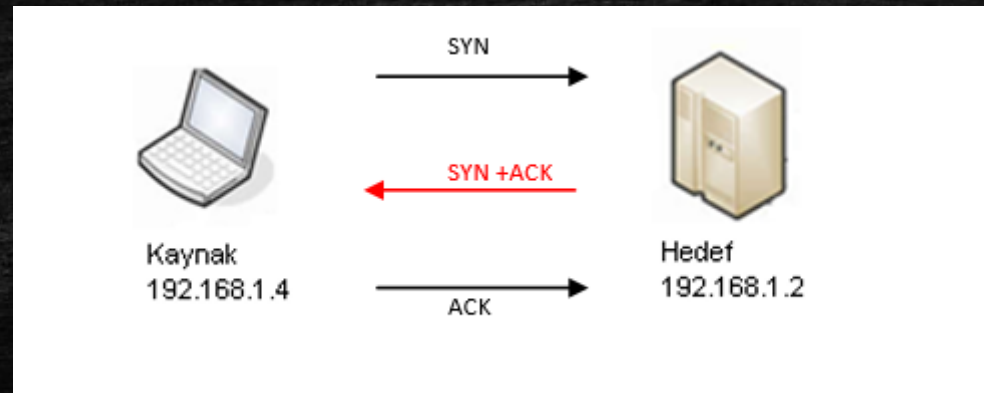
TCP Connect Scan

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



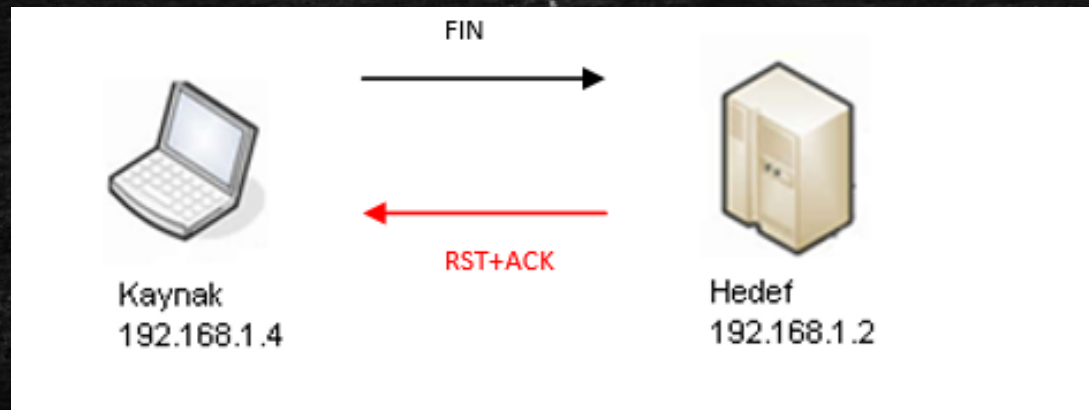
TCP Connect Scan

- 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.
- `#nmap -sT -v 192.168.1.2`



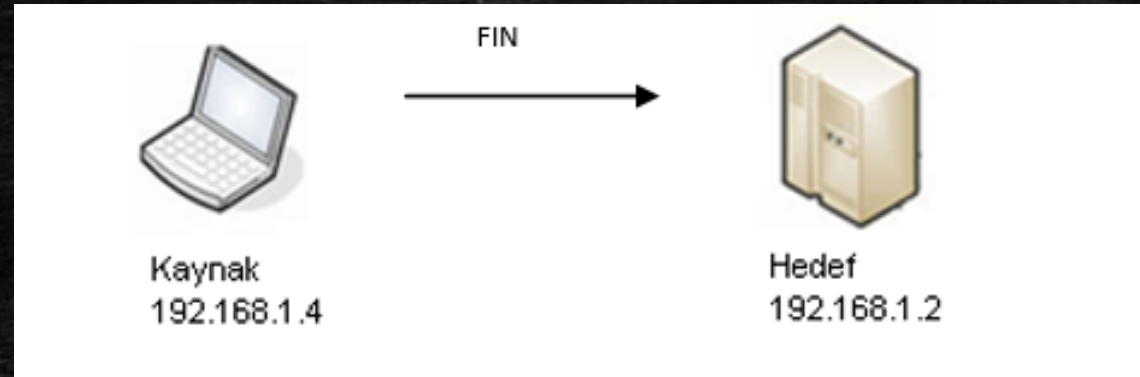
FIN Scan

- FIN Scan ilişkin “saklı” frameler olağandışıdır çünkü hedef makineye 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 .



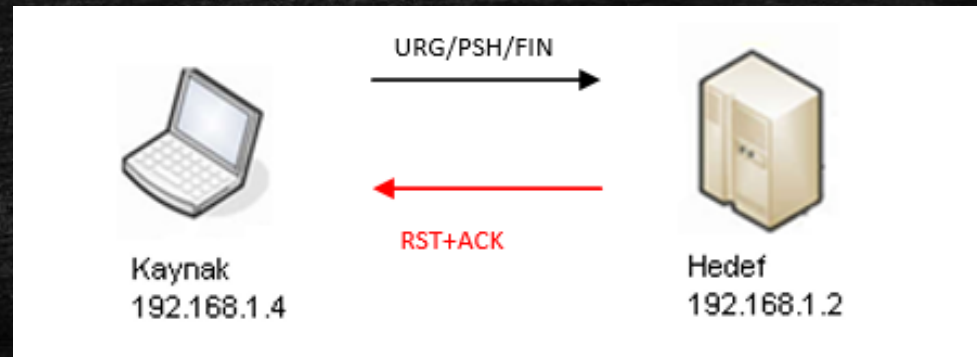
FIN Scan

- Eğer port açık olursa hedef makinadan herhangi bir tepki dönmeyecektir .
- `#nmap -sF -v 192.168.1.2`



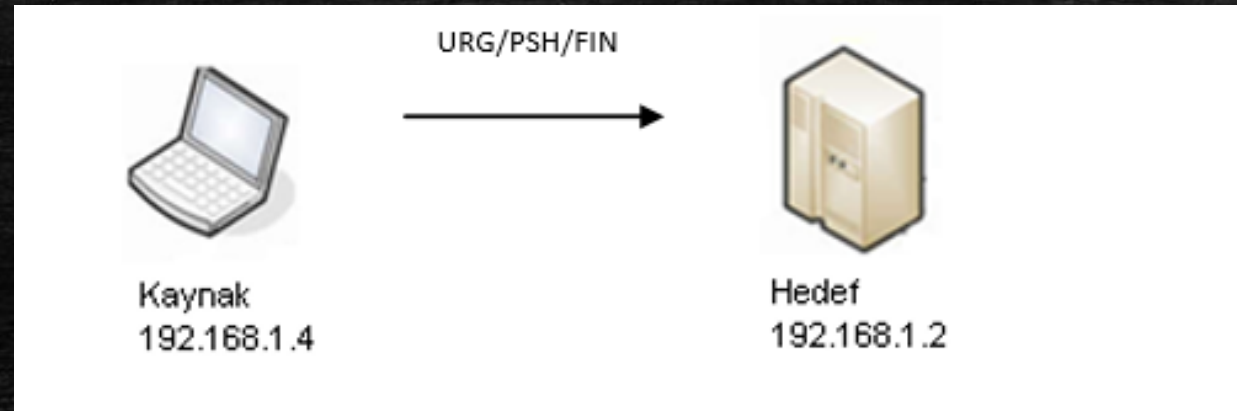
XMas Tree Scan

- Kaynak makinanın TCP frame içine URG, PSH ve FIN bayraklarını set edeceği paket hedef makinaya gönderilir. Hedef makinanın döndüreceği cevaplar FIN Scan ile aynıdır.
- 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 .
- `#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 .
- `#nmap -sN -v 192.168.1.2`

Ping Scan

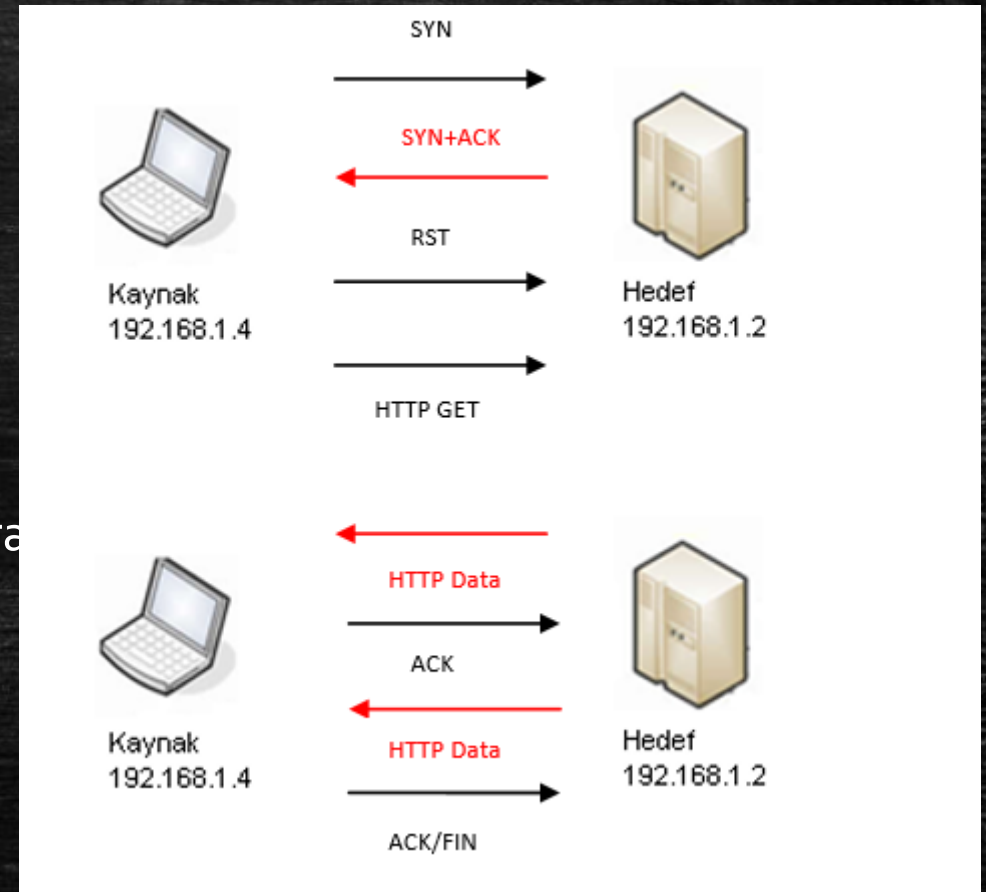
- Kaynak makinanın hedef makinaya tek bir ICMP Echo istek paketi göndereceği bu tarama türünde, IP adresi erişilebilir ve ICMP filtreleme bulunmadığı sürece, hedef makina ICMP Echo cevabı döndürecektir.
- Eğer hedef makina erişilebilir değilse veya paket filtreliyiçi ICMP paketlerini filtreliyorsa, hedef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

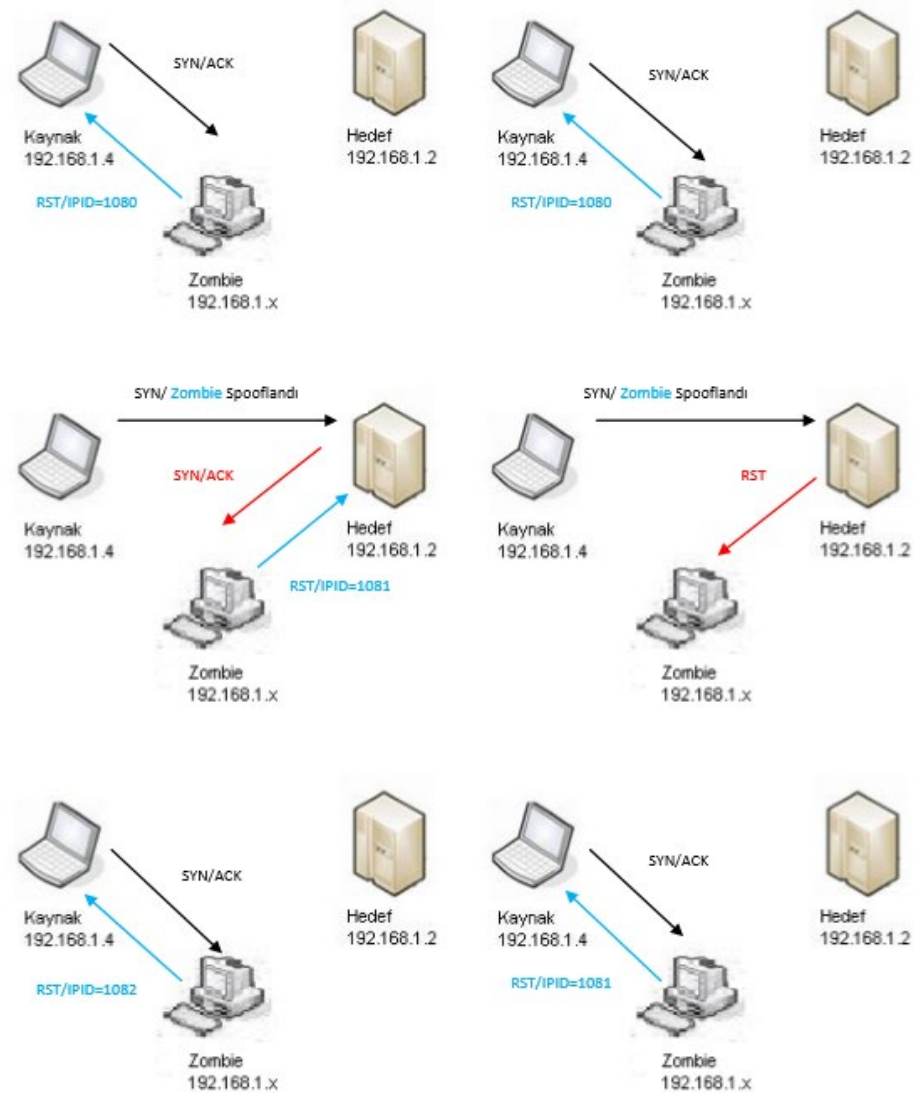
RPC Scan

- RPC Scan, hedef makina üzerinde kořan RPC uygulamalarını keřfeder. Bařka bir tarama tőrő ile aık portlar keřfedildikten sonra, RPC Scan hedef makinanın aık portlarına RPC null gőndererek, eęer alıřan bir RPC uygulaması varsa, RPC uygulamasını harekete geirir.
- RPC Scan, Version Detection Scan iřlemi esnasında otomatik olarak alıřtırılır.
- `#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



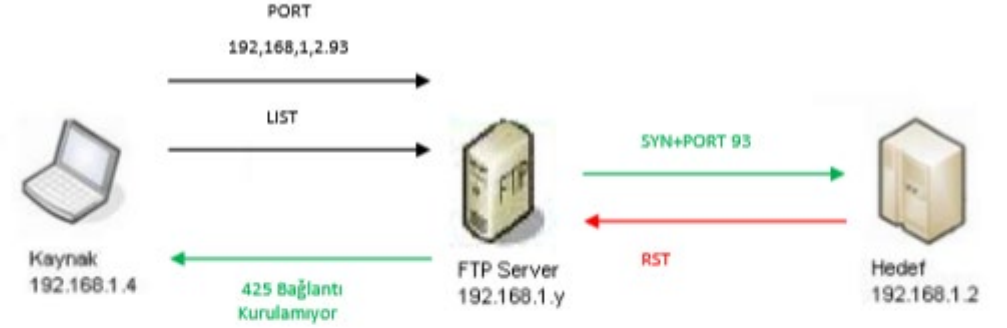
FTP Bounce Scan

- 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 .

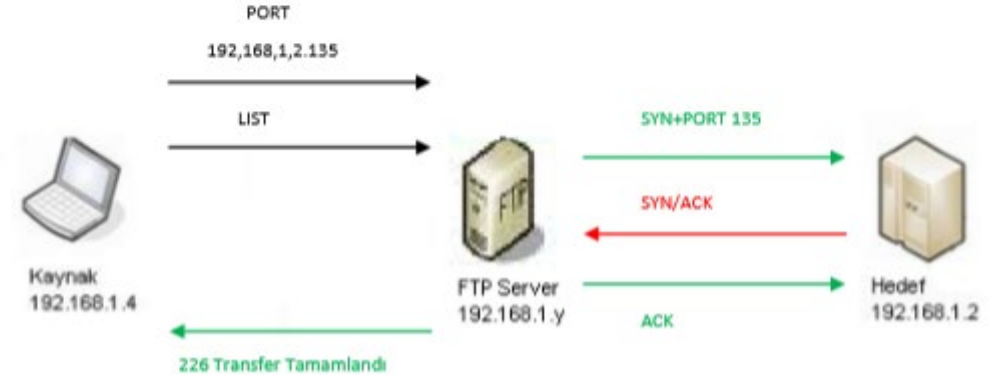
FTP Bounce Scan

- Bu taramayı gerçekleştirmek için aşağıdaki komut kullanılmalıdır :
- `nmap -b -v [user@ftpserver] [Hedef_IP]`

HEDEF KAPALI DURUMDA



HEDEF AÇIK DURUMDA



Nmap Ping Seçenekleri

- 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.
- 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 dönebileceği 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]`

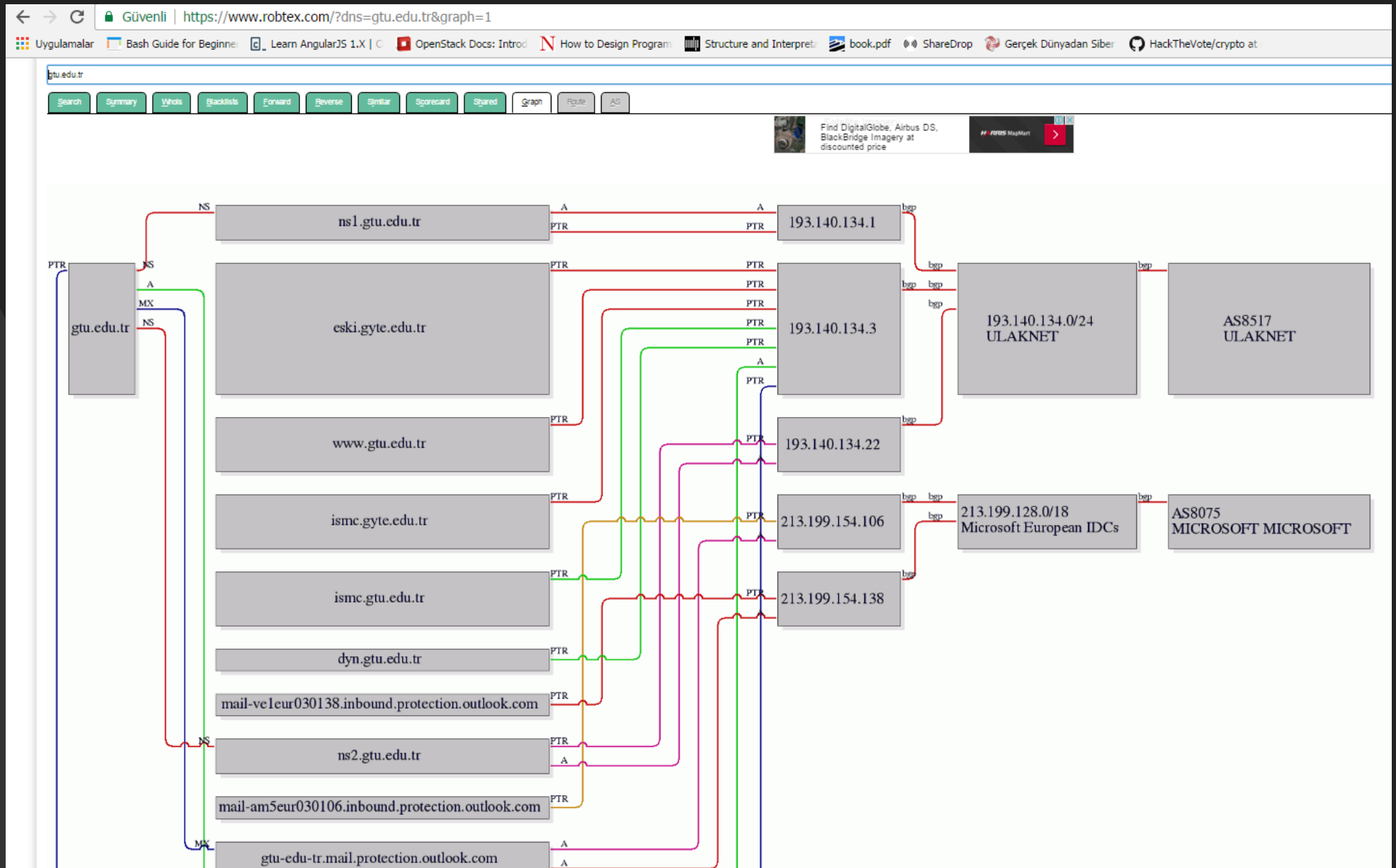
Spoofing

- 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

Ayarlar

Genel Protokol Bilgisi

Protokol Detayı

Yakalanan paket özeti

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

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)

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

0000 00 13 64 22 39 3f 00 02 44 a6 eb b0 08 00 45 00 ..d'9?.. D....E.

0010 00 28 31 a2 80 00 de 06 84 cf c0 a8 01 02 50 5d .(1.8....P]

0020 d4 56 07 41 00 50 21 4f ba d1 f5 ab 5d f7 50 11 .V.A.P!o].P.

0030 f8 44 99 db 00 00 ..D....

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 selected packet is a TCP SYN packet from 192.168.2.7 to 178.210.160.70 on port 21.

Overlaid on the main window is the "Wireshark: Capture Options" dialog box. The "Capture" tab is active, showing a table of available interfaces:

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

Below the table, the "Capture on all interfaces" checkbox is unchecked, and the "Use promiscuous mode on all interfaces" checkbox is checked. The "Capture Filter" field is set to "tcp port 21", which is highlighted with a red box. A red arrow points from this field to the "tcp port 21" filter in the main packet list.

The "Capture Files" section shows options for saving the capture to a file, including "Use multiple files", "Use pcap-ng format", and "Next file every" settings.

The "Display Options" section includes checkboxes for "Update list of packets in real time", "Automatically scroll during live capture", "Hide capture info dialog", "Resolve MAC addresses", and "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 title bar indicates the capture interface is *Wi-Fi: en0 and the version is 1.10.0. The menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Tools, Internals, and Help. The toolbar contains various icons for file operations, capture control, and analysis. The filter bar at the top shows the display filter `tcp.srcport == 80`. Below this, a table lists captured packets. A red box highlights the filter bar, and a red arrow points from it to the first packet in the list.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	64.15.117.144	192.168.2.7	HTTP	1506	Continuation or non-HTTP traffic
2	0.003427000	64.15.117.144	192.168.2.7	HTTP	1506	Continuation or non-HTTP traffic
4	0.005600000	64.15.117.144	192.168.2.7	HTTP	1506	Continuation or non-HTTP traffic
6	0.007184000	64.15.117.144	192.168.2.7	HTTP	1506	Continuation or non-HTTP traffic
7	0.010307000	64.15.117.144	192.168.2.7	HTTP	1506	Continuation or non-HTTP traffic
9	0.013352000	64.15.117.144	192.168.2.7	HTTP	1506	Continuation or non-HTTP traffic
11	0.014929000	64.15.117.144	192.168.2.7	HTTP	1506	Continuation or non-HTTP traffic
13	0.027134000	64.15.117.144	192.168.2.7	HTTP	1506	Continuation or non-HTTP traffic
14	0.028909000	64.15.117.144	192.168.2.7	HTTP	1506	Continuation or non-HTTP traffic
16	0.030938000	64.15.117.144	192.168.2.7	HTTP	1506	Continuation or non-HTTP traffic
18	0.032596000	64.15.117.144	192.168.2.7	HTTP	1506	Continuation or non-HTTP traffic
19	0.034151000	64.15.117.144	192.168.2.7	HTTP	1506	Continuation or non-HTTP traffic
21	0.036695000	64.15.117.144	192.168.2.7	HTTP	1506	Continuation or non-HTTP traffic
23	0.040135000	64.15.117.144	192.168.2.7	HTTP	1506	Continuation or non-HTTP traffic
24	0.041737000	64.15.117.144	192.168.2.7	HTTP	1506	Continuation or non-HTTP traffic
26	0.053536000	64.15.117.144	192.168.2.7	HTTP	1506	Continuation or non-HTTP traffic

Below the packet list, the details pane shows the structure of the first packet (Frame 1):

- 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 packet bytes pane at the bottom shows the raw data in hexadecimal and ASCII:

```
0000  20 c9 d0 86 56 91 00 1c a8 59 5e 25 08 00 45 60  ...V...Y^..E
0010  05 d4 80 33 40 00 38 06 44 42 40 0f 75 90 c0 a8  ...38.B.D80.u...
0020  02 07 00 50 c0 43 fc 8b 9e 7b c1 3b 51 94 50 10  ...P.C...{.;Q.P.
0030  01 30 d8 c4 00 00 c3 7d 41 d6 50 f4 72 d8 ac d5  .0.....} A.P.r...
0040  ce e2 dd 89 9a 8e b9 11 03 d5 e2 23 b0 f4 59 b3  .....#..Y.
```

The status bar at the bottom indicates: File: "/var/folders/jb/czplsn... Packets: 1255 · Displayed: 731 (58,2%) · Dropped: 0 (0,0%) Profile: 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. The 'Filter' field is empty. The 'Expression...' button is visible. The 'Find Packet' dialog box is open, showing the 'Find' section with 'By: Display filter', 'Hex value', and 'String' options. The 'String' option is selected, and the search string 'berbergokmen' is entered in the 'Filter' field. The 'Search In' section shows 'Packet list', 'Packet details', and 'Packet bytes' options. The 'String Options' section shows 'Case sensitive' and 'Character width' options. The 'Direction' section shows 'Up' and 'Down' options. The 'Find' button is highlighted. The background shows a packet capture of a DNS query for 'berbergokmen.com'.

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	92	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

Frame 264: 76 bytes on wire (608 bits), 76 bytes captured (608 bits) on interface 0
Ethernet II, Src: Apple_86:56:91 (20:c9:d0:86:56:91), Dst: Airtie...
Internet Protocol Version 4, Src: 192.168.2.7 (192.168.2.7), Dst: 8.8.8.8
User Datagram Protocol, Src Port: 50757 (50757), Dst Port: domain...
Domain Name System (query)
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)

0010 00 3e 7d 63 00 00 ff 11 6b 8c c0 a8 02 07 08 08 .>).c... 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 00 00 00 00 00 00 00
0040 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
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 shows the Wireshark Protocol Hierarchy Statistics window. The main window displays 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 traffic by protocol.

