Network Attack & Solution

ดร. ธนัญชัย ตรีภาค

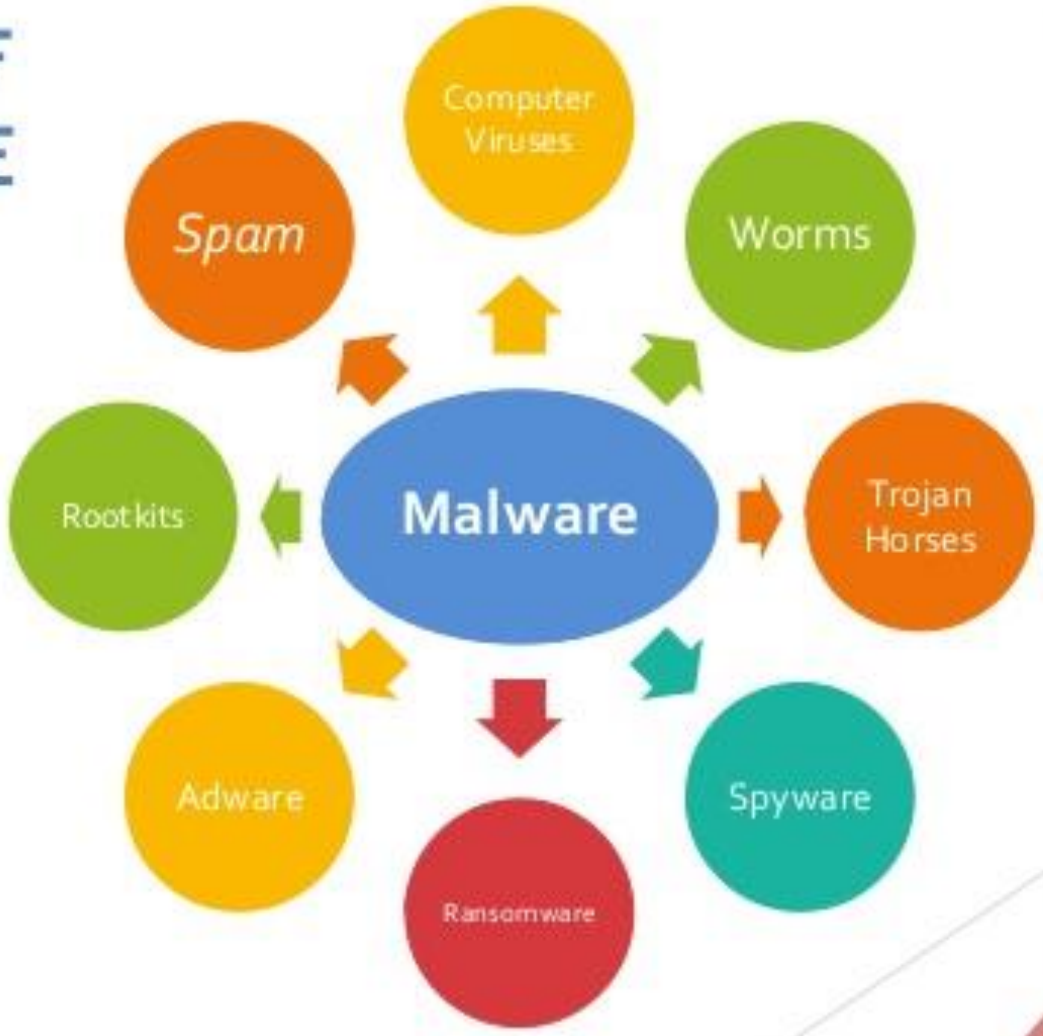
คำศัพท์สำคัญ

- ภัยคุกคาม (Threats)
- ช่องโหว่ (Vulnerability)
- การอาศัยช่องโหว่เพื่อโจมตีระบบ (Exploit)

