

X-Attack 網路攻擊訊務的監測

國立中央大學 電算中心

楊素秋

Mar-26, 2003

大綱

- 1. 前言
- 2. 網路轉送訊務紀錄的擷取
- 3. 網路攻擊模式
- 4. 攻擊訊務的監測
- 5. 結語

1. 前言

- 網路快速擴展
 - 多元的網路應用
 - 網路攻擊訊務的大量感染與癱瘓網路服務
- 協助網路管理者
 - 了解網路訊務量測工具
 - 了解基本的X-Attack網路攻擊模式
 - 監測所管理互連網路的攻擊訊務

2. 網路轉送訊務紀錄的擷取

- Tcpdump
 - 典型的LAN區域網路封包監聽程式
 - Layer 2 MAC addresses,
 - Layer 3 IP addresses,
 - layer 4 application ports (TCP operand)
 - Packet payload
 - Tcpdump & Tcpshow

轉送訊務紀錄的擷取(cont)

– 網路用戶

- 藉由Tcpdump監聽log, 確認主機或應用程式傳訊功能.
- 篩選/追蹤特定轉送log
 - host IP
 - network
 - protocol
 - 應用port

轉送訊務紀錄的擷取(cont)

– 網管人員

- 透過TCPdump監聽廣播網段的end-to-end封包轉送紀錄,
- 依據各紀錄項, 統計與分析確切的連網運務量
 - IP address & packet length
 - » Monitoring Top-10 users
 - TCP/UDP socket ports & packet length
 - » Prevalent Application Traffic Composition

轉送訊務紀錄的擷取(cont)

- NetFlow
 - Router座於 WAN網路的閘門位置, 負責轉送匯集於此的所有 Internet封包, 暫存/加總每一過境封包的header資訊.
 - source IP. source port & destination IP. destination port
 - source & destination routing interface
 - protocol identifier, packet count, byte count

轉送訊務紀錄的擷取(cont)

- Flow-based的 Netflow 能支援
 - light-weight訊務統計與多樣的訊務特徵追蹤
- 利用國外傳訊router訊務轉送log
 - 追蹤攻擊訊務與Streaming media訊務傳訊特質
 - 統計與實作UDP應用訊務監測網頁.

3. 網路攻擊模式

- 基本的網路偵錯工具
- Typical Attack Program
- DOS網路供攻擊
 - DDOS
 - DRDOS
- Network Worm
 - W32. CodeRed. Worm, W32. Nimda. Worm
 - FreeBSD. Scalper. Worm, Linux. Slapper. Worm

基本的網路偵錯工具

– Ping

- ICMP echo request/reply
- ping packet size option
- Loop ping

– Echoping

- Loop ping option
- ping packet size option
- chargen, discard option
- HTTP, SMTP option

```
cyang# echoping -n 3 -h / www.nchu.edu.tw
```

```
Elapsed time: 0.061612 seconds
```

```
Elapsed time: 0.069475 seconds
```

```
Elapsed time: 0.060976 seconds
```

```
---
```

```
Minimum time: 0.060976 seconds (4198 bytes per sec.)
```

```
Maximum time: 0.069475 seconds (3685 bytes per sec.)
```

```
Average time: 0.064021 seconds (3999 bytes per sec.)
```

```
Standard deviation: 0.003785
```

```
Median time: 0.061612 seconds (4155 bytes per sec.)
```

```
cyang# echoping -n 3 -h http://www.nchu.edu.tw proxy.ncu.edu.tw:3128
```

```
Elapsed time: 0.120405 seconds
```

```
Elapsed time: 0.068761 seconds
```

```
Elapsed time: 0.058727 seconds
```

```
---
```

```
Minimum time: 0.058727 seconds (4359 bytes per sec.)
```

```
Maximum time: 0.120405 seconds (2126 bytes per sec.)
```

```
cyang# echoping -n 3 -u -v -P 0x19 cc.ncu.edu.tw
```

```
Setting IP type of service octet to 25 (0x19)
```

```
Trying to send 256 bytes to internet address 140.115.17.111...
```

```
Sent (256 bytes)...
```

```
Timeout
```

```
256 bytes read from server.
```

```
Setting IP type of service octet to 25 (0x19)
```

```
Trying to send 256 bytes to internet address 140.115.17.111...
```

```
Sent (256 bytes)...
```

```
Timeout
```

```
256 bytes read from server.
```

```
Setting IP type of service octet to 25 (0x19)
```

```
Trying to send 256 bytes to internet address 140.115.17.111...
```

```
Sent (256 bytes)...
```

```
readline error: -1 bytes read, 256 bytes requested (Connection refused)
```

