

Toollar 101



İçerik

Toollar 101

Toollar Nelerdir?

01

03

04

05

06

07

08

10

12





Toollar Nelerdir?

Siber güvenlik uzmanları, siber tehditlere karşı organizasyonların veya bireylerin bilgi güvenliğini korumak ve siber saldırıları önlemek veya saptamak için çeşitli araçlar ve yazılımlar kullanırlar.

Bu araçlar ve yazılımlar, tehdit analizi yapmak, güvenlik açıklarını tespit etmek, siber olayları izlemek ve yanıtlamak gibi işlevleri içerir.



SAINT (Security Administrator's Integrated Network Tool)

```
..      ..
pd'      bq      db      7MMF' 7MN. 7MF'MMP""MM""YMM
6P      YA      ;MM:      MM      MMN.      M      P'      MM
M' ,pP""Ybd `Mb      ,V^MM.      MM      M YMb      M      MM
N 8I      "      8M      ,M `MM      MM      M `MN. M      MM
N `YMMMa. 8M      AbmmmqMA      MM      M `MM.M      MM
M. L.      I8 ,M9      A'      VML      MM      M      YMM      MM
Mb M9mmmP' dM .AMA. .AMMA..JMML..JML.      YM      .JMML.
Yq.      .pY
..      ..
```





SAINT

SAINT, aslında bir güvenlik tarama ve analiz aracının kısaltmasıdır. SAINT, ağ güvenliği testleri ve izleme işlemleri için kullanılan genel bir terimdir. SAINT, açık kaynaklı ve ticari sürümleri bulunan bir güvenlik tarama aracını ifade eder. SAINT tarama işlemlerini gerçekleştirirken kullanılan araçların genel adıdır.

Saint Security Suite

Saint Security Suite, bir kuruluşun güvenlik gereksinimlerini karşılamak için kullanılan bir bütünleşik güvenlik yazılımı paketidir. SAINT, bu paketin bir parçasıdır ve özellikle güvenlik taramaları ve izlemeleri için kullanılır. Saint Security Suite, tarama sonuçlarının analizi, güvenlik açıklarının yönetimi ve raporlamayı içeren daha geniş bir güvenlik yönetimi çerçevesine sahiptir.