Q : ภัยคุกคามทาง Network ที่นักศึกษารู้จักมีอะไรบ้าง แต่ละอันทำงานอย่างไร

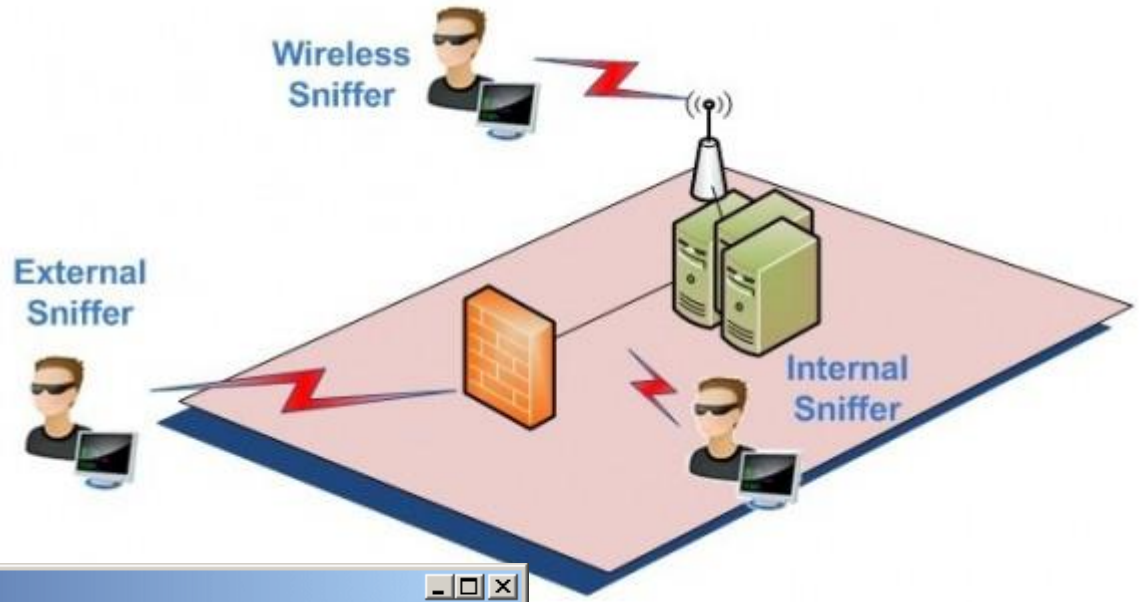
แต่ละกลุ่มทำ MindMap ของภัยคุกคามที่รู้จัก

TYPES OF MALWARE



Q : จะป้องกัน / แก้ไข Malware ได้อย่างไร

Sniffer



SmartSniff

File Edit View Options Help

I...	Protocol	Local Address	Remote Address	Local Port	Remot...	Service Name	Packets	Data Size
24	TCP	192.168.0.5	66.218.71.233	1084	80	http	44	36,592 Byte
25	TCP	192.168.0.5	212.199.29.6	1085	80	http	26	11,532 Byte
26	TCP	192.168.0.5	212.199.29.13	1086	80	http	4	1,221 Bytes
27	TCP	192.168.0.5	212.199.29.6	1087	80	http	10	7,257 Bytes
28	TCP	192.168.0.5	216.136.131.30	1088	80	http	6	826 Bytes

```
GET /pa?q=nirsoft&s=2766679 HTTP/1.1
Accept: */*
Referer: http://search.yahoo.com/search?p=nirsoft&ei=UTF-8&fr=fp-tab-web-t&cop=
Accept-Language: en-us
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Host: pa.yahoo.com
Connection: Keep-Alive


HTTP/1.0 200 OK
Date: Wed, 30 Jun 2004 08:37:19 GMT
P3P: policyref="http://p3p.yahoo.com/w3c/p3p.xml", CP="CAO DSP COR CUR ADM DEV
```

