Information Gathering

Contents

- What is information gathering
- Passive information gathering
- Active information gathering

1. What is information gathering

1. What is information gathering

- Information gathering is the first step in conducting a penetration test and is arguably the most important.
- Information gathering is the process of collecting the information from different places about individual company, organization, Server, IP address or person.

Information Gathering

- Types of information gathering
  - Passive information gathering
  - Active information gathering

2. Passive Information Gathering

2. Passive Information Gathering

- Passive information gathering focuses on collecting information archived on systems not located in our client's network.
- We try to gather as much information about our target network and systems without connecting to them directly.

Information Searches

- Locate the target Web presence
- Gather search engine results regarding the target
- Look for Web groups containing employee and/or company comments
- Examine the personal Web sites of employees
- Search archival sites for additional information
- Look for job postings submitted by the target
- Query the domain registrar
- Domain name system (DNS) information

Results

- The penetration tester will have a wealth of information regarding the target without ever visiting the target's network.
- All passive information is gathered from third-party sources that have collected information about our target, or have legal requirements to retain this data.

Tools

- **Netcraft** (http://www.netcraft.com)

Site title	HCM.PTIT.EDU.VN - Học Viện Công Nghệ Bưu Chính Viễn Thông Cơ sở TP. Hồ Chí Minh	**Date first seen**	October 2013

Netblock owner	IP address	OS	Web server	Last seen Refresh
VietNam Post and Telecom Corporation FTTH Service	113.161.98.131	Windows Server 2003	Apache/2.2.17 Win32 mod_ssl/2.2.17 OpenSSL/0.9.8o PHP/5.3.4 mod_perl/2.0.4 Perl/v5.10.1	31-Aug-2015

IPv6 address	*Not Present*	**Reverse DNS**	static.vnpt.vn
Domain registrar	*unknown*	**Nameserver organisation**	*unknown*
Organisation	*unknown*	**Hosting company**	VDC
Top Level Domain	Vietnam (.edu.vn)	**DNS Security Extensions**	*unknown*
Hosting country	VN		

Tools

- **Whois** Lookups (*root@kali:~# whois bulbsecurity.com*)

```
root@kali:~# whois facebook.com

Whois Server Version 2.0

Domain names in the .com and .net domains can now be registered
with many different competing registrars. Go to http://www.internic.net
for detailed information.

   Domain Name: FACEBOOK.COM
   Registrar: MARKMONITOR INC.
   Sponsoring Registrar IANA ID: 292
   Whois Server: whois.markmonitor.com
   Referral URL: http://www.markmonitor.com
   Name Server: A.NS.FACEBOOK.COM
   Name Server: B.NS.FACEBOOK.COM
   Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
   Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
   Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
   Status: serverDeleteProhibited https://icann.org/epp#serverDeleteProhibited
   Status: serverTransferProhibited https://icann.org/epp#serverTransferProhibited
   Status: serverUpdateProhibited https://icann.org/epp#serverUpdateProhibited
   Updated Date: 29-nov-2016
   Creation Date: 29-mar-1997
   Expiration Date: 30-mar-2025

>>> Last update of whois database: Thu, 06 Apr 2017 12:06:05 GMT <<<

For more information on Whois status codes, please visit https://icann.org/epp

NOTICE: The expiration date displayed in this record is the date the
```

Tools

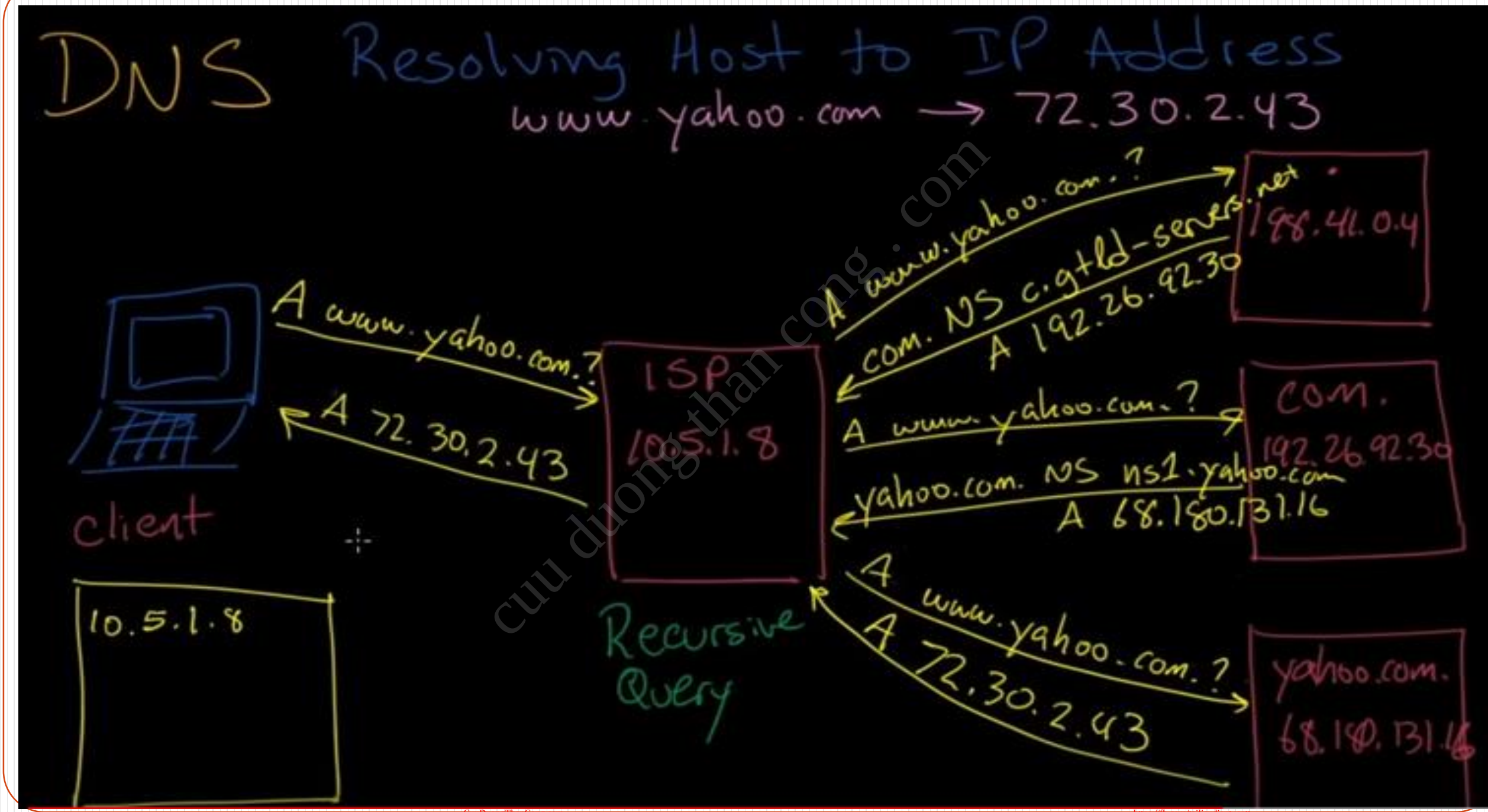
- **DNS Reconnaissance: Domain Name System(DNS)** DNS is used to translate domain names into IP addresses and vice versa.
- Record in DNS:
  - A: Address
  - CNAME: Canonical Name
  - MX: Mail Exchange

CNAME	**cấu hình bí danh, nghĩa là 1 ip có thể gắn vào nhiều tên.** **1 IP có thể gắn nhiều CNAME** **server.movie.edu. IN CNAME terminator.movie.edu.**
A	Ánh xạ tên miền vào địa chỉ IP. Vd: terminator.movie.edu. IN A 192.168.11.100
MX	Dùng để chuyển mail trên internet t3h.com IN MX 0 mail.t3h.com.