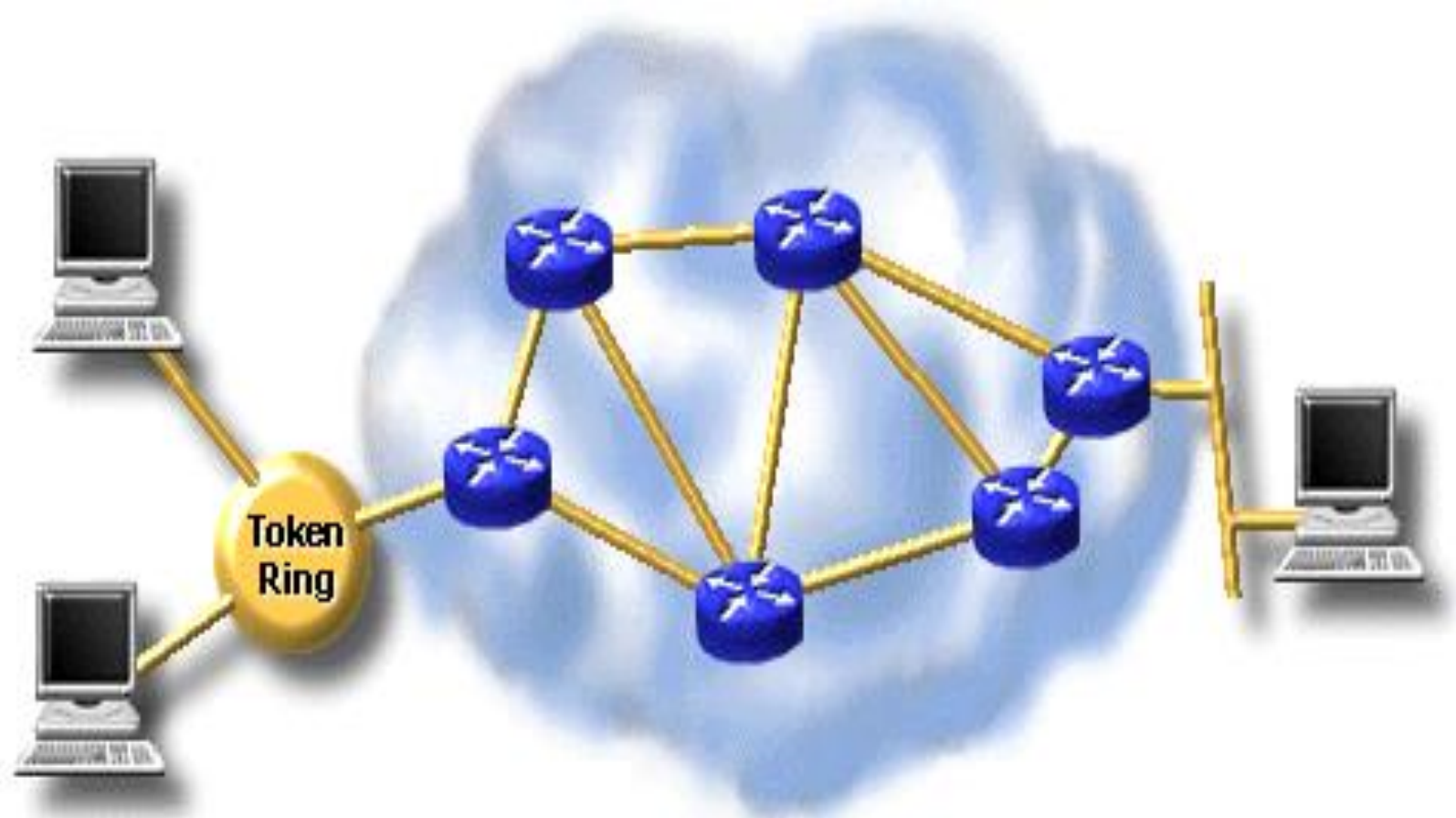
```
cyang#
```

Typical Attack Program

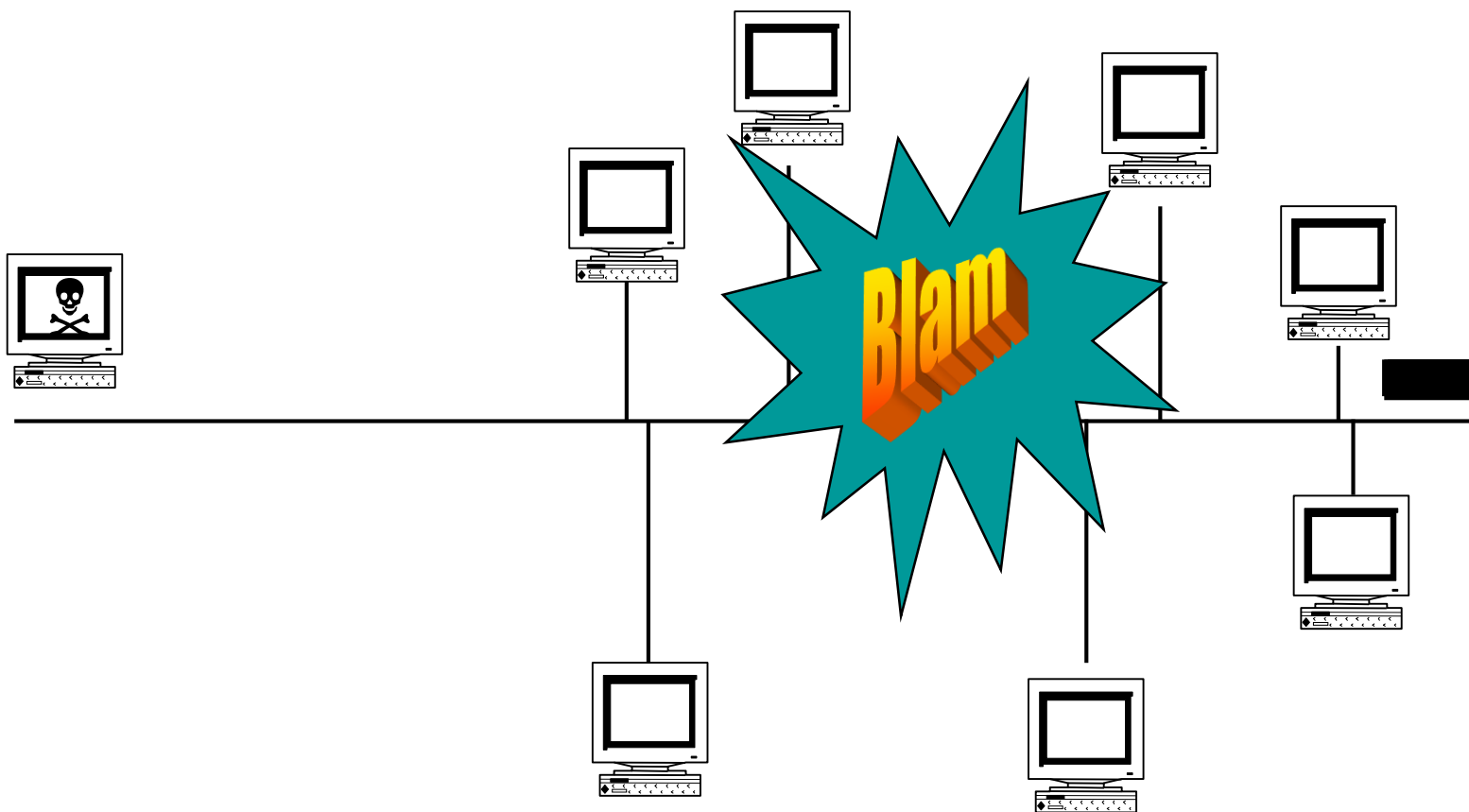
- Nestea
 - Stupid remote DOS attack
 - April 1998
 - Send massive UDP attack packets to the target victim
 - The loop usleep parameter
 - Send attack packets with hundreds of spoofed IP source addresses
- *Nestea 10. 1. 1. 1 153. 35. 85. 1 153. 35. 85. 254 -s 4444 -t 5555 -n 500*

