

Mastering the Network HackingFU

y3dips {y3dips/at/echo/or/id}

Ada apa dengan TCP/IP

- Sudah Tua, kurang lebih 30 tahun.
- Dibuat tanpa memperhatikan keamanan
 - Contoh : Telnet, FTP, SMTP
- Celah sesungguhnya pada *layer* IP (v4)
 - Tidak ada metode verifikasi & enkripsi
 - Rentan terhadap *IP spoofing* dan *MITM*

Terkenal

- Tunneling
- Spoofing
- Sniffing
- ddos/botnet

Tunneling

- TOR (the Onion Router)
 - “Emerge tor privoxy”
 - Konfigurasi untuk jalan berbarengan
 - Forward-socks4a / 127.0.0.1:9050 .
- Node TOR bisa dibuat siapa saja
 - Gov, Mil, Mafia, dan siapa saja
- Gunakan enkripsi, atau prinsip dual tunnel
- <https://www.torproject.org/>

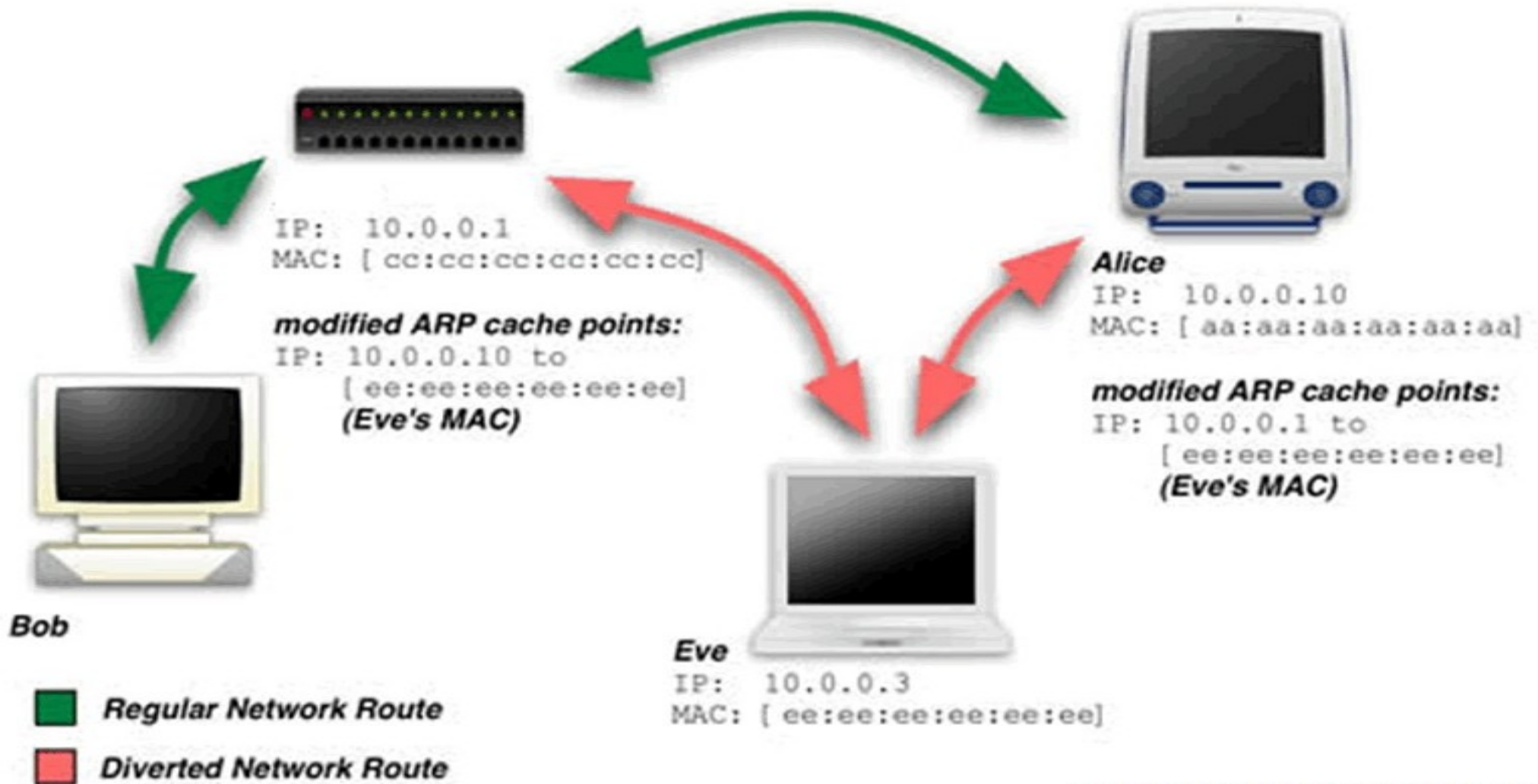


Tunneling

- SSH Tunneling
 - “ssh `user@server` -D port
- Stunnel - stunnel.org
- Mengamankan transaksi melalui protokol2 tanpa enkripsi
 - Tunneling http, smb melalui ssh/stunnel



Spoofting



Images taken from: <http://www.acm.org>

Monkey In the middle attack

The screenshot shows the main interface of Cain & Abel. The left sidebar lists various protocols, with 'HTTP (4)' selected. The main window displays a table of intercepted traffic. The table has columns for Timestamp, HTTP server, Client, Username, Password, and URL. The data shows a successful MITM attack where the user's password is captured and the URL is redirected to a phishing site.

