BiltekCyber

Toollar 101

BiltekCyber

İçerik

BiltekCyber

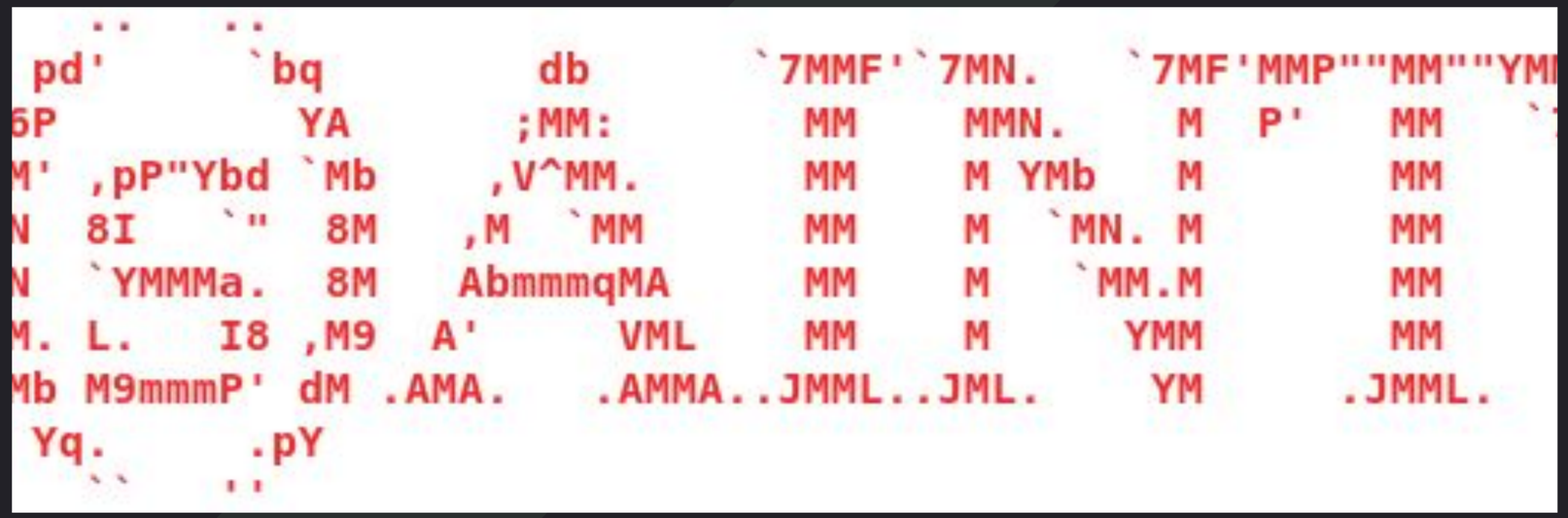
Toollar Nelerdir?

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.

BiltekCyber

SAINT (Security Administrator's Integrated Network Tool)