DOS網路攻擊

- DOS (Denial Of Service) Attack
 - Consume the resources of a **remote host or networks**
 - Degrading services to legitimate users
 - Introduce hardest security problem
 - Simple to implement
 - Hard to prevent
 - Snoofed IP addresses
 - Difficult to trace



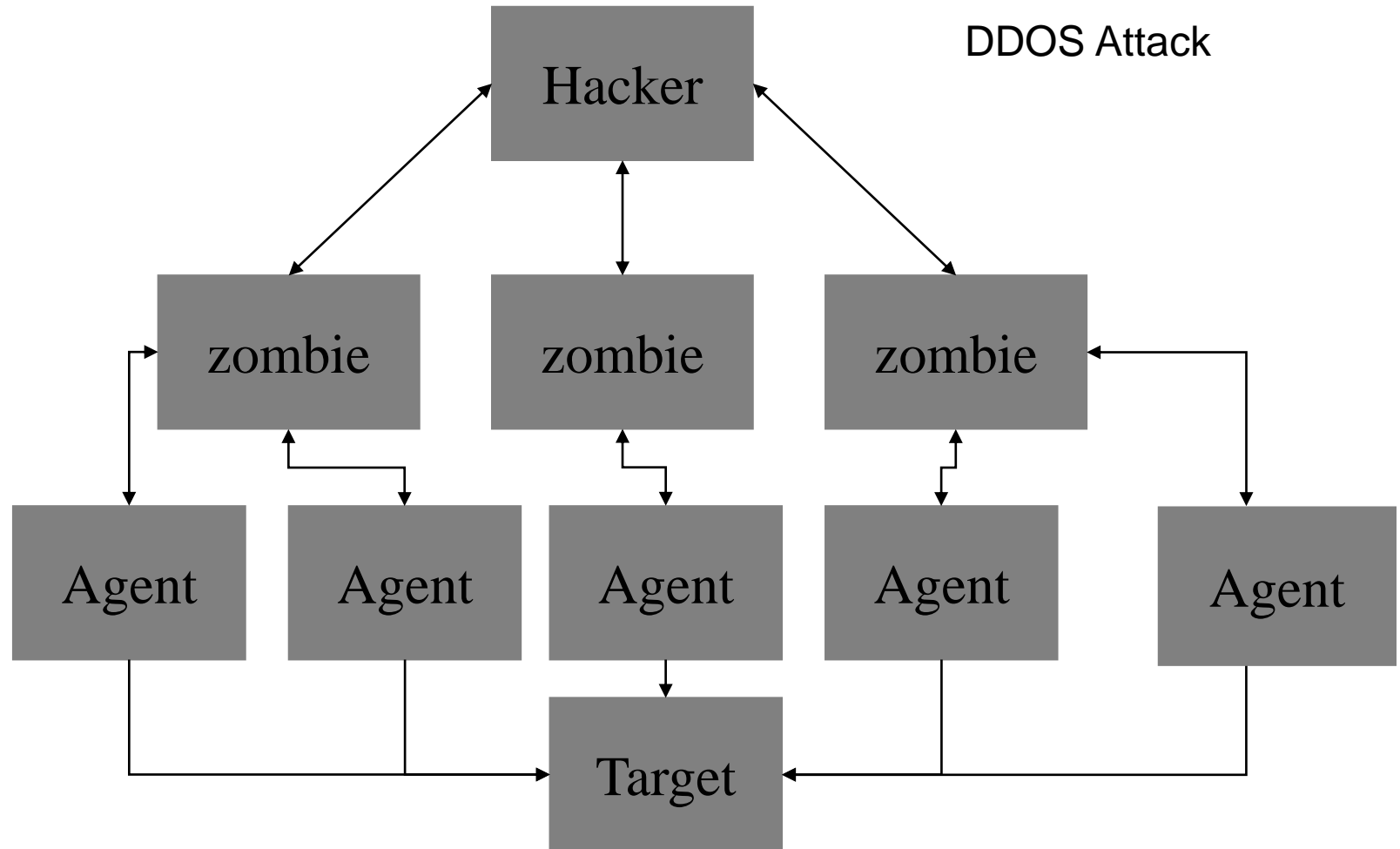
- DOS has increased in frequency
 - Ping floods
 - SYN floods
 - Code Red
 - UDP Bombs
 - Echo (7/UDP)
 - Discard (9/UDP)
 - Chargen (19/UDP)