Wireshark: Protocol Hierarchy Statistics

Display filter: none

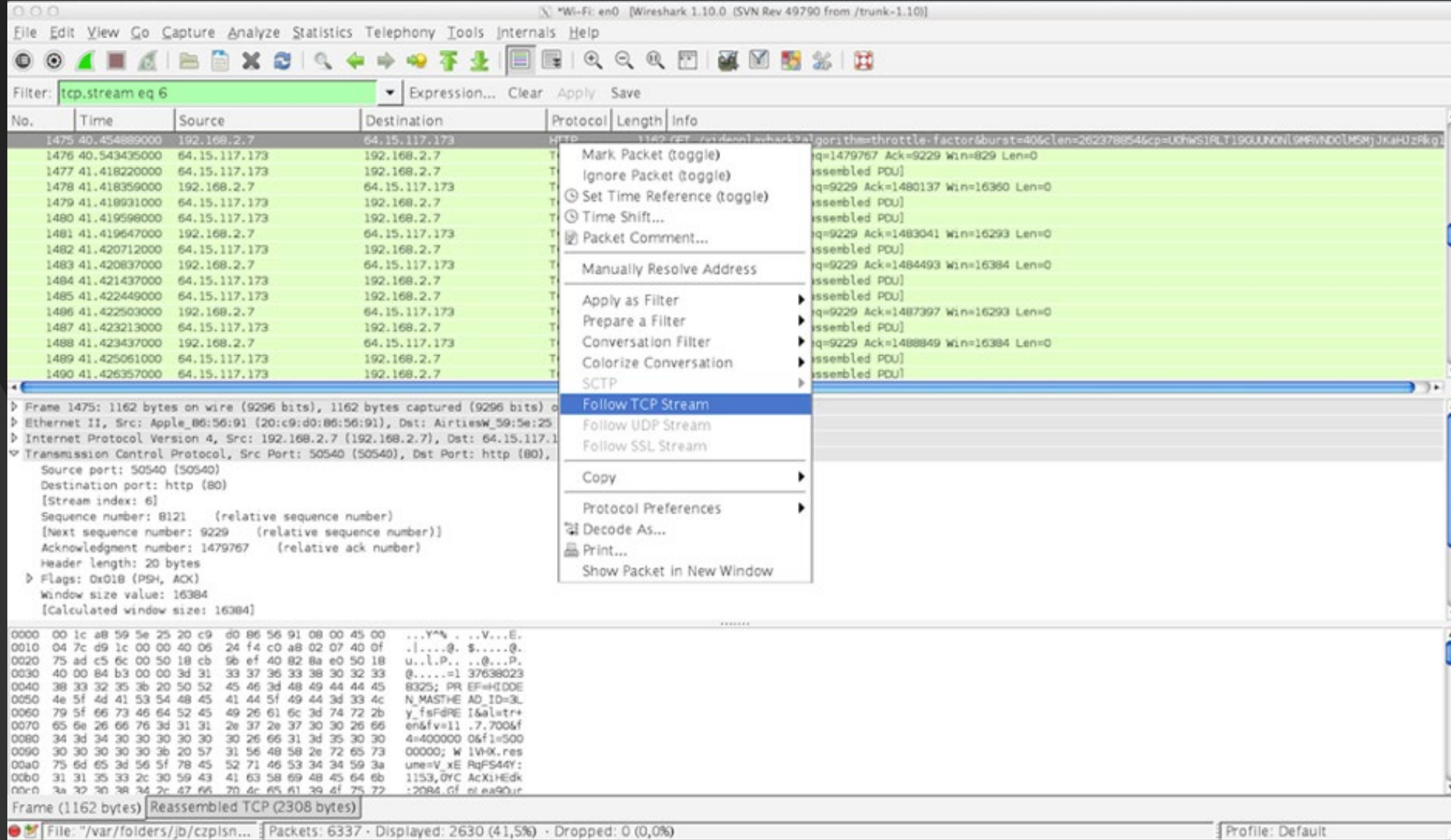
Protocol	% Packets	Packets	% Bytes	Bytes	Mbit/s	End Packets	End Bytes	End Mbit/s
Frame	100,00 %	6337	100,00 %	6157061	0,436	0	0	0,000
Ethernet	100,00 %	6337	100,00 %	6157061	0,436	0	0	0,000
Internet Protocol Version 4	99,07 %	6278	99,96 %	6154583	0,435	0	0	0,000
User Datagram Protocol	1,01 %	64	0,12 %	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 shows: 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.



İstek sayıları . http istek sayılarının görüntülenmesi.

Wireshark

The image shows the Wireshark network protocol analyzer interface. The main window displays a list of captured packets. The packet list on the left shows packets 324 through 339. The packet details pane on the right shows the structure of a 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, showing a table of HTTP requests by host.

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)

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
- ⌚ Necmettin Çarkacı

Bilgi Güvenliđi ve Risk Analizi

BSP 572 Ağ ve Bilgi Güvenliđi Dersi – Necmettin ÇARKACI

Sunumda özgün katkım çok azdır. Sunum büyük çoğunluğu kaynaklardan derlenmiştir.

Haftalık Ders Takip Listesi

- Siber Güvenliğe Genel Bakış ve Güncel Trendler
- Bilgi Güvenliğinde Risk Analizi
- Kriptoloji
- Sızma Testi ve Bilgi Toplama Teknikleri
- Ağ Güvenliği ve Keşif ve Zafiyet Tarama
- Dijital Adli Analiz
- Nüfuz Tespit, Güvenlik Duvarı ve Biyometrik Güvenlik
- Zararlı Yazılım Analiz Yöntemleri
- Bilgi Toplama ve Sosyal Mühendislik Saldırıları
- Exploit Geliştirmenin Temelleri

Geçen Haftadan...

Maslov İhtiyaç piramidi



Geçen Haftadan...

- ⌚ Siber savunma ile ilgili yanlış düşünceler
- ⌚ Bilgi Güvenliği ve Siber Güvenlik
- ⌚ Siber Tehditlerin Özellikleri
- ⌚ Dünyada ne değişti
- ⌚ Siber Tehditlerin Hedefleri
- ⌚ Siber Savaş mı?
- ⌚ APT (Hedef Odaklı Saldırıları)

Bilgi Güvenliğinde Risk Analizi

Bilgi Güvenliđi Yönetimi

- ⌚ Güvenlik yönetimi ilgilendiren bir konudur.
- ⌚ Varlıkları korumak için oluşturulur.
- ⌚ Başlayıp bitirilen deđil devam eden bir süreçtir.



Bilgi Güvenliği Programı

İyi bir bilgi güvenliği programı

- ⌚ Bilgiyi sınıflandırmayı
- ⌚ Politika, prosedür ve standartlarını
- ⌚ Güvenlik eğitimi
- ⌚ Güvenlik örgütlenmesini
- ⌚ Risk yönetimini içerir.

Güvenlik Programının Hedefleri

- ⌚ Kısa vadeli **Operasyonel** hedefleri olmalıdır. Örn : İşletim sistemi güncellemesi
- ⌚ Orta vadeli **Taktik** hedefleri olmalıdır. Örn : Bütün makineler domain yapısına dahil edilecek.
- ⌚ Uzun vadeli **Stratejik** hedefler olmalıdır. Örn : Merkezi bir bilgi güvenliği yapısının olması

Hedefler

- ⌚ Kurumdan kuruma ve aynı kurumda zamanla değişir
 - ⌚ Askeri Kurumlar : Gizlilik
 - ⌚ Bankalar : Bütünlük
 - ⌚ Bireysel Yapılar : Prestij
 - ⌚ Ticari Kurumlar : Erişebilirlik
 - ⌚ Devlet kurumları : Gizlilik, bütünlük, prestij, erişebilirlik

Bilgi Güvenliđi Risk Yönetiminin Amacı

Bilgi güvenliđini en uygun maliyetle sağlamak

Bilgi Güvenliđi Risk Yönetiminin Amacı



0 Halde Ne kadar Güvenlik Gerekli?

⌚ **Ne tür varlıklar** korumak gereklidir?

Korunacak Varlıklar

- ⌚ İnsanlar (*personel, müşteriler, tedarikçiler..*)
- ⌚ Bilgi (*kağıt ve elektronik ortamdaki*)
- ⌚ Yazılım varlıkları
- ⌚ Fiziksel varlıklar (*bilgisayar ve iletişim donanımı, altyapı varlıkları*)
- ⌚ Hizmetler (*bilişim, ısıtma, havalandırma..*)
- ⌚ Kurum imajı ve itibarı

0 Halde Ne kadar Güvenlik Gerekli?

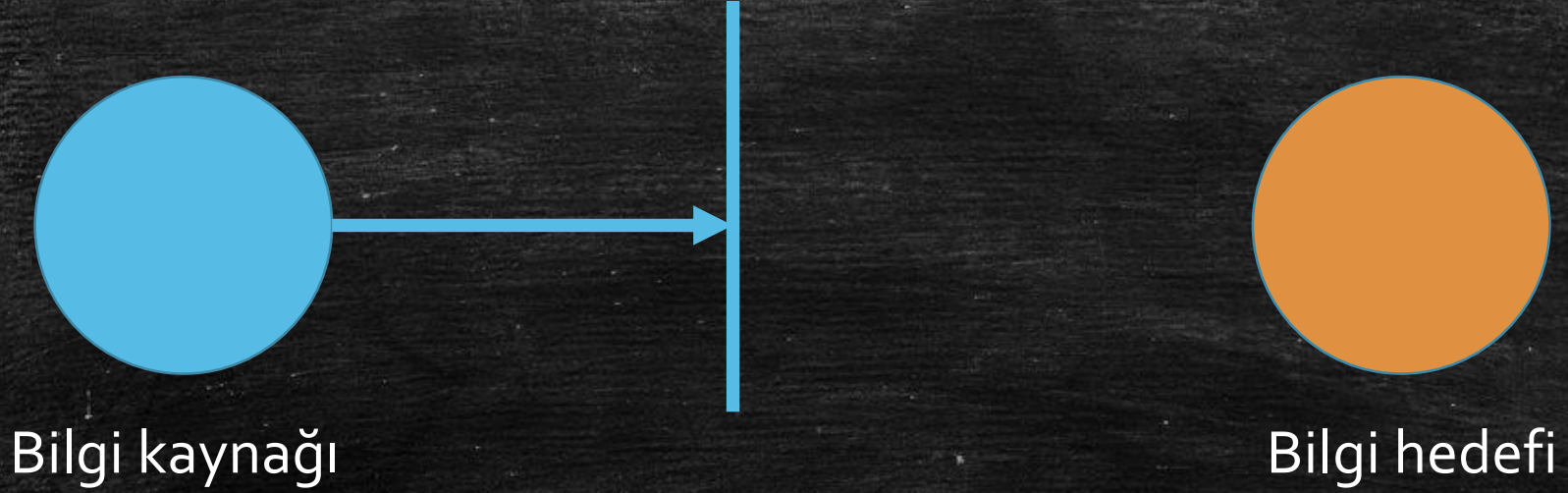
- ⌚ **Ne tür varlıklar** korumak gereklidir?
- ⌚ Bu varlıkları **nelere karşı** korumalıyız?

Saldırıların Sınıflandırılması

Süreçsel

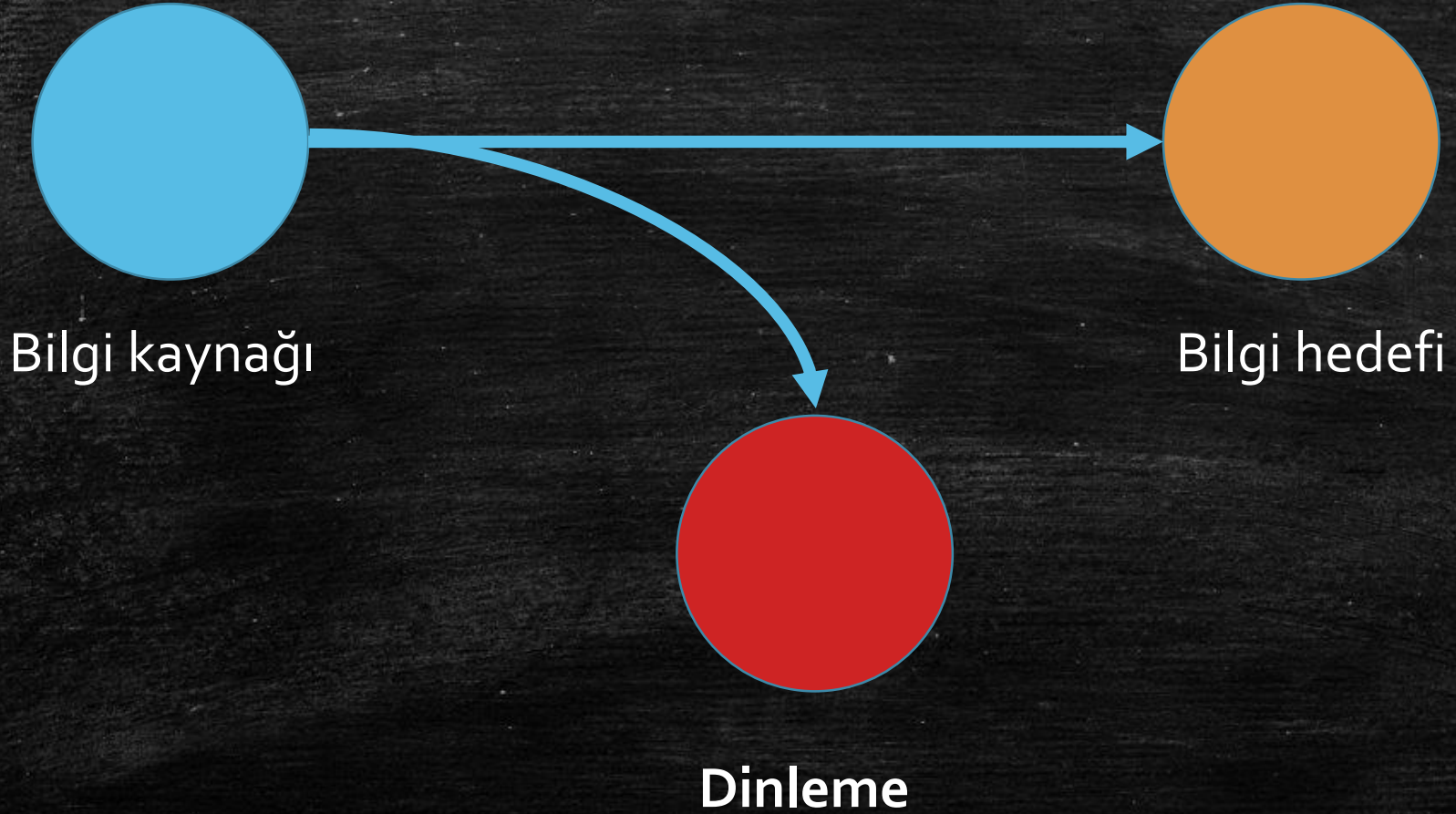
İşlemsel

Süreçsel Sınıflandırma

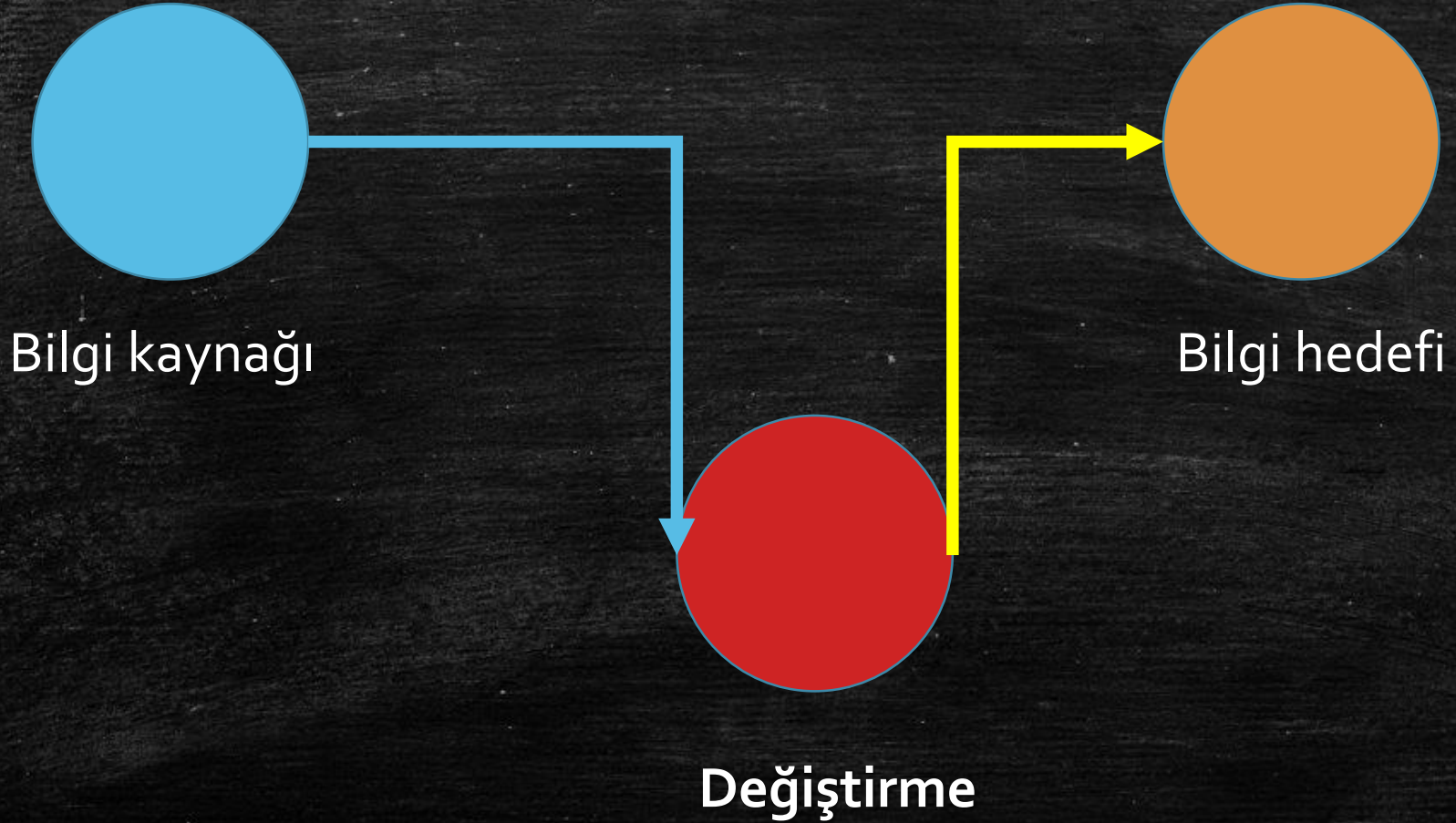


Engelleme

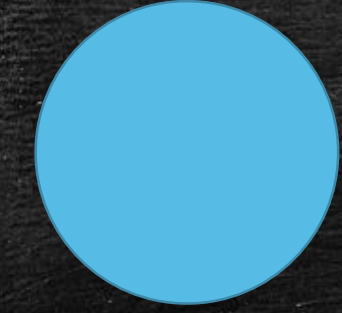
Süreçsel Sınıflandırma



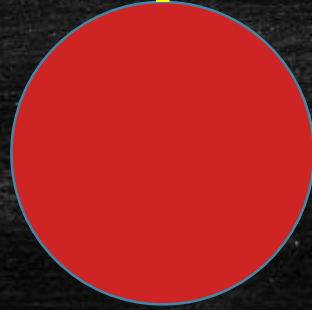
Süreçsel Sınıflandırma



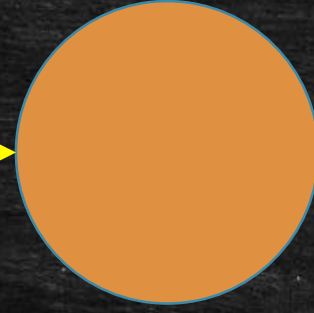
Süreçsel Sınıflandırma



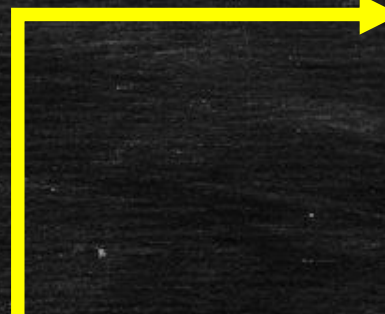
Bilgi kaynağı



Oluşturma



Bilgi hedefi



İşlemsel Sınıflandırma



0 Halde Ne kadar Güvenlik Gerekli?

- ⌚ **Ne tür varlıklar** korumak gereklidir?
- ⌚ Bu varlıkları **nelere karşı** korumalıyız?
- ⌚ Bize **kim** tehlikeli **saldırı** yapabilir ve ne kazanabilir?

Saldırganlar ve Amaçları

Saldırganlar	Araçlar	Erişim	Sonuç	Amaç
Bilgisayar Korsanları	Kullanıcı komutları	Uygulama zayıflıkları	Bilgi bozma	Finansal kazanç
Casuslar	Komut dosyası veya program	Tasarım zayıflıkları	Bilgi çalma yada açığa bilgi çıkarma	Politik kazanç
Teröristler	Araç takımı	Yapılandırma zayıflıkları	Hizmet çalma	Sosyal statüye meydan okuma
Meraklılar	Dağıtık araçlar	İzinsiz erişim	Hizmet önleme	Zevk için
Profesyonel Suçlular	Veri dinleyici sistemler			

* **Kötü niyetli saldırganlar**

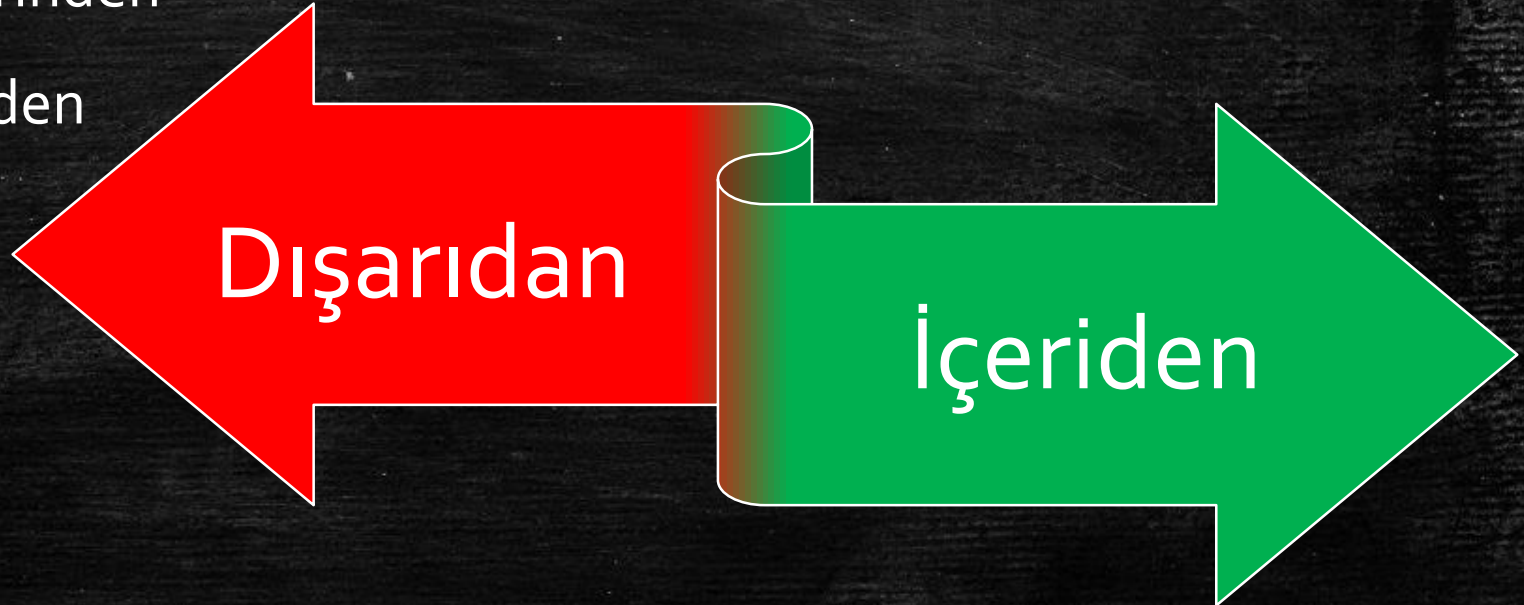
** **Kötü niyetli olmayan saldırganlar**

Bize kim tehlikeli saldırı yapabilir

- ⌚ Çalışan İşçiler
- ⌚ Geçici veya Danışman Personel
- ⌚ Rakipler
- ⌚ Organizasyonun görüş ve amaçlarından çok farklı düşünceye sahip olan şahıslar.
- ⌚ Organizasyona düşmanlığı olan şahıslar veya onları personeli
- ⌚ Sizin Organizasyonunuzun halka açık görüntüsünden dolayı şöhret kazanmak isteyen kişiler.

Potansiyel Saldırı Kaynakları

- ⌚ Dahili Sistemler
- ⌚ Çevre ofis erişim noktaları
- ⌚ Bir iş ortağına olan geniş alan ağ bağlantısı üzerinden
- ⌚ İnternet bağlantısı üzerinden
- ⌚ Modem havuzu üzerinden



Örnek Saldırı Senaryoları

- ⌚ Sistem Yöneticisi : Diploma sahte, referanslar sahte
- ⌚ Bakanlık : Kurumda yetkili kullanıcı «RedHack» üyesi

0 Halde Ne kadar Güvenlik Gerekli?

- ⌚ **Ne tür varlıklar**ı korumak gereklidir?
- ⌚ Bu varlıkları **nelere karşı** korumalıyız?
- ⌚ Bize **kim** tehlikeli **saldırı** yapabilir ve ne kazanabilir?
- ⌚ Bir **tehdit**'in varlıklarımızı **bozma olasılığı** ne kadardır?

Bir Saldırı İhtimali Nedir?

- ⌚ Kaynakları ve olabilecek saldırı türlerini belirlemek gereklidir, kuruluşun saldırılara karşı potansiyel risklerinin değerlendirilmesi gereklidir.
- ⌚ **Risk analizi ve Risk Yönetimi**

Risk Yönetimi

⌚ Riski

- ⌚ Belirlemek
- ⌚ Değerlendirilmesi : Risk Analizi ve Risk Derecelendirme
- ⌚ Kabul edilebilir seviyeye çekmektir.

⌚ **%100 güvenlik yoktur.**

- ⌚ Riskler bertaraf edilmeli veya devredilmelidir
- ⌚ Riski %100 ölçmekte mümkün değildir. Sadece ölçeklendirilebilir.

Risk Analizi Amaçları

- ⌚ Varlıkları ve değerlerini belirlemek
- ⌚ Zafiyet ve tehditleri belirlemek
- ⌚ Zararın maddi boyutunu belirlemek
- ⌚ Kabul edilebilir maliyetli çözümler ortaya koymak

Risk Nedir?

⌚ **Varlık** üzerinde **tehdit** oluşturan bir **zafiyetin** bir **tehdit ajanı** tarafından kullanılmasına bağlı **zarar beklentisidir**.

$\text{Risk} = f(\text{varlık, açıklık, tehdit}) \rightarrow \text{zarar beklentisi}$



Risk Çeşitleri

- ⌚ Fiziksel tehditler
- ⌚ İnsan etkeni
- ⌚ Cihaz hatası
- ⌚ İç ve dış saldırılar
- ⌚ Verinin yanlış kullanılması
- ⌚ Veri kaybı
- ⌚ Uygulama hatası

Risk Terimleri

- ⌚ Varlık (Assets)
- ⌚ Zafiyet (Vulnerability)
- ⌚ Tehdit (Threat)
- ⌚ Tehdit ajanı (Threat agent)
- ⌚ Risk (Risk)
- ⌚ Karşı önlem ve Koruma (Countermeasure)

Risklerin Belirlenmesi

- ⌚ **Varlıkların** ve varlık **sahiplerinin** belirlenmesi
- ⌚ Varlığa yönelik **tehditlerin** belirlenmesi
- ⌚ Bu tehditlerin kullanabileceği **zafiyetlerin** belirlenmesi
- ⌚ Tehdit ve açıklıkların varlığın gizlilik, bütünlük veya erişilebilirliğine **etkisinin belirlenmesi**

Varlıklar

- ⌚ İnsanlar (*personel, müşteriler, tedarikçiler..*)
- ⌚ Bilgi (*kağıt ve elektronik ortamdaki*)
- ⌚ Yazılım varlıkları
- ⌚ Fiziksel varlıklar (*bilgisayar ve iletişim donanımı, altyapı varlıkları*)
- ⌚ Hizmetler (*bilişim, ısıtma, havalandırma..*)
- ⌚ Kurum imajı ve itibarı

Varlık Sahipleri

- ⌚ **Varlık sahibi** = Birey veya birim
- ⌚ Varlığın **üretilmesinden**, geliştirilmesinden, bakımından, **kullanımından** ve **güvenliğinden** sorumludur.
- ⌚ İş sürecine, bir uygulamaya veya veri setine sahip atanabilir.

Varlık Listesi Oluşturma

- ⌚ Neyi korumak istediğimizi listeleriz
- ⌚ Risk analizi için başlangıç noktasıdır
- ⌚ Varlık listesine, varlıkların fiziksel yeri, formatı, yedeği olup olmadığı gibi olası bir felaketten kurtarma durumunda gerekli olacak bilgiler girilir.
- ⌚ Varlıkların sahipleri ve değeri belirlenerek varlık envanteri oluşturulur

Varlık Listesinin Oluřturulması

Varlıkların İsimlerinin Belirlenmesi

Güvenlik Kriterlerinin Belirlenmesi



Varlık Listesi Oluşturma

- ⌚ Önce varlıkların isimleri tespit edilmeli
- ⌚ Donanım varlıkları en somut varlıklar olduğu için buradan başlanması kolaylık sağlayacaktır.
- ⌚ Donanım varlıkları listelenirken bilgi işleyen her türlü varlık listelenir. Klavye, fare gibi bilgi işlemeyenler yazılmayacak.
- ⌚ Tabloda varlıkların bulunduğu yerin olması da tüm varlıkların sıralandığı tespitini doğrulacaktır.
- ⌚ Donanım varlıkları listesi üzerinden yazılım varlıkları listelenecektir
- ⌚ Bu yazılımların işlediği bilgiler üzerinden bilgi varlıkları listelenecektir

Varlık Envanteri

	Sahibi	Değeri	Konumu
Personel			
Bilgi (Elektronik / Basılı)			
Yazılım Varlıkları			
Donanım			
Hizmetler			

Varlık Envanteri Oluřturma

- ⌚ Varlık listesindeki her bir varlık için daha somut tanımlayıcı olacak (seri no, sahibi, lisans bilgisi vs.) kullanılarak varlık envanteri oluşturulur.