DNS

Resolving Host to IP Address

www.yahoo.com → 72.30.2.43



DNS Reconnaissance

```
root@kali:~# nslookup hcm.ptit.edu.vn
Server:         192.168.206.2
Address:        192.168.206.2#53

Non-authoritative answer:
Name:   hcm.ptit.edu.vn
Address: 113.161.98.131

root@kali:~#
```

#nslookup –type=ns example.com 8.8.8.8

DNS Reconnaissance

```
#!/bin/sh

for HOSTNAME in `cat DomainNames.txt`

do

        echo "Getting name servers for [$HOSTNAME]"

        nslookup -type=ns $HOSTNAME 8.8.8.8

done
```

DNS Reconnaissance

- Domain Information Groper (Dig)

#dig example.com

```
; <<>> DiG 9.7.0-P1 <<>> example.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 56376
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;example.com.          IN    A

;; ANSWER SECTION:
example.com.       78294    IN    A    10.1.1.1

;; Query time: 32 msec
;; SERVER: 8.8.8.8#53(8.8.8.8)
;; WHEN: Sun ***  * **:**:** ****
;; MSG SIZE  rcvd: 45
```

Dig

- ***# dig +qr www.example.com any***

```
;; QUESTION SECTION:
;www.example.com.       IN    ANY

;; ANSWER SECTION:
example.com.        86400   IN    NS    ns1.example.com.
example.com.        86400   IN    MX    10 mx111.example.com.
example.com.        86400   IN    A    127.208.72.107
example.com.        86400   IN    NS    ns2.example.com.
example.com.        86400   IN    SOA    ns2.example.com. hostmaster.
example.com. 2011020501 28800 7200 604800 86400
example.com.        86400   IN    MX    10 mx99.example.com.
```