BiltekCyber

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

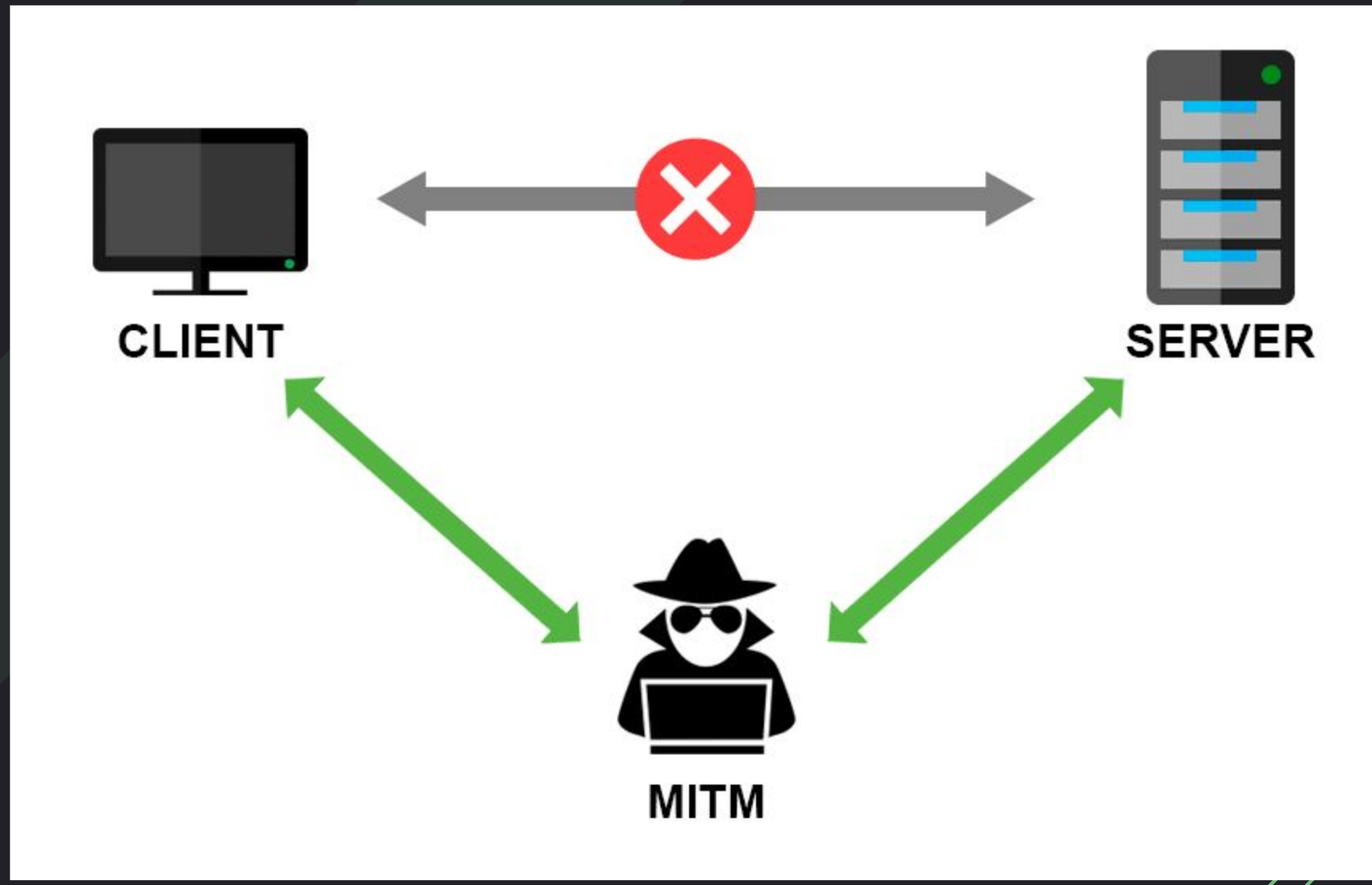
BiltekCyber

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.

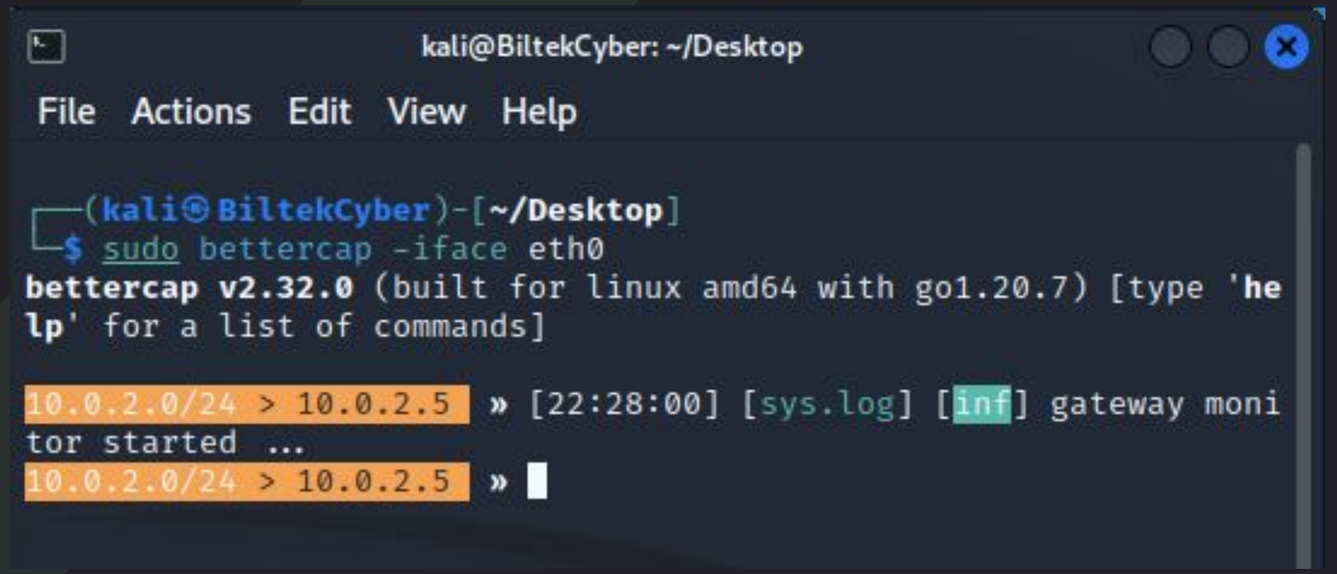
Sistemimize kurmak için ‘apt-get install bettercap’ yazarak kurulumunu gerçekleştirebilir ‘bettercap’ yazarak aracı kullanabilirsiniz.



Bettercap

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

Bettercap modüller aracılıyla 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.