Timestamp	HTTP server	Client	Username	Password	URL
26/04/2005 - 05:24:50	202.134.0.12	192.168.1.77	nakula26	aha	http://www.plasa.com/
26/04/2005 - 05:25:02	209.73.168.74	192.168.1.77	y3dips		https://login.yahoo.com/config/login_verify2?&.src=
26/04/2005 - 05:25:17	66.249.89.103	192.168.1.77	y3dips	djenc	https://www.google.com/accounts/ServiceLogin?ser
26/04/2005 - 05:42:48	209.11.168.242	192.168.1.77	jamput@palsu....	anjrot	http://www.friendster.com/

DEMO

Bertahan dengan Unix

- Paper Baca di

<http://www.slideshare.net/y3dips/arpwall-protect-from-arp-spoofing/>

- ARPWatch ,Swatch, PyGTK (*alert.py*)

ARPWALL

- Arp -s [ip] [mac]

<http://code.google.com/p/arpwall/> Wanna help ?



dDOS

- Untuk Dos, lihat
<http://www.slideshare.net/y3dips/denial-of-services/>
- Deteksi Botnet via SNMP
 - 6666 – 7000 open
- Syn attack v.s Syn Cookies
- Teknik baru (sebenarnya lama)
 - <http://it.slashdot.org/article.pl?sid=08/10/01/0127245>

Dunia Liar

- Tidak Standar (proprietary)
- Tertutup (closed source)
- Selamat tinggal anak-anak (kiddo)
- Kuat?

Dunia Liar

- Aplikasi scanner umumnya tak berdaya
NMAP, Nessus, superscan
- Bekerja berdasarkan data yang di input
- Metode handshake berbeda

Perlengkapan

- Python [kemampuan programming]
- Scapy (paket Manipulating platform)
- Spoofing
- Sniffing (tcpdump only?)
- Some l33t tools (THCAmapcrap)

NMAP vs AMAP

```
venom pri # nmap localhost -p 31337
```

```
Starting Nmap 4.76 ( http://nmap.org ) at 2008-12-12 13:08 WIT
```

```
Interesting ports on localhost (127.0.0.1):
```

```
PORT      STATE SERVICE
```

```
31337/tcp open  Elite
```

```
Nmap done: 1 IP address (1 host up) scanned in 0.23 seconds
```

```
venom pri # amapcrap 127.0.0.1 31337
```

```
# Starting AmapCrap on 127.0.0.1 port 31337
```

```
# Writing a "+" for every 10 connect attempts
```

```
#
```

```
# Put this line into appdefs.trig:
```

```
PROTOCOL_NAME::tcp:0:"cpacbucczoqaenwgtwjwstpxuacjdhifxihybk yp baviuqrpjgjcbbelemtjharebacays  
ztuglix pfbrcwshgjrnrkgjrguldljaccgoken iopprkfzqpoczuanucybdaeknonamvoaieknbaapb  
ivhhakdbncfyqtjqeccelhpyiozqxqdkclrcwudixiemanaeqdiakyztlwoasskvcaxyu epgiagwakletlpqi\r\n"
```

```
# Put this line into appdefs.resp:
```

```
PROTOCOL_NAME::tcp::"<head>\n<title>Error response</title>\n</head>\n<body>\n<h1>Error response  
</h1>\n<p>Error code 400.\n<p>Message: Bad request syntax  
( 'cpacbucczoqaenwgtwjwstpxuacjdhifxihybk yp baviuqrpjgjcbbelemtjharebacays ztuglix  
pfbrcwshgjrnrkgjrguldljaccgoken iopprkfzqpoczuanucybdaeknonamvoaieknbaapb  
ivhhakdbncfyqtjqeccelhpyiozqxqdkclrcwudixiemanaeqdiakyztlwoasskvcaxyu epgiagwakletlpqi' ) .\n<p>  
Error code explanation: 400 = Bad request syntax or unsupported method.\n</p>\ny>\n"
```

DEMO

Scapy

```
>>> sr(IP(dst="192.168.1.1")/TCP(sport=RandShort(),dport=[440,441,442,443],flags="S"))
>>> ans,unans = _
>>> ans.summary()
IP / TCP 192.168.1.100:ftp-data > 192.168.1.1:440 S =====> IP / TCP
192.168.1.1:440 > 192.168.1.100:ftp-data RA / Padding
IP / TCP 192.168.1.100:ftp-data > 192.168.1.1:441 S =====> IP / TCP
192.168.1.1:441 > 192.168.1.100:ftp-data RA / Padding
IP / TCP 192.168.1.100:ftp-data > 192.168.1.1:442 S =====> IP / TCP
192.168.1.1:442 > 192.168.1.100:ftp-data RA / Padding
IP / TCP 192.168.1.100:ftp-data > 192.168.1.1:https S =====> IP / TCP
192.168.1.1:https > 192.168.1.100:ftp-data SA / Padding

>>> ans.summary( lambda(s,r): r.strftime("%TCP.sport% \t %TCP.flags%") )
440      RA
441      RA
442      RA
https    SA
```

DEMO

Aplikasi Pribadi

- Tidak kuat, bahkan “relatif” lebih lemah
Hanya telnet secara multiple dan mereka mati
- Tcp/ip memang bercelah, Aplikasi yang berjalan di atasnya membawa dosa yang sama
 - Tanpa metode verifikasi + enkripsi
- Tidak ada akses kontrol, otentikasi, session timeout, limitasi koneksi

Tips Info di Jaringan

- **Snmp** (default community strings)
- **Sntp** (vrfy dan expn verbs ; enumerate user)
- **Ftp** (user enum)
- **Pop3** (user enum)

Bertahan?

- IPV6
- Medukung Autentikasi , IP proteksi dan Trafik Kontrol
- Alasan politis dan bisnis maka belum populer.

Santai

Tanya & Jawab

Terima Kasih

- Komite
- himatif UPN
- Kamu!, ya kamu yang mendukung acara ini.