Dig

Shortening the output

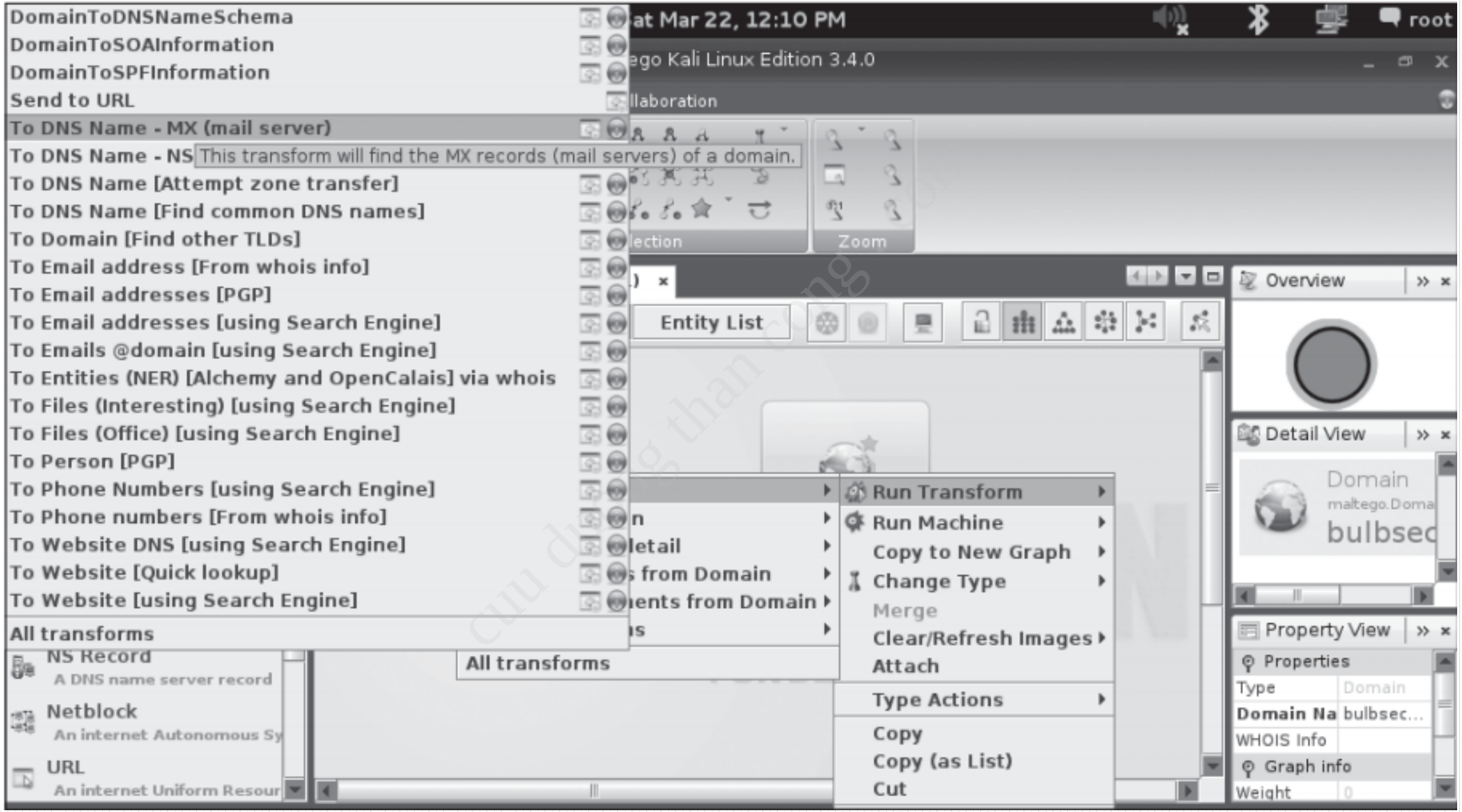
#dig +nocmd +noall +answer example.com

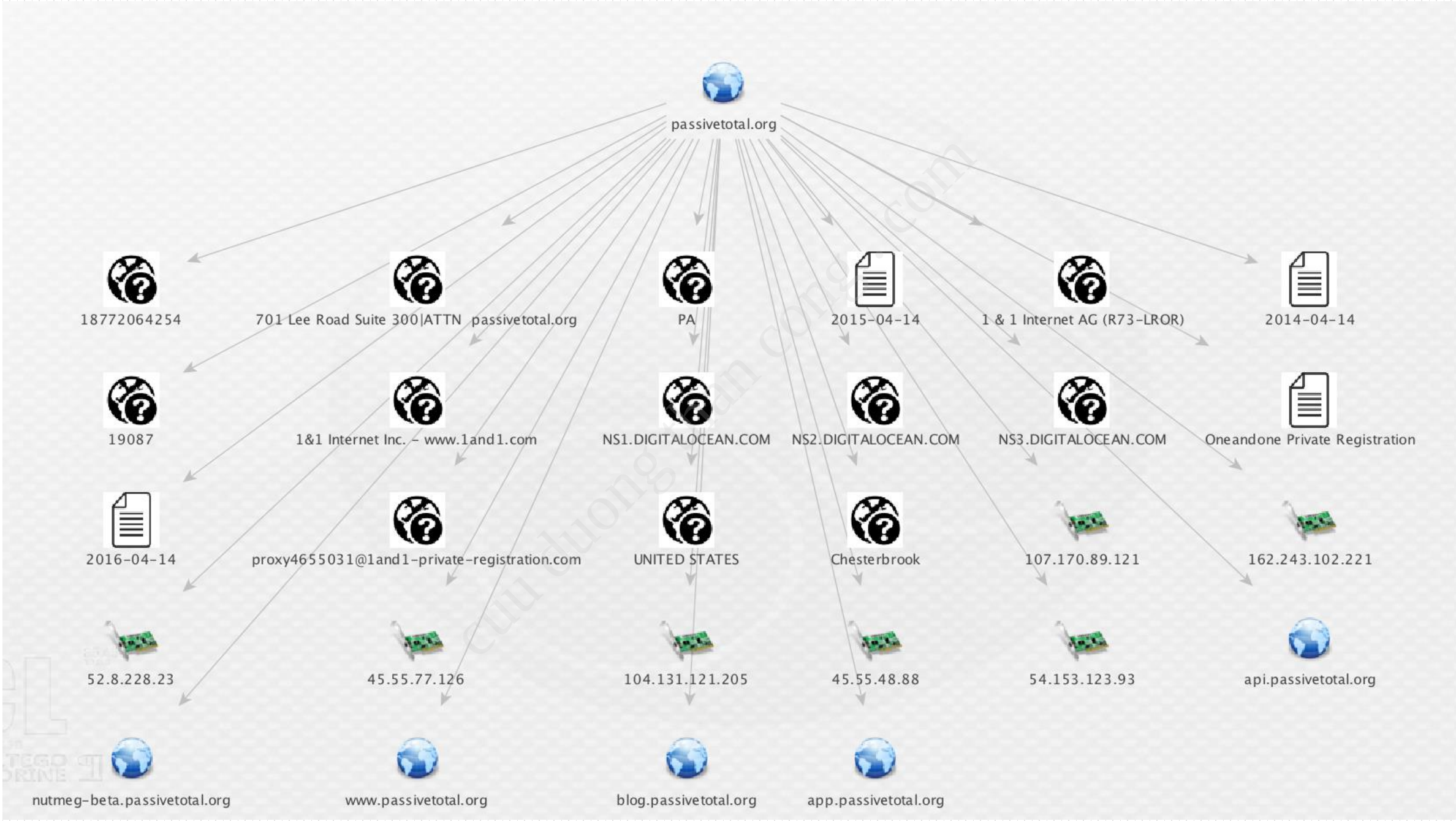
example.com. 44481 IN A 192.168.1.10

Tool

Maltego: Paterva's Maltego is a data-mining tool designed to visualize open source intelligence gathering.

- **#maltego**





Tools

- Searching for Email Addresses

Tool

- http://earth.google.com
- https://www.shodan.io/

Extracting metadata from photos

#exiftool t/images/FotoStation.jpg

 # exiftool t/images/FlashPix.ppt

- Title
- Subject
- Author
- Comments
- Software
- Company
- Manager
- Hyperlinks
- Current User

```
File Size                       : 4.2 kB
File Modification Date/Time     : 2011:04:30 05:32:11-04:00
File Permissions                : rw-r--r--
File Type                       : JPEG
MIME Type                       : image/jpeg
Image Width                     : 8
Image Height                    : 8
Encoding Process                : Baseline DCT, Huffman coding
Bits Per Sample                 : 8
Color Components                : 3
Y Cb Cr Sub Sampling            : YCbCr4:2:0 (2 2)
Original Image Width            : 1536
Original Image Height           : 1024
Color Planes                    : 3
XY Resolution                   : 38.626
Rotation                        : 90
Crop Left                       : 18.422%
Crop Top                        : 24.458%
Crop Right                      : 83.035%
Crop Bottom                     : 77.817%
```