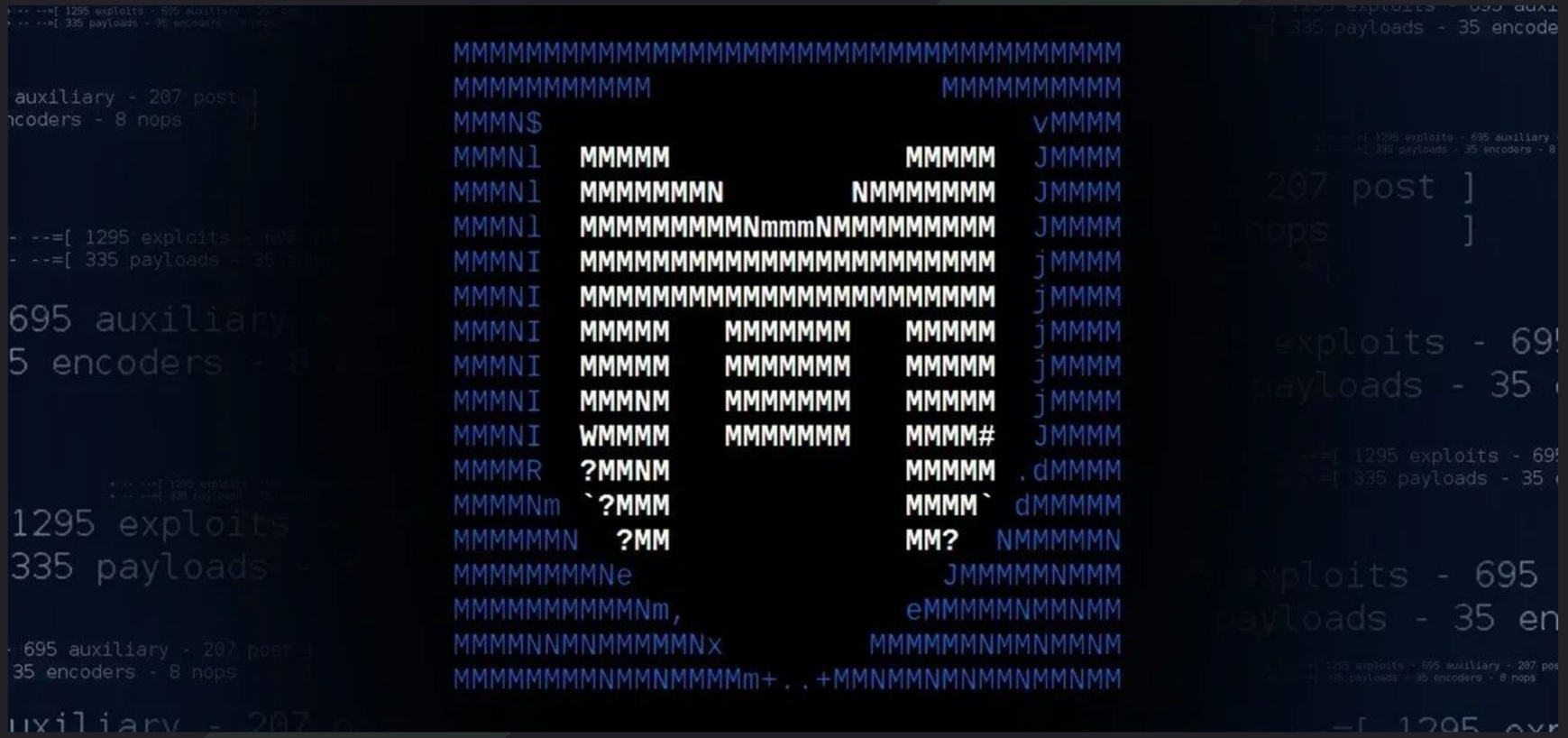
Bettercap

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 networ
k 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=tru
e)
      net.probe.nbns : Enable NetBIOS name service discovery prob
es. (default=true)
  net.probe.throttle : If greater than 0, probe packets will be t
hrottled by this value in milliseconds. (default=10)
      net.probe.upnp : Enable UPNP discovery probes. (default=tru