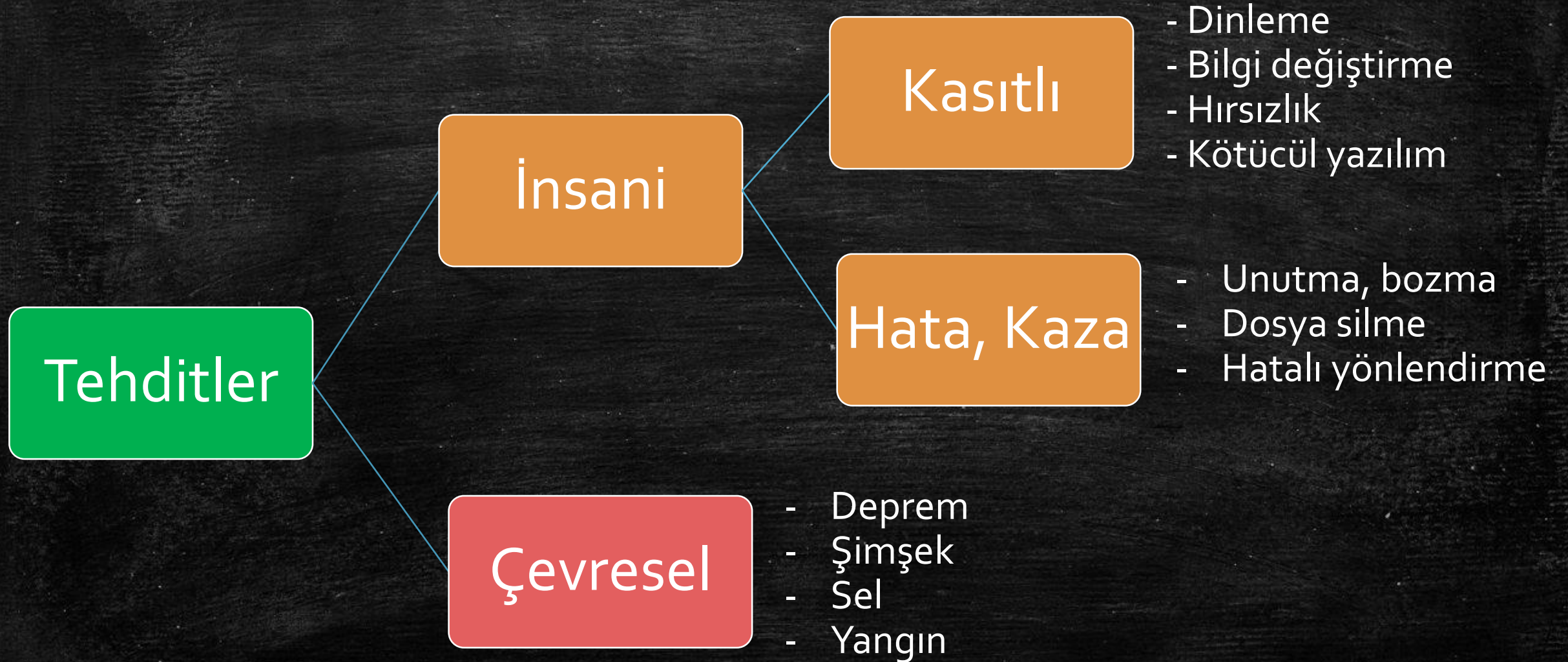
Uygulama 1 – Risk Belirleme Tablosu

⌚ Bir kurumsal iş sürecinin;

- Bilgi
- Yazılım
- Donanım, altyapı
- İnsan
- Alınan hizmet

varlıklarını ve varlık sahiplerini Risk Belirleme Tablosu.xls dosyasına listeleysiniz.

Tehditler



Uygulama 2 – Tehdit Listesi

- ⌚ Tehdit Listesi dosyasını inceleyiniz.
- ⌚ Uygulama-1’de listelenen bilgi varlıklarına yönelik *tehditleri* aynı dosyada ilgili varlığın karşısına kaydediniz.

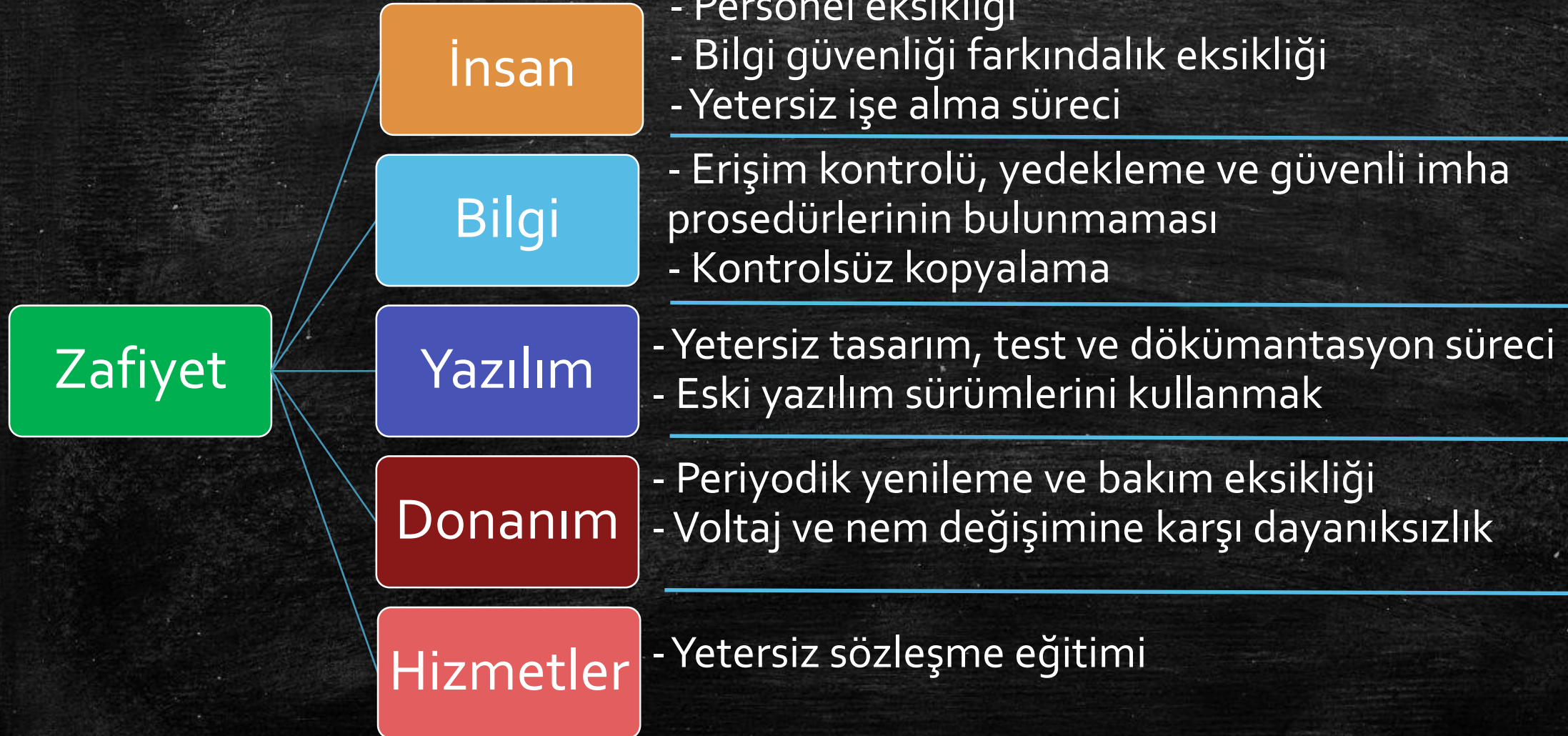
Zafiyet

⌚ Saldırgana fırsat verebilecek yazılım, donanım, prosedüre zafiyeti

Örnek :

- Güncellenmemiş yazılımlar
- Açık modemler
- Lisansız yazılımlar
- Server odasının açık olması

Zafiyet Nedenleri



Uygulama 3 – Zafiyet Listesi

⌚ Zafiyet Listesi dosyasını inceleyiniz.

⌚ Uygulama-2’de belirlediğiniz tehditlerin kullanabileceği *zafiyetleri* aynı dosyaya kaydediniz.

Tehdit Ajanı

- ⌚ Zafiyetten faydalanacak kişi veya örgüt

Varlıklara Değer Atanması

- ⌚ Varlığın güvenliğinin sağlanamaması sonucu karşılaşılabilecek zararın tahmini değerini atamaktır.
- ⌚ Varlıkla ilgili sağlanması gereken bilgi güvenliği seviyesi ile eşdeğerdir

Varlıklara Değer Atanması

⌚ **Gizlik (Confidentiality)** : Verilerin , başkaları tarafından öğrenilmesi istenmeyebilir.

â Amaç : Herşeyi gizlemek değil, veriye sadece yetkisi olanların ulaşabilmesini sağlamak; trafik akışının analiz edilmekten korunması.

⌚ **Bütünlük (Integrity)** : Sahip olunan verilerin başkaları tarafından değiştirilmesi istenmeyebilir.

â Amaç :Veri üzerinde yetkisiz ve izinsiz değişiklikler engellenir.

⌚ **Erişebilirlik (Availability)** : Verilerin istendiği zaman ulaşılabilir olup kullanıma hazır olması istenir.

â Amaç : Veriyi iletmek, depolamak ve işlemekten sorumlu hizmetlerin devamlılığının sağlanması

Varlıklara Değer Atanması

İnsan varlığının değeri nasıl atanacaktır?

İnsan Varlığı

- ⌚ Tüm çalışanlar varsa üçüncü taraflar olarak listelenir.
- ⌚ Listelemeyi gruplar halinde yapmak faydalı olmaktadır.
- ⌚ Riskler gruplara karşı farklılık göstermektedir.
- ⌚ Gruplar **Karar Vericiler, Kullanıcılar, Sistemi İşletenler** ve **Uygulama Geliştiriciler** şeklinde düzenlenebilir.
- ⌚ Kurum insan kaynağını kişi bazında mı, iş unvanı/tanımı bazında mı tanımlamalıdır?
- ⌚ Kişiler değişebilir ancak iş tanımlarının (rollerin) kalıcı olduğu düşünülerek iş unvanı/tanımı bazında bir listeleme kullanışlı olacaktır.

İnsan Varlığı İçin Gizlilik Değeri

<i>Gizlilik Değeri</i>	<i>Açıklaması</i>
Düşük	İlgili rol veya üçüncü taraf erişimi “Tasnif Dışı” olarak sınıflandırılmış bilgi varlıklarıyla sınırlıdır. Bu rollerdeki kişilerden kaynaklanacak gizlilik ihlali iş operasyonlarını etkilemez/az etkiler.
Orta	İlgili rol veya üçüncü tarafın erişimi “Tasnif Dışı” ve “Hizmete Özel” olarak sınıflandırılmış bilgi varlıklarıyla sınırlıdır. Bu rollerdeki kişilerden kaynaklanacak gizlilik ihlali iş operasyonlarını orta derecede etkiler.
Yüksek	İlgili rol veya üçüncü taraf “Gizli” olarak sınıflandırılmış bilgileri veya kritik BT varlıklarını içerecek şekilde her türlü erişime sahiptir. Bu rollerdeki kişilerden kaynaklanacak gizlilik ihlali iş operasyonlarını ciddi derecede etkiler.

İnsan Varlığı İçin Bütünlük Değeri

<i>Bütünlük Değeri</i>	<i>Açıklaması</i>
Düşük	İlgili rol ve üçüncü taraf sadece “Tasnif Dışı” veya “Hizmete Özel” olarak sınıflandırılmış bilgi varlıklarını değiştirme hakkına sahiptir ve izlemeye tabidir. Bu rollerdeki kişilerden kaynaklanacak bütünlük ihlali iş operasyonlarını etkilemez/az etkiler.
Orta	İlgili rol ve üçüncü taraf sadece “Tasnif Dışı” veya “Hizmete Özel” olarak sınıflandırılmış bilgi varlıklarını değiştirme hakkına sahiptir. Bu rollerdeki kişilerden kaynaklanacak bütünlük ihlali iş operasyonlarını orta derecede etkiler.
Yüksek	İlgili rol ve üçüncü taraf sadece “Gizli” olarak sınıflandırılmış bilgi varlıklarını veya kritik BT varlıklarını değiştirme hakkına sahiptir. Bu rollerdeki kişilerden kaynaklanacak bütünlük ihlali iş operasyonlarını ciddi derecede etkiler.

İnsan Varlığı İçin Erişebilirlik Değeri

<i>Erişilebilirlik Değeri</i>	<i>Açıklaması</i>
Düşük	İlgili rolün atandığı kişinin mevcut olmayışı/ erişilememesi iş operasyonlarını etkilemez/az etkiler.
Orta	İlgili rolün atandığı kişinin mevcut olmayışı/ erişilememesi iş operasyonlarını orta derecede etkiler.
Yüksek	İlgili rolün atandığı kişinin mevcut olmayışı/ erişilememesi iş operasyonlarını ciddi derecede etkiler.

Uygulama 4 -

⌚ Uygulama-2 ve Uygulama-3'te belirlenen tehdit ve zafiyetlerin bilgi varlıklarının

- Gizlilik,
- Bütünlük ve
- Erişilebilirliğine

etkisini belirleyiniz.

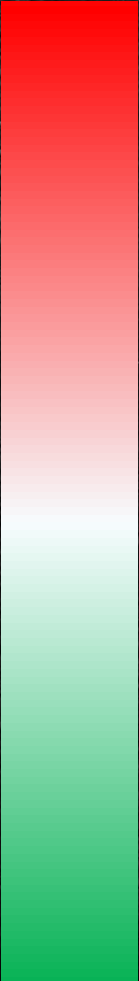
Risk Değerlendirme

- ⌚ Risk analizi ve risk derecelendirme süreçlerinin bütünü
- ⌚ Risk değerlendirmesi sonucunda:
 - Kabul edilebilir risk seviyesi belirlenir
 - Hangi risk için ne yapılacağı belirlenir:
 - Risk işleme
 - Diğer seçenekler
 - Riskler kritiklik sırasına göre sıralanır.
 - Azaltılacak risk kalemlerinin öncelikleri belirlenir.

Risk Analizi ve Derecelendirme

- ⌚ Güvenlik ihlalinin oluşması sonucunda kurumun karşılaşacağı **zararın belirlenmesi**
- ⌚ Güvenlik ihlalinin oluşma **olasılığının belirlenmesi**
- ⌚ Riskin hesaplanması
- ⌚ Riskin, önceden tanımlanmış olan risk ölçeğine göre değerlendirilmesi

Zarar Belirleme Ölçeği



Zararın Etki Derecesi		Zararın Açıklaması
4	Çok yüksek	- Kurumun itibarının kaybolması - Hayati tehlike / can kaybı - Çok yüksek düzeyde maddi kayıp
3	Yüksek	- Kurumun itibarının ciddi düzeyde zarara uğraması - Belirgin hayati tehlike / can kaybı olasılığı - Yüksek düzeyde maddi kayıp
2	Orta	- Kurumun itibarının orta düzeyde zarara uğraması - Orta düzeyde hayati tehlike - Orta düzeyde maddi kayıp
1	Düşük	- Kurumun itibarının hafif düzeyde zarara uğraması (durum kurtarılabilir) - Düşük düzeyde hayati tehlike - Düşük düzeyde maddi kayıp

Uygulama 5 -

- ⌚ Güvenlik ihlallerinin oluşması halinde kurumun karşılaşacağı zararı belirleyiniz.

Tehdit Olasılığı Belirleme Ölçeği

Tehdit ajanın zafiyetten yararlanma olasılığı

Olasılık Değeri	Gerçekleşme sıklığı	Değer Adı
5	Günde en az bir defa	ÇY (Çok yüksek)
4	Haftada en az bir defa	Y (Yüksek)
3	Üç ayda bir defadan çok	O (Orta)
2	Yılda bir defadan çok	D (Düşük)
1	Yılda bir defadan az	ÇD (Çok düşük)

Uygulama 6

- ⌚ Güvenlik ihlallerinin oluşma olasılıklarını belirleyiniz

Riskin Hesaplanması

$$\text{Risk} = F(\text{Varlık}, \text{Açıklık}, \text{Tehdit})$$



The diagram illustrates the components of the risk formula. A light blue rectangular box contains the text 'ZARAR x OLASILIK'. Three white arrows point from the terms in the formula above to this box: a vertical arrow from 'Varlık' to 'ZARAR', a vertical arrow from 'Açıklık' to 'OLASILIK', and a diagonal arrow from 'Tehdit' to the 'x' operator.

ZARAR x OLASILIK

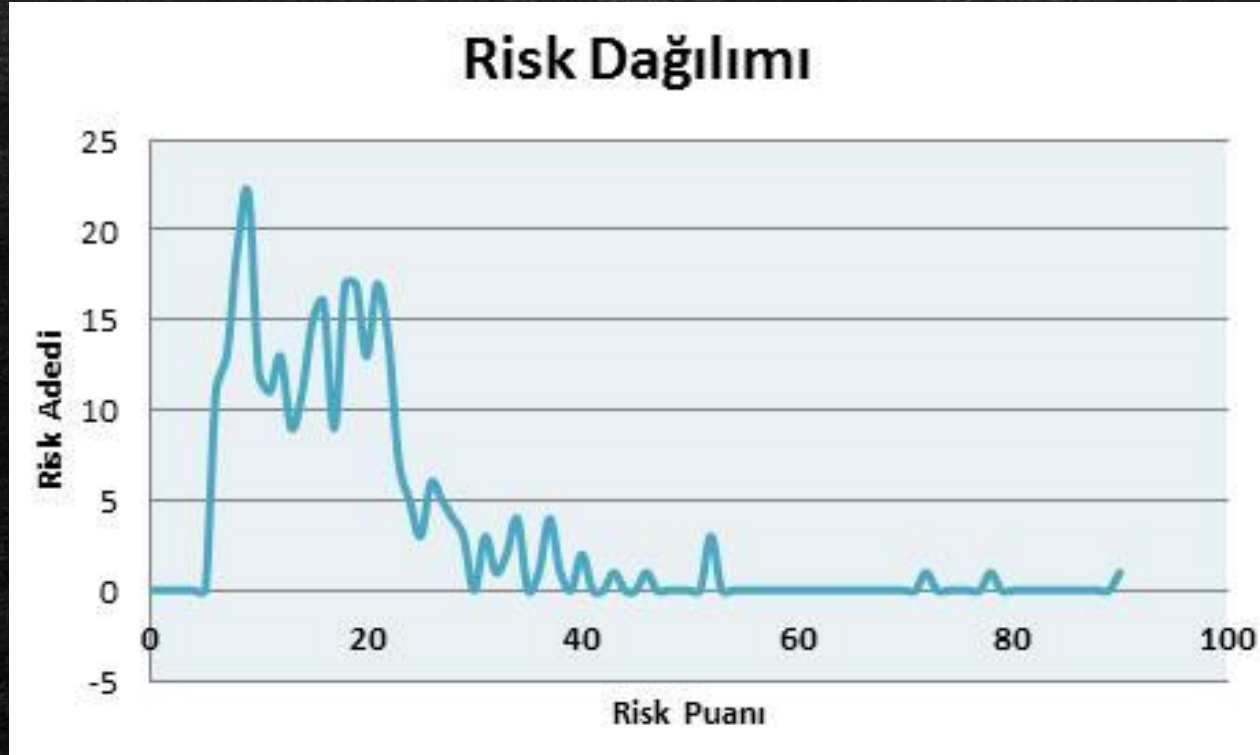
Uygulama 8

- ⌚ Risk değerlerini belirleyiniz.

Riske Karşı Üç Temel Seçim

- ⌚ **Kabul** : Eğer korunmasızlık çok küçük boyutlarda ve onu koruma altına almak büyük maliyet getiriyorsa, politikanız riski kabul edebilir.
- ⌚ **Devretme** : Bazı durumlarda riske karşı direk olarak koruma almaktansa onun için birini görevlendirmek daha az maliyet getirebilir.
- ⌚ **Kaçınma** : Güvenlik olaylarının neredeyse hiç olmayacağı yerleri korumaya almak maliyet getireceğinden bundan kaçınılmalıdır.

Kabul Edilebilir Risk Seviyesi



Uygulama 9

- ⌚ Risk değerleri gözden geçirilerek kabul edilebilir risk seviyesini belirleyiniz.

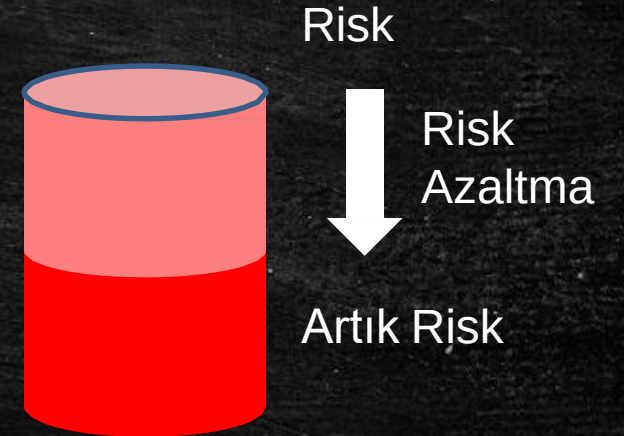
Artık Risk

Risk işleme sonrasında kalan risk (“residual risk”)

Artık riski değerlendirin (Kabul edilebilir / edilemez...)

- Daha fazla kontrol uygulayın
- Kabul etmek zorunda kalınabilir

🕒 **Yönetim onayı gerekir.**



Karşı Önlem ve Koruma

- ⌚ Potansiyel riskleri azaltmak için alınacak önlemler
- ⌚ Bir tehdit ajanın zafiyeti istismar etmesini önleyecek bir önlem
- ⌚ % 100 önlem olmaz

0 Halde Ne kadar Güvenlik Gerekli?

- ⌚ **Ne tür varlıklar** korumak gereklidir?
- ⌚ Bu varlıkları **nelere karşı** korumalıyız?
- ⌚ Bize **kim** tehlikeli **saldırı** yapabilir ve ne kazanabilir?
- ⌚ Bir **tehdit**'in varlıklarımızı **bozma olasılığı** ne kadardır?
- ⌚ Eğer bir tehlikeli saldırı olursa bunun **ivedi maliyeti** ne olacaktır?

Acil Maliyet Nedir?

- ⌚ Saldırı sonucunda fonksiyonunu yapamayacak olan her bir varlık için acil maliyetin hesaplanması gereklidir.
- ⌚ Örneğin bir sabit disk bozulmasından dolayı sunucunun kapalı kalmasının kabaca dakikada 14.50 dolarlık bir ivedi maliyeti olacağı söylenebilir.
- ⌚ Bazen ivedi maliyetin hesabı oldukça güç olabilir.
- ⌚ Örneğin, bazı rakiplerin çalacağı şema, çizim, ve yeni üretilecek parçaların projelerinden dolayı maliyet daha fazla olacaktır. Bu ise rakiplerin daha gelişmiş ürün tasarımlarına neden olacaktır. Böyle bir kayıp çok daha yıkıcı olabilecektir.

0 Halde Ne kadar Güvenlik Gerekli?

- ⌚ **Ne tür varlıklar**ı korumak gereklidir?
- ⌚ Bu varlıkları **nelere karşı** korumalıyız?
- ⌚ Bize **kim** tehlikeli **saldırı** yapabilir ve ne kazanabilir?
- ⌚ Bir **tehdit**'in varlıklarımızı **bozma olasılığı** ne kadardır?
- ⌚ Eğer bir tehlikeli saldırı olursa bunun **ivedi maliyeti** ne olacaktır?
- ⌚ Bir atak veya bozulmanın **geri kazanma maliyeti** ne olacaktır?

Geri Kazanma Maliyeti Nedir?

- ⌚ Bozulma veya zararlı saldırının başlangıç maliyetini hesapladıktan sonra bu bozulmanın getireceği toplam maliyetin hesaplanması gereklidir.

Geri Kazanma Maliyeti Nedir?

- ⌚ Örneğin şirket bilgisini saklayan bir sunumcu bozulmasındaki maliyetler için;
- ⌚ Bütün kullanıcıların bağlantılarının kesilmesinin ani maliyeti ne olur.
- ⌚ Yapılan saldırının hangi kaynakları ne kadar süre erişilemez yaptığının maliyeti nedir.
- ⌚ Silinen veya bozulan kritik dosyaların onarım maliyeti nedir.
- ⌚ Her bir donanım elemanının onarım maliyeti nedir.
- ⌚ Bütünüyle bir sunumcunun onarım maliyeti nedir.
- ⌚ Bilgi çalınmış ve hırsız bulunamamış ise bunun maliyeti ne olacaktır..

0 Halde Ne kadar Güvenlik Gerekli?

- ⌚ **Ne tür varlıklar**ı korumak gereklidir?
- ⌚ Bu varlıkları **nelere karşı** korumalıyız?
- ⌚ Bize **kim** tehlikeli **saldırı** yapabilir ve ne kazanabilir?
- ⌚ Bir **tehdit**'in varlıklarımızı **bozma olasılığı** ne kadardır?
- ⌚ Eğer bir tehlikeli saldırı olursa bunun **ivedi maliyeti** ne olacaktır?
- ⌚ Bir atak veya bozulmanın **geri kazanma maliyeti** ne olacaktır?
- ⌚ Bu varlıklar, **etkin maliyet** ile nasıl korunabilir?

Bu Varlıklar Etkin Maliyet İle Nasıl Korunabilir?

- ⌚ Maliyetin en az olmasına dikkat edilmelidir.
- ⌚ Bu nedenle koruncak olan varlıkların risk analizlerinden korumanın seviyesi belirlenmiş olacaktır
- ⌚ Bazı güvenlik seçimlerinde güçlüklerle karşılaşabiliriz.
 - â Örneğin Internet bağlantısında paket filtreleme yeterli midir.? Yoksa bir güvenlik duvarı yatırımı yapılmalı mıdır.?
- ⌚ Bunlar güvenlik uzmanlarının düşünüp çözüm bulacakları önemli sorulardır.

Güvenlik Önlemleri Bütçesinin Çıkarılması

- ⌚ Uygulanacak Güvenlik önlemlerinin maliyetinin çıkartılarak tahmini bütçenin ne olduğunun belirlenmesi gereklidir.
- ⌚ Bunlar Sunumcu donanımı güvenlik duvarı ve güvenli bölgelerin kurulumunu ve güvenlik personeli, testler, ve sistem bakımını içerebilir.
- ⌚ Burada hiçbir zaman “bütün yumurtaları aynı sepete koyma” sözünü unutmamak gerekir.

Bulunanların Yazılı Olarak Dökümente Edilmesi

- ⌚ Bu çalışmalar sonucunda elde edilen bulguların yazılı olarak raporlanması gereklidir.
- ⌚ Çünkü bu doküman daha sonraki güvenlik önlemlerinin geliştirilmesinde temel kaynak olacaktır.
- ⌚ Ayrıca daha sonra yapılan işlemlerin günlük olarak kayıtlarının tutulması gereklidir.

Güvenlik Politikası

- ⌚ Kolay anlaşılabilir olmalıdır
- ⌚ Öneri tavsiye değil emir kipi kullanır
- ⌚ Teknik değildir
- ⌚ Güvenlik işlerini tüm kurum faaliyetlerine entegre etmeyi amaçlar
- ⌚ Zamanla güncellenmelidir

Güvenlik Politikası Oluşturulması

- ⌚ Güvenlik politikası aynı zamanda kuruluşun tamamının güvenlik hedeflerini açıklamalıdır.
- ⌚ Politika, güvenliğin temelini oluşturur.
- ⌚ Kurumun önemli gördüğü ve korunması gereken bilgiler ile bu bilgileri tehdit eden hareketleri belirler.
- ⌚ İdeal güvenlik, ağ tasarımı, bilginin gizlilik derecesini ve kullanıcı hakları ile uygulama sınırlamalarını hesaba katan sağlam bir güvenlik politikası ile başlar.