BiltekCyber

Bettercap



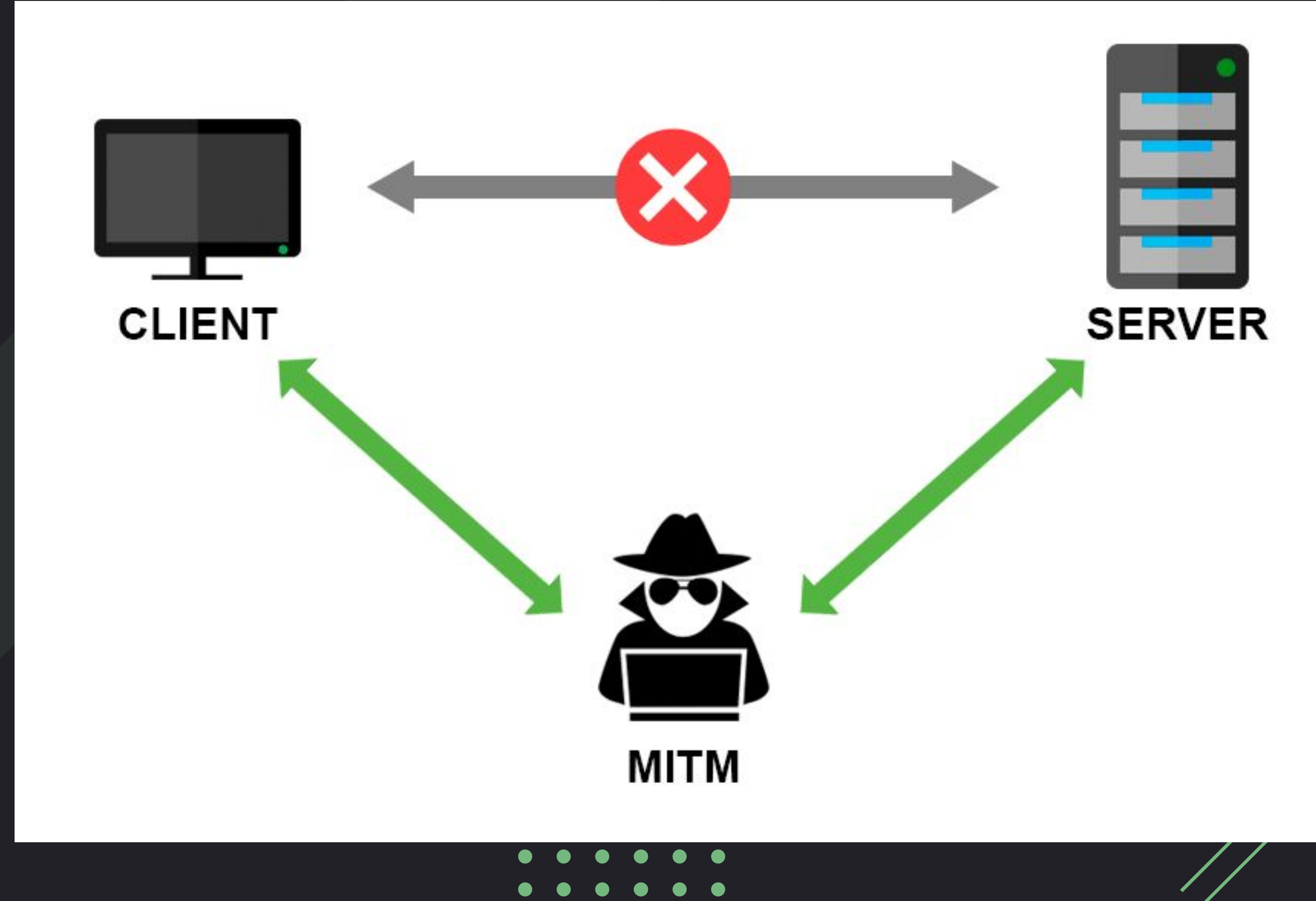


Bettercap

Bettercap, ağ üzerinde çeşitli saldırılar gerçekleştirmek ve güvenlik açıklarını tespit etmek için kullanılır.

Bettercap kullanarak ağ izleme ve sniffing, ARP spoofing, DNS spoofing, HTTP ve HTTPS izleme gibi işlemleri gerçekleştirebilirsiniz.

Sistemimize kurmak için 'apt-get install bettercap' yazarak kurulumunu gerçekleştirebilir 'bettercap' yazarak aracı kullanabilirsiniz.





Bettercap

‘sudo bettercap -iface eth0’ komutu ile kendi bağlantımızı belirterek uygulamaya erişim sağlıyoruz.

Bettercap modüller aracılığıyla yönetilen bir araçtır. ‘help’ komutu yardımıyla hangi modüllerin bulunduğunu görebilirsiniz. Modül listesindeki herhangi bir modülün ne işe yaradığı hakkında bilgi edinmek istiyorsanız ‘help -modül_adı’ komutunu kullanabilirsiniz.

```
kali@BiltekCyber: ~/Desktop
File Actions Edit View Help

(kali@BiltekCyber)-[~/Desktop]
$ sudo bettercap -iface eth0
bettercap v2.32.0 (built for linux amd64 with go1.20.7) [type 'help' for a list of commands]

10.0.2.0/24 > 10.0.2.5 » [22:28:00] [sys.log] [inf] gateway monitor started ...
10.0.2.0/24 > 10.0.2.5 »
```





Bettercap

Örneğin modüllerden biri olan 'net.probe' komutu sistemde bulunan cihazların ip adresi, mac adresi gibi bilgilerinin elde edilmesinde görev alır.

Elde edilen ip adreslerini görüntülemek için 'net.show' komutunu kullanabilirsiniz.

```
10.0.2.0/24 > 10.0.2.5 » help net.probe
```

```
net.probe (not running): Keep probing for new hosts on the network by sending dummy UDP packets to every possible IP on the subnet.
```

```
net.probe on : Start network hosts probing in background.  
net.probe off : Stop network hosts probing in background.
```