e)
       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 st
arting 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 pr
obing 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).
```

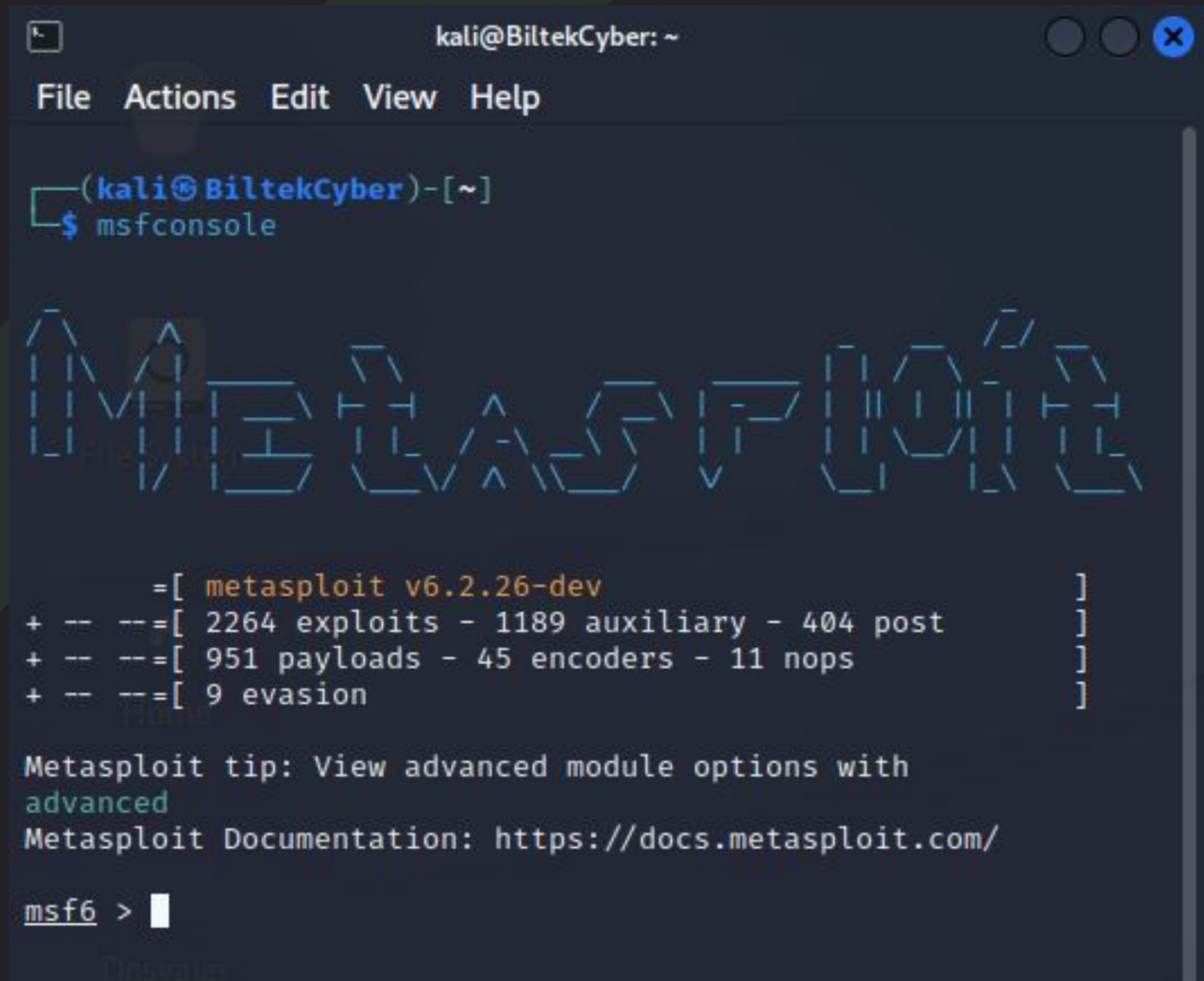
MsfConsole


MMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMM
MMMMMMMMMMM MMMMMMMMMM
MMMN$ vMMMM
MMMNl MMMMM MMMMM JMMMM
MMMNl MMMMMMMN NMMMMMMM JMMMM