Güvenlik Politikası Oluşturulması

① Güvenlik politikasının oluşturulmasında sorulacak anahtar sorular şunlardır.

1. Kime, nereye, ne zaman, nereden ve hangi yetkiyle izin verilebilir ?
2. Hangi aktiviteler tehdit olarak görülür ve güvenlik riski yaratırlar ?
3. Ne tip gözden kaçmalar ve dikkatsizlikler olabilir?
4. Güvenlik politikasının gerçekleştirilmesinde kim, ne yetki ve sorumluluğa sahiptir?

Güvenlik Politikası Temelleri

- ⌚ Farklı tiplerdeki bilgilere erişim için kişilere yetki sağlar.
- ⌚ Ne tür ve ne kadar güvenlik zorunluluğu ve ölçülerine uyulması gerektiğine bakarak kuralları ve standartları belirler.
- ⌚ Neredeyse bütün kurumların bir bilgi güvenliği politikası vardır. Fakat bazı kurumlarda politika açıkça yazılmamıştır.
- ⌚ Politika yazılmazsa, organizasyon çalışanların yanlış anlamalarından dolayı risk altındadır demektir.
- ⌚ Ayrıca bir güvenlik problemi olması durumunda cezanın boyutu da belirsiz olacaktır.
- ⌚ Bir politika yazmak, organizasyonun kararlılığının başlangıcıdır.

Güvenlik Politikası Yazılması

- ⌚ Bir bilgi güvenliği politikası bir vakum içinde yazılmaz.
- ⌚ O kurumun ihtiyaçlarıyla direkt olarak ilişkilidir. Bütün kurumlara tam olarak uyan genel bir güvenlik politikası yoktur.
- ⌚ Güvenlik politikası oldukça kısa olmalıdır. Yaklaşık olarak beş sayfa olabilir.
- ⌚ Platform bağımlı terimler olmamalı, genel olmalıdır.
- ⌚ Yapı ve teknolojiye göre esnek olarak hazırlanmalıdır.
- ⌚ Birkaç yıllık bir ömrü olmalıdır.
- ⌚ Politika yayınlanmalı ve bütün kullanıcılara açık olmalıdır

Güvenlik Politikası Yazılması

Güvenlik Politikası

Standartlar ve Ana Kurallar

Kullanıcı Sözleşmeleri

Prosedürler

Güvenlik Politikası Kavramlar

🕒 **Yönerge** : Önerilerdir; kural değil işin daha iyi yapılmasını sağlayacak yol göstericilerdir.

â Politika'nın uygulanmasına yönelik detayları belirler. Örnek : Şifre en az 8 karakterden oluşmalıdır.

🕒 **Temel (Baseline)** : Bir sistem veya ağ için asgari güvenlik önlemleri

â Örnek : İşletim sistemleri güncel olmalıdır

🕒 **Standart** : Yapılması zorunlu kurallar

🕒 **Prosedür** : Belirli bir durumda yapılması gerekenleri adım adım anlatır. Politika'nın en alt basamağıdır. Politika'nın kişiye yansıyan halidir. Örnek . Windows kurulumu için izlenecek adımlar.

Güvenlik Politikası Kavramlar

⌚ İşe Alım Süreçleri :

- â Çalışanların geçmişi araştırılmalı
- â Çalışanlar gizlilik sözleşmesi imzalamalı
- â Eğitim / Öğrenim durumu kontrolü yapılmalı
- â Referans kontrolü yapılmalı

⌚ Rotasyon :

- â Görevler arasında rotasyon olmalı
- â Süreçler birden fazla kişinin hakim olması sağlanmalı. Tek bir kişinin belirli süreçler üzerinde fazla yetkiye sahip olması engellenmeli. Görevler Ayrılığı : tek bir kişinin kritik bir süreci tamamlayamaması sağlamak

⌚ Görevler Ayrılığı : tek bir kişinin kritik bir süreci tamamlayamaması sağlamak

⌚ Zorunlu İzin :

- â Başkalarının süregelen usulsüzlükleri bulabilmesini sağlar.
- â Sürecin personelden bağımsız işleyebildiğini gösterir.

Güvenlik Politikası Kavramlar

⌚ Bilginin Bölünmesi :

- â Tek bir kişinin kritik bir süreci tamamlayacak bilgiye sahip olmasını engeller
 - ⌚ Örnek : Kasa parolasının sadece yarısını bilen banka müdürleri

⌚ İşten Çıkarmalar :

- â Personelin nasıl işten ayrılacağı net bir şekilde belirlenmeli
- â Çıkış mülakatı
- â Giriş kartlarının teslim edilmesi
- â Hesaplara erişimin kesilmesi
- â E-posta hesaplarının kapatılması

Güvenlik Sorumluluğu

- ⌚ Politika, güvenlik için kimlerin sorumlu olduğunu belirtmek zorundadır.
- ⌚ Politika bütün kullanıcılardan sahip oldukları sistem ve veriler için, güvenlik bilgi ve sorumluluklarının anlaşılmasını ve sözleşme yapılarak imzalanmasını ister.

İyi Bir Güvenlik Politikası Nasıl Olmalı

- ⌚ Kuruluşun bütün üyeleri tarafından kolaylıkla erişilebilmelidir.
- ⌚ Güvenlik hedeflerini açıkça tanımlamalıdır.
- ⌚ Politikada açıklanan her bir konu doğru bir şekilde tanımlanmalıdır.
- ⌚ Her bir konuda kuruluşun konumunu açıkça göstermelidir.
- ⌚ Her konu hakkındaki politikanın savunulmasını açıklamalıdır.
- ⌚ Ne koşullarda konseptin uygulanabileceğini açıklamalıdır.

İyi Bir Güvenlik Politikası Nasıl Olmalı

- ⌚ Kuruluş üyelerinin görev ve sorumlulukları, açıklanan sonuçlarda belirtilmelidir.
- ⌚ Açıklanan politikaya uymayanların durumu hecelenerek açıklanmalıdır.
- ⌚ Açıklanan konseptin sonraki detaylarının veya açıklamalar için başvuru bilgisi içermelidir.
- ⌚ Kullanıcıdan beklenen gizliliğin seviyesini tanımlamalıdır.
- ⌚ Tanımlanmayan konulardaki kuruluşun tutumunu içermelidir.

Bir Güvenlik Politikası Örneği

- ⌚ Bu politika özel olarak, "Internet tabanlı Web sunucu kaynaklarına erişim" i amaçlar
- ⌚ Kuruluşun konumu, "iş ilişkili olan görevlerin yapılmasında kullanılacaktır" şeklinde açıklanır. Web browsing sadece iş ilişkili aktivitelerde kullanılacaktır.
- ⌚ Bu politika sadece ağ kaynaklarının etkin ve verimli bir şekilde kullanımını amaçlar.
- ⌚ Politika bütün çalışanlara eşit olarak uygulanacaktır. Bu politika üretimde ve üretim dışındaki zaman periyodunda kullanılacaktır.

Bir Güvenlik Politikası Örneđi

- ⌚ Politikada ađ personeli web sunucuyu gözleyecek, Ayrıca her bir çalışan web erişimi için yöneticisinden izin alacaktır. Bunun anlamı her yöneticinin web erişimi için izin verme yetkisi olacađıdır.
- ⌚ Bu politikaya uymayanların yazılı olarak ikaz edileceğinin belirtilmesi gereklidir.
- ⌚ Daha fazla bilgi için lütfen doğrudan ađ yöneticiniz ile irtibata geçiniz. şeklinde olacaktır.
- ⌚ Bütün web erişimleri ađ personeli tarafından izlenecektir. Böylece personeli gizlilik seviyesi sıfırdır.

Sözleşmenin İçereceği Konular

- ⌚ Kurumun sistem ve verileri vardır
- ⌚ Kullanıcılar yetkilerinin olmadığı veri ve yazılım kopyalarına erişmemeyi kabul etmelidirler
- ⌚ Kullanıcılar parolalarını uzun olarak seçmeli ve gizli yerlerde saklamayı kabul etmelidirler
- ⌚ Kullanıcılar güvenlik için kurum haklarını koruduklarını bilmelidirler

ISO 27001

- ⌚ ISO 1946'dan beri standart hazırlıyor.
- ⌚ 27000 türevleri bilgi güvenliği konularını içeriyor.
- ⌚ Bilgi Güvenliği Yönetim Sistemi Standardı
- ⌚ Bilgi güvenliği risklerini değerlendirmek
- ⌚ Bu değerlendirmeye göre riskleri yönetmek

Kaynakça

- ⌚ İbrahim Soğukpınar, [Veri ve Ağ Güvenliği Ders Notları](#)
- ⌚ Alper Başaran, [Siber Güvenlik ve Hacking](#)
- ⌚ Tahsin Türköz, [Bilgi Güvenliğinde Risk Yönetimi](#)
- ⌚ Tolga Mataracioğlu, Ünal Tatar, [Örnek Varlık Envanteri Oluşturma Metodolojisi](#)
- ⌚ Günce Öztürk, [Varlık Değerlemesinde İnsan](#)

Bilgi Toplama

Biz kimiz

İstihbarat Çeşitleri

Pasif Bilgi Toplama

- Hedef sistemden bağımsız

Aktif Bilgi Toplama

- Hedef sistemle doğrudan iletişime geçerek

Pasif Bilgi Toplama

Pasif bilgi toplama, penetrasyon testlerinde bilgi toplama bölümünün ilk adımını teşkil etmektedir. **Hedef sistem ile doğrudan iletişime geçilmez, herhangi bir iz bırakmadan internetin imkanları kullanılarak yapılır.** Hedef ile ilgili tüm bilgiler internet üzerinden kuruma ait sistem ve sunuculara erişmeden toplanmaya çalışılır.

Pasif Bilgi Toplama

⌚ OSINT (Open Source Intelligence) : Açık istihbarat toplama.



Bilginin değerli olması için illaki gizli olması gerekmiyor.

İstihbarat kaynakları değerli bilgilerin çoğunu açık kaynaklardan elde ediyor.



pipl



SIK KULLANILAN YÖNTEMLER:

- ⌚ Whois: DNS sorgularını yapabileceğimiz ve pasif bilgi toplamak için kullanılan özel web sayfaları
- ⌚ Arama motorları (Google, Bing, Yahoo vs.)
- ⌚ Sosyal paylaşım ağları (Twitter, Facebook, LinkedIn, Pipl vs.)
- ⌚ Bloglar ve tartışma forumları
- ⌚ Kariyer siteleri
- ⌚ Github

whois

- ⌚ Eğer elinizde bir domain varsa <http://www.whois.com.tr/> 'ye girip:
- ⌚ Bu domain kime ait?
- ⌚ Hangi sunucu bu web hizmetini sağlıyor?
- ⌚ Adres ne zaman alındı?
- ⌚ Nereden satın alındı?
- ⌚ Şirketin IP aralığı ne, sorumlu yöneticisi kim? gibi soruların cevabını bulabilirsiniz.

Whois Bilgisi

🕒 whois gtu.edu.tr

```
** Registrant:
GEBZE TEKNİK ÜNİVERSİTESİ REKTÖRLÜĞÜ
GEBZE TEKNİK ÜNİVERSİTESİ REKTÖRLÜĞÜ
PK.141
Kocaeli,
Türkiye
dnsadmin@gyte.edu.tr
+ 90-262-6051000-
+ 90-262-6538490-

** Administrative Contact:
NIC Handle      : gtu50-metu
Organization Name : Gebze Teknik Üniversitesi Rektörlüğü
Address         : Gebze Teknik Üniversitesi Rektörlüğü
                  P.K 141
                  Kocaeli,41400
                  Türkiye
Phone           : + 90-262-6051000-
Fax             : + 90-262-6538490-

** Technical Contact:
NIC Handle      : gtu50-metu
Organization Name : Gebze Teknik Üniversitesi Rektörlüğü
Address         : Gebze Teknik Üniversitesi Rektörlüğü
                  P.K 141
                  Kocaeli,41400
                  Türkiye
Phone           : + 90-262-6051000-
Fax             : + 90-262-6538490-
```


Link Extraction

🕒 lynx -listonly -dump gtu.edu.tr

References

🏠 Home

Desktop

Documents

Downloads

Visible links

1. <http://www.gtu.edu.tr/#content>
2. <http://www.gtu.edu.tr/?languageId=1>
3. <http://www.gtu.edu.tr/kategori/3/3/display.aspx?languageId=1>
4. <http://www.gtu.edu.tr/kategori/2/3/display.aspx?languageId=1>
5. <http://www.gtu.edu.tr/kategori/4/3/display.aspx?languageId=1>
6. <http://www.gtu.edu.tr/kategori/5/3/display.aspx?languageId=1>
7. <http://www.gtu.edu.tr/kategori/6/3/display.aspx?languageId=1>
8. <http://www.gtu.edu.tr/kategori/2280/0/display.aspx>
9. <http://anibal.gyte.edu.tr/portal/>
10. <https://ebys.gtu.edu.tr/enVision/Login.aspx>
11. <http://www.gtu.edu.tr/kategori/2281/0/display.aspx>
12. <http://www.gtu.edu.tr/kategori/975/5/display.aspx?languageId=1>
13. <http://www.gtu.edu.tr/icerik/2140/2699/display.aspx?languageId=1>
14. <http://www.gtu.edu.tr/kategori/1013/3/display.aspx?languageId=1>
15. <http://www.gtu.edu.tr/icerik/972/629/display.aspx?languageId=1>
16. <http://www.gtu.edu.tr/?cl=2>
17. [javascript:;](#)
18. <http://www.gtu.edu.tr/icerik/9/4266/display.aspx?languageId=1>
19. <http://www.gtu.edu.tr/icerik/9/4240/display.aspx?languageId=1>
20. <http://www.gtu.edu.tr/icerik/9/4180/display.aspx?languageId=1>
21. <http://www.gtu.edu.tr/kategori/975/5/display.aspx?languageId=1>

Ödev :

- ⌚ External ve internal linkleri toplayan crawler yazın.
- ⌚ Bulunan alt domainler içindeki linklerde listeye eklensin
- ⌚ Bulunan linkler türüne göre sıralansın.

ARIN(American Registry for Internet Numbers)

🕒 <https://www.arin.net/> e girip bulduğunuz IP yi arattığınızda IP aralığını i verir.

The screenshot shows the ARIN website's WHOIS-RWS search results. The search was performed for the IP address 50.63.202.28. The results are displayed in a table format, showing the network details and contact information.

Network

Net Range	50.62.0.0 - 50.63.255.255
CIDR	50.62.0.0/15
Name	GO-DADDY-COM-LLC
Handle	NET-50-62-0-0-1
Parent	NET50 (NET-50-0-0-0-0)
Net Type	Direct Allocation
Origin AS	AS26496
Organization	GoDaddy.com, LLC (GODAD)
Registration Date	2011-02-02
Last Updated	2014-02-25
Comments	Please send abuse complaints to abuse@godaddy.com
RESTful Link	https://whois.arin.net/rest/net/NET-50-62-0-0-1

Function

Function	Point of Contact
NOC	NOC124-ARIN (NOC124-ARIN)
Tech	NOC124-ARIN (NOC124-ARIN)

RELEVANT LINKS

- > [ARIN Whois/Whois-RWS Terms of Service](#)
- > [Report Whois Inaccuracy](#)
- > [Whois-RWS API documentation](#)
- > [ARIN Technical Discussion Mailing List](#)
- > [Sample stylesheet \(xsl\)](#)

NETCRAFT

🕒 http://toolbar.netcraft.com/site_report



Site report for www.gtu.edu.tr



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

Lookup another URL:

Background

Site title	Gebze Teknik Universitesi	Date first seen	March 2015
Site rank		Primary language	Turkish
Description	Büyük Bir Devlet Üniversitesi		
Keywords	Not Present		

Network

Site	http://www.gtu.edu.tr	Netblock Owner	Gebze Yuksek Teknoloji Enstitusu
Domain	gtu.edu.tr	Nameserver	ns1.gtu.edu.tr
IP address	193.140.134.3	DNS admin	dnsadmin@gtu.edu.tr
IPv6 address	Not Present	Reverse DNS	dyn.gtu.edu.tr
Domain registrar	nic.tr	Nameserver organisation	whois.nic.tr
Organisation	GEBZE TEKNİK ÜNİVERSİTESİ REKTÖRLÜĞÜ	Hosting company	gyte.edu.tr
Top Level Domain	Turkey (.edu.tr)	DNS Security Extensions	unknown
Hosting country	 TR		

Hosting History

Netblock owner	IP address	OS	Web server	Last seen	Ref
Gebze Yuksek Teknoloji Enstitusu	193.140.134.3	Windows Server 2008	Microsoft-IIS/7.5	15-Jun-2016	Ref

Security

Netcraft Risk Rating [FAQ]	1/10 	On Exploits Block List	No
On Spamhaus Block List	No	On Domain Block List	No
On Policy Block List	No		

Sender Policy Framework

CENTRALOPS:

centralops.net/co/

Central Ops .net

Advanced online Internet utilities

Utilities

- Domain Dossier
- Domain Check
- Email Dossier
- Browser Mirror
- Ping
- Traceroute
- NsLookup
- AutoWhois
- TcpQuery
- AnalyzePath

Domain Dossier

Investigate domains and IP addresses

domain or IP address

☒ domain whois record ☒ DNS records ☐ traceroute

☒ network whois record ☐ service scan

user: anonymous [85.97.174.44]
balance: 45 units
[log in](#) | [account info](#)

Central Ops .net

Address lookup

canonical name [onedio.com.](#)

aliases

addresses **2400:cb00:2048:1::6814:17f7**
2400:cb00:2048:1::6814:18f7
104.20.23.247
104.20.24.247

Domain Whois record

Queried [whois.internic.net](#) with "dom onedio.com"...

```
Domain Name: ONEDIO.COM
Registrar: NAME.COM, INC.
Sponsoring Registrar IANA ID: 625
Whois Server: whois.name.com
Referral URL: http://www.name.com
Name Server: HEATHER.NS.CLOUDFLARE.COM
Name Server: WOZ.NS.CLOUDFLARE.COM
Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Updated Date: 01-apr-2015
Creation Date: 27-nov-2010
Expiration Date: 27-nov-2018
```

>>> Last update of whois database: Fri, 14 Oct 2016 19:32:19 GMT <<<

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

Queried [whois.name.com](#) with "onedio.com"...

```
Domain Name: ONEDIO.COM
Registry Domain ID: 1627560233_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.name.com
Registrar URL: http://www.name.com
Updated Date: 2015-04-01T19:59:07Z
Creation Date: 2010-11-27T15:20:17Z
Registrar Registration Expiration Date: 2018-11-27T15:20:17Z
Registrar: Name.com, Inc.
```


Utilities

Domain Dossier
Domain Check
Email Dossier
Browser Mirror

Ping
Traceroute
Nslookup
AutoWhois
TcpQuery
AnalyzePath

```
Registrar: onedio.com
Reseller:
Domain Status: clientTransferProhibited
Registry Registrant ID:
Registrant Name: Onedio Bilisim
Registrant Organization: Onedio Bilisim Yazilim Medya Tekn. San. Tic. A.S
Registrant Street: ODTU Teknokent Silikon Blok No:35
Registrant City: Ankara
Registrant State/Province: Cankaya
Registrant Postal Code: 06060
Registrant Country: TR
Registrant Phone: +90.3122101048
Registrant Email: onediocom@gmail.com
Registry Admin ID:
Admin Name: Arsen Nurmagomedov
Admin Organization: Onedio Bilisim Yazilim Medya Tekn. San. Tic. A.S
Admin Street: ODTU Teknokent Silikon Blok No:35
Admin City: Ankara
Admin State/Province: Cankaya
Admin Postal Code: 06060
Admin Country: TR
Admin Phone: +90.5301040767
Admin Email: arsen@onedio.com
Registry Tech ID:
Tech Name: Ekin Koc
Tech Organization: Onedio Bilisim Yazilim Medya Tekn. San. Tic. A.S
Tech Street: ODTU Teknokent Silikon Blok No:35
Tech City: Ankara
Tech State/Province: Cankaya
Tech Postal Code: 06060
Tech Country: TR
Tech Phone: +90.5327980532
Tech Email: ekin@onedio.com
Name Server: woz.ns.cloudflare.com
Name Server: heather.ns.cloudflare.com
DNSSEC: Unsigned Delegation
Registrar Abuse Contact Email: abuse@name.com
Registrar Abuse Contact Phone: +1 7203101849
URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/
>>> Last update of WHOIS database: 2016-10-14T13:32:29-06:00 <<<
```

Network Whois record

Queried **whois.arin.net** with "n 104.20.23.247"...

```
NetRange:      104.16.0.0 - 104.31.255.255
CIDR:          104.16.0.0/12
NetName:       CLOUDFLARENET
NetHandle:     NET-104-16-0-0-1
Parent:        NET104 (NET-104-0-0-0-0)
NetType:       Direct Assignment
OriginAS:      AS13335
Organization:  CloudFlare, Inc. (CLOUD14)
RegDate:       2014-03-28
Updated:       2015-10-01
```


IPAddress.com

onedio.com.ipaddress.com

 **IPAddress.com**
The Best IP Address Tools

[My IP](#) [IP Tools](#) [Email Tools](#) [Speed Test](#) [Articles](#)

My IP: 85.97.174.44

Search for a IP Address, Domain or Hostname

Onedio.com

Onedio Website and Webhosting Information

Advertisements

We found that the organization hosting Onedio.com is CloudFlare in San Francisco, California, United States.

A more detailed IP address report for Onedio.com is below. At the time you pulled this report, the IP of Onedio.com is 104.20.23.247 and is located in the time zone of America/Los_Angeles. The context of Onedio.com is "Onedio" and could reflect the theme of the content available on the resource. More IP details of Onedio.com are shown below along with a map location.

IP Address of Onedio is 104.20.23.247			
Hostname:	onedio.com	City:	San Francisco
IP Address:	104.20.23.247	Country:	United States 
Organization:	CloudFlare	State:	California
ISP/Hosting:	CloudFlare	Postal Code:	94107
Updated:	10/09/2016 09:06 PM	Timezone:	America/Los_Angeles
		Local Time:	10/14/2016 12:41 PM

Top of the page

Onedio.com Reverse IP | Websites on the same Webhosting

We found 1 hostname for IP Address 104.20.23.247

1	onedio.com
---	------------

Top of the page

Map location for Onedio.com | Onedio



onedio.com.ipaddress.com

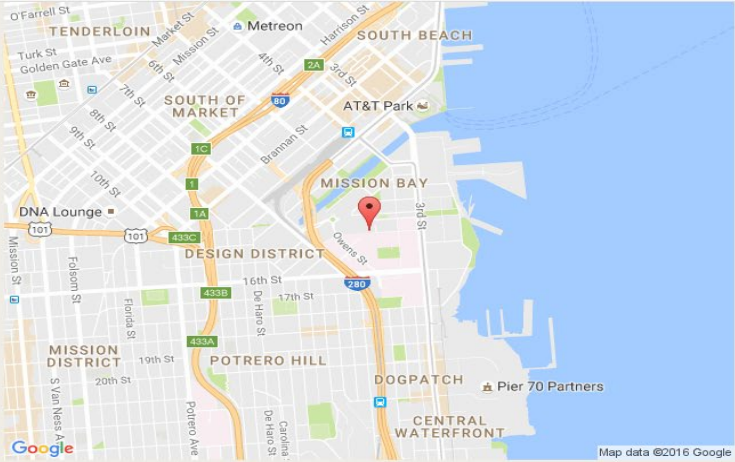
 **IPAddress.com**
The Best IP Address Tools

[My IP](#) [IP Tools](#) [Email Tools](#) [Speed Test](#) [Articles](#)

My IP: 85.97.174.44

Search for a IP Address, Domain or Hostname

Map location for Onedio.com | Onedio



Map data ©2016 Google

[Top of the page](#)

Onedio.com Whois

 Registrar

Name.com, Inc.

 Whois Server

whois.name.com

 Referral URL

http://www.name.com

Wayback Machine

🕒 1966 dan bu yana web sitelerin önceki kaydedilmiş bilgilerini tutar.



Waybackmachine



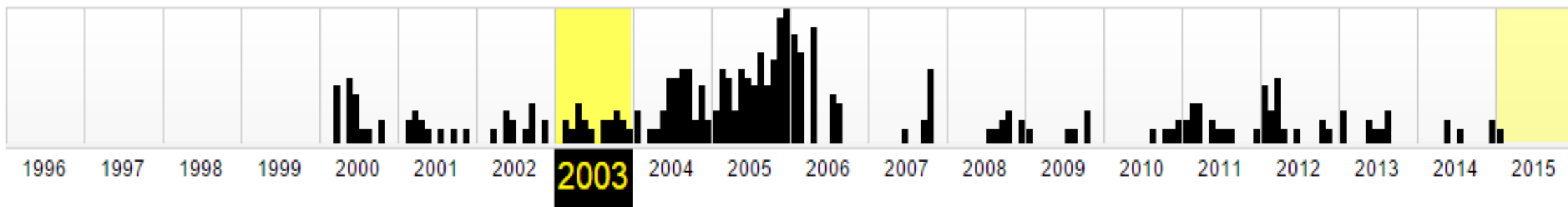
<http://www.mynet.com.tr>

BROWSE HISTORY

<http://www.mynet.com.tr>

Saved **474 times** between Mart 1, 2000 and Ocak 1, 2015.