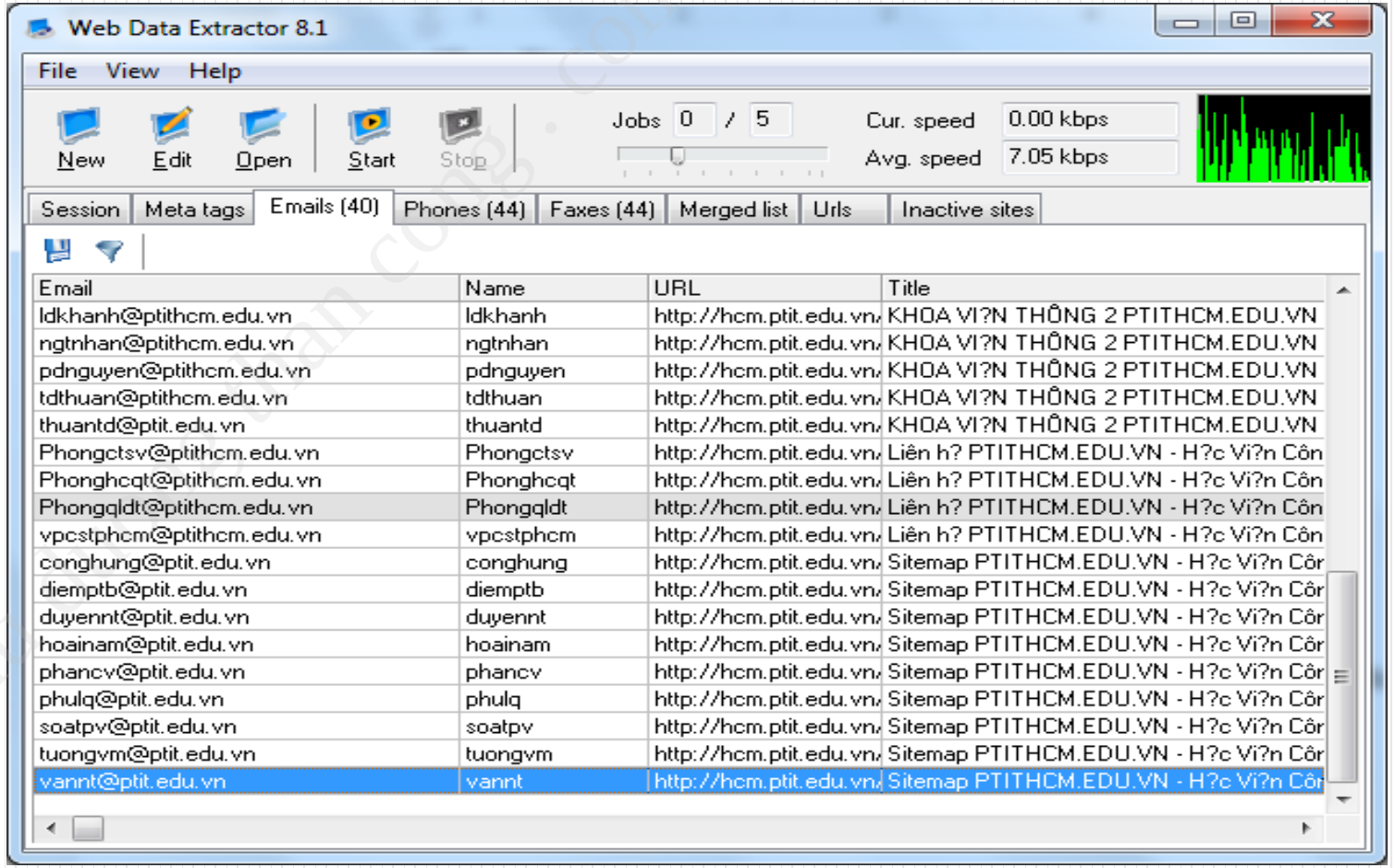
3. Active Information Gathering

Active Information Gathering

- We interact directly to our targets. Active information gathering will find results similar to what we already found using passive measures
- The advantage to include passive gathering in a penetration test is two fold:
  - Identify historical information
  - Confirm findings with active methods.

Tools

- E-mail Accounts
- DNS Interrogation
- Network Scanning



DNS Interrogation

Listing the bind version

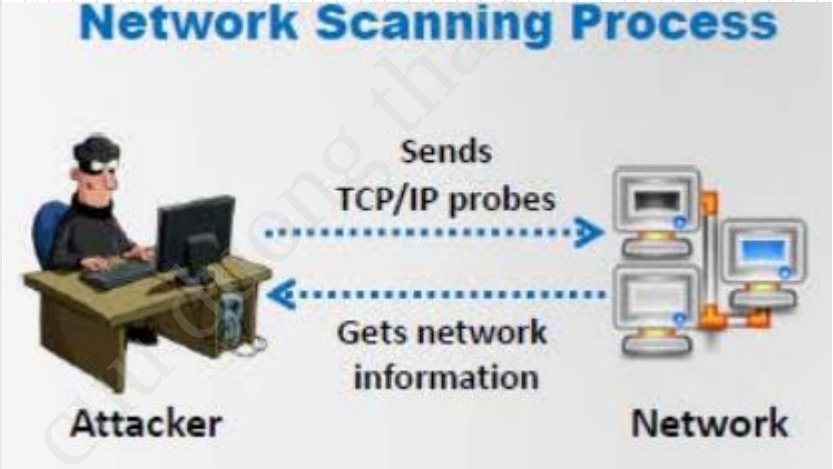
#dig +nocmd txt chaos VERSION.BIND @ns1.example.com +noall +answer

```
VERSION.BIND.           0    CH    TXT    "8.4.X"
```

```
bt ~ # nslookup
> server ns1.titan.net
Default server: ns1.titan.net
Address: 64.13.134.58#53
> set type=mx
> nmap.org
```

Network Scanning

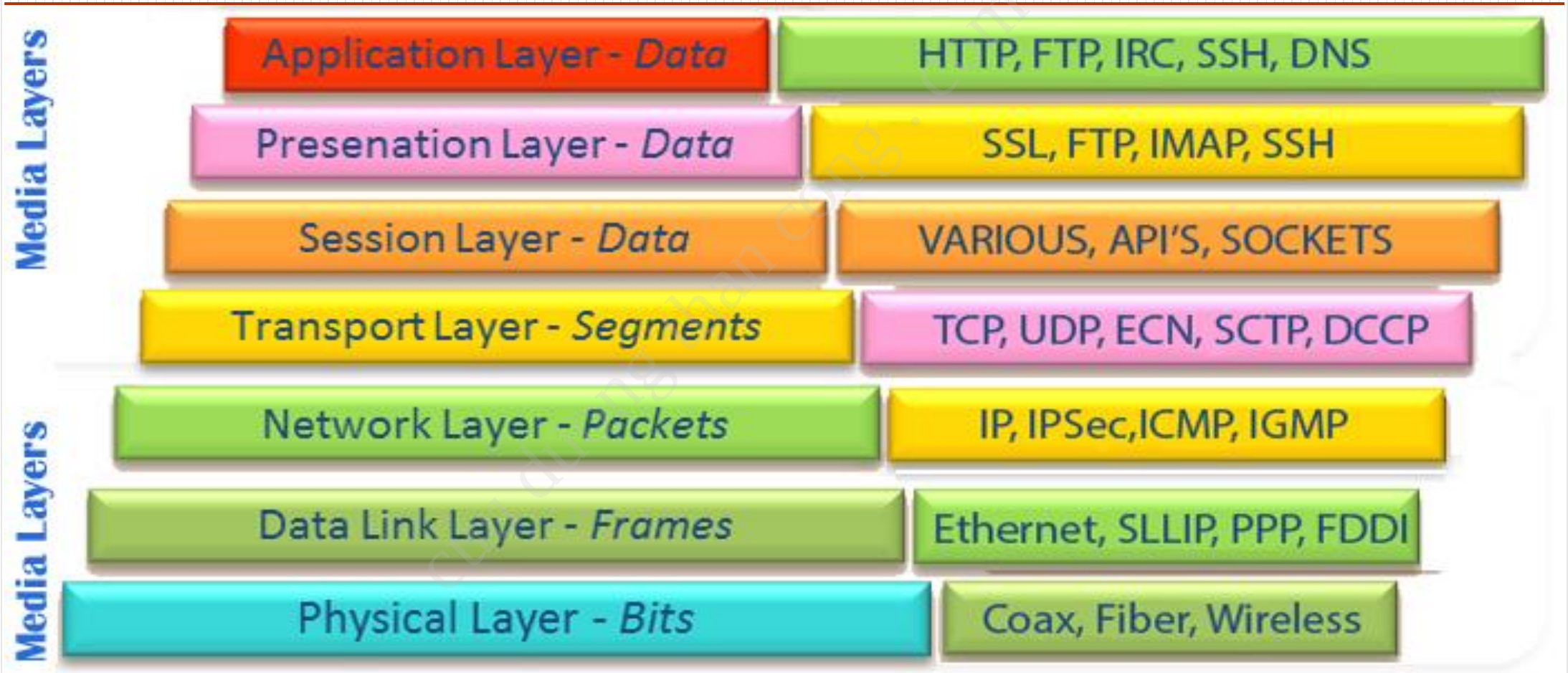
- Network scanning refers to to set of procedures for identifying hosts, ports and services in a network.