MMMNl MMMMMMMMMNmmmNMMMMMMMMM JMMMM
MMMNI MMMMMMMMMMMMMMMMMMMMMM jMMMM
MMMNI MMMMMMMMMMMMMMMMMMMMM jMMMM
MMMNI MMMMM MMMMMMM MMMMM jMMMM
MMMNI MMMMM MMMMMMM MMMMM jMMMM
MMMNI MMMNM MMMMMMM MMMMM jMMMM
MMMNI WMMMM MMMMMMM MMMM# JMMMM
MMMMR ?MMNM MMMMM .dMMMM
MMMMNm `?MMM MMMM` dMMMMM
MMMMMMN ?MM MM? NMMMMMN
MMMMMMMMNe JMMMMMNMMM
MMMMMMMMMNm, eMMMMMNMNMNM
MMMMNNMNMMMMMNx MMMMMMNMMNMMNM
MMMMMMMMNMMNMMMMm+..+MMNMMNMNMMNMMNMM

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.



BiltekCyber

Social-Engineer Toolkit (SET)

BiltekCyber

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

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.

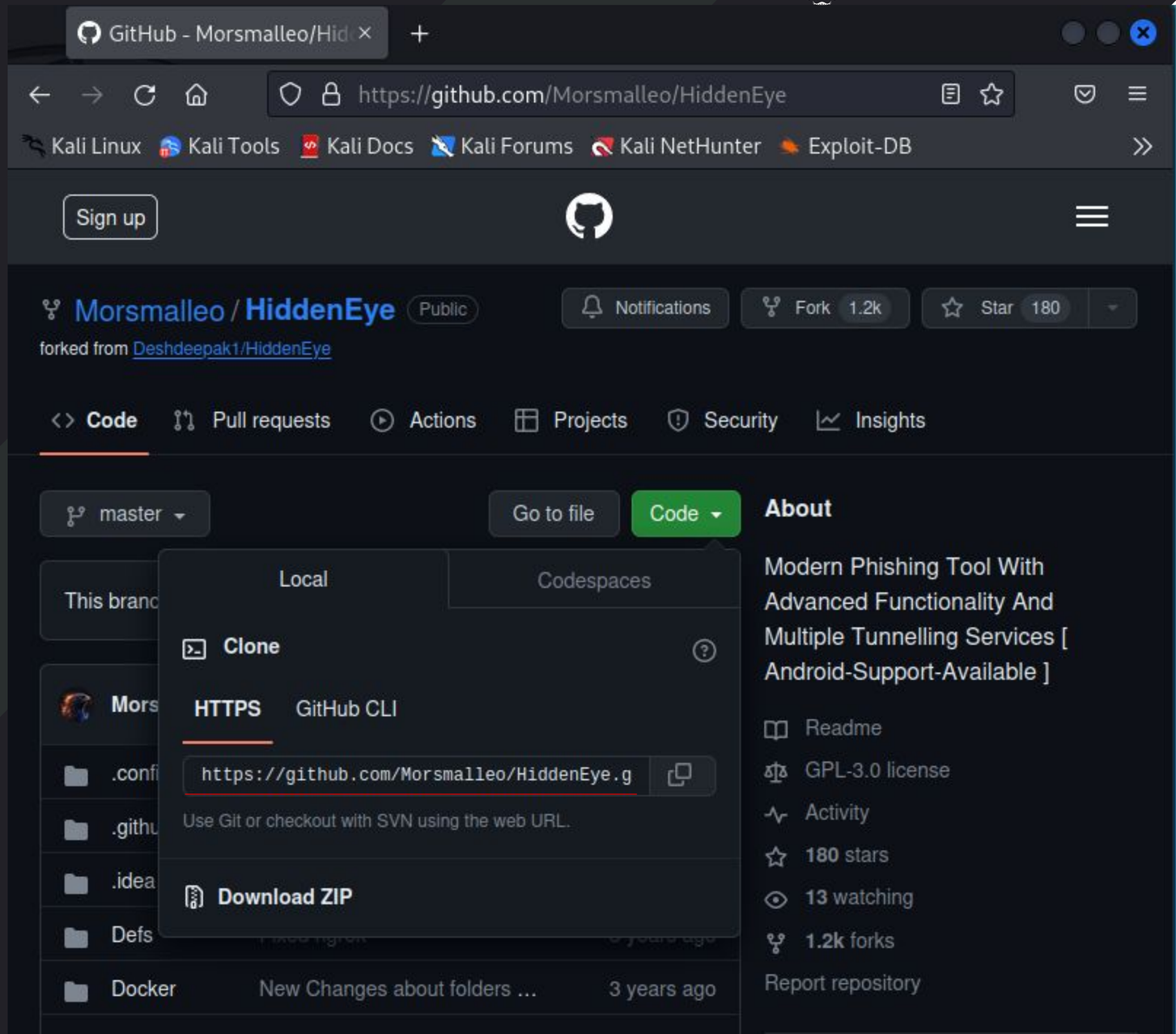
Root kullanıcısı olduktan sonra terminale '*setoolkit*' yazarak uygulamayı çalıştırıyoruz.

BiltekCyber

HIDDEN EYE

HIDDEN EYE

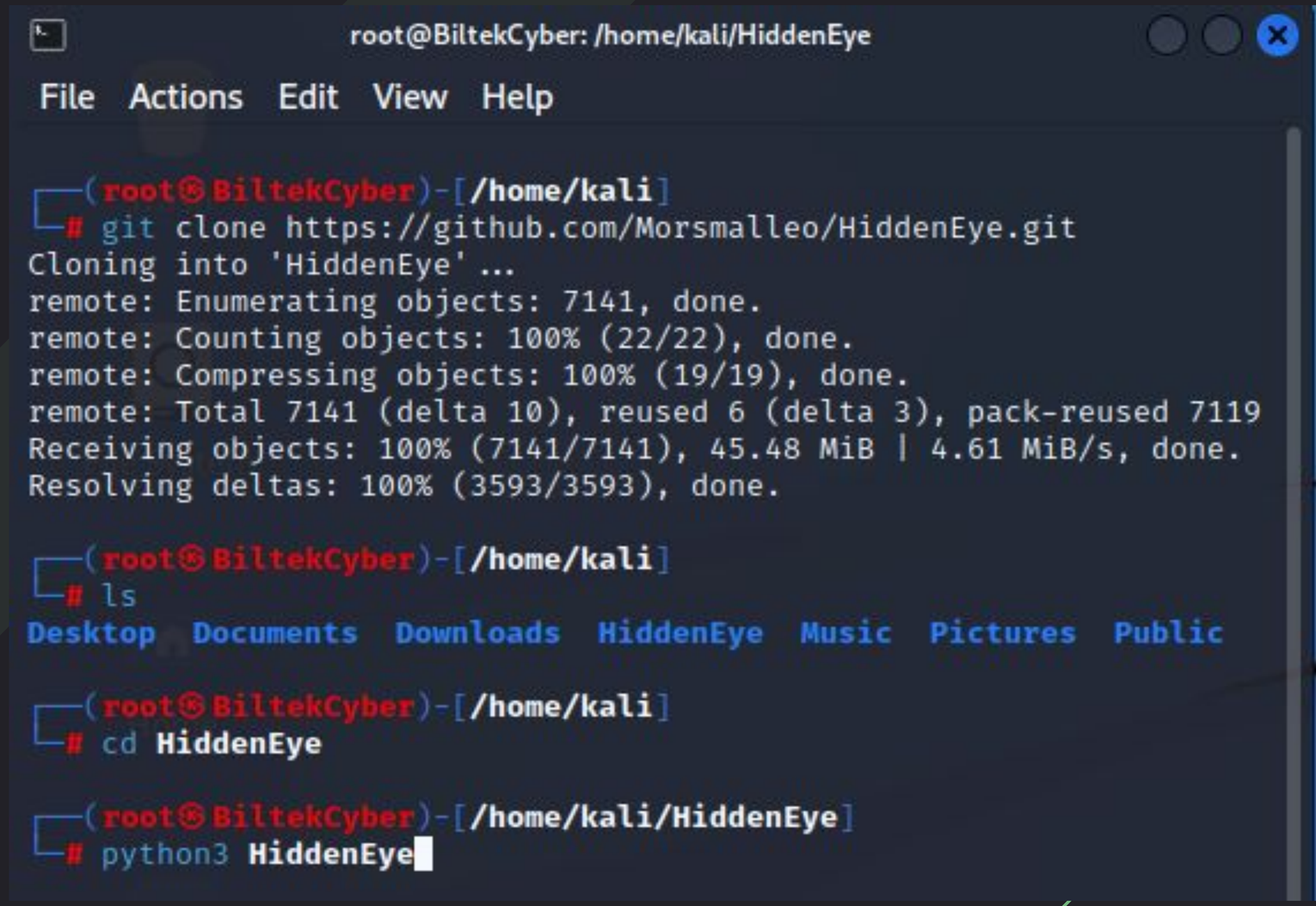