Parameters

```
net.probe.mdns : Enable mDNS discovery probes. (default=true)  
net.probe.nbns : Enable NetBIOS name service discovery probes. (default=true)  
net.probe.throttle : If greater than 0, probe packets will be throttled by this value in milliseconds. (default=10)  
net.probe.upnp : Enable UPNP discovery probes. (default=true)  
net.probe.wsd : Enable WSD discovery probes. (default=true)
```

```
10.0.2.0/24 > 10.0.2.5 » net.probe on
```

```
10.0.2.0/24 > 10.0.2.5 » [22:35:33] [sys.log] [inf] net.probe starting net.recon as a requirement for net.probe
```

```
10.0.2.0/24 > 10.0.2.5 » [22:35:33] [sys.log] [inf] net.probe probing 256 addresses on 10.0.2.0/24
```

```
10.0.2.0/24 > 10.0.2.5 » [22:35:33] [endpoint.new] endpoint 10.0.2.3 detected as 08:00:27:d3:e3:a5 (PCS Computer Systems GmbH).
```


[illegible]



MsfConsole

Metasploit Framework'ün konsol tabanlı bir kullanıcı arayüzüdür ve bu çerçeve aracılığıyla güvenlik açıklarını tespit etmek, siber saldırıları gerçekleştirmek ve güvenlik testleri yapmak için kullanılır.

KaliLinux işletim sisteminde sistemle birlikte yüklendiği için *'msfconsole'* komutu ile direk erişim sağlanabilir.

```
kali@BiltekCyber: ~  
File Actions Edit View Help  
  
(kali@BiltekCyber)-[~]  
$ msfconsole  
  
Metasploit  
  
=[ metasploit v6.2.26-dev ]  
+ -- --=[ 2264 exploits - 1189 auxiliary - 404 post ]  
+ -- --=[ 951 payloads - 45 encoders - 11 nops ]  
+ -- --=[ 9 evasion ]  
  
Metasploit tip: View advanced module options with  
advanced  
Metasploit Documentation: https://docs.metasploit.com/  
  
msf6 >
```



BiltekCyber

Social-Engineer Toolkit (SET)





Social-Engineer Toolkit (SET)

SET, bilgisayar korsanları ve bir çok pentester tarafından kullanılan, sosyal mühendislik tabanlı saldırıları için Python dilinde yazılmış open-source hack aracıdır. Genellikle banka ve sosyal medya hesapları, e-posta bilgileri gibi kişisel gizli bilgileri ele geçirmek için kullanılır. Bu uygulamayı kullanarak yapabileceğiniz bazı saldırı işlemleri aşağıda belirtilmiştir.

- Phishing Saldırıları
- Payload Oluşturma
- Dinleme ve İzleme
- Raporlama ve Veri Analizi



```
root@BiltekCyber: /home/kali
File Actions Edit View Help

.. ##### .. ##### .. #####
.. ## ..... ## ..... ## .....
.. ## ..... ## ..... ## .....
.. ##### .. ##### ..... ## .....
.. ..... ## ..... ## ..... ## .....
.. ## ..... ## ..... ## .....
.. ##### .. ##### ..... ## .....

[—] The Social-Engineer Toolkit (SET) [—]
[—] Created by: David Kennedy (ReL1K) [—]
      Version: 8.0.3
      Codename: 'Maverick'
[—] Follow us on Twitter: @TrustedSec [—]
[—] Follow me on Twitter: @HackingDave [—]
[—] Homepage: https://www.trustedsec.com [—]
Welcome to the Social-Engineer Toolkit (SET).
The one stop shop for all of your SE needs.

The Social-Engineer Toolkit is a product of TrustedSec.

Visit: https://www.trustedsec.com

It's easy to update using the PenTesters Framework! (PTF)
Visit https://github.com/trustedsec/ptf to update all your tools!

Select from the menu:

1) Social-Engineering Attacks
2) Penetration Testing (Fast-Track)
3) Third Party Modules
4) Update the Social-Engineer Toolkit
5) Update SET configuration
6) Help, Credits, and About

99) Exit the Social-Engineer Toolkit

set> 
```



BiltekCyber

SET Kullanımı

KaliLinux işletim sistemlerinde sistemle birlikte gelen bir araç olduğu için sadece root(kök) kullanıcısına geçerek bu aracın kullanılmasını sağlayabiliyoruz. Bu işlem için 'sudo su' komutunu girdikten sonra çalışmakta olan kullanıcı hesabının şifresini girerek root kullanıcısı oluyoruz.

Root kullanıcısı olduktan sonra terminale 'setoolkit' yazarak uygulamayı çalıştırıyoruz.