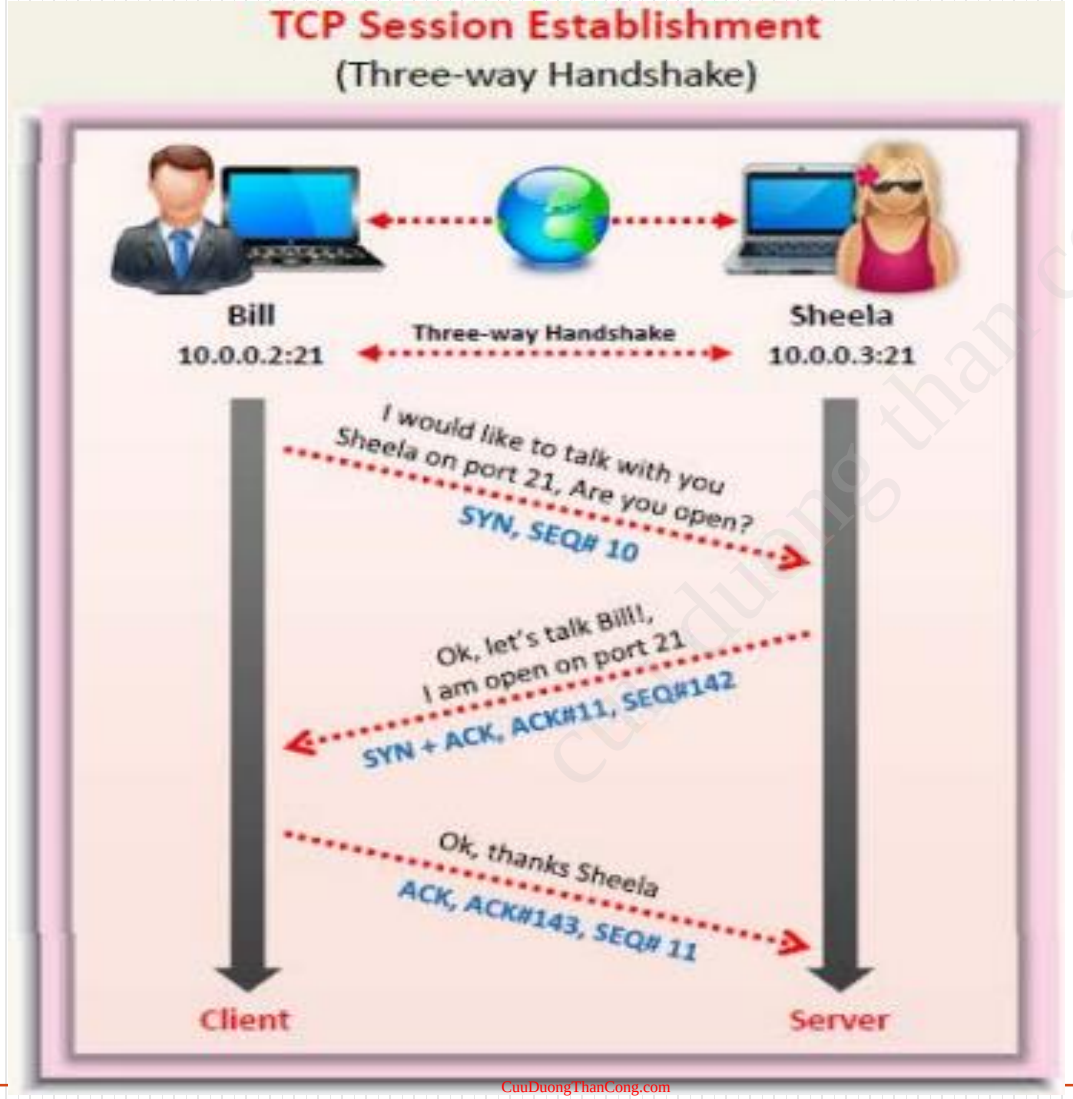
Network Scanning

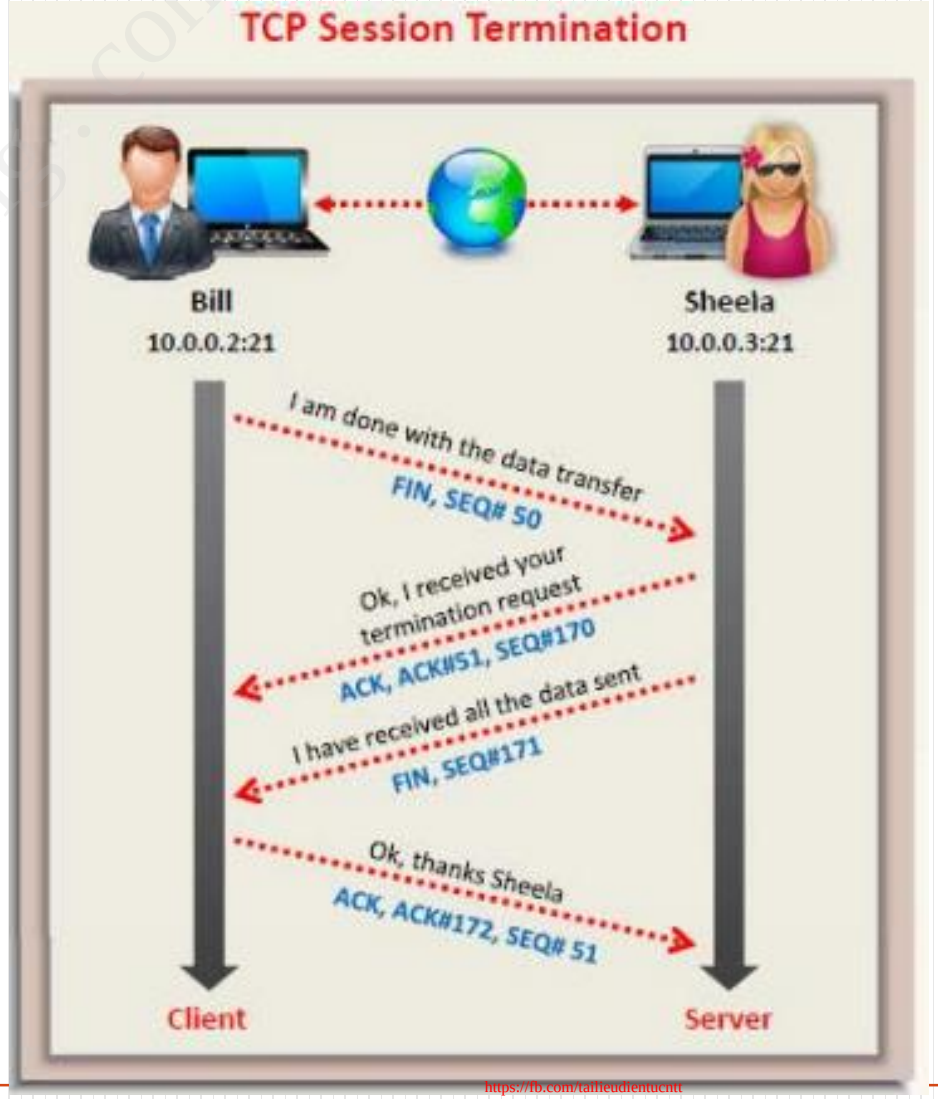
- Objectives of network scanning
  - To discover alive host, IP address and open ports of alive hosts
  - To discover operating systems and system architechture
  - To discover services running on hosts