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



Facebook

- Anne kızlık soyadı
- Doğum tarihi
- En sevdiği film
- En sevdiği renk
- Tuttuğu takım



Pipl.com

→  **Pipl, Inc [US]** | <https://pipl.com/search?q=halil+öztürkçi&l=&loc=&in=6>

pipl 

Search By

First

Last

+ MORE OPTIONS 

☒ All Locations

☐ Turkey

☐ Istanbul

☐ United States

Results for **Halil Öztürkçi**

 **Halil Ozturkci**
Istanbul, Turkey
SPONSORED: [Contact Details](#) | [Username Report](#)
Partner at ADEO IT Consulting Services and 3 more jobs

 **Halil Öztürkci**
Istanbul, Turkey
SPONSORED: [Social Profile](#) | [Username Report](#)
Known online as halilozturkci

 **Halil Öztürkci, halilozturkci**
soundcloud.com/halilozturkci
 Member's Profile - SoundCloud

 **Halil Öztürkci**
Associated with Uğur Güngör
SPONSORED: [Vital Records](#) | [Contact Details](#)

 **Halil Öztürkci**
Istanbul, Turkey
SPONSORED: [Contact Details](#)

 **Halil Öztürkci, halil.ozturkci**
facebook.com/people/_/100003080037125
 Personal Web Profile - Facebook

İş ilanları - Kariyer.net

linkedin

Haberler

Theharvester Script

```
root@kali:~# theharvester
```

```
*****
*
* | | | | _ _ _ _ _ / \ / \ _ _ _ _ _ | | _ _ _ _ _
* | | | | _ _ _ _ _ / \ / \ / \ / \ / \ / \ / \ / \
* | | | | | | | | | | | | | | | | | | | | | | | | |
* \ | | | | | | | | | | | | | | | | | | | | | | | |
*
* TheHarvester Ver. 2.2a
* Coded by Christian Martorella
* Edge-Security Research
* cmartorella@edge-security.com
*****
```

Usage: theharvester options

- d: Domain to search or company name
- b: Data source (google,bing,bingapi,pgp,linkedin,google-profiles,people123,jigsaw,all)
- s: Start in result number X (default 0)
- v: Verify host name via dns resolution and search for virtual hosts
- f: Save the results into an HTML and XML file
- n: Perform a DNS reverse query on all ranges discovered
- c: Perform a DNS brute force for the domain name
- t: Perform a DNS TLD expansion discovery
- e: Use this DNS server
- l: Limit the number of results to work with(bing goes from 50 to 50 results,
- h: use SHODAN database to query discovered hosts
google 100 to 100, and pgp doesn't use this option)

Examples: theharvester -d microsoft.com -l 500 -b google
 theharvester -d microsoft.com -b pgp
 theharvester -d microsoft -l 200 -b linkedin

Theharvester Script

⌚ root@kali:~# theharvester -d kali.org -l 500 -b Google

⌚ root@kali:~# theharvester -d kali.org -l 200 -b linkedin

⌚ root@kali:~# theharvester -d kali.org -l 500 -b all

Discover Script

- ⌚ <https://github.com/leeбайд/discover> adresinden indirip kurun.
- ⌚ `./discover.sh`
- ⌚ 1 domain için
- ⌚ 1 pasif tarama
- ⌚ `gtu.edu.tr` taranacak adres
- ⌚ `/root/result.html` sonuçları çıktı olarak al



Google Hacking Database (GHDB)



[Home](#) [Exploits](#) [Shellcode](#) [Papers](#) [Google Hacking Database](#) [Submit](#) [Search](#)

Google Hacking Database (GHDB)

Search the Google Hacking Database or browse GHDB categories

Any Category ▼

Search

SEARCH

Date	Title	Category
2016-08-16	inurl:/Portal/Portal.mwsl	Various Online Devices
2016-08-16	intitle:"bandwidthd" "programmed by david hinkle, commissioned by derbytech wireless networking."	Network or vulnerability data
2016-08-16	inurl:index of driver.php?id=	Error Messages
2016-08-08	inurl:/FCKeditor/editor/filemanager/upload/	Sensitive Directories
2016-08-05	inurl:/Dialin/Conference.aspx	Pages containing login portals
2016-07-27	inurl:/pictures intitle:index.of	Sensitive Directories
2016-07-25	inurl:/sgms/auth	Advisories and Vulnerabilities
2016-07-20	site:static.ow.ly/docs/ intext:@gmail.com Password	Files containing passwords
2016-07-15	inurl:/DiGIR.php	Files containing juicy info
2016-07-07	filetype:sql intext:wp_users phpmyadmin	Files containing juicy info



Google Hacking Database (GHDB)

Özellik	Komut	Örnek
Url arama	inurl	hostname:"google"
Başlıkta arama	intitle	port:"21"
Dosya tipinde arama	filetype	country:"United States"
City	intext	city:"New York"
Organization/Company	author	org:"Amazon"
Internet Service Provider	site	isp:"Hostwinds LLC"
OS/Product/Platform	link	product:"Apache httpd"
Product Version	datarange	version:"2.2.15"
Geo Location	numrange	geo:"39.6949,-83.1383"
Date	insubject	before:"12-12-15"
IP Address/Subnet	msgid	net:"74.91.246.0/24"



Google Hacking Database (GHDB)

- ① [inurl:private_files](#) özel klasörler
- ① [site:https://github.com/ inurl:ssh/id_rsa](#) github adresinde bulunan private keyler
- ① ["BEGIN RSA PRIVATE KEY" filetype:key -github](#)



Google Hacking Database (GHDB)

- ⌚ Kategoriler :
- ⌚ [Files Containing Juicy Info](#)
- ⌚ [Files Containing Passwords](#)
- ⌚ [Sensitive Online Shopping Info](#)
- ⌚ [Network or Vulnerability Data](#)
- ⌚ [Vulnerable Servers](#)

SiteDigger :

- ⌚ Google 'ın arama tekniklerini kullanan ve Google 'ın ön belleğinde bulunan sayfalarda yukarıdaki bilgi toplama tekniklerini ve sayfa üzerindeki zafiyetleri raporlayan SiteDigger aracı **pasif bilgi toplamada** kullanılması gereken araçlardandır.

⌚ Google ve Google için yazılmış pasif bilgi toplama araçlarını kullanarak kuruma ait kritik bilgiler, mail adresleri, veritabanı dosyaları, yönetici erişimleri ve daha bir çok bilgi elde edilebilir. Elde edilen bilgiler penetrasyon testinin diğer aşamaları için ciddi değer ve önem taşır.

⌚ Linkten indirebilirsiniz:

<http://www.mcafee.com/us/downloads/free-tools/sitedigger.aspx#>

SiteDigger

File Edit Tools Help

- FSDB(175)
 - Backup Files(12)
 - Configuration Manage
 - Error Messages(39)
 - Privacy Related(30)
 - Remote Administration
 - Reported Vulnerabilit
 - Technology Profile(43)
 - "# Dumping data
 - "# phpMyAdmin M
 - "# phpMyAdmin M
 - "#mysql dump" file
 - "cacheserverrepo
 - "Host Vulnerability
 - "Index of" / "chat
 - "Most Submitted f
 - "Network Host As
 - "Network Vulnera
 - "phpinfo.php" -ma
 - "robots.txt" + "Dis
 - "Select a databas
 - "Thank you for yo
 - "These statistics v
 - "This file was gen
 - "This report lists"
 - "This report was g
 - "This summary wa
 - "Welcome to PHF
 - "YaBB SE Dev To
 - filetype htaccess
 - intitle:"Ganglia" "
 - intitle:"Index of" "
 - intitle:"Index of" m
 - intitle:"Index of" s
 - intitle:"vberm" con
 - intitle:admin intitle
 - intitle:Index of rob
 - intitle:Index of "Ap
 - intitle:Index of cgi
 - intitle:Index of hac

Site/Domain: [Optional]

Cancel

Clear

Queries Scanned:

Selected Entry Info:

161 intitle:index.of robots.txt F95
 162 intitle:index.of "Apache" "server at" F75
 163 intitle:index.of cgiirc.config' F64
 164 intitle:index.of haccess.cgi F69
 165 intitle:index.of master.passwd F23
 166 inurl:admin intitle:login F82
 167 inurl:'cgiirc.config' F65
 168 inurl:changepassword.asp F83
 169 inurl:ipsec.conf -intitle:manpage F87
 170 inurl:ipsec.secrets "holds shared secrets" F89
 171 inurl:ipsec.secrets -history -bugs F88
 172 inurl:main.php phpMyAdmin F84

Scanning...

Results: [Double click a link to open in default browser]

URL	Query	Category



Shodan.io Üzerinden Bilgi Toplama

[Shodan](#) [Scanhub](#) [Developers](#) [View All...](#)

 **SHODAN**

Shodan
World's first search engine for the Internet of Things.

Maps
Intuitive map interface to search the Shodan database.

Images
A stream of screenshots from crawled devices.

Exploits
Search across a variety of vulnerability databases at once.

Scanhub
Make your Nmap results searchable by uploading them to Scanhub.

Blog
Stay up to date with the latest developments and research.

My Account
Manage your account settings, API key, and more.

Developer API
Access the Shodan database via the Shodan API.

Maltego Add-On
Integrate Shodan with Maltego for enhanced threat intelligence.

Chrome Browser Plugin
Search Shodan directly from your Chrome browser.

Firefox Plugin
Search Shodan directly from your Firefox browser.

ICS Map 2014
Map of Industrial Control Systems (ICS) on the Internet.

Webcam Browser
Browse and search for webcams.

ICS Radar
Real-time radar for Industrial Control Systems (ICS).

Shodan CLI
Command-line interface for Shodan.

Map of the Internet
Visual representation of the Internet's structure.

Honeypot Or Not
Check if an IP is a honeypot or a real computer system.

Shodan 3D
3D visualization of Shodan search results.

presented at DHS ICS JWG

by @paulwebsec

presented at 4SICS

presented at Kaspersky SAS

Shodan, çevrimiçi bulunan belirli cihazları ve cihaz türlerini bulmak için kullanılan bir arama motorudur. En popüler aramalar web kamerası, linksys, cisco, netgear, SCADA vb. içindir.



Shodan.io Üzerinden Bilgi Toplama

Shodan Developers Book View All...

SHODAN

Explore Downloads Reports Enterprise Access Contact Us [My Account](#)

Explore

Discover the Internet using search queries shared by other users.

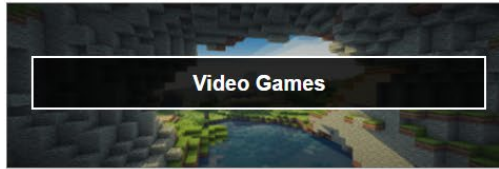
Featured Categories



Industrial Control Systems



Databases



Video Games

Top Voted

7,414

Webcam

best ip cam search I have found yet.

webcam

surveillance

cams

2010-03-15

2,620

Cams

admin admin

cam

webcam

2012-02-06

1,664

Netcam

Netcam

netcam

2012-01-13

Recently Shared

1

webcam

webcam

2016-08-16

2

matrimonio

2016-08-15

1

X-Pingback wordpres Denial of service

kelvinsecurity

2016-08-15



Shodan.io Üzerinden Bilgi Toplama

[Shodan](#) [Developers](#) [Book](#) [View All...](#)

 **SHODAN**  [Explore](#) [Downloads](#) [Reports](#) [Enterprise Access](#) [Contact Us](#)

[Exploits](#) [Maps](#) [Share Search](#) [Create Report](#)

TOP COUNTRIES



Turkey	80
--------	----

TOP CITIES

Istanbul	10
Ankara	6
Kocaeli	3
Sanayi	2
Mugla	1

TOP SERVICES

Telnet	48
HTTP	13
8081	6
8880	2
GlassFish Server	2

TOP ORGANIZATIONS

Turk Telekom	40
Vodafone Net İletişim Hizmetleri A.s	12
Tellcom İletişim Hizmetleri A.s.	4
TurkNet İletişim Hizmetleri A.S	3
Vodafone Turkey 3G IP Pool	2

TOP PRODUCTS

nginx	7
TP-LINK WR841N WAP http config	1
TP-LINK WR740N WAP http config	1
Microsoft IIS httpd	1

Total results: 79

213.254.131.44

Tellcom İletişim Hizmetleri A.s.

Added on 2016-11-20 10:55:23 GMT

 Turkey

[Details](#)

HTTP/1.1 200 OK
Server: nginx
Date: Sun, 20 Nov 2016 10:55:22 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Connection: keep-alive
Keep-Alive: timeout=20
Set-Cookie: iMSCP_Session=4ucncophigkb53v2dkbh48scd0; path=/
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Cont...

46.197.117.21

[mail.bioartmed.com](#)

Turksat Uydu-Net Internet

Added on 2016-11-20 07:14:29 GMT

 Turkey

[Details](#)

HTTP/1.1 200 OK
Server: nginx
Date: Sun, 20 Nov 2016 07:14:06 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Connection: keep-alive
Last-Modified: Sun, 20 Nov 2016 07:14:05 GMT
X-Frame-Options: SAMEORIGIN
Set-Cookie: PHPSESSID=7h381j0utqmtffv3co32ivc1tph2ojms; path=...

78.186.175.34

[78.186.175.34.static.ttnet.com.tr](#)

Turk Telekom

Added on 2016-11-20 07:13:45 GMT

 Turkey, Kocaeli

[Details](#)

<HTML>
<HEAD>
<META http-equiv="Pragma" content="no-cache">
<META http-equiv="Content-Type" content="text/html; charset=utf-8">
<title>Tenda ADSL2/2+ Modem with Wireless Router</title>

<script language="javascript" src="translate.js"></script>
<SCRIPT language=JavaScript>
TranslateDictio...

Shodan

Developers

Book

View All...

 SHODAN

default password country:tr



Explore

Downloads

Reports

Enterprise Access

Contact Us

 Exploits

 Maps

 Share Search

 Create Report

TOP COUNTRIES



| | |
|--------|----|
| Turkey | 80 |
|--------|----|

TOP CITIES

| | |
|----------|----|
| Istanbul | 10 |
| Ankara | 6 |
| Kocaeli | 3 |
| Sanayi | 2 |
| Mugla | 1 |

TOP SERVICES

| | |
|------------------|----|
| Telnet | 48 |
| HTTP | 13 |
| 8081 | 6 |
| 8880 | 2 |
| GlassFish Server | 2 |

TOP ORGANIZATIONS

| | |
|--------------------------------------|----|
| Turk Telekom | 40 |
| Vodafone Net Iletisim Hizmetleri A.s | 12 |
| Tellcom Iletisim Hizmetleri A.s. | 4 |
| TurkNet Iletisim Hizmetleri A.S | 3 |
| Vodafone Turkey 3G IP Pool | 2 |

TOP PRODUCTS

| | |
|--------------------------------|---|
| nginx | 7 |
| TP-LINK WR841N WAP http config | 1 |
| TP-LINK WR740N WAP http config | 1 |
| Microsoft IIS httpd | 1 |

Total results: 79

213.254.131.44

Tellcom Iletisim Hizmetleri A.s.

Added on 2016-11-20 10:55:23 GMT

 Turkey

Details

HTTP/1.1 200 OK

Server: nginx

Date: Sun, 20 Nov 2016 10:55:22 GMT

Content-Type: text/html; charset=UTF-8

Transfer-Encoding: chunked

Connection: keep-alive

Keep-Alive: timeout=20

Set-Cookie: IMSCP_Session=4ucncohpigkb53v2dkbh48scd0; path=

Expires: Thu, 19 Nov 1981 08:52:00 GMT

Cache-Cont...

46.197.117.21

mail.bioartmed.com

Turksat Uydu-Net Internet

Added on 2016-11-20 07:14:29 GMT

 Turkey

Details

HTTP/1.1 200 OK

Server: nginx

Date: Sun, 20 Nov 2016 07:14:06 GMT

Content-Type: text/html; charset=UTF-8

Transfer-Encoding: chunked

Connection: keep-alive

Last-Modified: Sun, 20 Nov 2016 07:14:05 GMT

X-Frame-Options: SAMEORIGIN

Set-Cookie: PHPSESSID=7h381j0utqmtffv3co32ivc1tph2ojms; path=...

78.186.175.34

78.186.175.34.static.ttnet.com.tr

Turk Telekom

Added on 2016-11-20 07:13:45 GMT

 Turkey, Kocaeli

Details

<HTML>

<HEAD>

<META http-equiv="Pragma" content="no-cache">

<META http-equiv="Content-Type" content="text/html; charset=utf-8">

<title>Tenda ADSL2/2+ Modem with Wireless Router</title>

<script language="javascript" src="translate.js"></script>

<SCRIPT language=JavaScript>

TranslateDictio...

Shodan.io parametreler

| Özellik | Komut | Örnek |
|---------------------------|--------------|-------------------------|
| Host/Domain | hostname | hostname:"google" |
| Port/Service | port | port:"21" |
| Country | country | country:"United States" |
| City | city | city:"New York" |
| Organization/Company | org | org:"Amazon" |
| Internet Service Provider | isp | isp:"Hostwinds LLC" |
| OS/Product/Platform | product | product:"Apache httpd" |
| Product Version | version | version:"2.2.15" |
| Geo Location | geo | geo:"39.6949,-83.1383" |
| Date | before/after | before:"12-12-15" |
| IP Address/Subnet | net | net:"74.91.246.0/24" |

Uygulama - Shodan.io

- ⌚ Markalara göre ürünlerin varsayılan şifreleri:
<http://www.phenoelit.org/dpl/dpl.html>
- ⌚ linux upnp avtech country:tr city:İstanbul (Ip kameralar)
- ⌚ country:tr port:3389 (Mysql veritabanları))
- ⌚ country:tr port:21 "Anonymous access granted" (Anonim ftp hesapları)
â ftp://85.105.213.197/Matica/ROKETSAN_20160811/



Metadata Analiz Aracı

Microsoft - FOCA Free 2.6

File Metadata Domain Enumeration Software Recognition Tools Logs Options About

Network data Metadata

Documents (0/248)
Metadata Summary
Users
Folders
Printers
Software
Emails
Operating Systems

Download the New
FOCA 2.6
-DNS Snooping
-Fingerprinting
-HTTP Methods
-...and more

Search engines
☒ Google
☒ Bing
☒ Exalead

Extensions
☒ doc ☒ pptx ☒ sxi ☒ pdf
☒ ppt ☒ ppsx ☒ odt ☒ wpd
☒ pps ☒ xlsx ☒ ods ☒ svg
☒ xls ☒ sxw ☒ odg ☒ svgz
☒ docx ☒ sxc ☒ odp ☒ indd

[Custom search](#) Search All

| Id | Type | URL | Download |
|----|------|--|----------|
| 0 | doc | http://www.microsoft.com/korea/sharepoint/techinfo/development/BuildCorpPortalusingXP_kr.doc | × |
| 1 | doc | http://www.microsoft.com/southafrica/partner/2002_exams.doc | × |
| 2 | doc | http://www.microsoft.com/exchange/evaluation/tiwin2003.doc | × |
| 3 | doc | http://www.microsoft.com/usability/UEPostings/DesirabilityToolkit.doc | × |
| 4 | doc | http://www.microsoft.com/usability/UEPostings/ProductReactionCards.doc | × |
| 5 | doc | http://www.microsoft.com/office/dataanalyzer/evaluation/DAGuide.doc | × |
| 6 | doc | http://www.microsoft.com/Spain/HomePage/PosturaUE.doc | × |
| 7 | doc | http://www.microsoft.com/Presspass/presskits/dynamics/docs/conv11/0412sonata.doc | × |
| 8 | doc | http://www.microsoft.com/exchange/evaluation/overview/ECSReleaseNotes.doc | × |
| 9 | doc | http://www.microsoft.com/taiwan/business/licensing/Software_Assurance_Briefing.doc | × |
| 10 | doc | http://www.microsoft.com/biztalk/techinfo/biztalkframework20.doc | × |
| 11 | doc | http://www.microsoft.com/business/downloads/health/enhancingpsq.doc | × |
| 12 | doc | http://www.microsoft.com/exchange/evaluation/ti/tiwin2003.doc | × |
| 13 | doc | http://www.microsoft.com/investor/reports/ar09/downloads/MS_2009_AR.doc | × |
| 14 | doc | http://www.microsoft.com/colombia/socios/downs/GuideLicenciamientoparaSocios.doc | × |
| 15 | doc | http://www.microsoft.com/usability/UEPostings/HCI-kirstenrisden.doc | × |
| 16 | doc | http://www.microsoft.com/solutions/edi/download/na/BOM_Request_EBISXML_10.doc | × |

Search stopped



Metadata Analiz Aracı

- ⌚ Windows ortamında çalışıyor.
- ⌚ Online ortamda ilgili adrese ait dosyaları toplayıp metada datalarını analiz ediyor.
- ⌚ Metada bilgisi üzerinde sisteme ait bilgi üretiyor.

Diğerleri

⌚ Diğer online bilgi toplama araçları : <http://www.dirk-loss.de/onlinetools.htm>

Aktif Bilgi Toplama

Traceroute

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

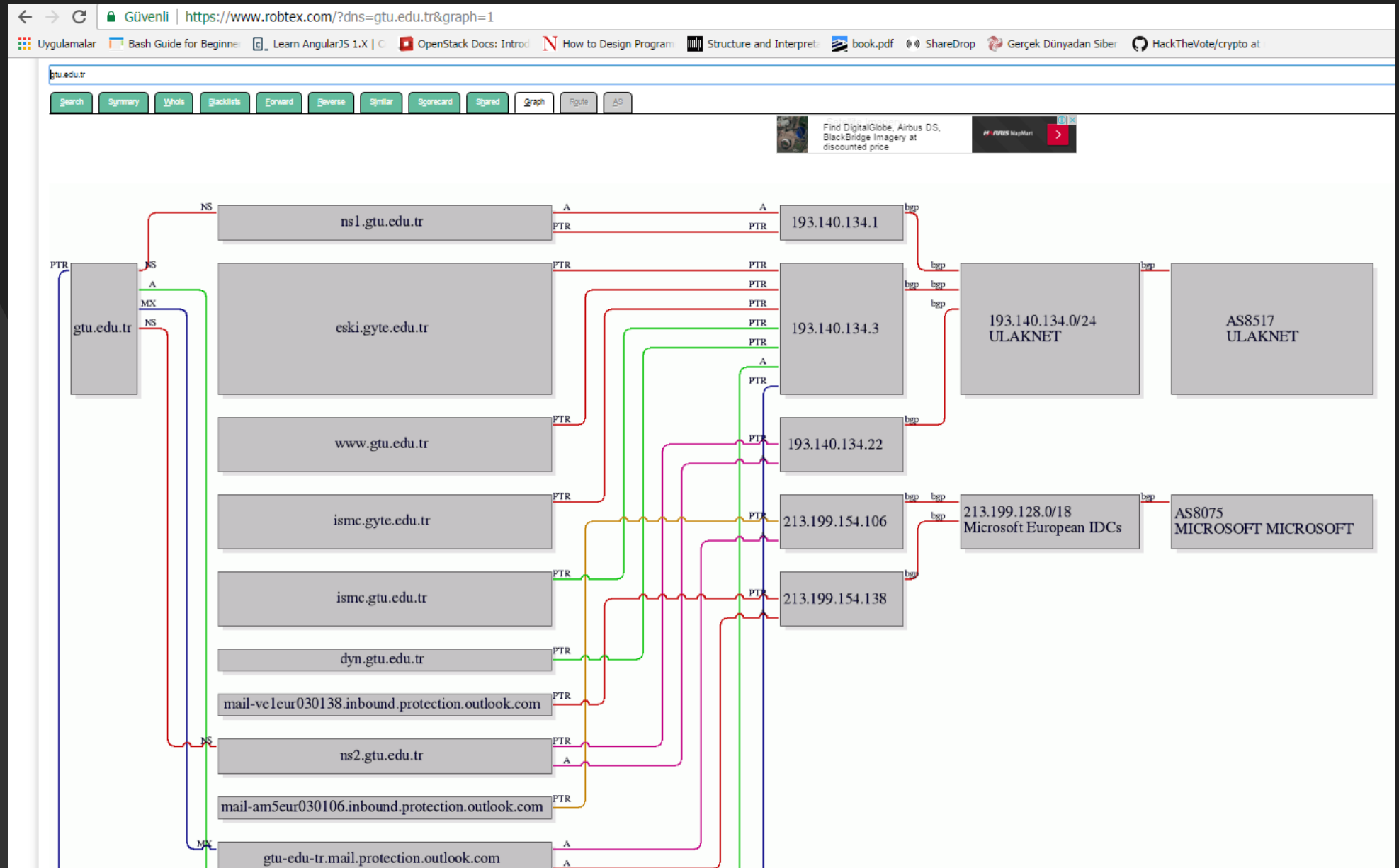
Dig

- ⌚ Detaylı DNS sorgulaması yapan gelişmiş bir araçtır.

Dirbuster

- ⌚ Hedef adresin alt dizinlerini bulmak için kullanılır.

Robtex

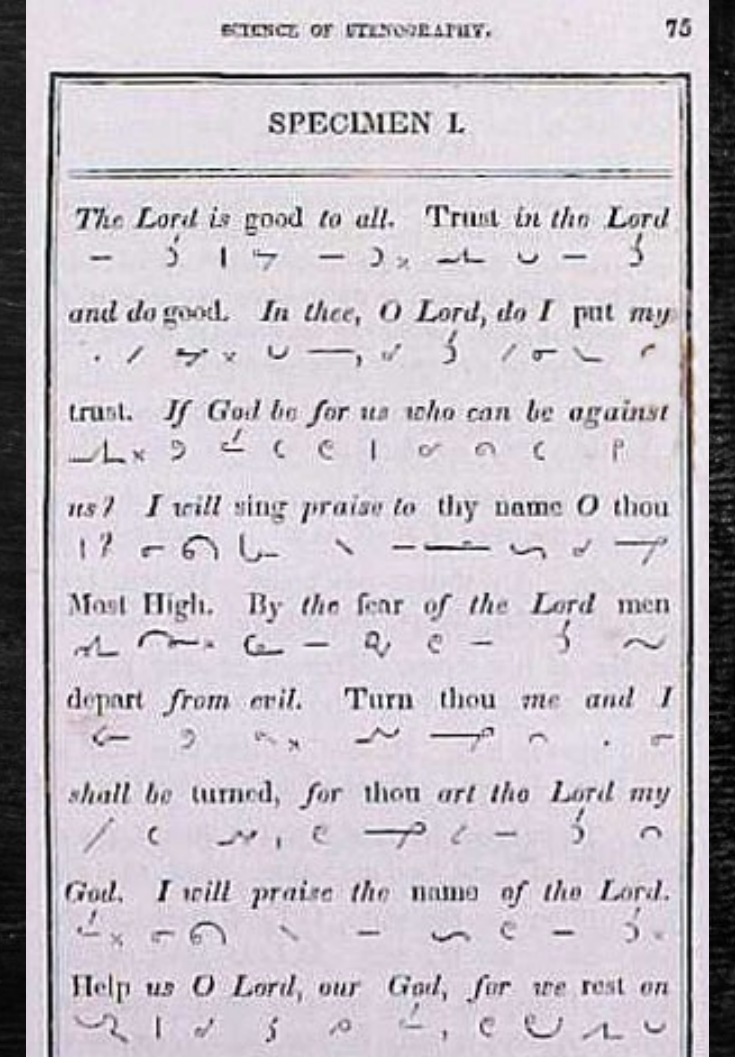


Kaynakça

Stenografi

Stenografi

- ⌚ Eski yunanca gizlenmiş bilgi anlamındadır.
- ⌚ Alfabenin harfleri, noktalama işaretleri, kelimeleri yerine semboller ve kısaltmalar kullanan **çabuk yazma; not tutma sistemi**.
- ⌚ İlk zamanlar katipler tarafından kullanılan bir yöntemdi.
- ⌚ Günümüzde hala aktif olarak kullanılıyor.
- ⌚ TBMM tutanakları. [TBMM Stenografi dokümanı](#).
- ⌚ Bilginin gizlenerek iletilmesi amacıyla da kullanılıyor.
- ⌚ Amaç, mesajı şifrelemek değil varlığını saklamak.



Stenografi

- ⌚ Günümüzde cep telefonlarının çekilen 1600 * 1200 çözünürlükteki bir resmin içine yaklaşık 2 mb'a kadar veri saklanabilir. (wikipedia)
- ⌚ Resim gizleme için fazla veri gizleme metodu bulunmaktadır. Bu yöntemler arasında en iyi en kötü ayrımı yapamayız! (wikipedia)
- ⌚ Günümüzde stenografi kolayca tespit edebilen yöntemler mevcut değil.
- ⌚ Tespit için genelde dosya büyüklüğü vb. değişikliklere bakılıyor. Dosya büyüklüğünü azaltan araçlar ve yöntemler günümüzde mevcut.
- ⌚ Daha çok istatiksel yöntemler kullanılıyor.
- ⌚ Resmin orijinal kopyası sahip olmak büyük avantaj sağlıyor.
- ⌚ Bazı resimlerde az bilgi çok fazla bozulmaya neden olabiliyor.

Stenografi Çeşitleri

- ⌚ **Metin içine** metin gizleme (Null chipher)
- ⌚ **Program içine** doküman / program gizleme Alternate Data Streams(ADS)
- ⌚ **Görüntü içine** doküman / program gizleme
- ⌚ **Ses içine** doküman / program gizleme
- ⌚ **Video içine** doküman / program gizleme

Metin Stenografi (Null Ciphering)

- ⌚ Mesaj başka bir mesajın içine belirli kurallar çerçevesinde saklanıyor.
- ⌚ Önceden belirlenmiş bir «codeword» var.
- ⌚ Genelde kısa mesajların iletiminde kullanılıyor.
- ⌚ Mesajın büyüklüğü iletilen taşıyıcı doküman büyüklüğünü de artırıyor.
- ⌚ Halka açık gazete, dergi, blog vb. yazıları üzerinden iletim sağlanıyor.

Mesaj : Apparently neutral's protest is thoroughly discounted and ignored. Isman hard hit. Blockade issue affects pretext for embargo on by-product, ejecting suets and vegetable oils.