BiltekCyber

HIDDEN EYE



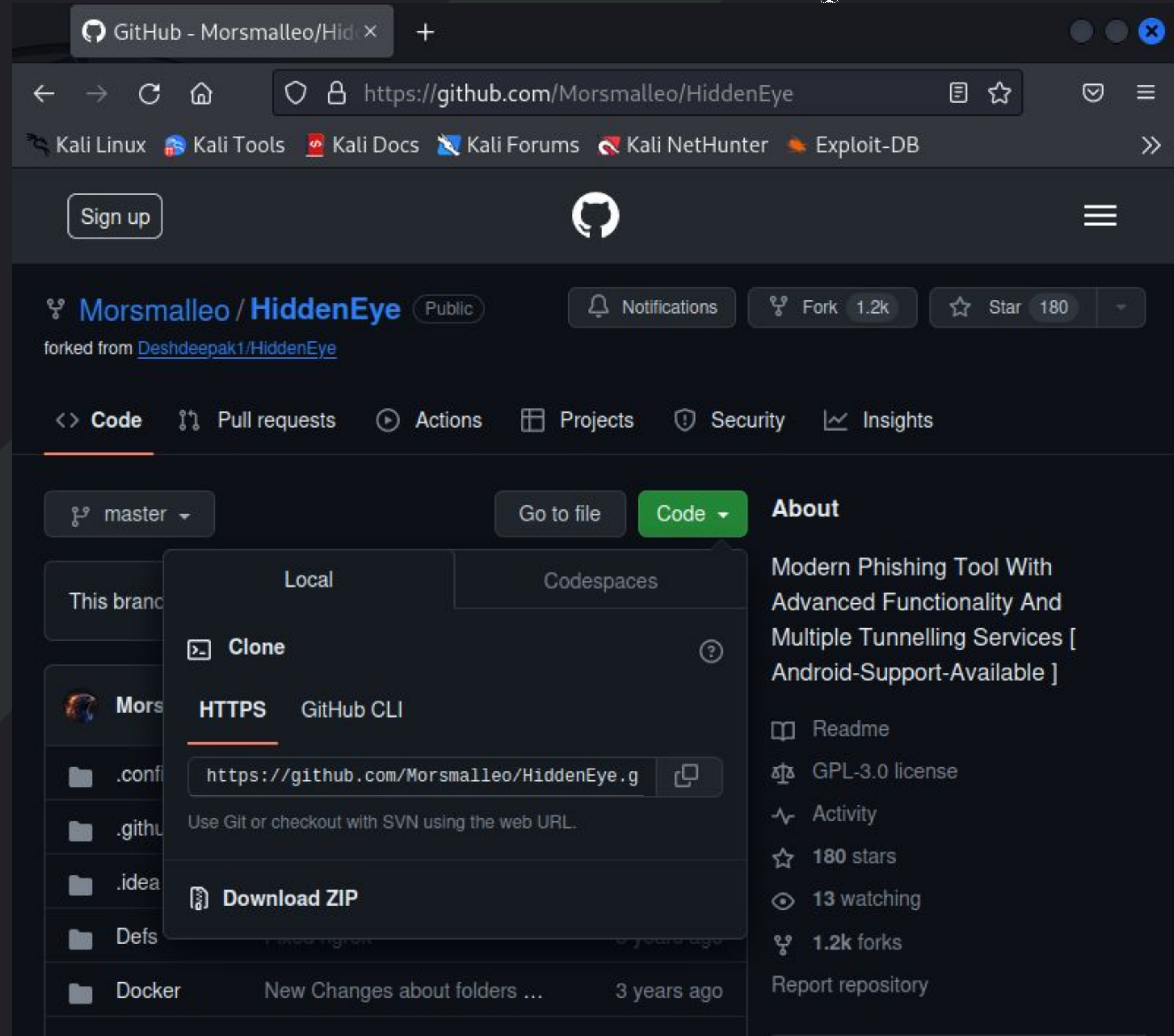
HIDDEN EYE





HIDDEN EYE

Hidden Eye, phishing (sosyal mühendislik) saldırıları simüle etmek için kullanılan bir açık kaynak araçtır. KaliLinux sistemine kurmak için *'git clone'* komutunu yazdıktan sonra yandaki ekran görüntüsünde altı çizili olan linki yapıştırarak kurulumu gerçekleştiriyoruz.





HIDDEN EYE

Uygulamayı kurduktan sonra uygulamanın kurulduğu dizini kullanarak uygulamanın içine 'cd' komutunu kullanarak girdikten sonra 'python3 HiddenEye' komutunu kullanarak uygulamanın açılmasını sağlıyoruz.