OSI Layers



TCP Protocol





nmap

nmap -{type(s)} -{opt(s)} {target}

Scan types	Title	Function
`-sA`	ACK scan	Checks if ports are stateful. Useful for testing firewalls.
`-sP`	Ping scan	Used for fast network discovery.
`-sR`	RPC scan	Locates RPC applications. May leave initiate log entries on successfully scanned hosts. This is now an alias to `-sV`.
`-sS`	TCP SYN scan	Very fast and stealthy. Half-open scan.
`-sT`	TCP scan	Makes full connections. Not efficient. Very noisy scan type that will be noticed easily.
`-sU`	UDP scan	Determines if certain UDP ports are open.
`-sX`	XMAS scan	Stealthy scan useful against certain firewall configurations. Looks for RST packets to determine if port is closed. Good for scanning UNIX systems.
`-sL`	List scan	Lists the IP addresses that will be scanned. Use `-n` to ensure no packets are sent on the network.
`-sO`	IP protocol scan	Searches for IP protocols in use on host.

Nmap - types

Scan types	Title	Function
-sM	FIN/ACK	Stealthy scan. Good against UNIX-based systems. Looks for RST packets.
-sI	Idle scan	Zombie Host Scan – very stealthy scan.
-sW	Window scan	Looks at RST packet TCP Window value to determine Open or Closed port.

Nmap - options

-e	Choose Ethernet Interface	Determines which eth to send and receive packets on.
-F	Fast scan	Reduces default scan to 100 ports in the nmap-services file.
-p	Specify port range	Determines which ports are scanned.
-R	Reverse lookup	Forces reverse lookup.
-N	DNS resolution	Performs reverse lookup.
-n	No DNS resolution	Does not do reverse lookup.
-h	Help text	Provides Nmap help text.
-6	IPv6 enable	Scans IPv6.
-A	Aggressive	Initiates many options at once such as version and script scanning. Use with caution.
-T(0-5)	Timing options	Determines how aggressive you want the scan to be.
--scan_delay	Add delay	Adds a delays between probes.
-sV	Service version	Probes for service software versions.

Nmap - options

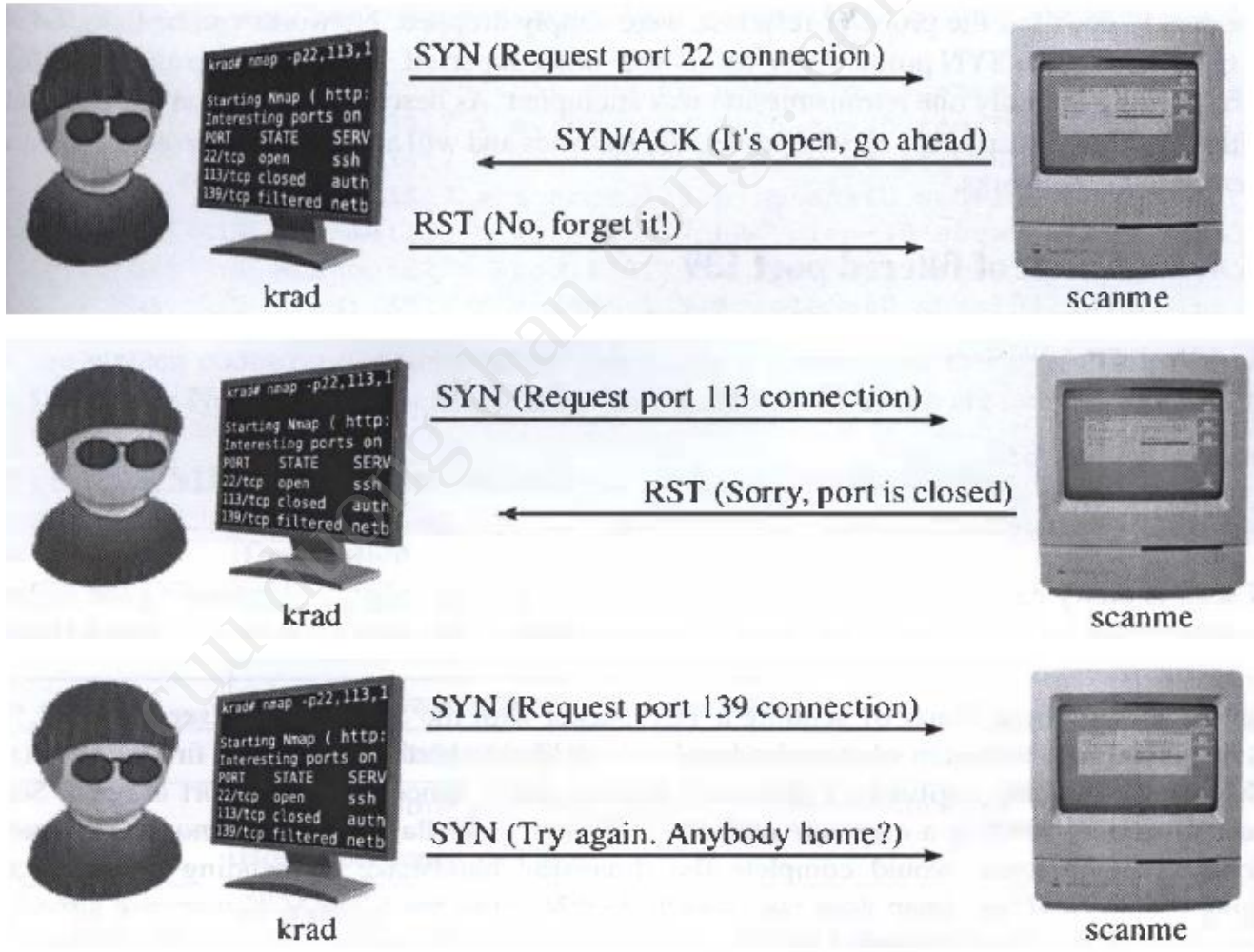
`-g`	Specify source port	Uses a specified source port to send packets.
`--spoof_mac`	Spoof Mac	Creates a fake Mac address to send packets from. Can randomize MAC.
`-S`	Source IP address	Spoofs a source IP address or tells Nmap which IP to use.

nmap:

SYN Scan (-sS): A SYN scan is a TCP scan that does not finish the TCP handshake.