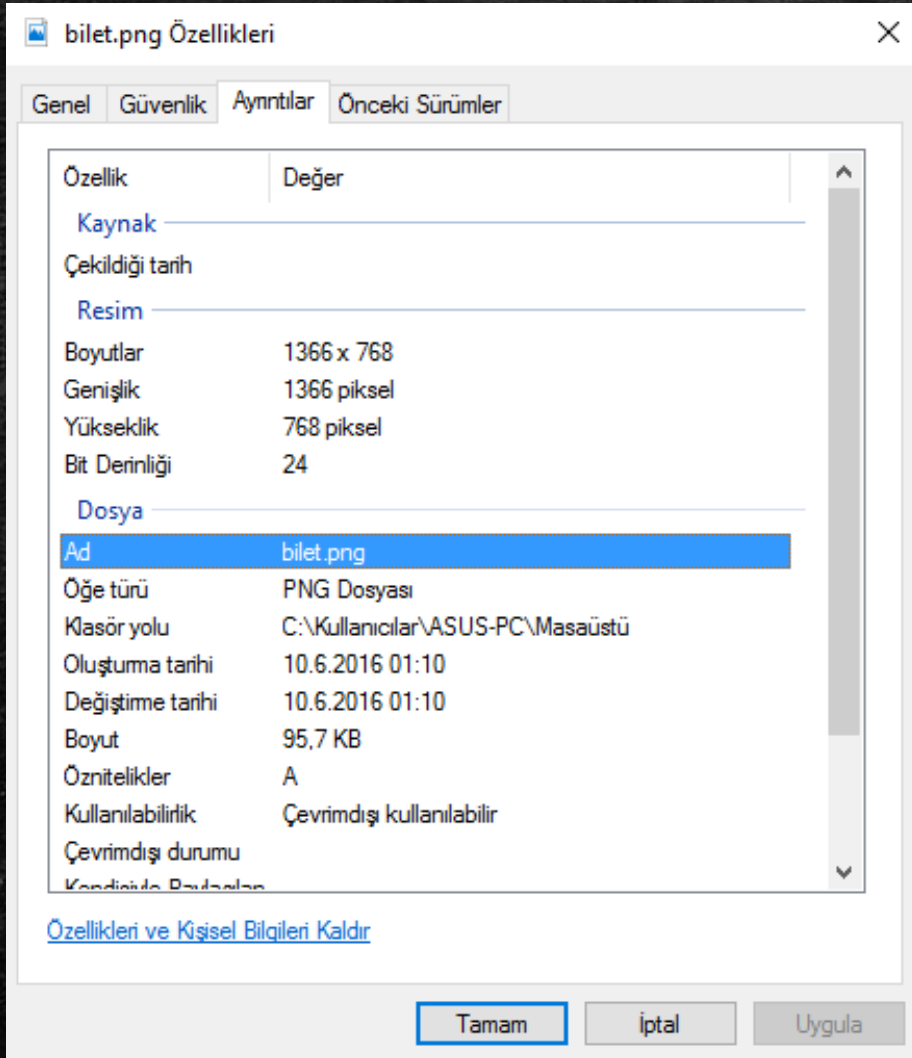
Gizli Mesaj : Pershing sails from NY June 1

1. Dünya Savaşında Almanlar tarafından kullanıldı

ADS (Alternate Data Streams)

- ⌚ Microsoft dosya sistemi NTFS (New Technology File System), Mac HFS (Hierarchical File System) uyumluluk gösterir .
- ⌚ HFS dosyayı ikiye böler, dosya ayarlarını gizli olarak dosyanın içinde tutar.
- ⌚ Bir dosya içine başka dosya gizlemesine olanak sağlar.
- ⌚ 1 kb'lık bir metin belgesinin içerisine boyutunu kesinlikle değiştirmeden 100'lerce megabyte veri saklamak mümkün.
- ⌚ Veriyi sadece tam olarak hangi isimle nerde olduğunu bilen kişi çalıştırabilir.
- ⌚ Dosyalar herhangi bir fat32 sisteme taşınırsa gizli dosyalar kaybolur.

ADS (Alternate Data Streams)



- ⌚ Dosya metadata bilgileri ADS ile tutulur.
- ⌚ Bir dosya için sınırsız sayıda ve boyutta bağlantı oluşturulabilir.
- ⌚ Dosya yanı sıra klasör ve dosya sisteminde bağlantı oluşturulabilir.
- ⌚ Sadece metin dosyaları değil, ses, görüntü ve çalıştırılabilir dosyalar içinde bağlantı oluşturulabilir.
- ⌚ Virüsler bu şekilde dosyalarla bağlanabilir.
- ⌚ Windows tarafından ADS görüntülemek için herhangi bir komut yada program yok.

Uygulama - ADS

- ① **%windir%\system32\notepad.exe belge.txt** komutuyla bir doküman oluşturun ve içine herhangi bir bilgi yazıp kaydedin.
- ① **dir belge.txt** komutyla dosyanın boyutunu öğrenin.
- ① **%windir%\system32\notepad.exe belge.txt:gizlibelge.txt** komutuyla belge.txt içerisinde gizlibelge.txt dosyası oluşturup dosyanın içerisine gizli belgeyi kaydedin.
- ① **dir** komutuyla klasörde gizlibelge.txt dosyasının oluşturulup oluşturulmadığını ve belge.txt dosyasının boyutunda değişiklik olup olmadığını kontrol edin.
- ① Klasör seçeneklerinden gizli dosyaları ve sistem korunan dosyalarını görünür hale getirin ve gizlibelge.txt dosyasının görünürlüğünü kontrol edin.
- ① **%windir%\system32\notepad.exe belge.txt:gizlibelge.txt** komutuyla gizli belgenin içeriğini gözlemleyin.

Uygulama - ADS

① **%windir%\system32\notepad.exe normal.txt**

① **type c:\resim.jpg>normal.txt:resim.jpg**

① **start .\normal.txt:resim.jpg**

① Normal dosya silindiğinde gizli dosyada silinir.

① Normal dosyayı silmeden gizli dosyayı silmek için aşağıdaki komutlar kullanılır.

① **ren belge.txt temp.txt**

① **type temp.txt > belge.txt**

① **del temp.txt**

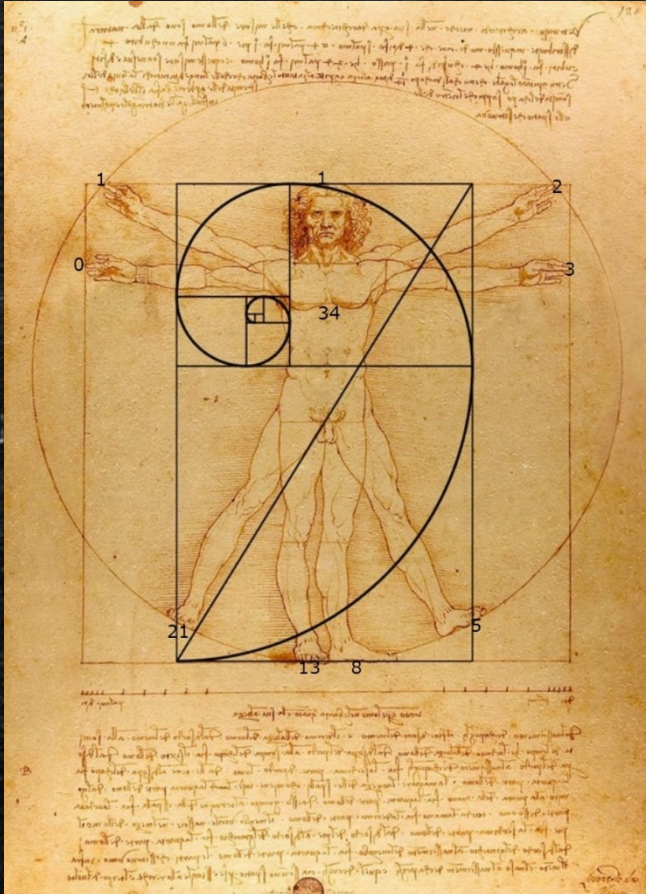
Uygulama - ADS

- ① **echo gizli bilgi > :hidden.dat** komutu kullanılarak herhangi bir metin klasöre gizlenebilir.
- ① Görüntülemek için **more < :hidden.dat** komutu kullanılır.
- ① Gizli belgeyi ayrı bir dosyaya ayırmak için.
- ① **more < belge.txt:gizlibelge.txt > gizli.txt** komutu kullanabiliriz.
- ① ADS kontrolü için 3part uygulamalar kullanılabilir : [AdsCheck](#), [Lads](#), [LNS](#), [Ads Spy](#), [Sfind](#), [Streams](#), [Hijackthis](#), [GMER](#), [Visual ADS Detector](#)

Resimde Veri Gizleme Yöntemleri

- ⌚ Resim içinde mantıksal veri gizleme
- ⌚ Resim içine veri ekleme
- ⌚ Metadata alanına veri gizleme
- ⌚ Parlaklık değeri üzerinden veri gizleme
- ⌚ En önemsiz bite ekleme
- ⌚ Maskeleye ve filtreleme
- ⌚ Diğer algoritmalar ve dönüşümler.

Resim İçinde Mantıksal Metin



Resim sonuna veri ekleme

- ⌚ Veri resmin yada dokümanın sonuna data olarak eklenir.
- ⌚ Herhangi bir metin editöre vb. ile kolayca tespit edilebilir.
- ⌚ JPEG dosyasının başlangıç (0xFFD8) ve bitiş değeri (0xFFD9) değerleri önemli ayırt edici özelliktir.
- ⌚ Bu değerlere göre veri eklemesi yapıldığı ve iki verinin birbirinden ayrılabilir.

Uygulama -

⌚ *Windows ortamında :*

⌚ *copy "<image file path>" + "<text file path>" "<new image path>"*

⌚ *Linux ortamında :*

⌚ *echo gizli bilgi >> resim.jpg* komutunu kullanarak bilgiyi resim dosyasına ekleyin.

⌚ *strings resim.jpg* komutunu kullanarak gizli bilgiyi resim dosyasından okuyun.

⌚ *Resim.jpg* dosyasını metin editörü ile açıp gizli bilgiyi elde edin.

⌚ *xxd resim.jpg* komutuyla resim dosyasının hex kodunu ve gizli bilgiyi görüntüleyin.

Uygulama -

- ⌚ *Veri gizleme işlemini orijinal dosyayı saklı tutarak yapın ve eklediğiniz dosya boyutu ve eklenen dosya boyutundaki değişimi gözlemleyin.*
- ⌚ ***diff orijinal.jpg clone.jpg** komutuyla dosyada değışiklik olup olmadığını gözlemleyin.*
- ⌚ ***xxd orijinal.jpg orijinal.hex, xxd clone.jpg clone.hex** komutlarıyla dosyaların hex kodlarını kaydedin ve **diff orijinal.hex clone.hex** komutuyla iki dosya arasındaki farkı gözlemleyin.*
- ⌚ *Veri gizleme işlemini farklı formattaki dokümanlar için tekrar edin. Resim içerisine mp3, zip formatında veriler ekleyin. Dosyanın görünür kalıp kalmadığını kontrol edin.*
- ⌚ *JPEG dosyasının başlangıç (0xFFD8) ve bitiş değeri (0xFFD9) özelliğini kullanarak eklenen dosyayı jpg dosyasından ayırın.*

Ödev -

- ⌚ Resim dosyaları için başlangıç ve bitiş hex değeri özelliklerini kullanarak resim dosyasına ekleme yapılıp yapılmadığını tespit eden program yazın.
- ⌚ Eğer veri eklenmiş ise eklenen veri türünü belirttin.
- ⌚ Eklenen dosyayı ayrı bir dosya olarak kayıt edebilme özelliği ekleyin.

Metadata Alanına Veri Gizleme

- ⌚ Yöntemlerin en kolayı.
- ⌚ Veri, resim dosyasının metadata alanında gizlenir.
- ⌚ İdeal bir yöntem değil; metadata alanının sınırı var.
 - â Örnek : yorum alanı 255 byte.
- ⌚ Bu yöntemde değişik resim dosya tipleri için değişik algoritmalar kurmanız gerekecektir.
- ⌚ Kolayca tespit edilebilir.
- ⌚ Resim dosyasına ait bir çok veri elde edilebilir. GPS lokasyonu, makine markası, tarih vb. Bu bilgiler güvenilir değildir, değiştirilebilir formattadır.

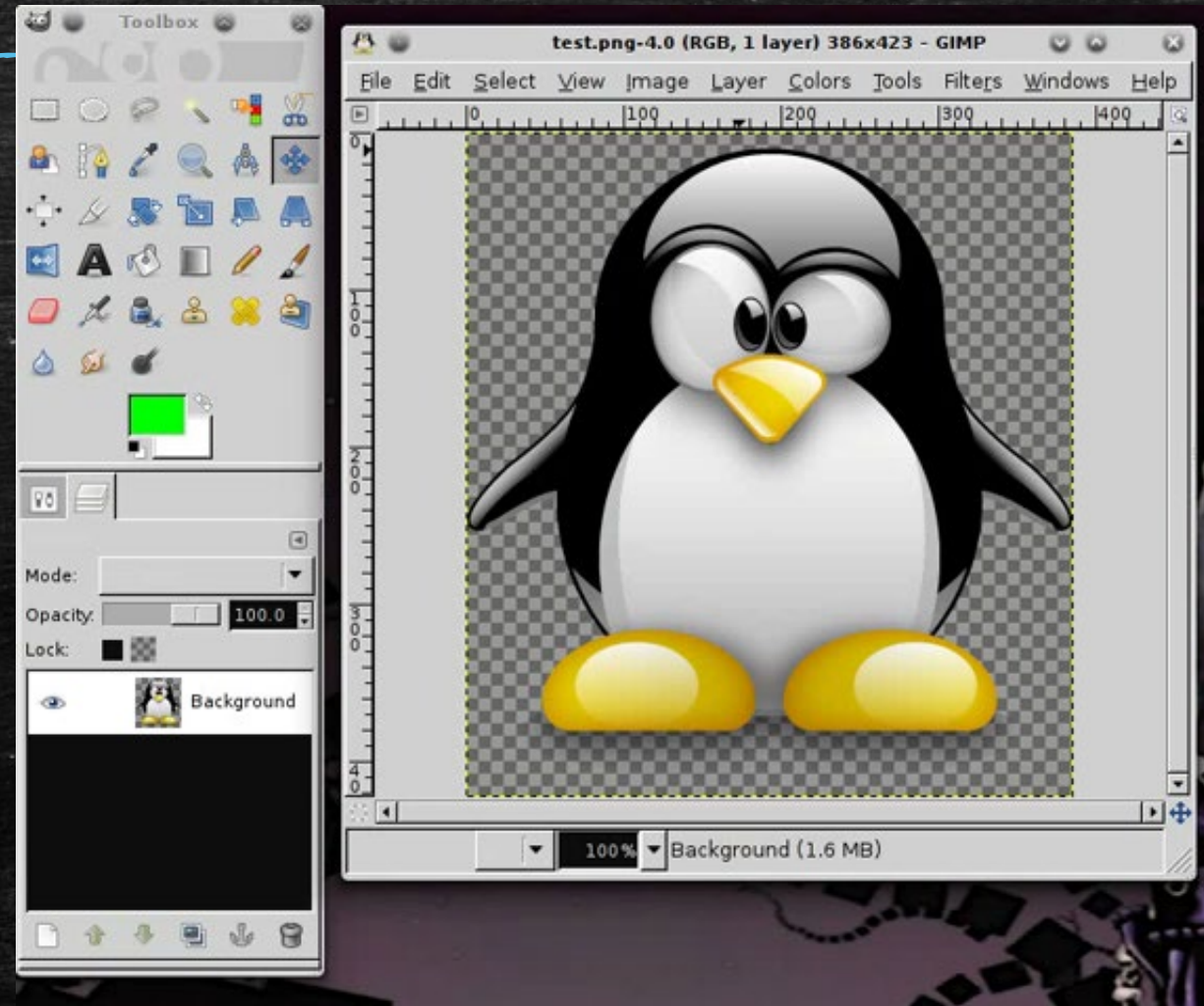
Uygulama – Resim Açıklama Alanına Gizleme

- ⌚ **exiftool resim.jpg**
- ⌚ **exiftool -Comment=«eklenen metin» resim.jpg**
- ⌚ **exiftool boya.jpg** komutunu kullanarak gps lokaysounu, kullanılan kamera, tarih vb. bilgi edinin.
- ⌚ *Longitude ve latitude değerlerini kullanarak adresinden veya farklı bir araç kullanarak gps lokasyonun nereye ait olduğunu araştırın.*
- ⌚ **exiftool -GPSLongitude="14.273586" -GPSLatitude="50.860361" boya.jpg** komutunu kullanarak boya.jpg dosyasına ait lokasyon bilgisini değiştirin.

Parlaklık Üzerinden Veri Gizleme

- ① Open your image in GIMP.
- ① Click *Windows > Dockable Dialogs > Palettes*. The image quality should degrade.
- ① Add a new Palette by clicking the blank document icon on the lower-left.
- ① Add 8 new colors by right clicking and bringing them from the foreground.
- ① Colors in order: ff0000:00ff00:0000ff:ffff00:ff00ff:00ffff:ffffff:000000
- ① Click *Image > Mode > Indexed*. Use our palette.
- ① Click *Windows > Dockable Dialogs > Colormap*.
- ① Change every color's FF to 02. The image should be almost black.
- ① Now click *Image > Mode > RGB*.
- ① Open a second image, and paste the first image we made into it.
- ① On the GIMP toolbar, anchor the image and select *Difference* from the mode menu.
- ① Click on *Image > Flatten Image*.
- ① Save as an uncompressed PNG file.

GIMP ile Veri Gizleme



Parlaklık Deęeri Üzerinden Veri Gizleme

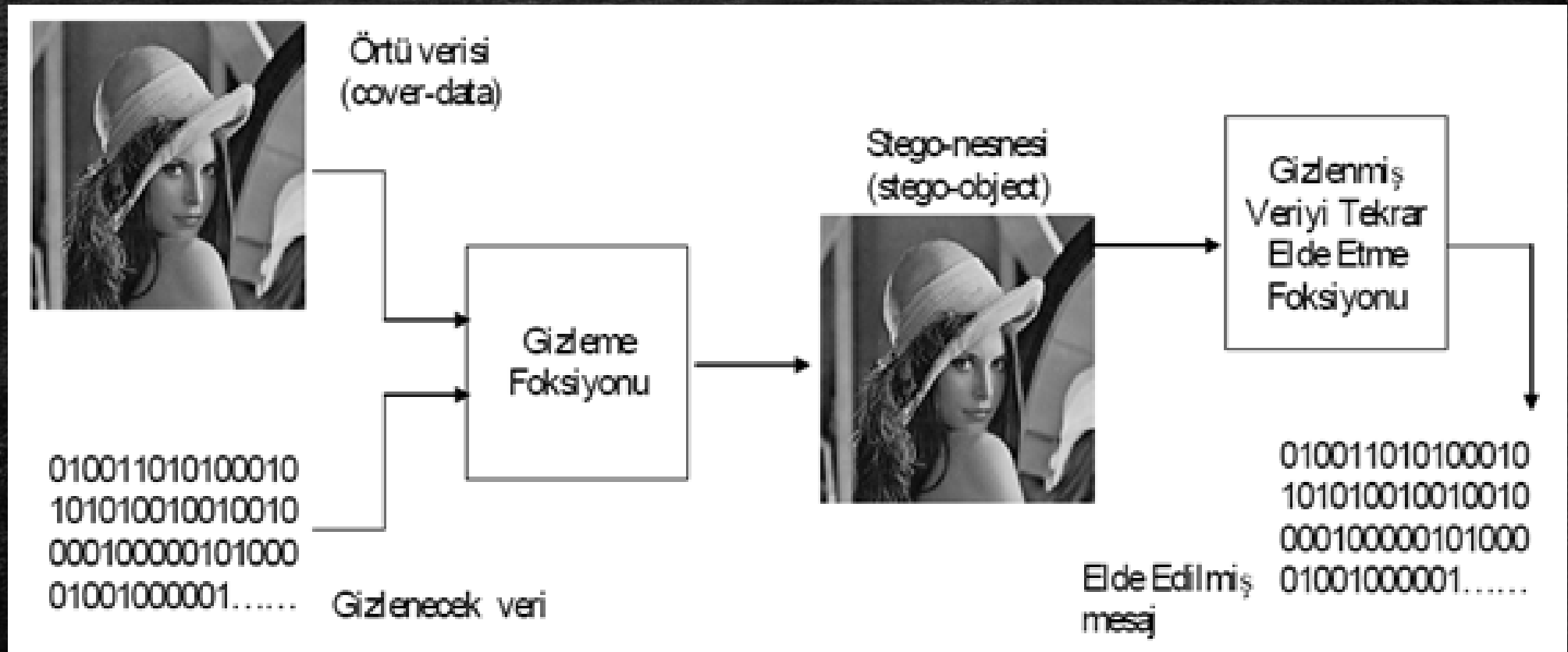


- ⌚ Metin resim üzerine kaydedilir ve parlaklık değeri değıştirilerek görünmez hale getirilir.
- ⌚ Yazılı metinlerin gizlenmesi için uygundur.
- ⌚ Genelde arka planı beyaz ve siyah olan resimler tercih edilir.
- ⌚ Küçük boyutlu veri gizleme için uygundur.
- ⌚ Resmin boyutunda büyük değışiklikler olmaz.

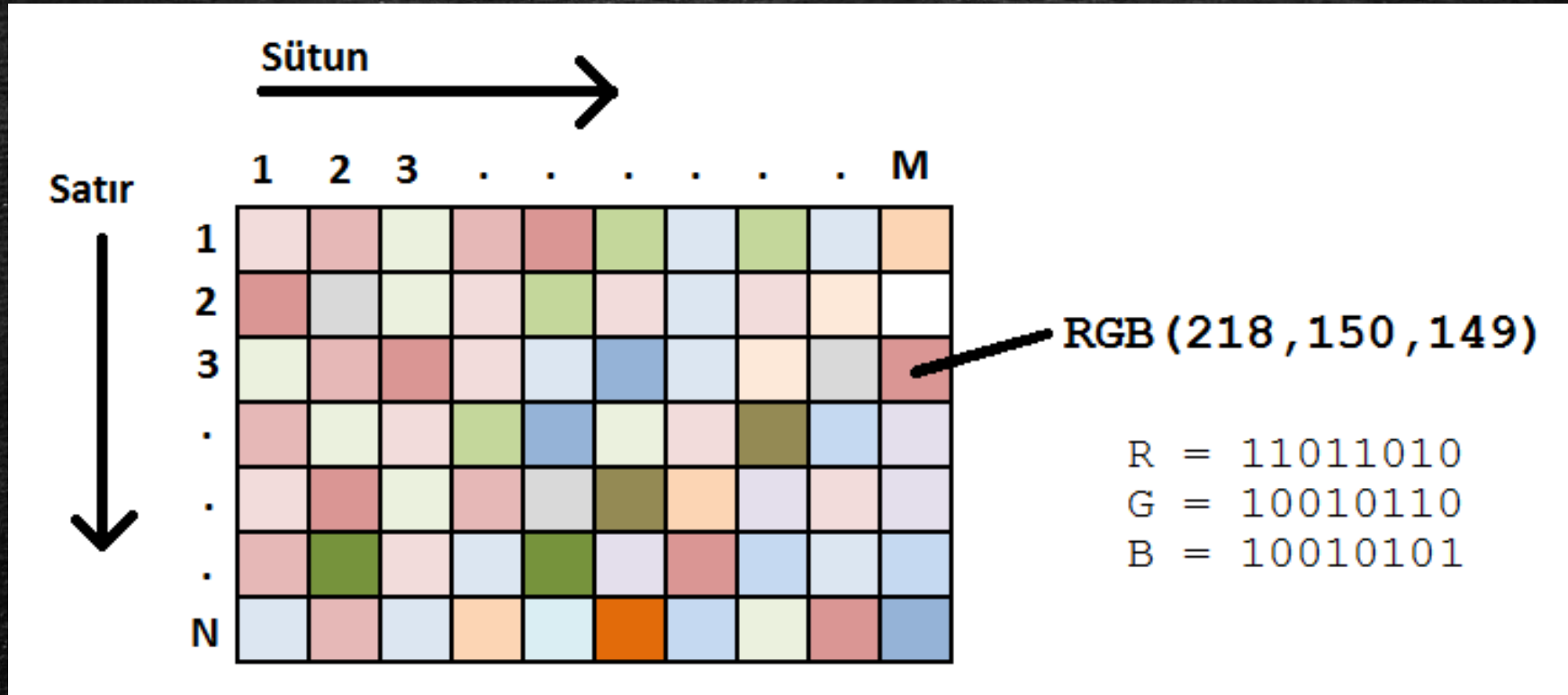
Uygulama – Parlaklık Değeri İle Gizleme

- ⌚ Resim içinde gizlenmiş veriyi parlaklık değerini değiştirerek bulun.
- ⌚ Resim içerisine parlaklık değerini değiştirerek veri gizleyin. Bunun için basit olarak paint kullanabilirsiniz. Daha iyi çalışmalar için gimp resim editörünü kullanarak katmanlar oluşturabilirsiniz.
- ⌚ Fotomakron.jpg dosyası içerisinde gizli bilgiyi bulun.

Resimde Veri Gizleme



Sayısal Resmin Yapısı



RGB (255, 127, 39)

RGB (255, 126, 39)

Sayısal Resmin Yapısı

- ⌚ Bütün resimler dosya başlığı (header) ve piksellerden oluşur.
- ⌚ Sayısal (dijital) resim N satır ve M sütunluk bir dizi ile temsil edilir.
- ⌚ Bir resim dizisinin elemanlarına piksel denir.
- ⌚ Her piksel sadece bir renk içeren/gösteren küçük bir bloktur.
- ⌚ Bütün renk değişimleri üç temel rengin birleştirilmesiyle elde edilir. Basit dijital resim dosyasını ele alırsak, her temel renk 1 bayt ile gösterilir ve 24 bitlik bir resimde her piksel için renk değerini taşıyan 3 byte kullanılır.

Resim Dosyalarında Renklerin Gösterimi

- ⌚ Günümüzde, analog bir imaj dosyasını dijital formata çevirdiğimiz zaman, renkleri sunmak için genelde üç farklı yol seçebiliriz:
- ⌚ **1 – 24 – bit color:** Her piksel 2^{24} renkten birine sahip olabilir ve bunlar her 8 bit (256 değer) tarafından verilen, üç temel rengin (R (red), gren (G), blue (B)) farklı miktarları olarak sunulur.
- ⌚ **8 – bit color:** Her piksel 2^8 (256) renkten birine sahip olabilir ve renklerin bir tablosundan veya bir paletten seçilirler.
- ⌚ **8 – bit gray scale (8 bit gri seviye):** Her piksel 2^8 (256) gri noktanın birine sahip olmalıdır.

Örnek Resimler

⌚ 8, 24, gray scale resim örnekleri

Resim Dosyalarında Renklerin Gösterimi

⌚ Her pikseldeki renk temel 3 rengin .(Red,Green,Blue) karışımından elde edilir. Her pikselde bu 3 rengin verileri tutulur. Her temel renk 1 pikselde 1 byte (0..255) yer kaplar, yani 1 piksel 3 byte (R,G,B) veri taşır.

⌚ **Örnek :**

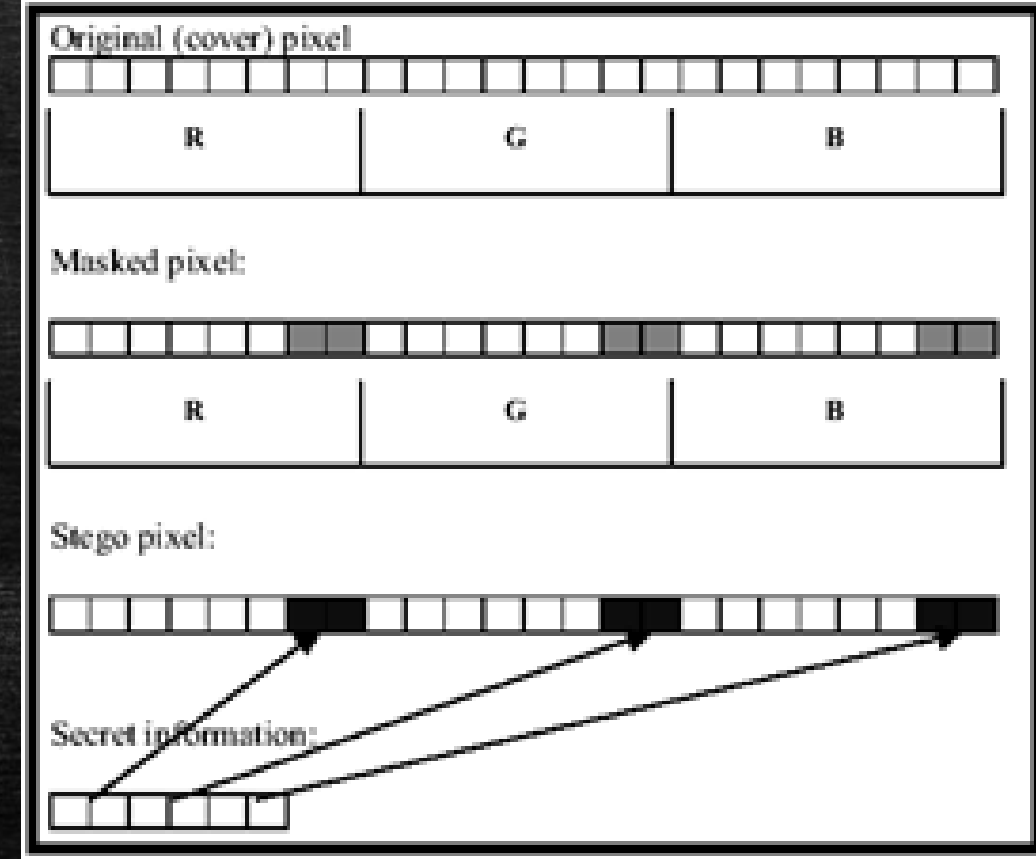
Beyaz Renk RGB formatında FF-FF-FF hex değeri ile ifade edilir.