- DDOS
 - Distributed DOS
 - Aim to saturate the bandwidth of a network link or crash network devices
 - A hacker plants a daemon on a server to transform it into zombie
 - Listen for commands sent by the hacker to launch an attack

- Smurf
 - IP floods to the broadcast subnetwork
 - » Hundreds amplification
 - Ingress filtering acl
- Fraggle
 - UDP echo floods
 - Use spoofed Source IP addresses
- TFN (Tribe Flood Network)
 - Adopt several methods for flooding and better control mechanism
 - **UDP** floods, **ICMP** flood, **SYN** flood
 - » Well known ports : 22/23, 25, 80, 179, 53, 6667

DDOS Attack



- DRDOS

- Distributed **Reflector** DOS

- A simple script

- be constructed to collect a large number of SYN packet reflections

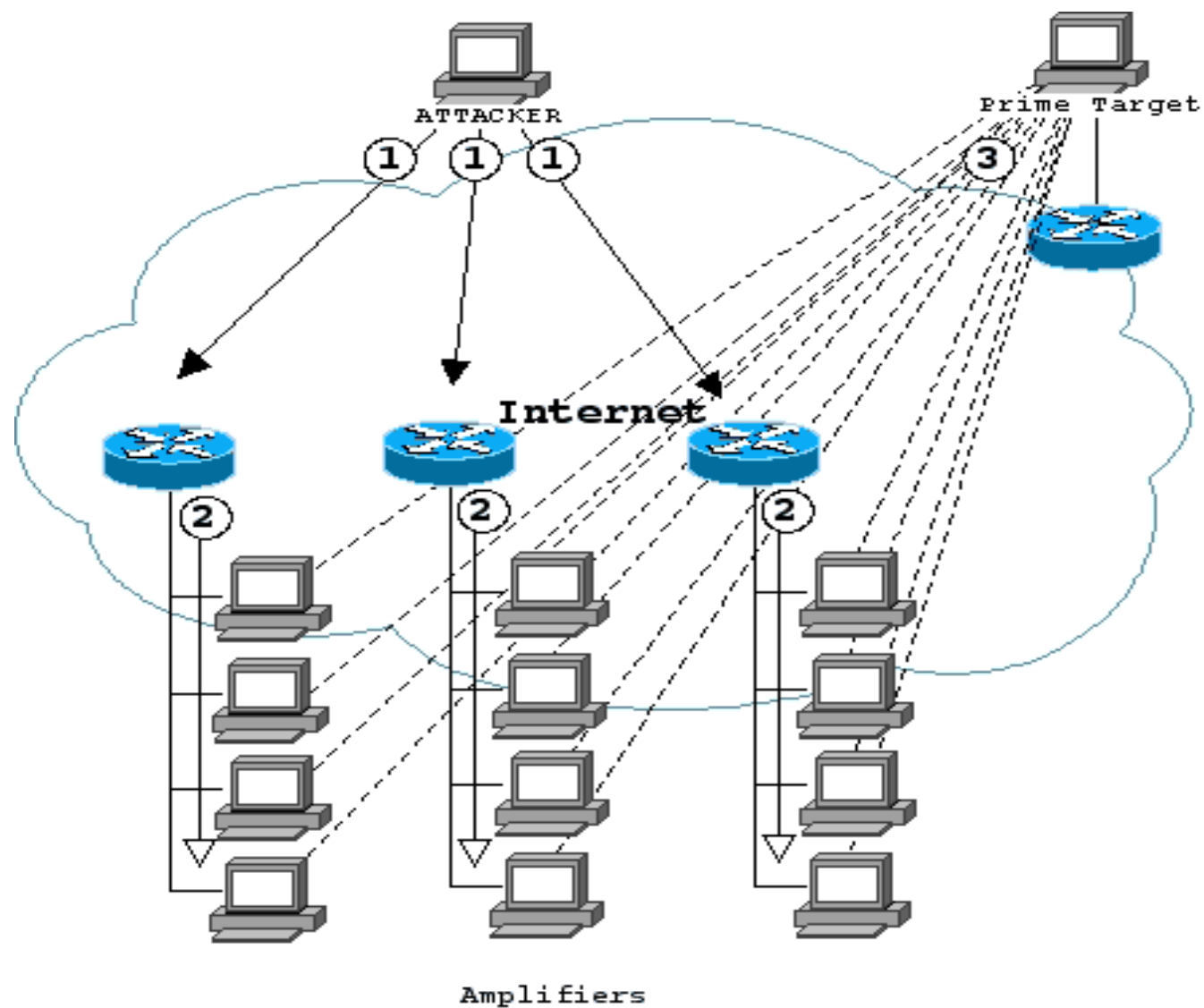
- Routers or servers

- Billions of packets were blocked to server

- Packet bounce Distributed DDOS

- Spoofed source IP addresses

<http://www.unixeunuchs.com>



- Protect yourself

- Hosts

- If system receives a large number of unresolved SYN requests in a short amount of time,
 - It should ignore any SYN request from that machine for a certain amount of time

- ISP

- Stop allowing traffic with spoofed return addresses out of their router
 - Egress Acl filtering
 - Simply sending SYN/ACK

Network Worm

- W32. CodeRed. Worm
 - Found in July 2001.
 - Utilize the .ida (indexing service) vulnerability in Microsoft Internet Information Server (IIS)
 - The buffer overflow allows the worm to execute code within IIS server
 - spread it & deface the server' s home page
 - Randomly attack other web servers and perform DOS attack

- Code Red worm execute only in memory
- First start 100 worm threads in memory
 - 100 copies of the worm were executed at the same time
 - Check c:\networm
 - 1th - 20th
 - Start infecting new system
 - 21th-27th
 - Start DOS attack