Not: Sistemde gerekli uygulamalar yüklü değilse 'sudo pip3 install -r requirements.txt' komutunu kullanarak paketlerin kurulumunu sağlayabilirsiniz

```
root@BiltekCyber: /home/kali/HiddenEye
File Actions Edit View Help

(root@BiltekCyber)-[/home/kali]
# git clone https://github.com/Morsmalleo/HiddenEye.git
Cloning into 'HiddenEye' ...
remote: Enumerating objects: 7141, done.
remote: Counting objects: 100% (22/22), done.
remote: Compressing objects: 100% (19/19), done.
remote: Total 7141 (delta 10), reused 6 (delta 3), pack-reused 7119
Receiving objects: 100% (7141/7141), 45.48 MiB | 4.61 MiB/s, done.
Resolving deltas: 100% (3593/3593), done.

(root@BiltekCyber)-[/home/kali]
# ls
Desktop Documents Downloads HiddenEye Music Pictures Public

(root@BiltekCyber)-[/home/kali]
# cd HiddenEye

(root@BiltekCyber)-[/home/kali/HiddenEye]
# python3 HiddenEye
```



BiltekCyber

MALTEGO

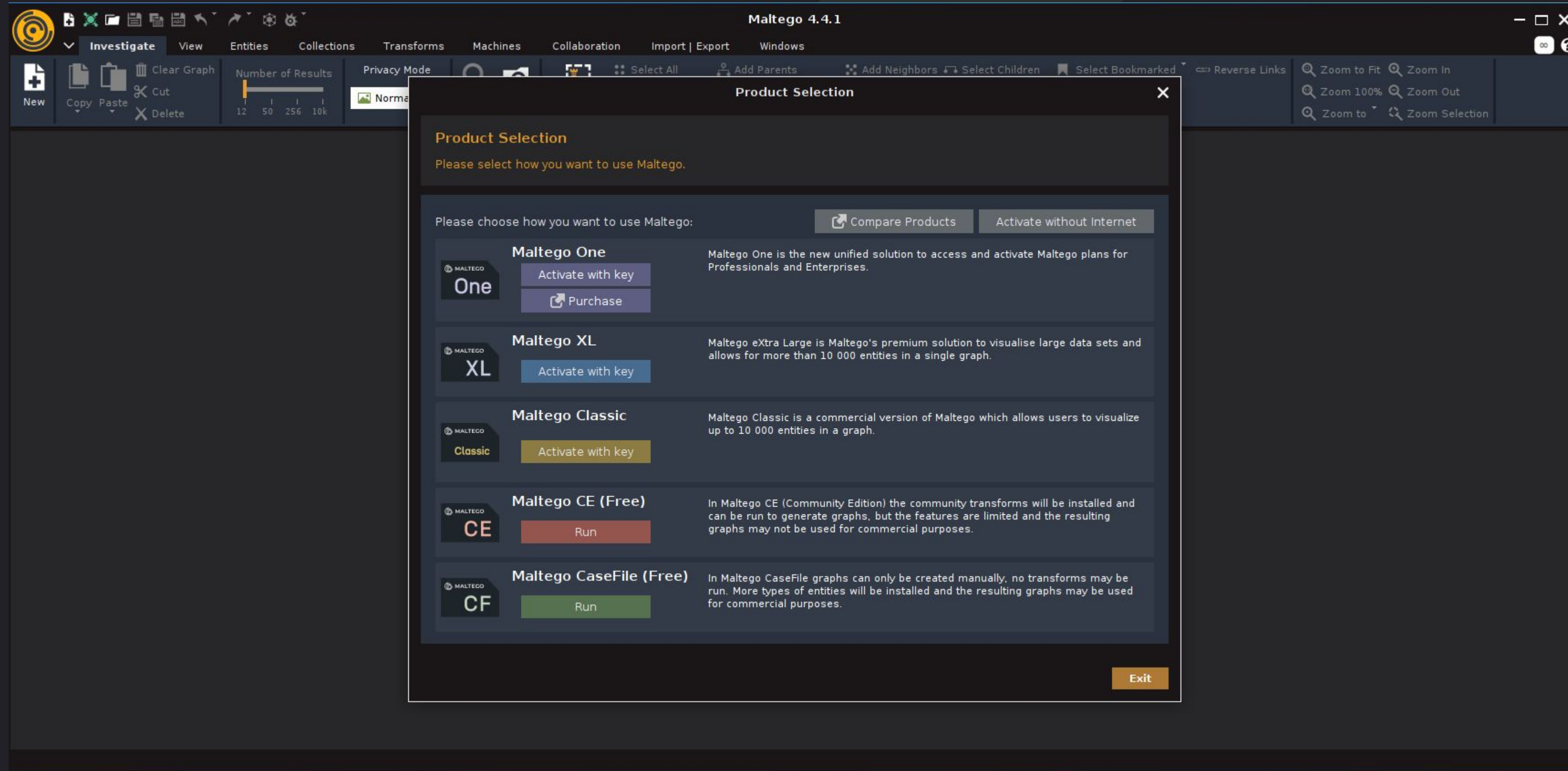
MALTEGO





MALTEGO

Maltego, siber güvenlik ve istihbarat toplamak amacıyla kullanılan bir görsel bağlantı analiz aracıdır. Maltego, açık kaynak istihbarat kaynaklarından veri toplamak, bu verileri görsel olarak analiz etmek ve farklı veri noktaları arasındaki ilişkileri keşfetmek için kullanılır.





Dirbuster





Dirbuster

Dirbuster özellikle web uygulamalarındaki gizli dizinleri ve dosyaları bulmak için kullanılır. Kısaca web uygulamalarının zayıf noktalarını tespit etmek amacıyla kullanılan bir araçtır.

Kurulumu için root(kök) kullanıcısı olarak 'apt-get install dirbuster' yazarak kurulumunu sağlayabilirsiniz.

The screenshot shows the OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing application window. The interface includes a menu bar (File, Options, About, Help) and a main configuration area. The 'Target URL' field is empty. The 'Work Method' section has two radio buttons: 'Use GET requests only' and 'Auto Switch (HEAD and GET)'. The 'Number Of Threads' is set to 10, with a 'Go Faster' checkbox. The 