Yani Red: FF(h), Green: FF(h), Blue: FF(h)
FF binary sistemde 11111111 in karşılığıdır.

1 pikselde beyaz rengi ifade etmek için 11111111- 11111111- 11111111 verisi kullanılır.

Önemsiz bite ekleme(Least Significant (LSB))

- ⌚ LSB insertion yönteminde genel olarak son bitlere ekleme yapılır. Bununla birlikte son bitinde değiştirme yapmak yerine son 2 veya daha fazla bitinde değiştirme yapan yöntemlerde vardır.
- ⌚ İçine veri gömülen resimdeki değişim %50 oranındadır.
- ⌚ Bu durum insan gözüyle algılanamayacak oranda bir değişimdir.
- ⌚ Ne kadar fazla bit üzerinde değişiklik yapılırsa resim üzerindeki değişim o oranda artacağından algılanması da artacaktır.

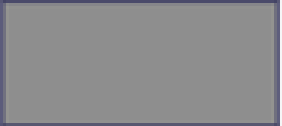


Önemsiz bite ekleme(Least Significant (LSB))

- ⌚ 24 bit renkli resimlerde renk spektrumu geniş olduğu için son 2 veya 3 bitteki değişim insan gözüyle algılanmayacak durumdadır.
- ⌚ Veri gömme işleminde ilk bayttan son bayta doğru bitlerin değişimi için bir sıra izleme zorunluluğu yoktur.
- ⌚ Verinin gömülmesi işleminde baytların hangi sırayla kullanılacağı genellikle “stego-key” anahtar vasıtasıyla düzenlenmekte ve tamamen karışık sırayla veri gömülmesi yapılabilmektedir.
- ⌚ Bazı akıllı yazılımlar koyu renkli alanları tespit edebilir ve bu alanların değiştirilmesini engeller.
- ⌚ Çünkü insan gözüyle koyu bölgelerdeki renk değişimlerinin algılanması daha kolaydır.

Gri-seviye Resimlerde LSB yöntemi

- ❶ Gri-seviye resimlerde her piksel, 0 (siyah) ile 255 (beyaz) arasında tam sayı değer alabilen 1 byte ile temsil edilmektedir.
- ❷ 0–255 arasındaki değerler gri'dir ve bundan dolayı bir resme ait tam sayı “gri ton seviye” (gray level) olarak isimlendirilmektedir.
- ❸ Örneğin, renk değeri 142 olan bir pikselin içine ikilik sayı sistemindeki 1 değeri saklandığında oluşan piksel ve renk değeri aşağıda gösterilmektedir.

| | Renk değeri | İkilik Sistemdeki Karşılığı | Rengi |
|------------------------|-------------|-----------------------------|---|
| Orijinal piksel | 142 | 10001110 |  |
| Bilgi saklanmış piksel | 143 | 10001111 |  |

Son bitin 1 ya da 0 olması gözle görülebilir bir fark yaratmamaktadır.

24-bit Renkli Resimlerde LSB yöntemi

- ① 24 bit resimler bir piksel başına 3 byte kullanmaktadır.
- ① Her pikselin rengi "Kırmızı (red), Yeşil (green), Mavi (blue)" olmak üzere üç ana renkten elde edilmektedir.
- ① Buna pikselin RGB değeri denmektedir.
- ① Her byte'ta son biti değiştirmek suretiyle bir pikselde 3 bitlik bilgi saklanabilir.
- ① Yani 24 bit derinliğine sahip 1024×768 piksel boyutundaki 2.359.296 bit (294.912 byte) bilgi saklanabilir.

10010101 00001101 11001001 (149,13,201)

10010110 00001111 11001010 (150,15,202)

10011111 00010000 11001011 (159,16,234)

"101101101" bilgisi gizlendiğinde;

10010101 00001100 11001001 (149,12,201)

10010111 00001110 11001011 (151,14,203)

10011111 00010000 11001011 (159,16,234)

LSB ile veri gizleme

🕒 <https://www.mertsarica.com/pi-hediyem-var-di-verdim-gitti-3/>

Uygulama -

- ⌚ stegdetect resim.jpg
- ⌚ steghide embed -cf icineGizlemeYapılacakDosya -ef gizlenecekDosya
- ⌚ steghide extract -sf [FILENAME]
- ⌚ steghide info [FILENAME]
- ⌚ stegbreak sözlük atağı
- ⌚ stegexpose
- ⌚ Hatıra resmi stegdetect ile gizleyiciyi bul
- ⌚ Basit bir wordlist ile steghide ile çöz

Uygulama – EzStego ile Gif Üzerinde Gizleme

- ⌚ EzStego gif imaj üzerinde daha karmaşık şifrelemeler yapılabilir.

Ödev -

- ⌚ Şifre anahtar değerine göre LSB ile resim içerisine veri gizleyen program yazın.
- ⌚ Anahtar değeri çift veya tek bite şifreleme yapacağını belirtecek.

Ses İçerisine Veri Gizleme

- ⌚ Ses melodisinde bozukluğa neden olur.
- ⌚ Anlaşılması daha kolaydır.
- ⌚ Klasik müziklerde daha kolay anlaşılır.
- ⌚ Gizleme için rock ve bir çok enstrümanın kullanıldığı çok sesli müzik türleri daha uygundur.

Ses İçerisine Veri Gizleme Yöntemleri

⌚ LSB CODING

⌚ PARITY CODING

⌚ PHASE CODING

⌚ SPREAD SPECTRUM

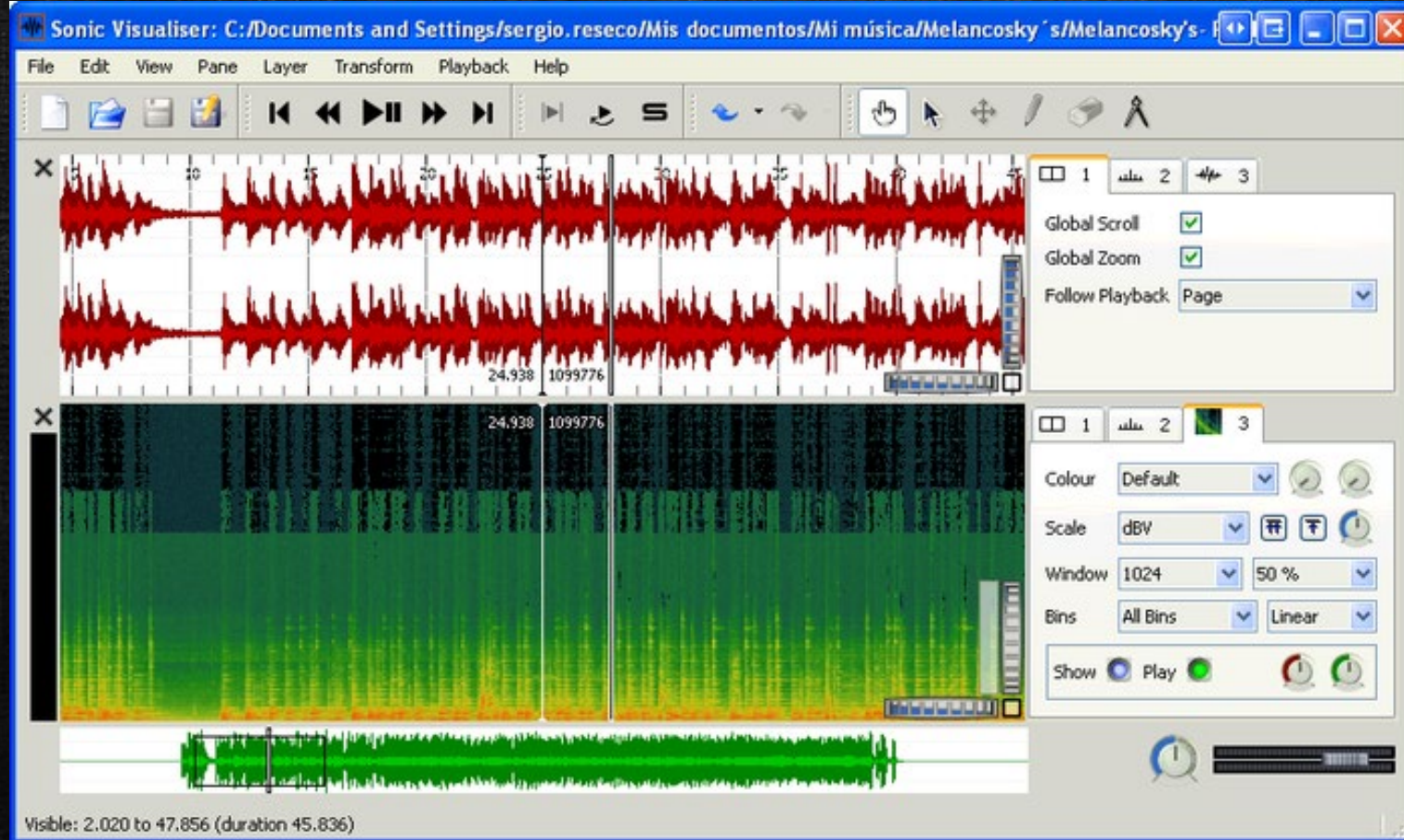
⌚ ECHO HIDING

⌚ <https://iicybersecurity.wordpress.com/2015/08/25/how-to-hide-secret-messages-in-music-files/>

⌚ <http://www.snotmonkey.com/work/school/405/methods.html>

Uygulama – Morse Şifreleme

Uygulama – Spread Spectrum



- ⌚ mix.mp3 müzik dosyasını dinleyip gizlenen bilgi olup olmadığı kontrol edin.
- ⌚ mix.mp3 dosyasını [sonic visualizer](#) programında açın.
- ⌚ Programın layer bölümünden add melodic range spectrogram seçip kanallar ile oynayarak gizli bilgiyi bulun.
- ⌚ World on fire.wav dosyası için benzer çalışmayı yapın.

Spread Spectrum Frekans İle Veri Gizleme



Uygulama - Spectrum Frekans İle Veri Gizleme

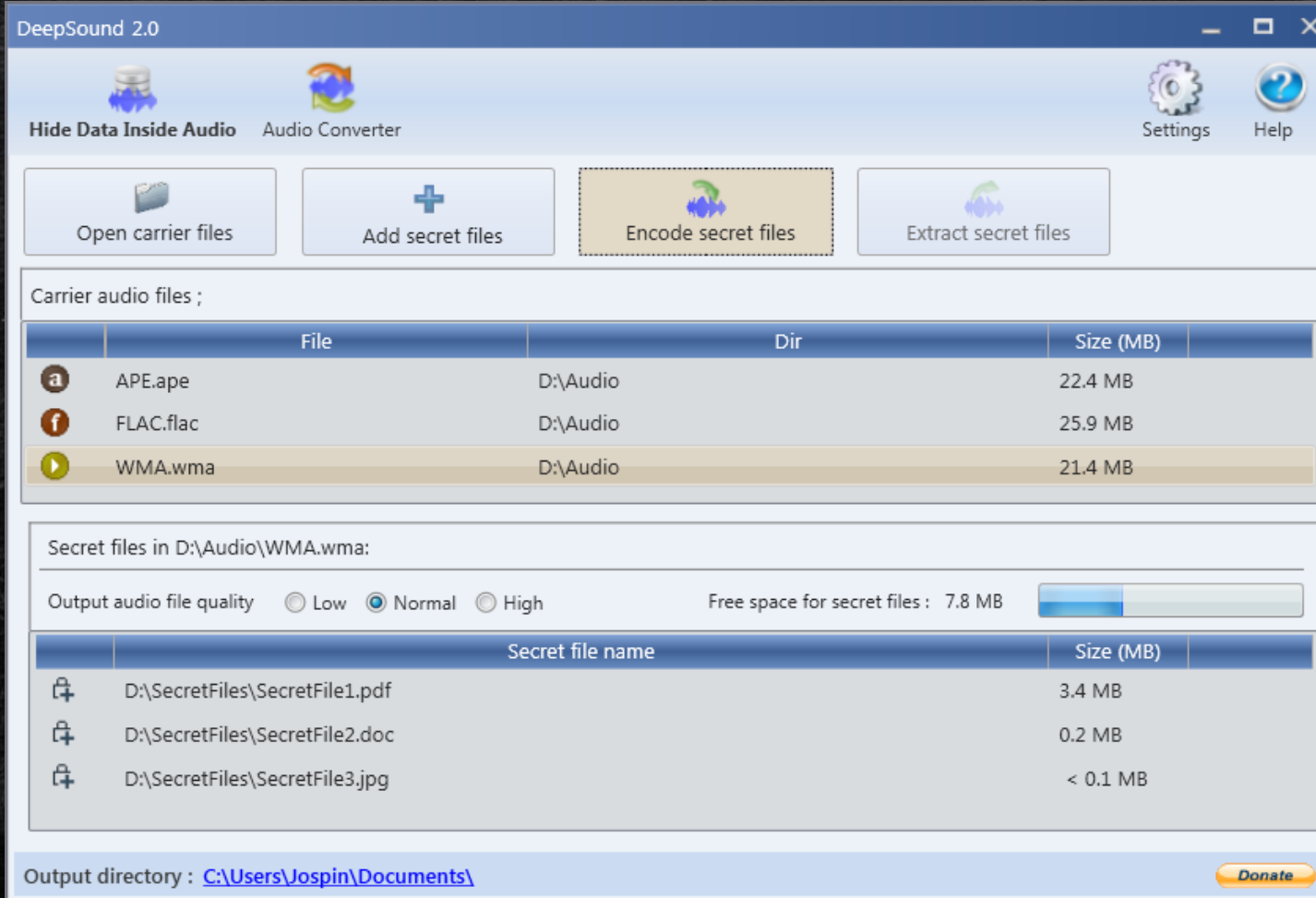
- ⌚ Şifrelenmesi istenen resmi oluşturun.
- ⌚ Siyah arkaplan üzerine beyaz metin daha iyi sonuç veriyor.
- ⌚ Fazla boş alan olmayan küçük resimler daha iyi sonuç veriyor.
- ⌚ Oluşturduğunuz resmi jpeg veya bmp formatında kaydedin.
- ⌚ Windows üzerinde çalışan [coagula](#) programını indirin.
- ⌚ Resmi Coagula programı ile açın. Ayarlar menüsünden "Render Image as Audio Without Blue/Noise" seçin.
- ⌚ Menüden "Save Audio File" seçerek ses dosyasını kaydedin.

Uygulama – Müziksel Şifreleme

- ① <https://p22.com/musicfont/> web sayfasından gizlemek istediğiniz bilgiyi müzik dosyasına dönüştürün.
- ① <http://www.dcode.fr/music-sheet-cipher> web sayfası üzerinden gizlemek istediğiniz veriyi notalara çevirin. ([Musical Cryptogram](#))

Uygulama – DeepSound ile Şifreleme

- ⌚ Windows üzerinde çalışan [deepSound](#) uygulamasını kurun.



DTMF (Dual-Tone Multi-Frequency) kodları

- ⌚ Amerikan ordusu için Bell telefon laboratuvarlarında geliştirilmiş bir kodlama sistemidir.
- ⌚ Telefon şebekelerinde bilgi yollamanın güvenli yolu olarak tercih edilmiş ve telefon abonesinin santrale aradığı abone ile ilgili bilgileri ilettiği standart yöntem olarak günümüzde yaygın olarak kullanılmaktadır.
- ⌚ Günümüzde telsiz cihazlarının çoğunda DTMF sinyallerini yollamaya ve almaya yarayan modüller ile tuş takımı bulunmaktadır.
- ⌚ Bu sinyallerin çözülmesi oldukça kritik ve karmaşık bir DSP – Digital Signal Processing – tekniği gerektirmektedir.
- ⌚ Çözümleme için geçerli bir ton çifti ve zamanlama aralığı gereklidir.
- ⌚ Çözüm için genelde Goertzel algoritması kullanılıyor.

DTMF (Dual-Tone Multi-Frequency) kodları

| DTMF tuş takımı frekansları | | | | |
|-----------------------------|----------|----------|----------|----------|
| | 1209 Hz | 1336 Hz | 1477 Hz | 1633 Hz |
| 697 Hz | <u>1</u> | <u>2</u> | 3 | <u>A</u> |
| 770 Hz | <u>4</u> | 5 | <u>6</u> | <u>B</u> |
| 852 Hz | <u>7</u> | <u>8</u> | 9 | <u>C</u> |
| 941 Hz | <u>*</u> | <u>0</u> | <u>#</u> | <u>D</u> |

Uygulama – Telefon Tuş Seslerinin Tespiti

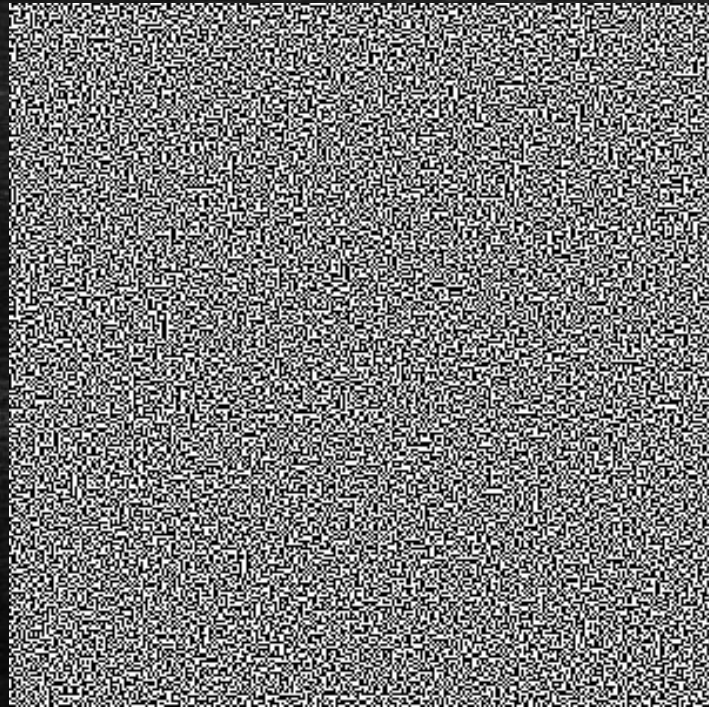
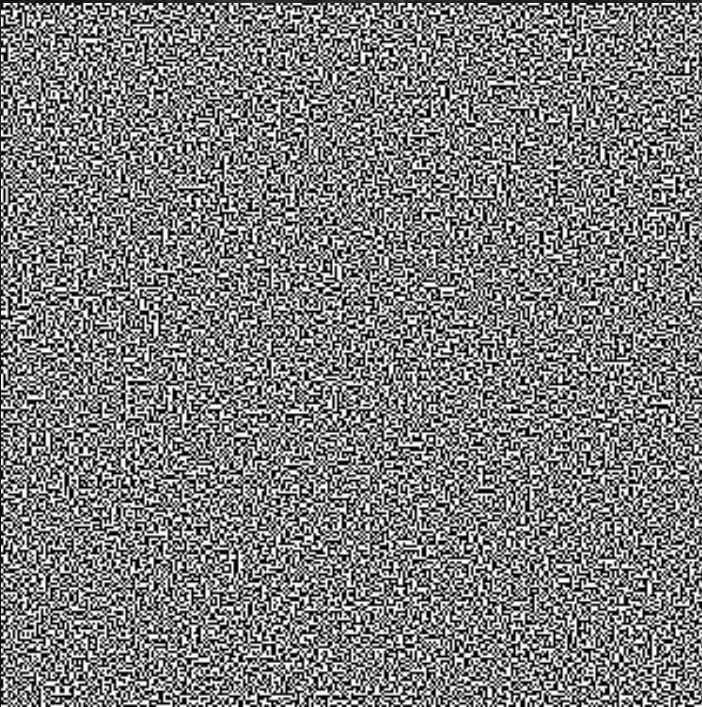
- ⌚ [Detect DTMF \(Dual Tone Multi Frequency\)](#) adresine DTMF_dialing.wav ses dosyasını yükleyerek tuşlanan numaraları bulun.
- ⌚ Çağrı merkezi görüşmesi ses dosyası içerisindeki kredi kartı numarasını elde edin. (Kredi kartı numara kısımlarını ayrı ayrı elde ederek çalışmak sizi daha kolay sonuca ulaştıracaktır.)
- ⌚ Online web sayfaları yanı sıra [dtmf2num](#), [DTMFChecker](#), [ToneDecoder](#) programı da kullanılabilir.

Uygulama – Ters Çevirilmiş Ses Dosyası

- ⌚ Auodacity programı ile reverse_sound ses dosyasını ters çevirip dinleyin.

Uygulama - XOR

Resimleri XOR'layıp ortak resmi bulun. [Stegsolver](#) aracını kullanabilirsiniz.



Uygulama -



binwalk moon.png veya
binwalk -Me firmware.bin
dd if=./moon.png of=./moon.zip skip=411781 bs=1

- ⌚ xxd carving-ex.jpg | less
- ⌚ PK değeri zip dosya sistemi oluşturan [Phil Katz](#) ifade ettiğinden resmin sonunda zip dosyası olduğunu anlayabiliyoruz.
- ⌚ printf '%d\n' 0x00008e23
- ⌚ dd if=carving-ex.jpg bs=1 skip=36387 of=foo.zip
- ⌚ Resim dosyasından zip dosyasını ayırmak için binwalk programını kullanabilirsin.

Uygulama -



Benzer işlemi yandaki
resim için uygulayın

Uygulama – Steg Solve



Video İçine Veri Gizleme

⌚ Stego Video

Kaynakça

1. Slaytlar Necmettin Çarkacıya aittir.
2. İsmail Saygılı, [ADS Kullanarak Veri Gizleme ve Steganography Tekniği](#)
3. Sawat Pathi, [Hide Data WITHOUT Steganography](#)
4. Chetan Gupta, [Dissecting NTFS Hidden Streams](#)
5. Selda Berker, [Steganografi ve LSB](#)
6. Adam Dachis, [How to Hide Secret Messages and Codes in Audio Files](#)
7. Mantisreligiosa, [DTMF Ton kodlama sistemi](#)
8. <https://ctfs.github.io/resources/topics/steganography/file-in-image/README.html>
9. <https://ctfwriteups.wordpress.com/tag/steganography/>

Kaynaklar

- ⌚ Alex Long, [A Guide to Steganography, Part 3: How to Hide Text and Images in Pictures](#)
- ⌚ Shankar Raman, [Archive for the 'Stegano' Category](#)
- ⌚ <https://github.com/ctfs/>

① <http://www.slideshare.net/nulloxoo/nullcon-2010-steganography-stegananalysis-a-technical-psychological-perspective>

YMT 311-Bilgi Sistemleri ve Güvenliđi

Ders hakkında Bilgilendirme ve temel kavramlar



Ders Hakkında Temel Bilgilendirme

Ders Sorumlusu: Dr. Muhammet BAYKARA

Ders. Lab. Yardımcısı : Arş. Gör. Fırat Artuğer

Ders Saatleri : 3 saat teori, 2 saat laboratuvar

Dersler A405'te uygulamalar ise laboratuvar ortamında yapılacaktır.

Devam / Devamsızlık Durumu : Teori : %30 – Uygulama : %20

Dersin Amacı : Bu derste; bilgi ve bilgisayar güvenliği konuları, unsurları ve süreçleri üzerinde durulacak ve yüksek derecede bir güvenlik için uygulanması gerekenler anlatılacaktır. Bilgi ve bilgisayar güvenliğine neden önem verilmesi gerektiği ve bilgi güvenliğinin en temel anlamda nasıl oluşturulabileceği gibi sorulara kapsamlı cevaplar aranmaya çalışılacak, bu kapsamda bilgi güvenliği yazılımları ve proje uygulamaları ortaya konulacaktır.

Dersin İşleniş Biçimi & Nasıl Geçerim!?

- Teorik anlatım
- Haftalık Ödevler
- Dönemlik araştırma ve uygulama projesi
 - Raporlama + Sunum
- Ara sınav, Final Sınavı ve Quizler
- Ders Geçme Notu = $(\text{Ara sınav}(\%33) + \text{Haftalık Ödevler}(\%33) + \text{Quizler}(\%34)) * 0,4 + ((\text{Final} + \text{Proje}) / 2) * 0,6$

Dersin Amacı

- Bilgi güvenliği konularında farkındalık ve temel düzeyde teorik ve pratik bilgiler öğrenmenizi sağlamak
- Bilgi güvenliği temel kavram, standart, metodoloji, yöntem ve stratejilerini öğrenmenizi sağlamak
- Araştırma yeteneğinizi geliştirmek
- Kişisel ve kurumsal bilgi güvenliğinin sağlanması konusunda fikir sahibi olmanızı sağlamak

Temel Kaynaklar

1. Kamil Burlu, *Bilişimin Karanlık Yüzü* , Nirvana yayınları, 3.baskı, 2010.
2. G. Canbek, Ş. Sağıroğlu, *Bilgi ve Bilgisayar Güvenliği: Casus Yazılımlar ve Korunma Yöntemleri*, Grafiker Ltd. Şti. Aralık 2006.
3. Türkay HENKOĞLU, *Adli Bilişim : Dijital Delillerin Elde Edilmesi ve Analizi*, Pusula Yayınları, 2011.
4. *Veri ve Ağ Güvenliği Ders Notları*, İ.Soğukpınar, G.Y.T.E.Bilg.Müh.Bölümü
5. Hamza Elbahadır, *Hacking Interface*, Kodlab Yayınları, 2010.
6. Bünyamin Demir, Dikeyksen Yayınları, *Yazılım Güvenliği Saldırı ve Savunma, 2013.*
7. Ömer Çıtak, Level Yayınları, *Ethical Hacking, 2016.*
8. Kevin D. Mitnick, Çevirmen(Nejat Eralp Tezcan) *Aldatma Sanatı*
9. Canan Çimen, Sedat Akleylek, Ersan Akyıldız, *Şifrelerin Matematiği: Kriptografi*, ODTU Yayınları, Ankara.
10. *Computer and Information Security* - Handbook
11. *Elements of Computer Security Book*
12. *Cryptography And Network Security Principles And Practices*" Stallings Will, Prentice Hall, 2003.
13. *Security Engineering*, R. Anderson, Wiley, New York, 2001.

Konu Başlıkları

- Bilgi ve bilgisayar güvenliğine giriş, temel kavramlar
- Siber bilgi güvenliği, güvenlik ve hacking kavramları
- Ağ güvenliği
- Şifreleme teknikleri
- Steganografi
- Yazılım güvenliği, bilgi güvenliği yönetimi ve ilgili mevzuatlar
- Sızma belirleme, Saldırı tespit ve engelleme sistemleri
- Bilgi güvenliğinde kullanılan temel araçlar
- Biyometrik güvenlik sistem ve araçları
- Bir siber saldırının senaryosu

Temel Kavramlar

- Bilgi Güvenliği Sistemleri: Information Security Systems
- Bilgisayar Güvenliği: Computer Security
- Saldırı, Sızma, Atak: Attack, Intrusion, Hack
- Saldırgan: Attacker, Hacker, Intruder
- Güvenlik Açığı, Açıklık: Vulnerability
- Bilgi: Information, Öz Bilgi: Knowledge
- Hikmet: Wisdom
- Saldırı Tespit Sistemleri: Intrusion Detection Systems
- Saldırı Önleme Sistemleri: Intrusion Prevention Systems
- Gizlilik: Confidentiality
- Bütünlük Doğruluk: Integrity
- Kullanılabilirlik, erişilebilirlik: Availability

Temel Kavramlar

- Sosyal Mühendislik: Social Engineering
- Şifreleme: Cryptology
- Bilgi Gizleme: Steganography
- Klavye dinleme sistemi: Keylogger
- Kötücül yazılım (analizi): Malware (analysis)
- Kaynak kod istismarı-korunmasızlık sömürücü: exploit
- Arka kapılar: backdoor
- Hizmet aksattırma saldırısı: DoS(Denial of the Service)
- Dağıtık hizmet aksattırma: DDoS
- Sağanak: spam
- Casus yazılım: spyware
- Solucan :worm
- Truva atı: trojan horse
- Kök kullanıcı takımı: rootkit
- Koklayıcı, ağ izleyici: sniffer

Temel Kavramlar

- Bilgi Güvenliğinin temel amacı, elektronik veya diğer ortamlarda bulunan her türlü bilgi için,
 - Gizlilik (Confidentiality)
 - Bütünlük (Integrity)
 - Kullanılabilirlik (Availability)...

temel özelliklerini sürekli olarak sağlamaktır.