28 TCP/IP conversations, 1 Selected

Q : จะป้องกัน / แก้ไข การดักจับข้อมูลต่างๆ ได้อย่างไร

Global Attack Map

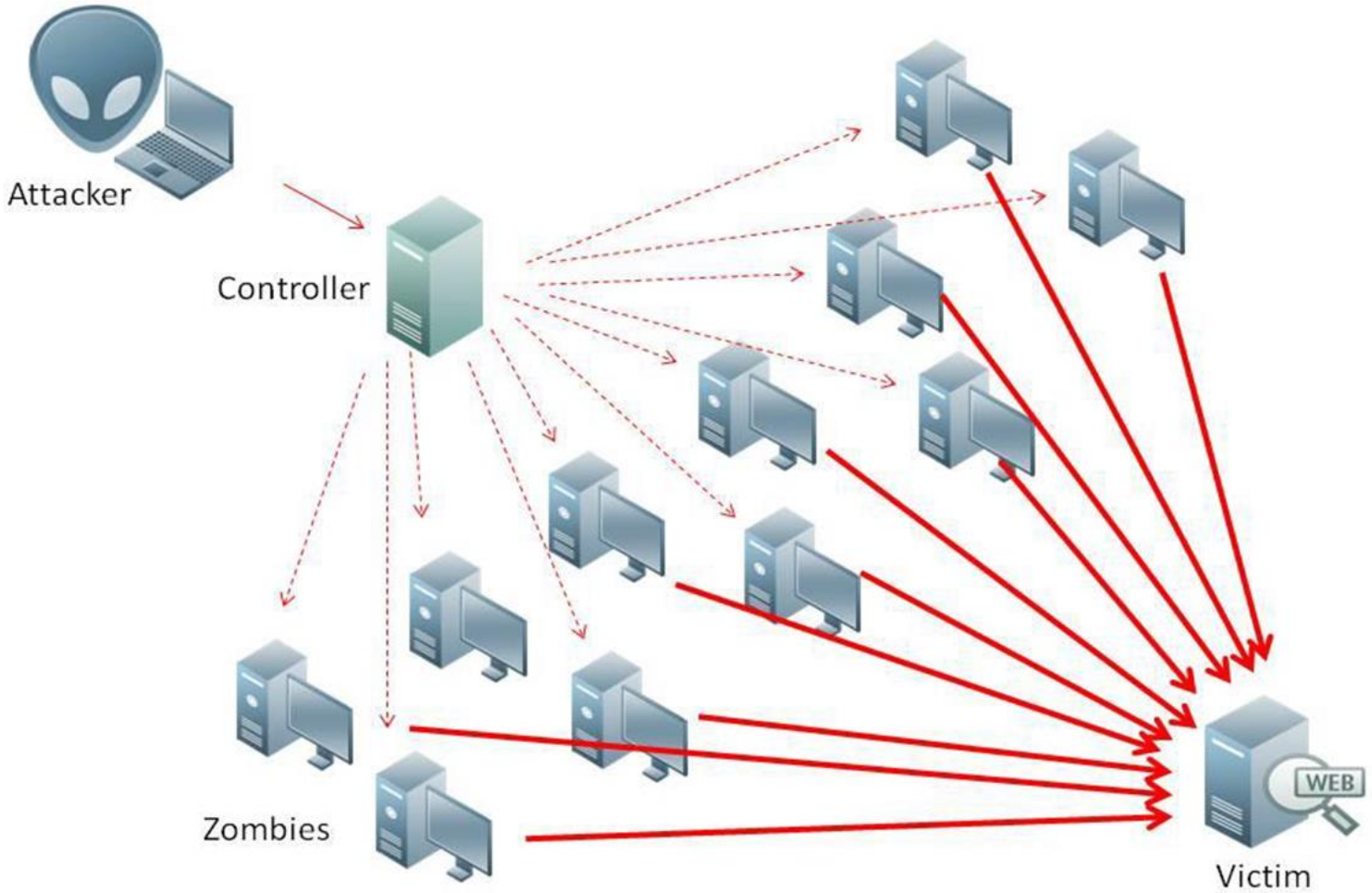