- Nmap sends the SYN and waits for the SYN-ACK if the port is open but never sends the ACK to complete the connection.
- If the SYN packet receives no SYN-ACK response, the port is not available; either it’s closed or the connection is being filtered.

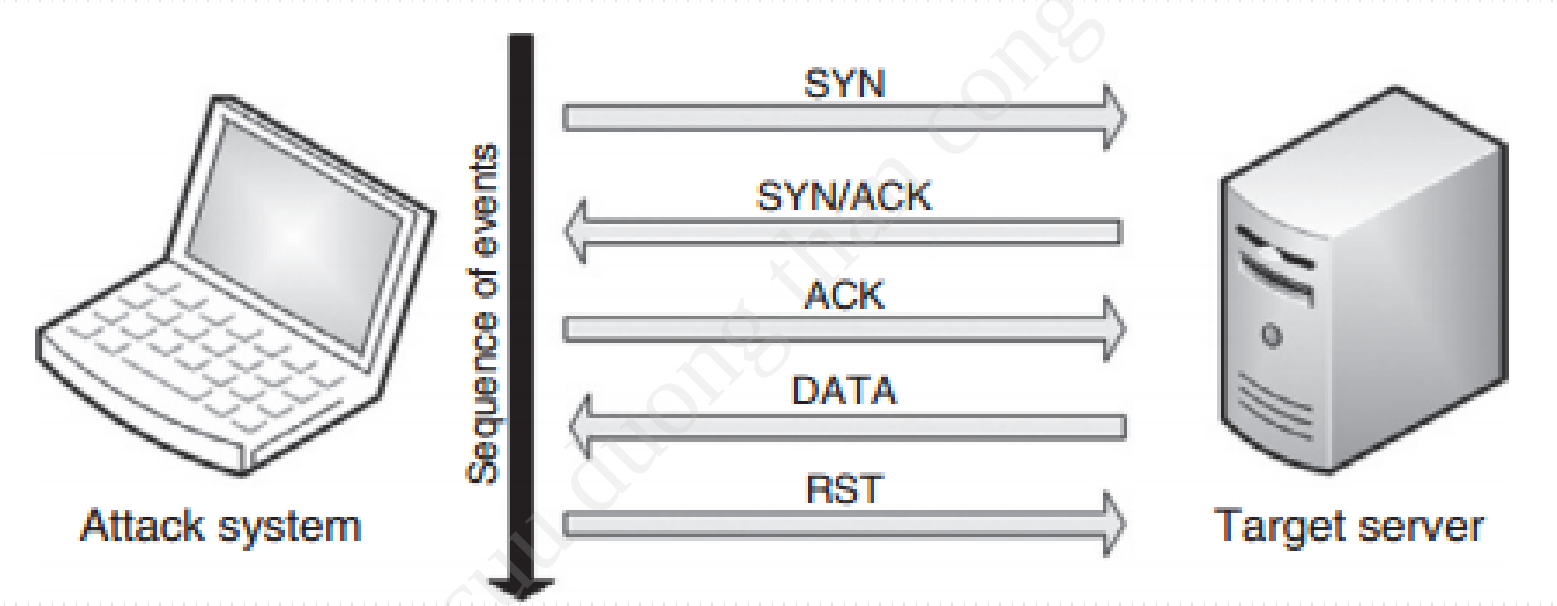
nmap - TCP Syn Scan (-sS)



```
root@kali:~# nmap -sS 192.168.20.10-12 -oA booknmap
Starting Nmap 6.40 ( http://nmap.org ) at 2015-12-18 07:28 EST
Nmap scan report for 192.168.20.10
Host is up (0.00056s latency).
Not shown: 991 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp ❷
25/tcp   open  smtp ❺
80/tcp   open  http ❸
106/tcp  open  pop3pw ❺
110/tcp  open  pop3 ❺
135/tcp  open  msrpc
139/tcp  open  netbios-ssn ❹
443/tcp  open  https ❸
445/tcp  open  microsoft-ds ❹
1025/tcp open  NFS-or-IIS
3306/tcp open  mysql ❻
5000/tcp open  upnp
MAC Address: 00:0C:29:A5:C1:24 (VMware)
```

Nmap - TCP Connect Scan (-sT):

- Make full connections



Nmap – UDP Scan (-sU)

- Nmap sends a UDP packet to a port. Depending on the port, the packet sent is protocol specific.
- If it receives a response, the port is considered open.
- If the port is closed, Nmap will receive an ICMP Port Unreachable message.
- If Nmap receives no response whatsoever, then either the port is open and the program listening does not respond to Nmap's query, or the traffic is being filtered

```
root@kali:~# nmap -sU 192.168.20.10-12 -oA bookudp

Starting Nmap 6.40 ( http://nmap.org ) at 2015-12-18 08:39 EST
Stats: 0:11:43 elapsed; 0 hosts completed (3 up), 3 undergoing UDP Scan
UDP Scan Timing: About 89.42% done; ETC: 08:52 (0:01:23 remaining)
Nmap scan report for 192.168.20.10
Host is up (0.00027s latency).
Not shown: 990 closed ports
PORT     STATE         SERVICE
69/udp   open|filtered tftp ❶
123/udp  open          ntp
135/udp  open          msrpc
137/udp  open          netbios-ns
138/udp  open|filtered netbios-dgm
445/udp  open|filtered microsoft-ds
500/udp  open|filtered isakmp
1026/udp open          win-rpc
1065/udp open|filtered syscomlan
1900/udp open|filtered upnp
MAC Address: 00:0C:29:A5:C1:24 (VMware)
```