Temel Kavramlar



Temel Kavramlar- Bilgi Güvenliđi



Bilgi Güvenliği Temel Unsurları

- **Gizlilik** : Bilginin yetkisiz kişilerin eline geçmemesidir.
- **Bütünlük** : Bilginin yetkisiz kişiler tarafından değiştirilmemesidir.
- **Erişilebilirlik** : Bilginin ilgili ya da yetkili kişilerce ulaşılabilir ve kullanılabilir durumda olmasıdır.



Temel Kavramlar- Standartlar

- **TS ISO IEC 27001** Bilgi Güvenliği Yönetim Sistemi
- UEKAE BGYS-0001 Bilgi Güvenliği Yönetim Sistemi Kurulum Kılavuzuna bilgiguvenligi.gov.tr den ulaşılabilir.

Bilgi Güvenliği - Kim Sorumlu?

- Bilgi güvenliğinin sağlanmasından **herkes sorumludur**.
- Bu sorumluluklar yasal olarak da ifade edilmiş ve **5651 sayılı kanun** *"İnternet ortamında yapılan yayınların düzenlenmesi ve bu yayınlar yoluyla işlenen suçlarla mücadele edilmesi"* amacı ile düzenlenmiştir.

Bilgi Güvenliği – Kim Sorumlu?

- Herhangi bir bilgi sisteminde aşağıdaki konumlardan **herhangi birisinde iseniz sorumluluğunuz var** demektir.
 - Bilginin sahibi
 - Bilgiyi kullanan
 - Bilgi sistemini yöneten
- Bu durum çok geniş bir kitleyi içerdiğinden *"bilgi güvenliğinin sağlanmasından herkes sorumludur"* diye genelleme yapmakta bir sakınca yoktur.

Bilgi

- İşlenmiş veridir.
- Bilgi diğer önemli iş kaynakları gibi kurum için değeri olan ve dolayısıyla uygun bir şekilde korunması gereken bir kaynaktır.
- Bir konu ile ilgili belirsizliği azaltan kaynak bilgidir.

(Shannon – Information Theory)

Güvenlik Üzerine...

- Güvenlik risk yönetimidir (Anonim)
- Bir sistem, yazılımı ihtiyaçlarınız ve beklentileriniz doğrultusunda çalışıyorsa güvenlidir (Practical UNIX and Internet Security)
- Güvenlik, bulunurluk, kararlılık, erişim denetimi, veri bütünlüğü ve doğrulamadır.

Güvenlik ve İnsan

- Güvenlik, teknoloji kadar insan ve o insanların teknolojiyi nasıl kullandığı ile ilgilidir.
- Güvenlik sadece doğru teknolojinin kullanılmasından daha ileride bir hedeftir.
- Doğru teknolojinin, doğru amaçla ve doğru şekilde kullanılmasıdır.

Teknoloji

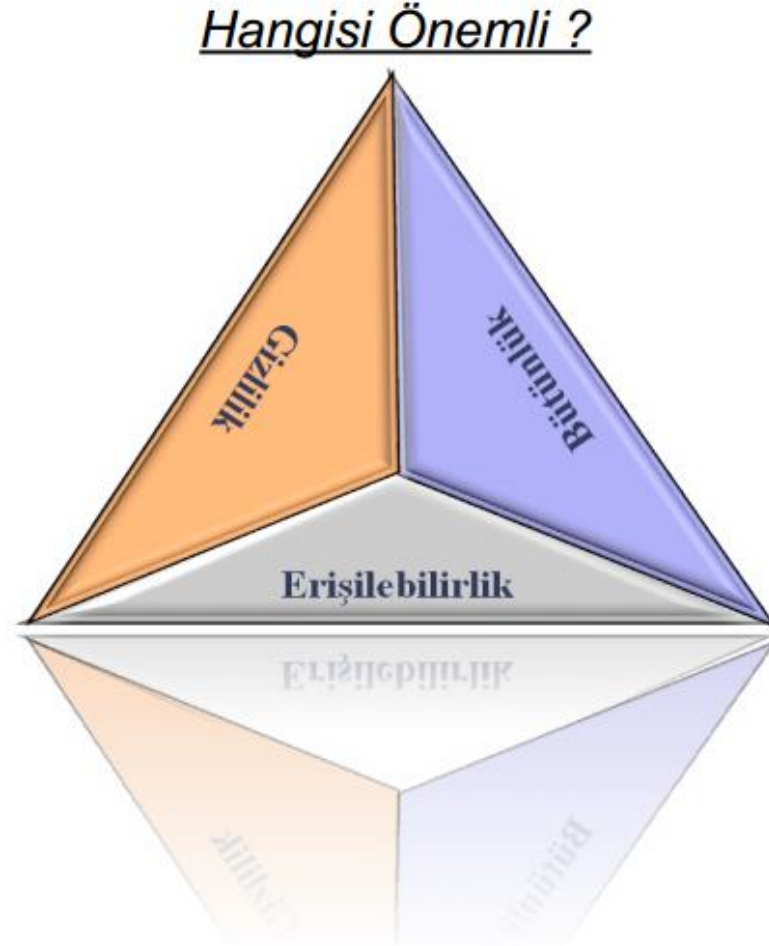
“Eğer teknolojinin tek başına güvenlik probleminizi çözebileceğini düşünüyorsanız, güvenlik probleminiz ve güvenlik teknolojileri tam anlaşılmamış demektir.”

(Bruce Schneier – Şifreleme Uzmanı)

Güvenlik Yönetim Pratikleri

- Gizlilik, Bütünlük, Erişilebilirlik
- Risk Değerlendirmesi ve Yönetimi
- Politika, Prosedür ve Rehberler
- Politika Uygulamaları
- Eğitim
- Denetim

Gizlilik, bütünlük, erişilebilirlik



Gizlilik

Kuruma özel ve gizliliği olan bilgilere, sadece yetkisi olan kişilerin sahip olması

Bütünlük

Kurumsal bilgilerin yetkisiz değişim veya bozulmalara karşı korunması

Erişilebilirlik

Kurumsal bilgi ve kaynakların ihtiyaç duyan kişilerce sürekli erişilebilir durumda olması

Risk Değerlendirmesi

- Kurumsal işleyişi etkileyebilecek olan risklerin belirlenmesi ve değerlendirilmesi sürecidir.
- Bir risk değerlendirilmesi yapılmadan, kurumsal işleyişin politika, prosedür ve uygulamalarıyla ne kadar korunduğu belirlenemez.
- Risk yönetimi konusunda yetkililere -tercihen üst yönetim- ihtiyaç duyulmaktadır.
- Üst yönetimin onayı ile sürecin önemi ve verimi artacak, çalışanlar politika ve prosedürlere daha fazla önem verecektir.

Risk Yönetimi

- Kurumun karşı karşıya olduğu risklerin belirlenmesi,
- Varlıkların zaafiyetlerinin ve karşı karşıya oldukları tehditlerin belirlenmesi,
- Ortaya çıkan riskin nasıl yönetileceği ve nasıl hareket edileceğinin planlanması sürecidir.

Risk Yönetimi

- Aşamalar:

- Risk yönetim ekibi kurma
- Tehdit ve zaafiyetleri doğrulama
- Organizasyon varlıklarının değerlerini belirleme
- Riske karşı yapılacak hareketleri belirleme

- Kavramlar:

- Tehdit
- Zaafiyet
- Kontroller

Risk Yönetimi Kavramları

- **Tehdit**

Organizasyonu olumsuz etkileyebilecek olan insan yapımı veya doğal olaylar

- **Zaafiyet**

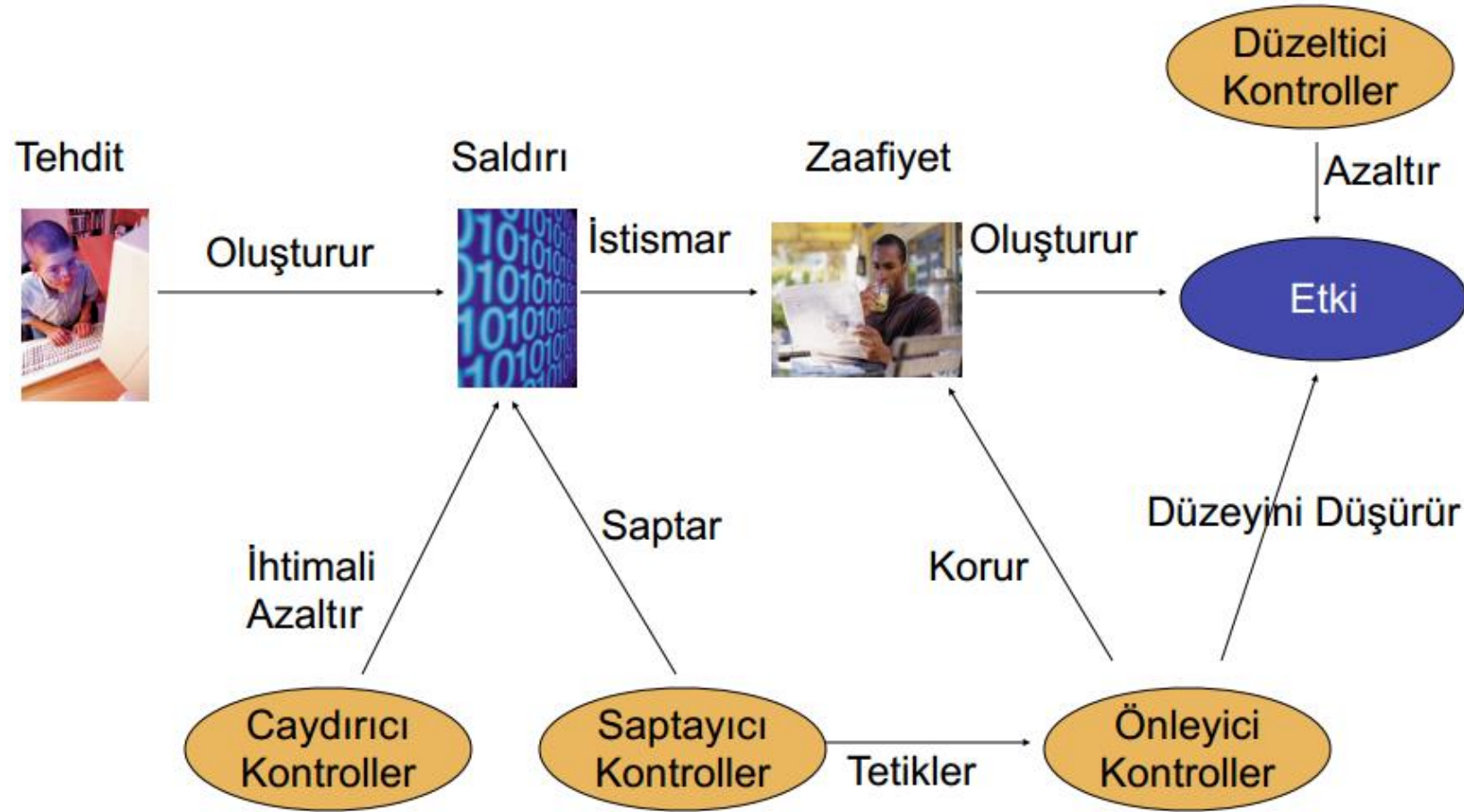
Varlıkların sahip olduğu ve istismar edilmesi durumunda güvenlik önlemlerinin aşılmasına neden olan eksiklikler

- **Kontroller**

Zaafiyetlerin boyutunu azaltıcı, koruyucu veya etkilerini azaltıcı önlemler

- Caydırıcı Kontroller
- Saptayıcı Kontroller
- Önleyici Kontroller
- Düzeltici Kontroller

Risk Yönetimi Kontrolleri



Risk Yönetimi Takımı

- Tek başına yapılabilecek bir iş değildir, yardımcılar ve diğer önemli departmanlardan çalışanlar ile yapılmalıdır. Böylece riski görmek ve kavramak daha kolay olacaktır.

Potansiyel Gruplar ;

- Bilişim Sistemleri Güvenliği
- Bilişim Teknolojileri ve Operasyon Yönetimi
- Sistem Yöneticileri

- İnsan Kaynakları
- İç Denetim
- Fiziksel Güvenlik
- İş Devamlılığı Yönetimi
- Bilgi Varlıklarının Sahipleri

Tehditleri Belirleme

- **Doğal Olaylar**

Deprem, Sel, Kasırga

- **İnsan Yapımı Olaylar**

-Dış Kaynaklı Olaylar

Virüs, Web Sayfası Değişimi, Dağıtık Servis Engelleme

-İç Kaynaklı Olaylar

*Çalışanlar

E-Posta Okuma, Kaynaklara Yetkisiz Erişim, Bilgi Hırsızlığı

*Eski Çalışanlar (Önceki Hakların Kullanımı, Bilgi Hırsızlığı, Gizli Bilgilerin ifşası)

Zaafiyet, tehdit ve risk

| Tehdit Tipi | Tehdit | Zaafiyet/İstismar | Oluşan Risk |
|---------------------------|----------------------|---|------------------------------------|
| İç Kaynaklı İnsan Yapımı | Çalışan | Kötü yetkilendirme ve izleme sistemi olmayışı | Veri değişimi veya yok edilmesi |
| Dış Kaynaklı İnsan Yapımı | Saldırgan | Hatalı güvenlik duvarı yapılandırması | Kredi kartı bilgilerinin çalınması |
| Doğal | Yangın | Kötü yangın söndürme sistemi | İnsan hayatı kaybı |
| Dış Kaynaklı İnsan Yapımı | Virüs | Güncellenmemiş anti-virüs sistemi | İş devamlılığının aksaması |
| Teknik İç Tehdit | Sabit Disk Bozulması | Veri yedeği alınmaması | Veri kaybı, çok miktarda iş kaybı |

Varlıkların Değerlerinin Belirlenmesi

- Gerçek risk yönetimi için hangi varlığın kurum için daha değerli olduğu doğru biçimde belirlenmelidir.
- Sayısal/Nicel Risk Değerlendirmesi yapılacak ise varlıklara para birimi cinsinden değer atanmalıdır.
- Eğer Sayılamayan/Nitel Risk Değerlendirmesi yapılacak ise varlıkların önceliklerinin belirlenmesi yeterlidir; ancak çıkacak sonuçların sayısal olmayacağı da ön görülmelidir.

Nicel Risk Değerlendirmesi

- Sayısal risk değerlendirme yöntemidir, sayılar ve para birimleri ile risk belirlenir.
- Sürecin tüm elemanlarına sayısal değer verilmelidir.
 - Varlık, Etki Düzeyi, Korunma Verimliliği, Korunma Maliyeti vb.
- Temel kavramlar ve formüller ile risk değerlendirmesi yapılır.
 - Tekil Kayıp Beklentisi (SLE)
 - * Tekil Kayıp Beklentisi = Varlık Değeri x Etki Düzeyi
 - Yıllık Gerçekleşme İhtimali (ARO)
 - * Tehditin bir yıl içinde gerçekleşme ihtimali
 - Yıllık Kayıp Beklentisi (ALE)
 - * Yıllık Kayıp Beklentisi = Tekil Kayıp Beklentisi x Yıllık Gerçekleşme İhtimali

Nitel Risk Değerlendirmesi

- Nicel tanımlama tüm varlıklara veya tehditlere kolayca uygulanamaz, Nitel tanımlama ise öncelik ve önem seviyelerine göre değerlendirmedir.
 - Değerlendirme çıktısı sayısal olmayacaktır, bu durum üst yönetim tarafından önceden bilinmelidir.
 - Soru/Cevap veya Öneriler ile öncelikler belirlenebilir
 - Örnek Önceliklendirme Değerleri : Düşük/Orta/Yüksek
 - Düşük : Kısa sürede telafi edilebilen durumlar için
 - Orta : Organizasyonda orta düzey maddi hasar oluşturan, giderilmesi için maddi harcamalar gereken durumlar için
 - Yüksek : Organizasyon sonlanması, müşteri kaybı veya yasal olarak önemli kayıp oluşturacak durumlar için
- * NIST 800-026 (National Institute of Standards and Technology)
(Security Self-Assessment Guide for Information Technology Systems)

Riske Karşı Davranış Belirleme

- **Riskin Azaltılması**

- Bir önlem uygulanarak veya kullanılarak riskin azaltılması

- **Riskin Aktarılması**

- Potansiyel hasar veya durumların sigorta ettirilmesi

- **Riskin Kabul Edilmesi**

- Riskin gerçekleşmesi durumunda oluşacak potansiyel kaybın kabul edilmesi

- **Riskin Reddedilmesi**

- Riskin inandırıcı bulunmaması ve gözardı edilmesi

Politika Prosedür ve Rehberler

- Organizasyonun güvenlik öncelikleri, organizasyon yapısı ve beklentileri yazılı olarak hazırlanmalıdır.
- Üst yönetim, organizasyonun güvenlik önceliklerini belirlemede kilit role ve en üst düzey sorumluluğa sahiptir.
- Hazırlanan politika, prosedür ve rehberler, yasalarla ve sektörel sorumluluklarla uyumlu olmalıdır.
- Hazırlanan dökümanlar, çalışanlardan beklentileri ve karşılanmayan beklentilerin sonuçlarını açıkça ifade etmelidir.

Politika Türleri

- **Duyuru Politikaları**

–Çalışanların, davranışlarının sonuçlarını bildiğinden emin olunması hedeflenmektedir.

- **Bilgilendirici Politikalar**

–Çalışanların bilgilendirilmesini ve eğitilmesini sağlayarak, görevlerinin ve beklentilerin bilincinde olmaları hedeflenmektedir.

- **Yasal Politikalar**

–Organizasyonun attığı adımların, yasal ve sektörel sorumluluklar ile uyumlu olmasının sağlanması hedeflenmektedir.

Güvenlik Kontrolleri

- Güvenlik kontrollerinin amacı, kurumun geliştirdiği güvenlik mekanizmalarının uygulanmasını sağlamaktır.
- Güvenlik Kontrol Türleri
 - Yönetimsel
 - *İşe Alım Süreci
 - *Çalışan Kontrolleri
 - *İşten Çıkarma Süreci
 - Teknik
 - Fiziksel

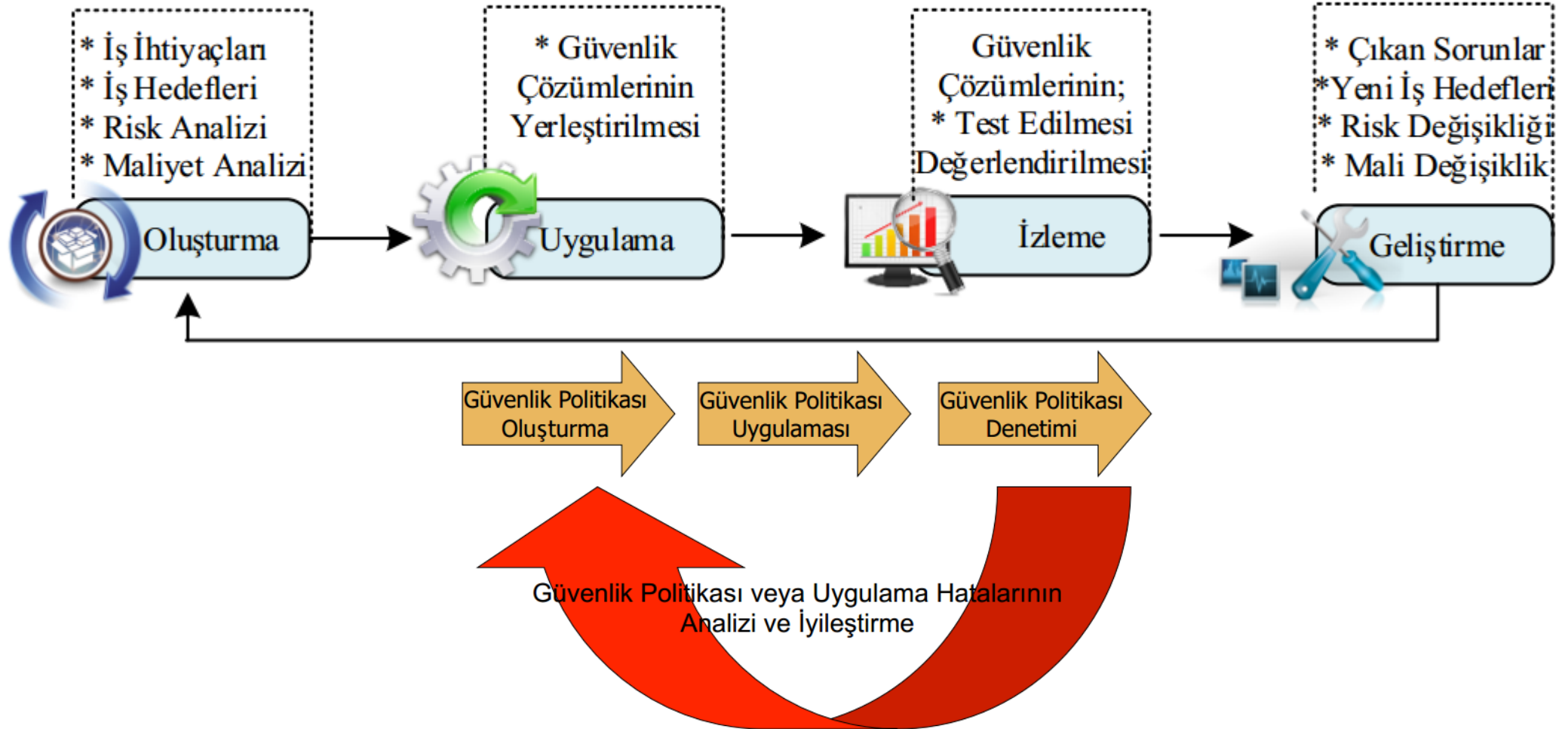
Eğitim

- Çalışanlar, kurum politikaları, görevleri, sorumlulukları, kullanmakta oldukları ekipmanlar ve gerekli teknolojiler konusunda eğitilmelidir.
 - Kısa Süreli Eğitimler
 - Uzun Süreli Eğitimler
 - Farkındalık Eğitimleri
- Eğitim Süreci Bileşenleri
 - Organizasyonun Hedefleri ve Gereksinim Değerlendirmesi
 - İhtiyaçlar Doğrultusunda Uygun Eğitimin Belirlenmesi
 - Eğitim Yöntemleri ve Araçlarının Belirlenmesi
 - Eğitim Verimlilik Değerlendirmeleri

Denetim

- Organizasyonun sahip olduğu güvenlik altyapısı ve güvenlik yönetim süreci periyodik olarak denetlenmelidir.
- Denetim süreci kullanılarak, politikalar ile uygulamaların uyumluluğu, doğru kontrollerin doğru yerlerde uygulandığı ve çalışanlara sunulan eğitimlerin gerçekten işe yaradığı doğrulanabilir.
- Politika denetimlerinde standart yöntem ve şekiller uygulanması zordur. Ancak uygulanan politikaların uyumlu olduğu standartların denetim süreçleri bu konuda rehberlik sağlayabilir.
- Kurum içi veya bağımsız denetçiler tarafından sağlanabilir.

Güvenlik Yönetim Süreci



Bilgi Güvenliği - Sertifikasyon

- CISA,
- CISSP,
- ISO 27001 LA,
- CEH

Bilgi Güvenliği Alanındaki Güncel Meslekler

- [#1 Information Security Crime Investigator/Forensics Expert](#)
- [#2 System, Network, and/or Web Penetration Tester](#)
- #3 Forensic Analyst
- #4 Incident Responder
- #5 Security Architect
- #6 Malware Analyst
- #7 Network Security Engineer
- #8 Security Analyst
- #9 Computer Crime Investigator
- [#10 CISO/ISO or Director of Security](#)
- #11 Application Penetration Tester
- #12 Security Operations Center Analyst
- #13 Prosecutor Specializing in Information Security Crime
- #14 Technical Director and Deputy CISO
- #15 Intrusion Analyst
- #16 Vulnerability Researcher/ Exploit Developer
- #17 Security Auditor
- [#18 Security-savvy Software Developer](#)
- #19 Security Maven in an Application Developer Organization
- #20 Disaster Recovery/Business Continuity Analyst/Manager

Bazı Kaynaklar

- <http://muhammetbaykara.com/>
- <http://www.nsa.gov/>
- <http://www.bilgiguvenligi.gov.tr/>
- <http://www.bga.com.tr/>
- <http://www.cehturkiye.com/>
- <http://www.iso27001bilgiguvenligi.com/>
- <http://www.bilgimikoruyorum.org.tr/>

<http://www.bilgiguvenligi.org.tr/>

Nasıl Bir Proje Gerçekleştirebilirim?

- Kurumsal Bilgi Güvenliği açısından ülkelerin geliştirdiği stratejilerin ve ülkelerin bilgi güvenliğine bakış açılarının değerlendirilmesi. (Model, yazılım, strateji, istatistik vb.)
- Saldırı Tespit Sistemlerinin incelenmesi ve geliştirilmesi.
- Snort, ossec, pokemon, bro, firestorm vb. incelenmesi ve olası yeni alanlara uyarlanması
- Anomali temelli saldırı tespit sistemi geliştirilmesi.mpute
- Verilerin güvenli bir şekilde iletilmesine yönelik olarak kriptosteganografi uygulamaları.
- Xss, sql injection açıklıklarının tespitine yönelik uygulamalar.
- Sosyal Mühendislik maillerinin tespit edilmesine yönelik uygulamalar.
- Spam maillere yönelik olarak spamsavar.
- Web loglarının incelenmesiyle saldırı analizi uygulaması.
- DOS, syn flood saldırılarının analiz ve tespiti için çeşitli uygulamalar

Nasıl Bir Proje Gerçekleştirebilirim?

- Web güvenliğini sağlamak amaçlı uygulamalar (CAPTCHA, vb...).
- Biyometrik güvenlik sistemleri, iris tanıma, parmak izi tanıma vb. sistem güvenliği yazılımları
- Tek kullanımlık şifre üretimi ve uygulamaları
- E ticaret güvenliğinin sağlanmasına yönelik geliştirmeler
- Yazılım güvenliği, güvenli kod çalışmaları ve uygulamalar
- Windows azure ile güvenli bir bulut bilişim uygulamaları
- Yazılım Tanımlamalı Ağlarda güvenlik uygulamaları
- Mobil yazılımlarda güvenlik açıklarını önleme-mobil güvenlik.
- Mobil Bulut Bilişim uygulamaları (MCC)
- Veri merkezi-bulut yapısı: Data center networking
- Kötücül yazılım tespitlerine yönelik uygulamalar-Antimalware

Nasıl Bir Proje Gerçekleştirebilirim?

- Güvenlik duvarı uygulamaları
- Antivirüs, antimalware, antispyware uygulamaları
- Web uygulama güvenlik duvarı uygulamaları
- Veritabanı güvenlik duvarı uygulamaları
- E-posta güvenliğinin sağlanmasına yönelik uygulamalar
- Zaafiyet tarama sistemleri
- Kayıt toplama ve korelasyon sistemleri- SIEM
- Sıfırgün zararlı yazılım tespit sistemleri- zeroday
- Ağ izleme, performans analizi ve veri kaçakları önleme sistemleri

Tubitak Yarışmaları ve Destekleri-Yönlendirme



- **DETAYLAR İÇİN RESİMLERİ TIKLAYINIZ**