http://map.norsecorp.com/

DoS

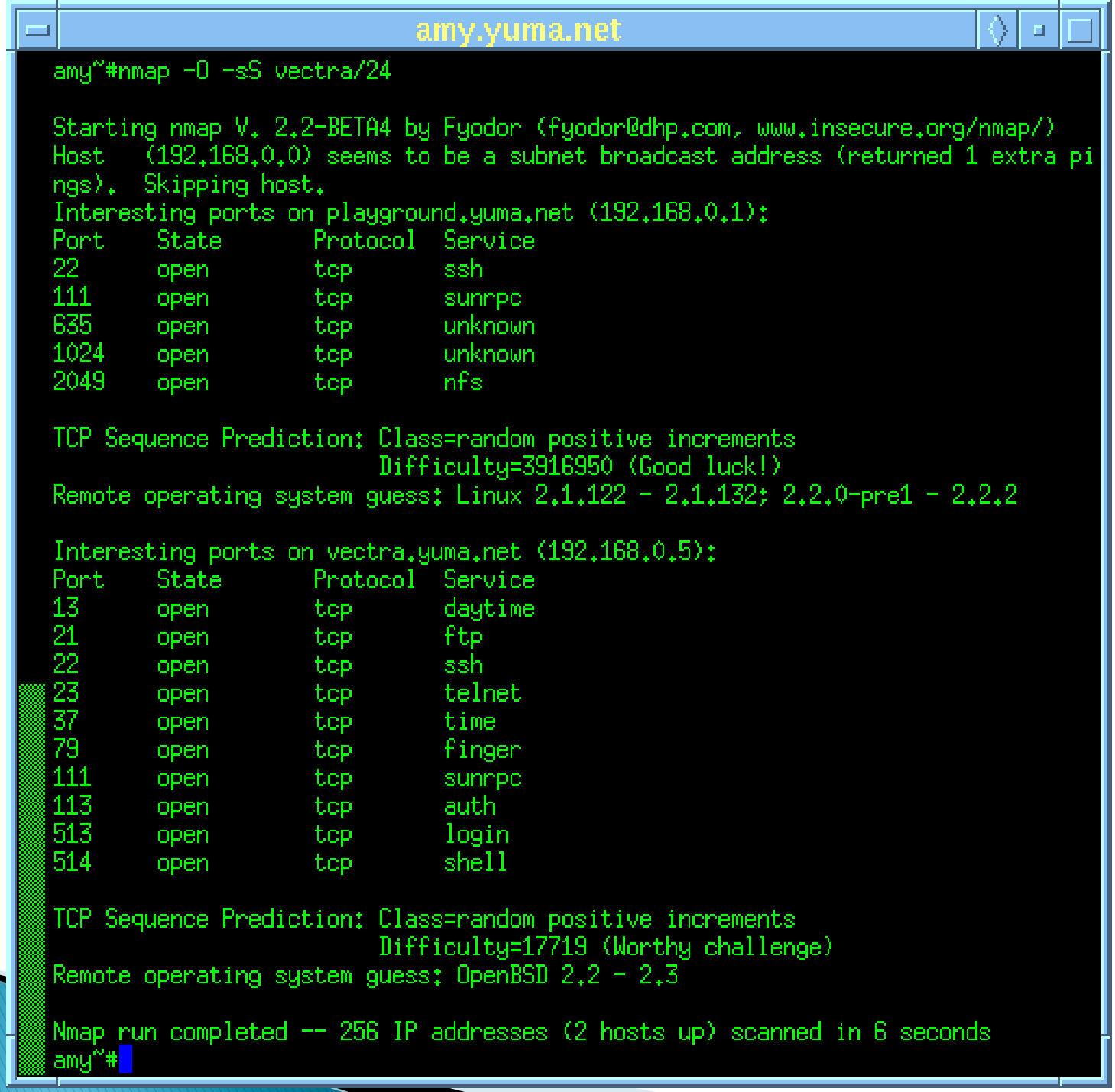
- SYN Flood
- Land Attack
- Smurf Attack
- Ping of Death
- Ping flood
- Teardrop Attack
- Fraggle