'Select scanning type' section has two radio buttons: 'List based brute force' and 'Pure Brute Force'. Below this is a 'File with list of dirs/files' field with a 'Browse' button and a 'List Info' button. The 'Char set' is set to 'a-zA-Z0-9%20-_', 'Min length' is 1, and 'Max Length' is 8. The 'Select starting options' section has two radio buttons: 'Standard start point' and 'URL Fuzz'. There are checkboxes for 'Brute Force Dirs', 'Be Recursive', 'Brute Force Files', and 'Use Blank Extension'. The 'Dir to start with' field is set to '/', and the 'File extension' field is set to 'php'. The 'URL to fuzz' field is set to '/test.html?url={dir}.asp'. At the bottom, there is an 'Exit' button and a 'Start' button. A message at the bottom says 'Please complete the test details'.



BiltekCyber

Aircrack-ng





Aircrack-ng

Aircrack-ng, kablosuz ağların güvenlik açıklarını tespit etmek ve kablosuz ağ şifrelerini kırmak için kullanılan bir açık kaynak araçtır.

'airmon-ng' kodu monitör modunu destekleyen wifi kartlarınızı gösterecektir. Eğer görünürde bişey yoksa wifi kartınız bu modülü desteklemiyor demektir.

```
root@BiltekCyber: /home/kali
File Actions Edit View Help

(root@BiltekCyber)-[/home/kali]
# airmon-ng

PHY      Interface      Driver      Chipset

(root@BiltekCyber)-[/home/kali]
# airmon-ng --help

usage: airmon-ng <start|stop|check> <interface> [channel or frequency]
```





Kaynakça

- 1-<https://www.kali.org/tools/bettercap/>
- 2-<https://github.com/trustedsec/social-engineer-toolkit>
- 3-<https://github.com/tiagorlampert/sAINT>
- 4-<https://github.com/Morsmalleo/HiddenEye>
- 5-<https://www.kali.org/tools/dirbuster/>
- 6-<https://www.kali.org/tools/maltego/>
- 7-<https://www.kali.org/tools/aircrack-ng/>





BiltekCyber

Hazırlayan

Adı: Yahya

Soyadı: Çakıcı

Fakülte: Mühendislik ve Doğa Bilimleri Fakültesi

Departman: Yazılım Mühendisliği 2.Sınıf

Linkedin: <https://www.linkedin.com/in/yahya-çakıcı-584004256/>