WORM SPREADING

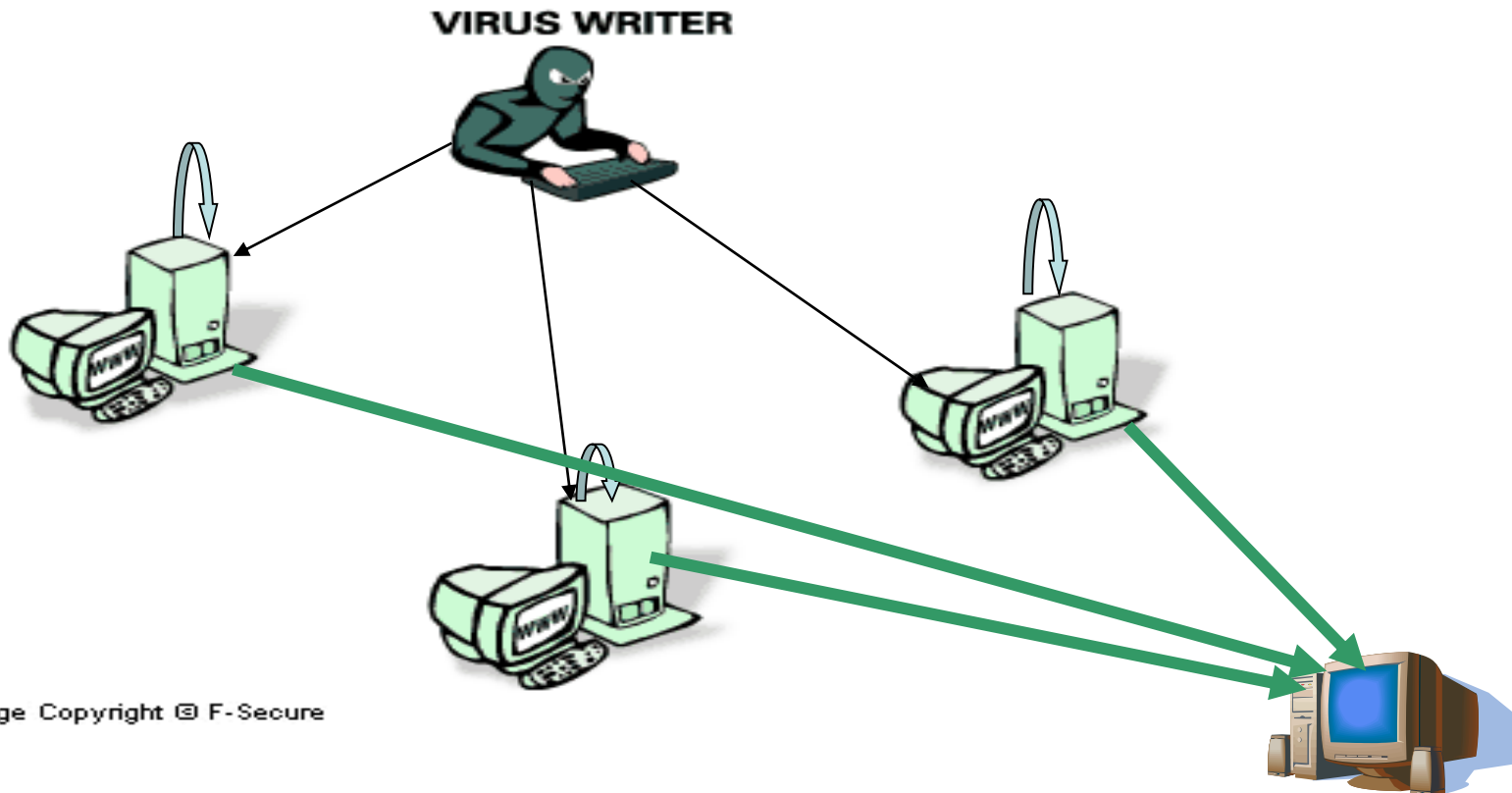


Image Copyright © F-Secure

- Code Red worm attack other systems by randomly generateing IP address
 - To see if it listening port 80
 - Send a copy of the buffer overflow attack to the machine
- The IP addresses could be probed over and over again
 - Each thread of the worm creating an effective DOS attack
 - $N * 100$

- W32. Nimda. A. Worm

- Found in Sep 2001.
- Nimda uses the Unicode exploit to infect IIS web servers
- A complex virus with
 - mass mailing worm
 - In named README.EXE
 - modify existing web sites to start offering infected files for download
 - use normal end user machines to scan for vulnerable web sites
 - Avoid Firewall

- **LIFECYCLE**

- The actual lifecycle of Nimda can be split to four parts:

- 1) Infecting files
 - 2) Mass mailing
 - 3) Web worm
 - 4) LAN propagation.