DDoS

- Trinoo
- TFN
- TFN2K

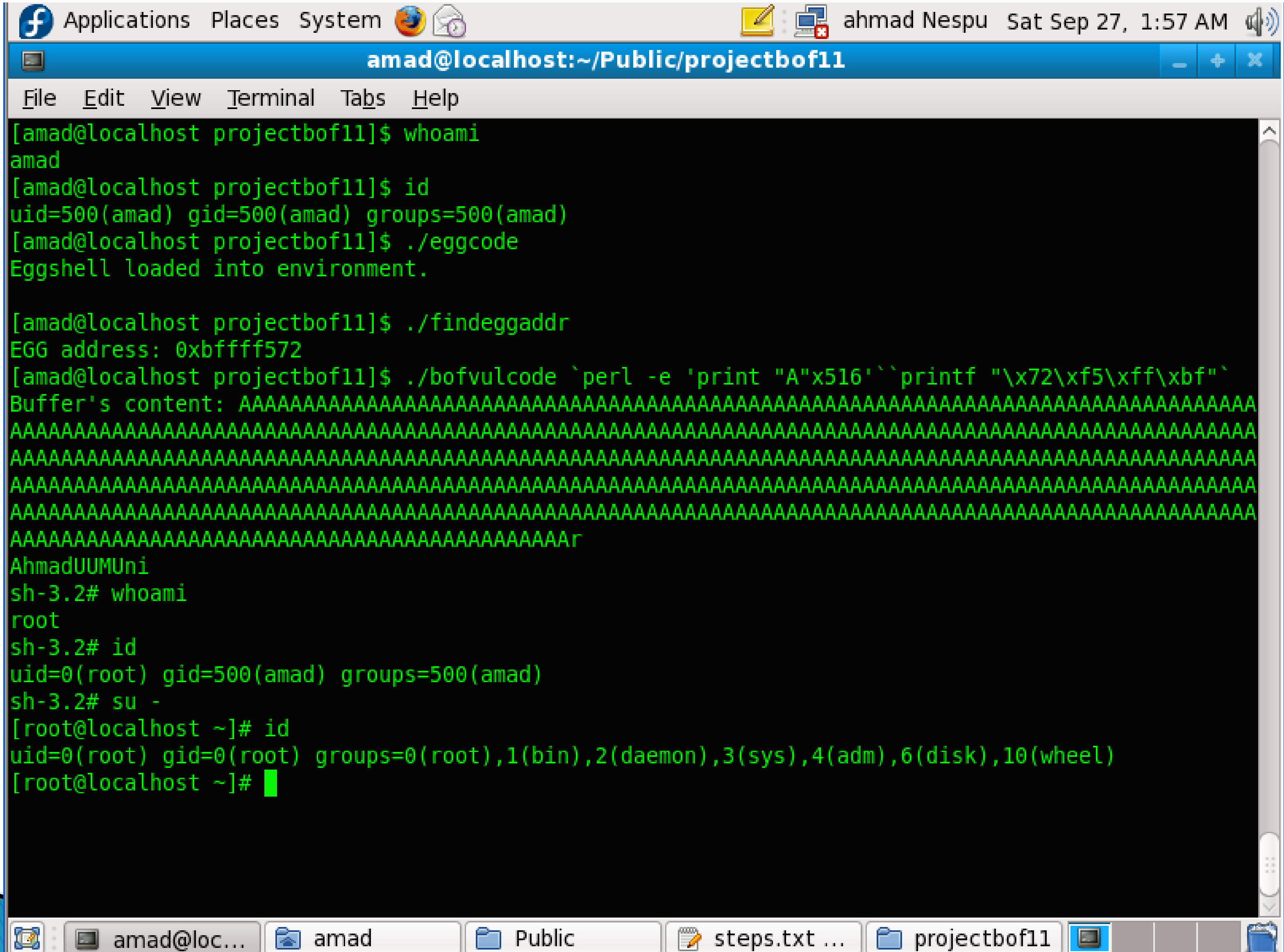


Q : จะป้องกัน / แก้ไข DoS ได้อย่างไร


amy.yuma.net
amy~#nmap -O -sS vectra/24
Starting nmap V. 2.2-BETA4 by Fyodor (fyodor@dhp.com, www.insecure.org/nmap/)
Host (192.168.0.0) seems to be a subnet broadcast address (returned 1 extra pi
ngs). Skipping host.
Interesting ports on playground.yuma.net (192.168.0.1):
Port State Protocol Service
22 open tcp ssh
111 open tcp sunrpc
635 open tcp unknown
1024 open tcp unknown
2049 open tcp nfs
TCP Sequence Prediction: Class=random positive increments
Difficulty=3916950 (Good luck!)
Remote operating system guess: Linux 2.1.122 - 2.1.132; 2.2.0-pre1 - 2.2.2
Interesting ports on vectra.yuma.net (192.168.0.5):
Port State Protocol Service
13 open tcp daytime
21 open tcp ftp
22 open tcp ssh
23 open tcp telnet
37 open tcp time
79 open tcp finger
111 open tcp sunrpc
113 open tcp auth
513 open tcp login
514 open tcp shell
TCP Sequence Prediction: Class=random positive increments
Difficulty=17719 (Worthy challenge)
Remote operating system guess: OpenBSD 2.2 - 2.3
Nmap run completed -- 256 IP addresses (2 hosts up) scanned in 6 seconds
amy~#