Hidden Eye, phishing (sosyal mühendislik) saldırıları simüle etmek için kullanılan bir açık kaynak araçtır. KaliLinux sistemine kurmak için *'git clone'* komutunu yazdıktan sonra yandaki ekran görüntüsünde altı çizili olan linki yapıştırarak kurulumu gerçekleştiriyoruz.



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.

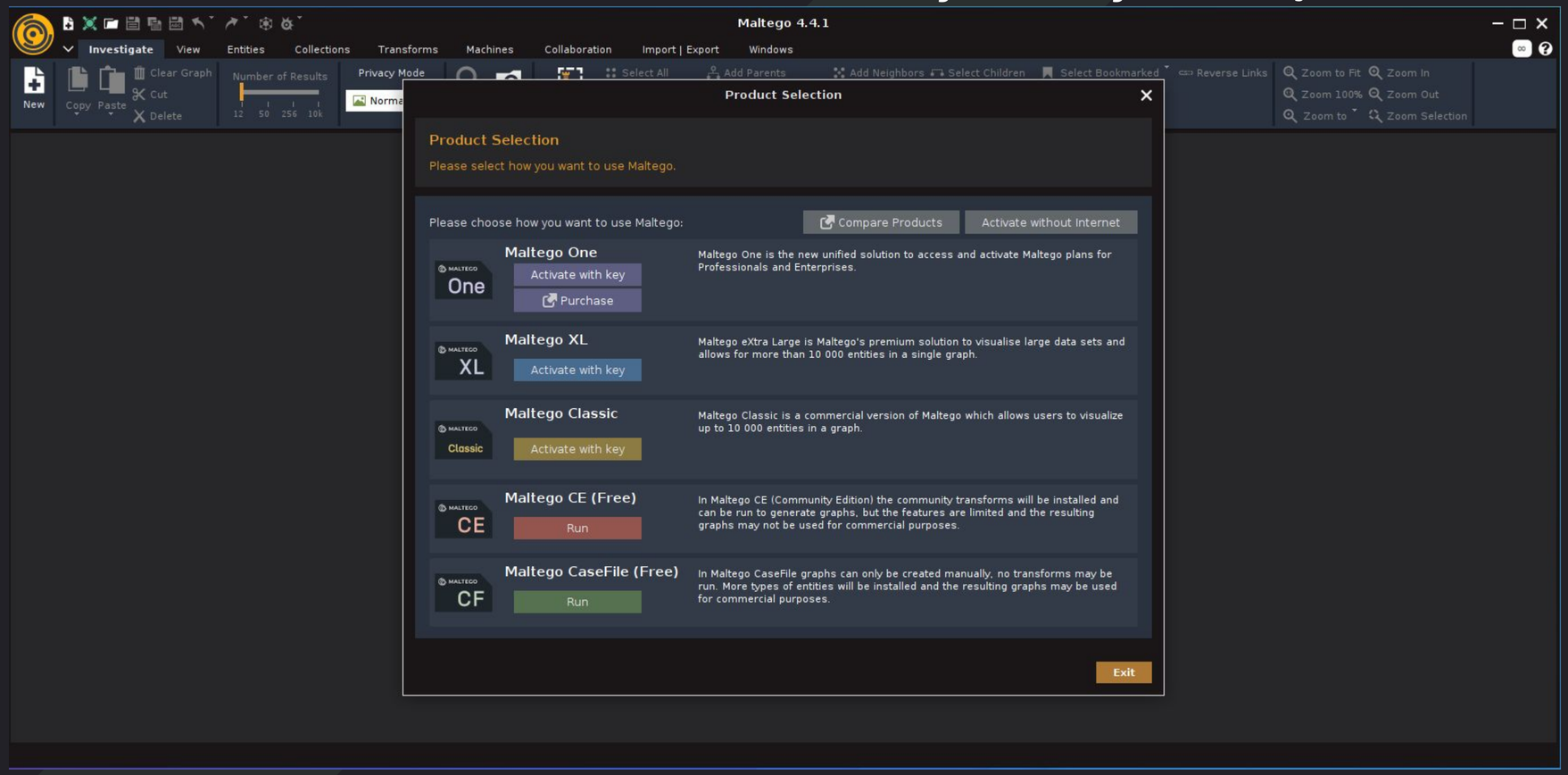


MALTEGO

BiltekCyber

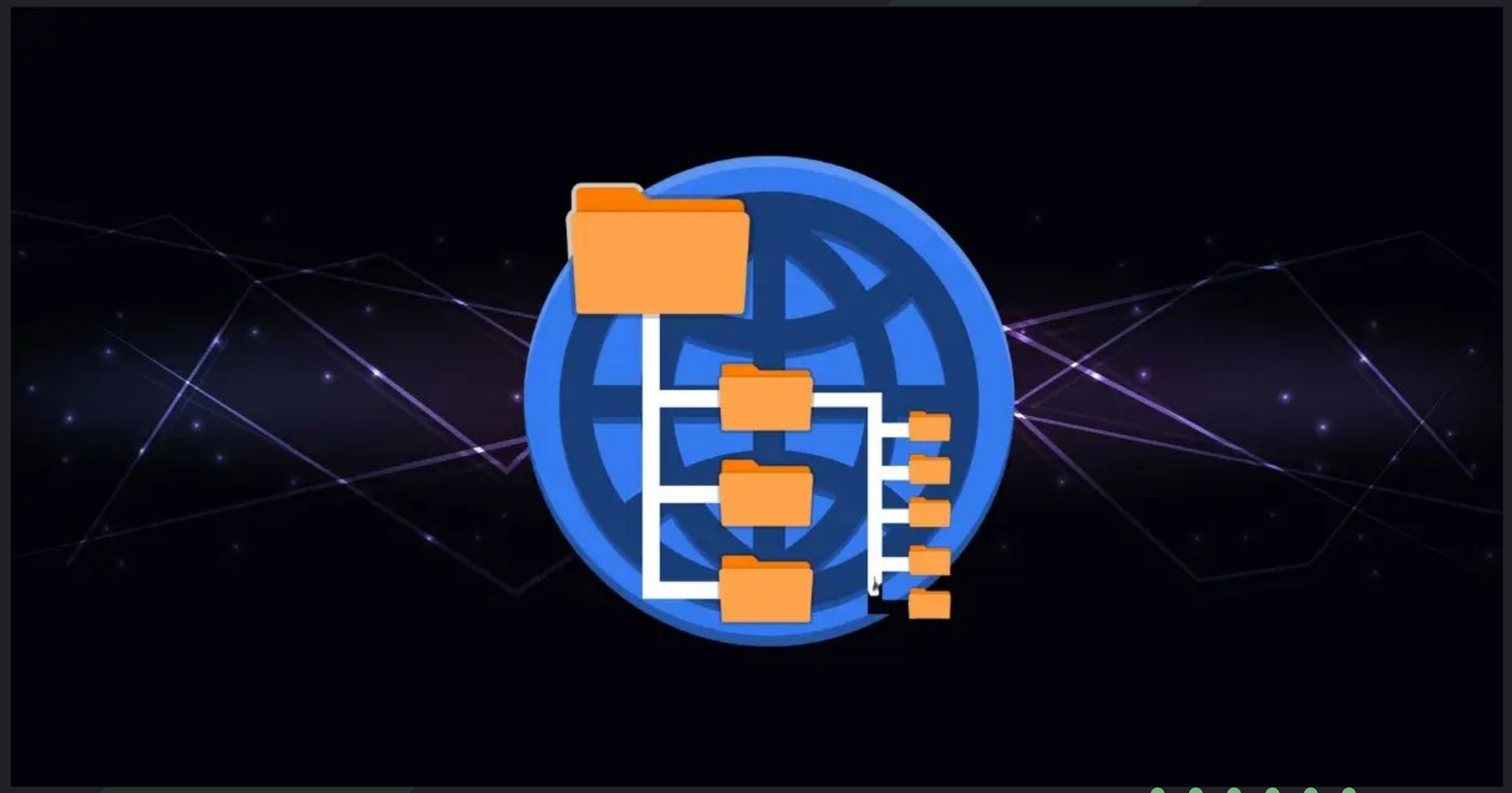