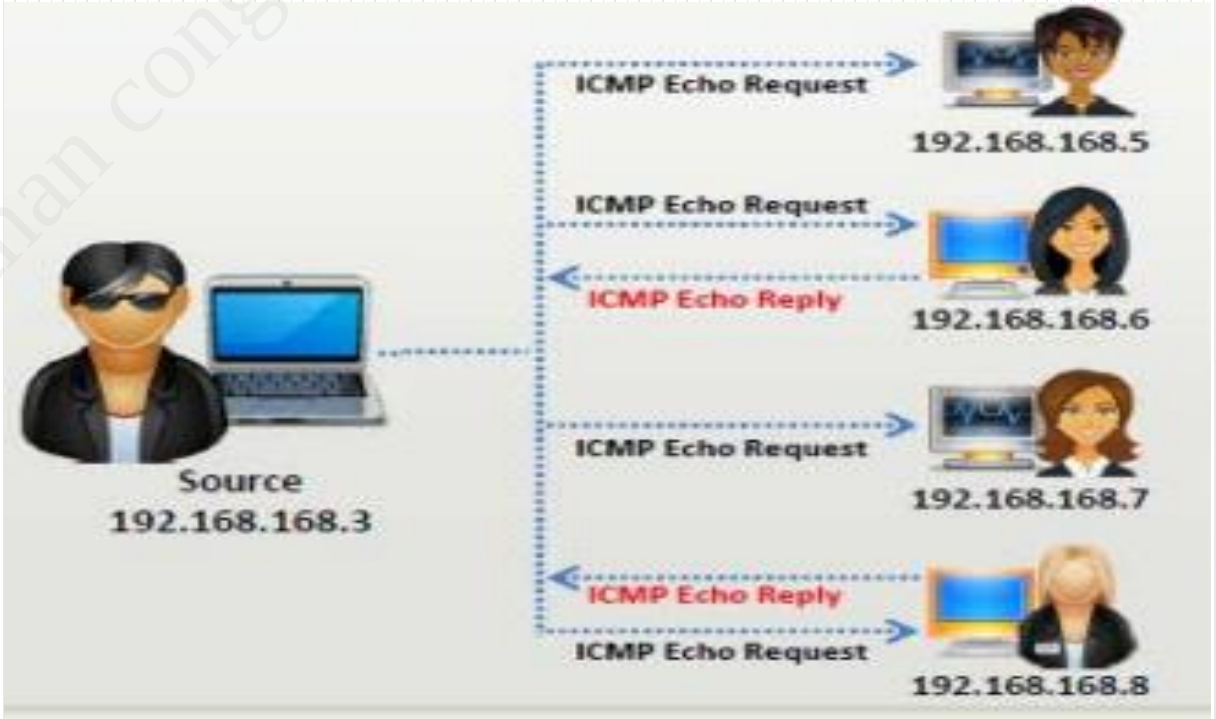
```
root@kali:~# nmap -sV -O 192.168.206.135

Starting Nmap 7.60 ( https://nmap.org ) at 2018-01-09 04:18 EST
Nmap scan report for 192.168.206.135
Host is up (0.00071s latency).
Not shown: 996 closed ports
PORT    STATE SERVICE      VERSION
25/tcp  open  smtp         SLmail smtpd 5.5.0.4433
135/tcp open  msrpc        Microsoft Windows RPC
139/tcp open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp open  microsoft-ds Microsoft Windows XP microsoft-ds
MAC Address: 00:0C:29:00:3A:77 (VMware)
Device type: general purpose
Running: Microsoft Windows XP
OS CPE: cpe:/o:microsoft:windows_xp::sp2 cpe:/o:microsoft:windows_xp::sp3
OS details: Microsoft Windows XP SP2 or SP3
Network Distance: 1 hop
Service Info: Host: georgia-8bb43d5; OSs: Windows, Windows XP; CPE: cpe:/o:micro
soft:windows, cpe:/o:microsoft:windows_xp

OS and Service detection performed. Please report any incorrect results at https
://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 14.61 seconds
```

Check for live systems

ICMP Scanning

- #nmap –sn 192.168.153.0/24
- #nmap –sn 192.168.153.2
- Options:

  -sn: Ping scan



Ping Sweep Tools

Check for open ports

- Netcat

```
root@kali:~# nc -vv 192.168.20.10 25
nc: 192.168.20.10 (192.168.20.10) 25 [smtp]❶ open
nc: using stream socket
nc: using buffer size 8192
nc: read 66 bytes from remote
220 bookxp SMTP Server SLmail 5.5.0.4433 Ready
ESMTP spoken here
nc: wrote 66 bytes to local
```

- Nmap

Nmap

nmap -sS 192.168.20.10-12

nmap -sS 192.168.20.10-12 -oA booknmap

Nmap

```
root@kali:~# nmap -sV 192.168.20.10-12 -oA bookversionnmap

Starting Nmap 6.40 ( http://nmap.org ) at 2015-12-18 08:29 EST
Nmap scan report for 192.168.20.10
Host is up (0.00046s latency).
Not shown: 991 closed ports
PORT     STATE SERVICE      VERSION
21/tcp   open  ftp          FileZilla ftpd 0.9.32 beta
25/tcp   open  smtp         SLmail smtpd 5.5.0.4433
79/tcp   open  finger       SLMail fingerd
80/tcp   open  http         Apache httpd 2.2.12 ((Win32) DAV/2 mod_ssl/2.2.12 OpenSSL/0.9.8k
                              mod_autoindex_color PHP/5.3.0 mod_perl/2.0.4 Perl/v5.10.0)
106/tcp  open  pop3pw       SLMail pop3pw
110/tcp  open  pop3         BVRP Software SLMAIL pop3d
135/tcp  open  msrpc        Microsoft Windows RPC
139/tcp  open  netbios-ssn
```

Nmap - UDP Scans

- In a UDP scan (-sU), Nmap sends a UDP packet to a port. Depending on the port, the packet sent is protocol specific.
- If it receives a response, the port is considered open.
- If the port is closed, Nmap will receive an ICMP Port Unreachable message.
- If Nmap receives no response whatsoever, then either the port is open and the program listening does not respond to Nmap’s query, or the traffic is being filtered.

nmap

#nmap -sS -sV 192.168.20.11

-sV: Probe open ports to determine service/version infoom

```
Nmap scan report for 192.168.20.11
Host is up (0.00065s latency).
Not shown: 993 closed ports
PORT     STATE SERVICE              VERSION
21/tcp   open  ftp                  vsftpd 2.3.4 ❶
22/tcp   open  ssh                  OpenSSH 5.1p1 Debian 3ubuntu1 (protocol 2.0)
80/tcp   open  http                 Apache httpd 2.2.9 ((Ubuntu) PHP/5.2.6-2ubuntu4.6 with
                                      Suhosin-Patch)
111/tcp  open  rpcbind (rpcbind V2) 2 (rpc #100000)
139/tcp  open  netbios-ssn          Samba smbd 3.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn          Samba smbd 3.X (workgroup: WORKGROUP)
2049/tcp open  nfs (nfs V2-4)       2-4 (rpc #100003)
MAC Address: 00:0C:29:FD:0E:40 (VMware)
```

Nmap –UDP scan

- nmap -sU 192.168.20.10-12
- nmap -sS -p 3232 192.168.20.10

Website Information gathering