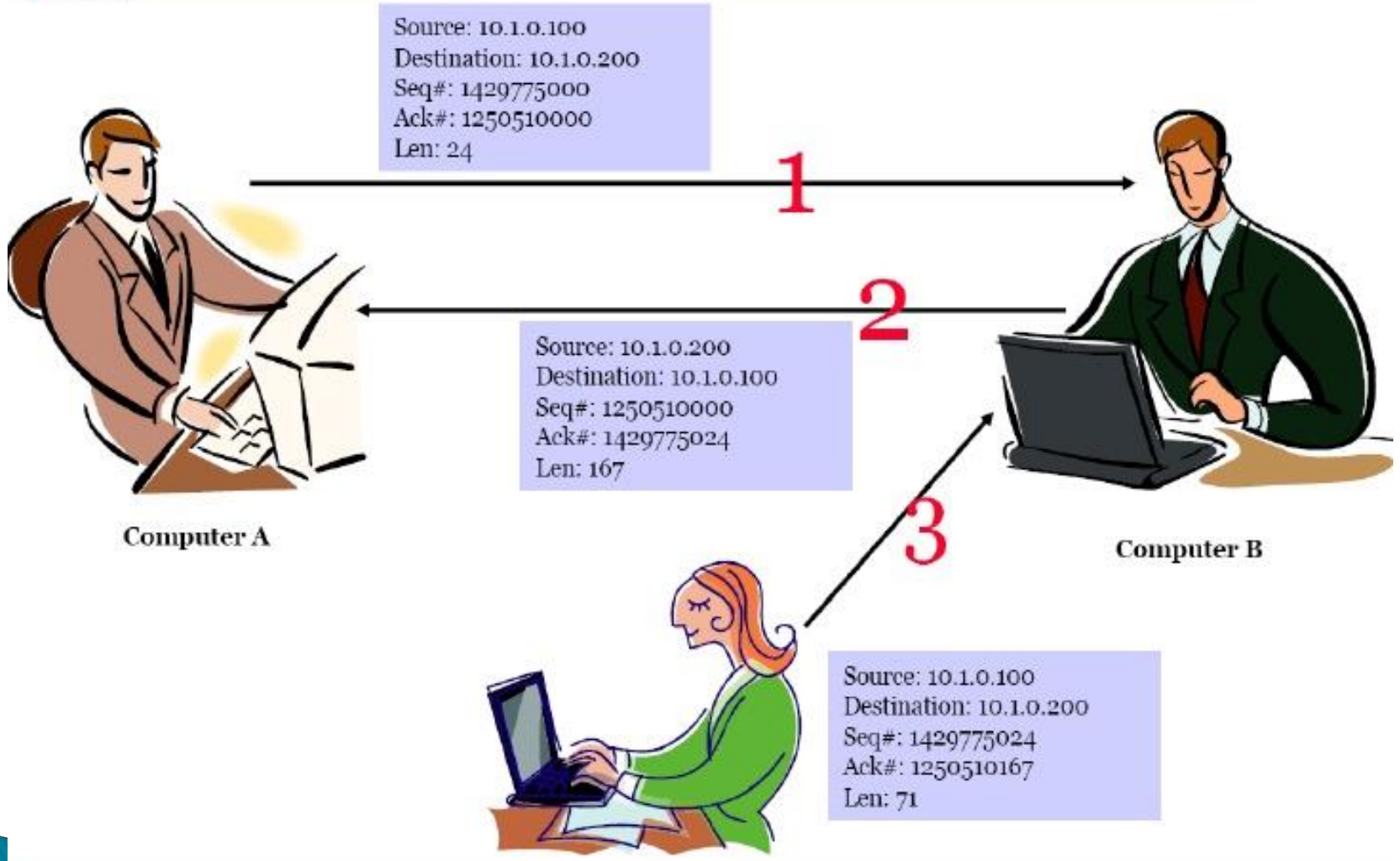
Scan Type	Syntax	Example
TCP SYN Scan	-sS	nmap –sS 10.20.3.100
TCP Connect Scan	-sT	nmap –sT 10.20.3.100
Fin Scan	-sF	nmap –sF 10.20.3.100
XMAS Scan	-sX	nmap –sX 10.20.3.100
Null Scan	-sN	nmap –sN 10.20.3.100
Ping Scan	-sP	nmap –sP 10.20.3.100
Version Detection	-sV	nmap –sV 10.20.3.100
UDP Scan	-sU	nmap –sU 10.20.3.100
IP Protocol Scan	-sO	nmap –sO 10.20.3.100
ACK Scan	-sA	nmap –sA 10.20.3.100
Windows Scan	-sW	nmap –sW 10.20.3.100
List Scan	-sL	nmap –sL 10.20.3.100