MALTEGO

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.



BiltekCyber

Dirbuster

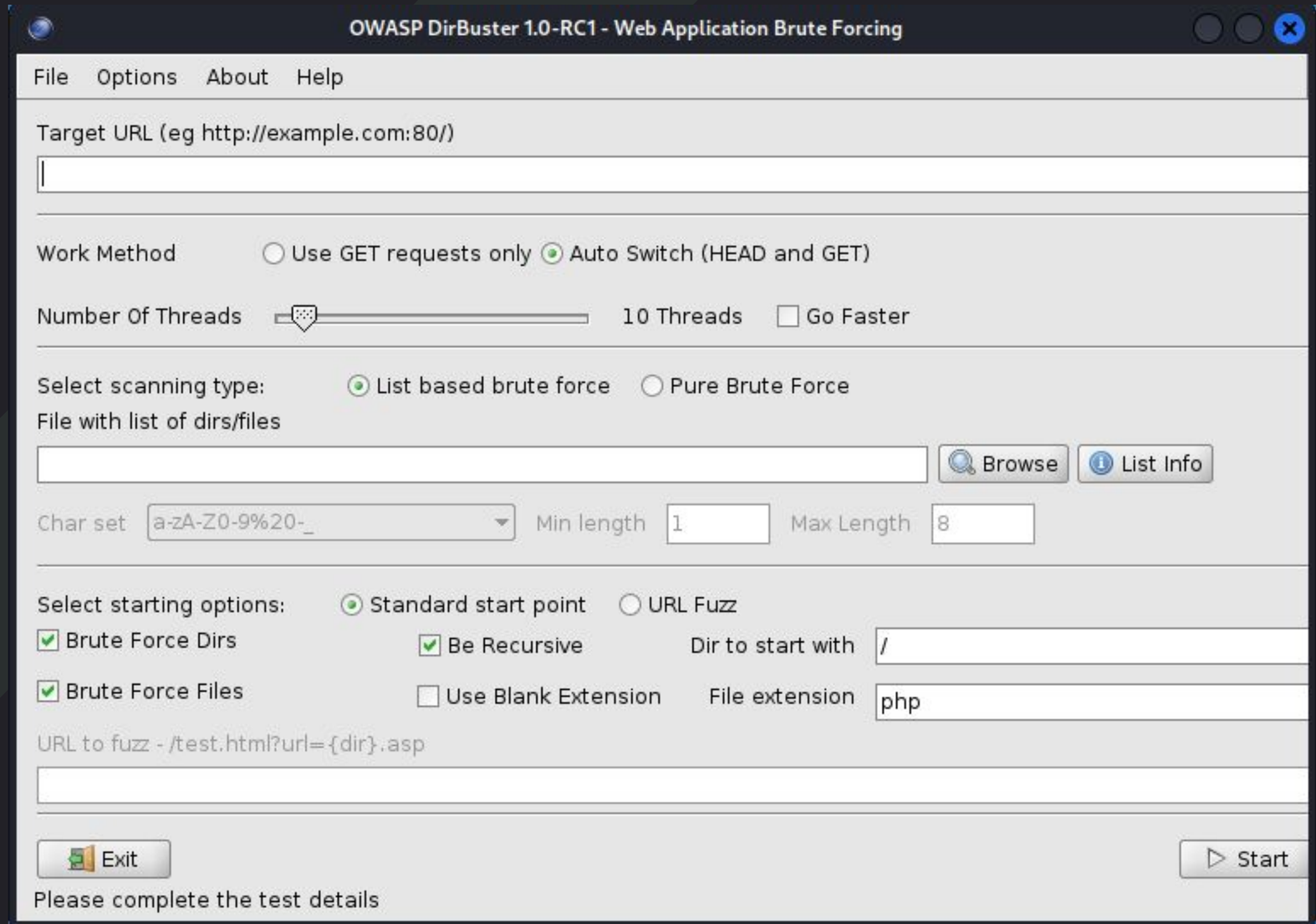


BiltekCyber

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.



BiltekCyber

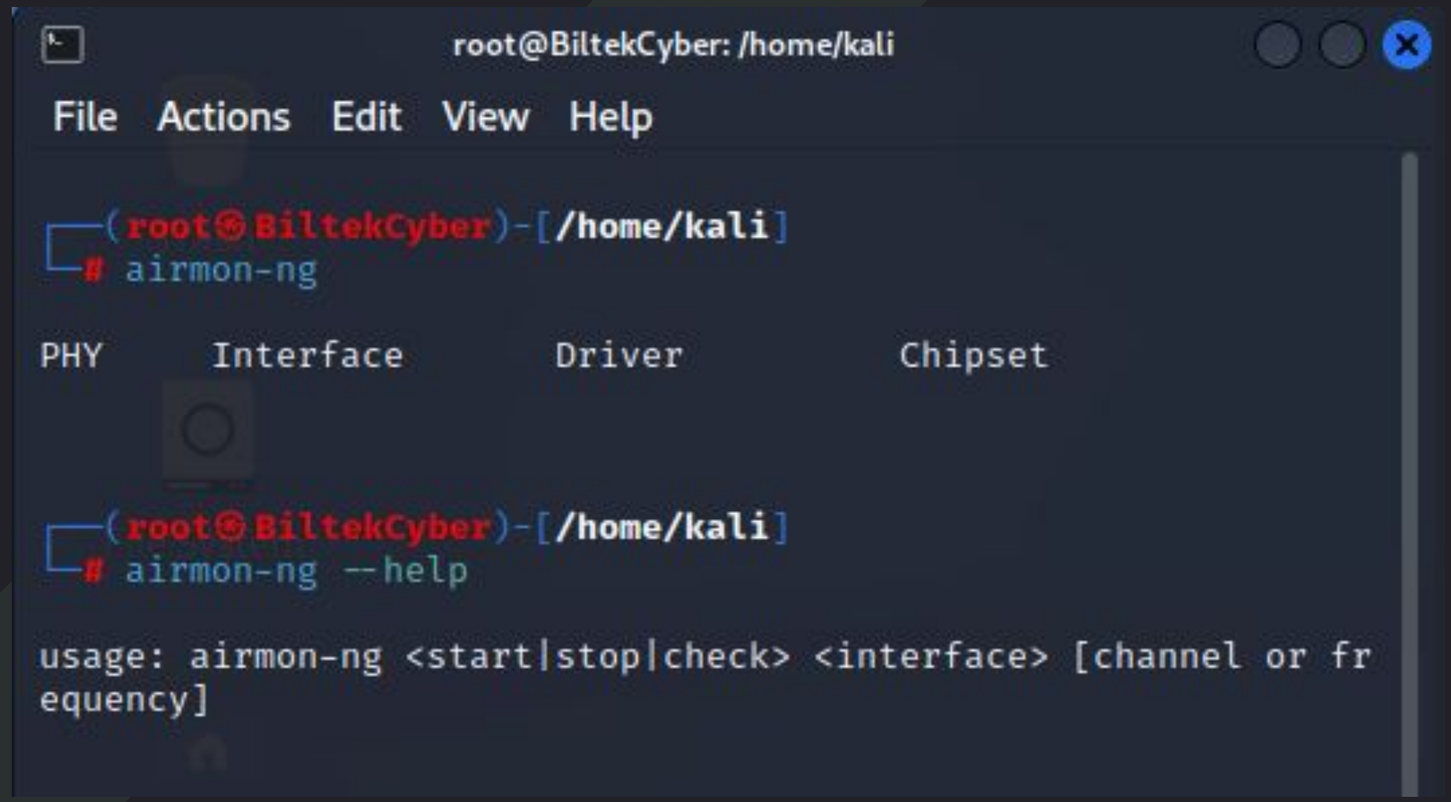
Aircrack-ng

BiltekCyber

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.



BiltekCyber

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/