Q : จะป้องกัน / แก้ไข การ Scan ต่างๆ ได้อย่างไร

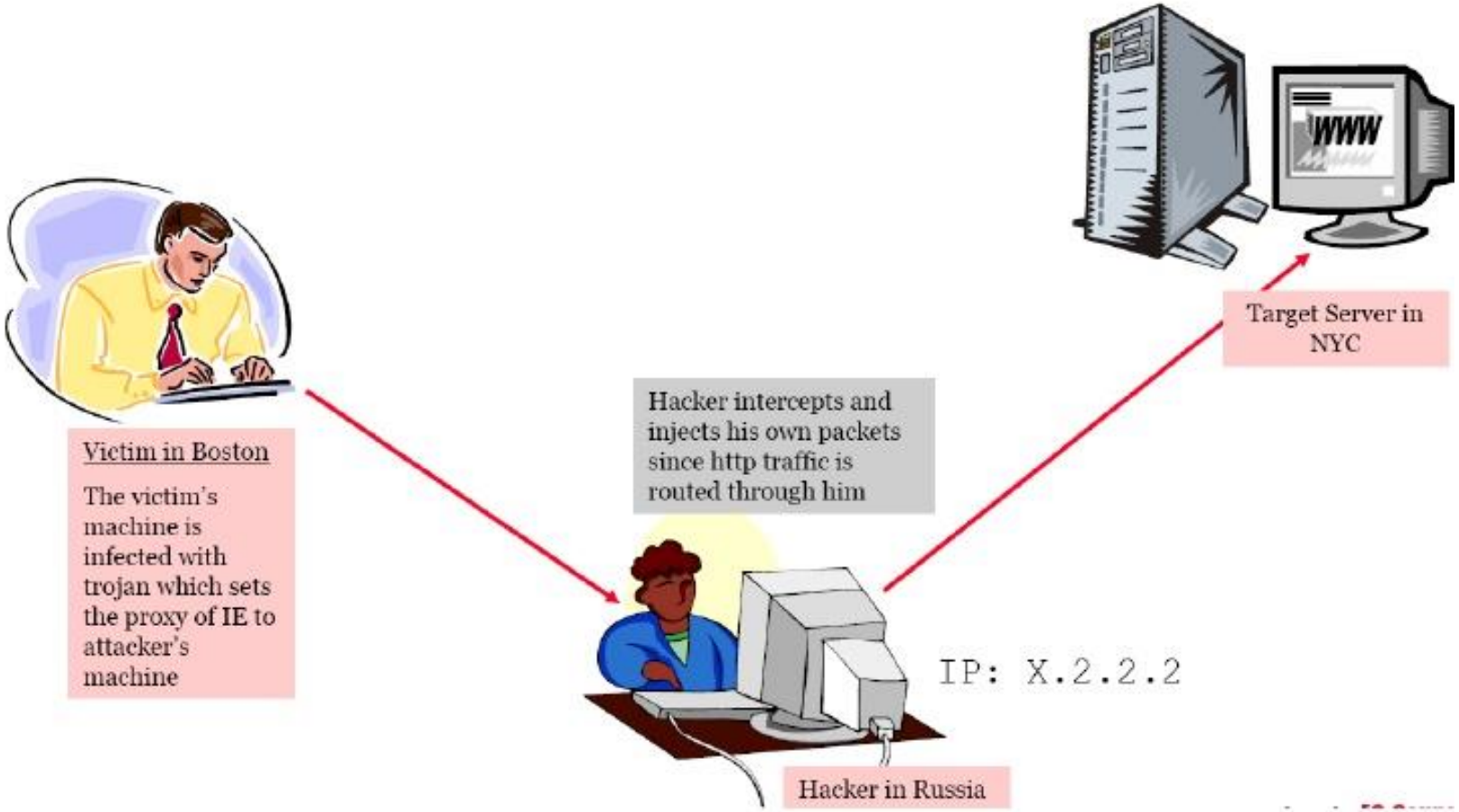

Applications Places System
ahmad Nespu Sat Sep 27, 1:57 AM
amad@localhost:~/Public/projectbof11
File Edit View Terminal Tabs Help
[amad@localhost projectbof11]$ whoami
amad
[amad@localhost projectbof11]$ id
uid=500(amad) gid=500(amad) groups=500(amad)
[amad@localhost projectbof11]$ ./eggcode
Eggshell loaded into environment.
[amad@localhost projectbof11]$ ./findeggaddr
EGG address: 0xbffff572
[amad@localhost projectbof11]$ ./bofvulcode `perl -e 'print "A"x516'``printf "\x72\xf5\xff\xbf"`
Buffer's content: AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAr
AhmadUUMUni
sh-3.2# whoami
root
sh-3.2# id
uid=0(root) gid=500(amad) groups=500(amad)
sh-3.2# su -
[root@localhost ~]# id
uid=0(root) gid=0(root) groups=0(root),1(bin),2(daemon),3(sys),4(adm),6(disk),10(wheel)
[root@localhost ~]#
amad@loc... amad Public steps.txt ... projectbof11

Q : จะป้องกัน / แก้ไข การ Exploit ต่างๆ ได้อย่างไร

TCP/IP Hijacking

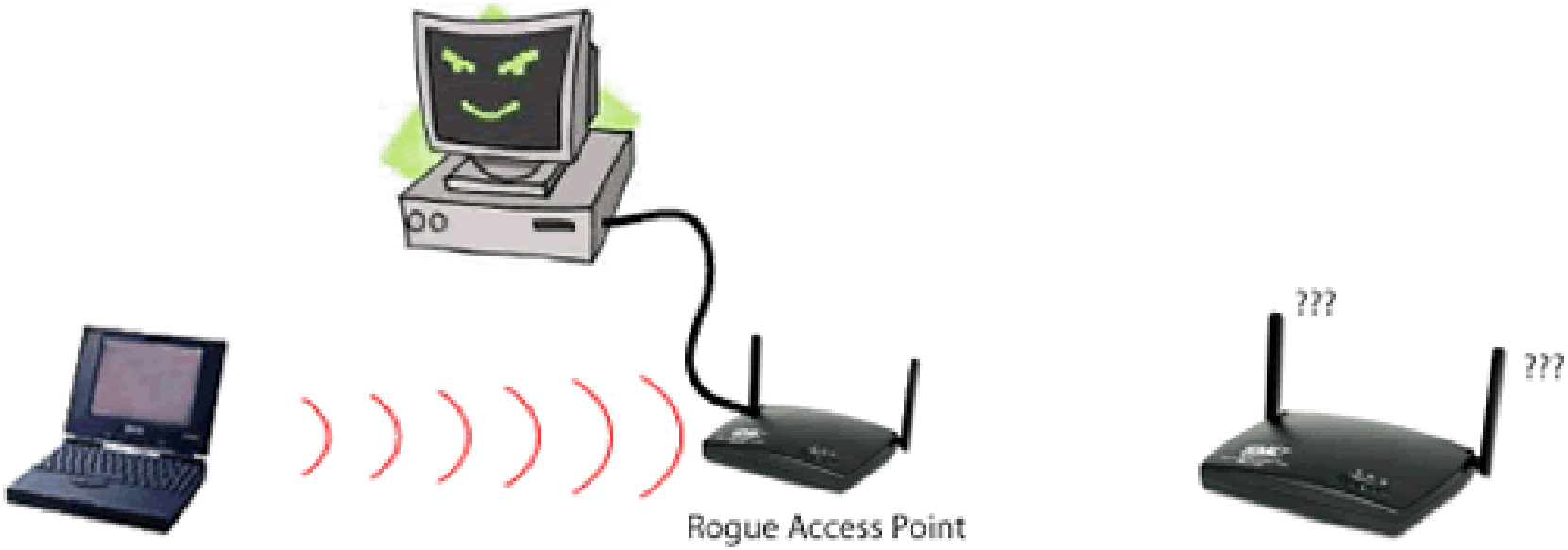


Paros HTTP Session Hijacking Tool



Q : จะป้องกัน / แก้ไข Session Hijack ได้อย่างไร

Rogue Access Point



Q : จะป้องกัน / แก้ไข Rogue Access Point ได้อย่างไร

Activity : ให้นักศึกษาเพิ่มการป้องกัน / แก้ไข การโจมตีต่างๆ ใน MindMap

Q : จากกรณีศึกษาตัวอย่าง นักศึกษามีแนวทางศึกษา และหาวิธีรับมือกับภัยคุกคามสารสนเทศต่างๆ อย่างไร

สรุป / สิ่งที่ได้เรียนรู้