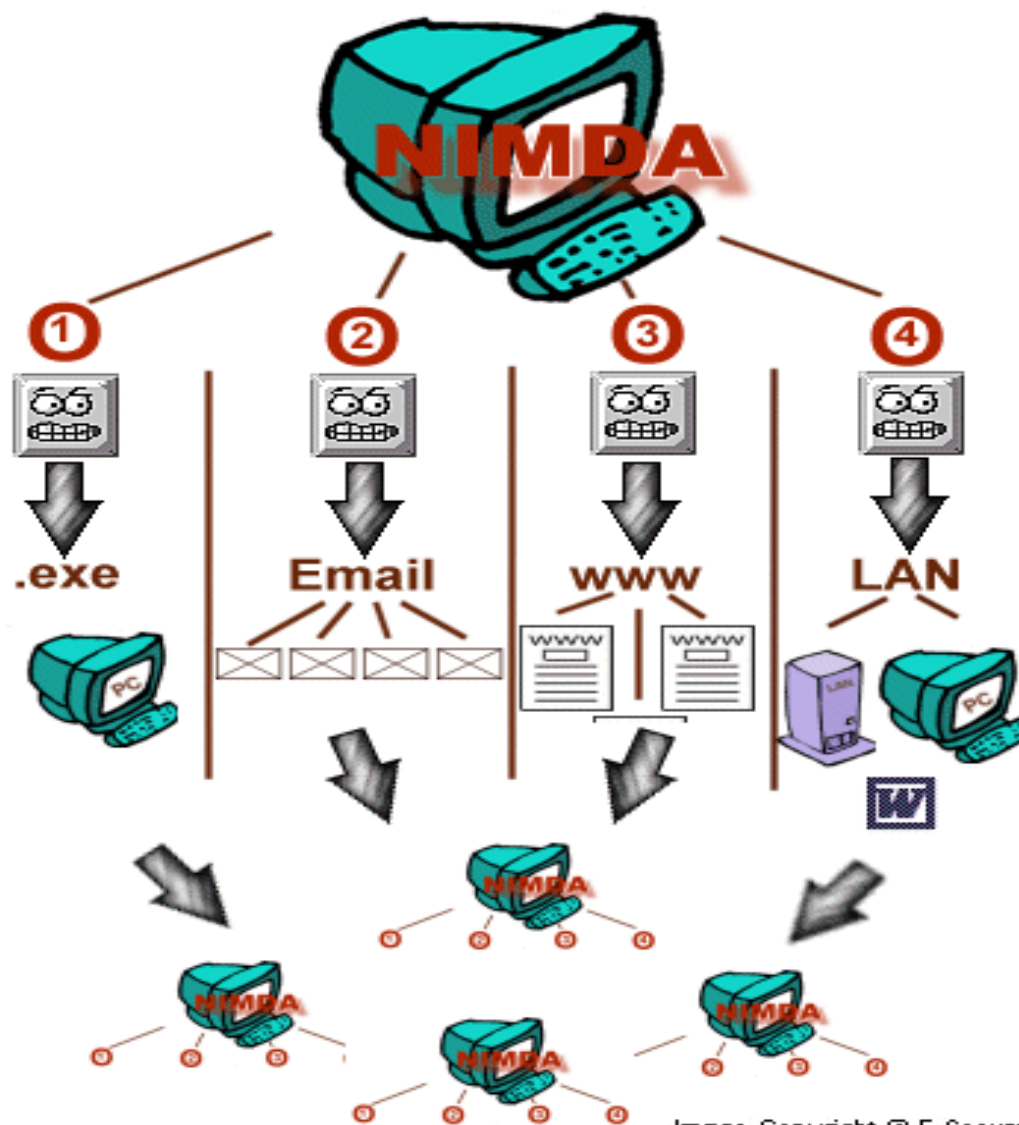


Image Copyright © F-Secure

- **1) File infection**

- Nimda locates EXE files from the local machine
- Infects them by putting the file inside its body as a resource
- 'assimilating' that file.
 - These files then spread the infection when people exchange programs such as games.

- **2) Mass mailer**

- Nimda locates e-mail addresses
 - via MAPI from your e-mail client
 - searching local HTML files for additional addresses.
- Then it sends one e-mail to each address
 - These mails contain an attachment called README.EXE,

- **3) Web worm**

- Nimda starts to scan the internet, trying to locate www servers.
- Once a web server is found, the worm tries to infect it by using **several known security holes**.
 - If this succeeds, the worm will modify random web pages on the site.
 - web surfers browsing the site will get automatically infected by the worm.

- 4) LAN propagation

- The worm will search for **file shares** in the local network
 - either from file servers or from end user machines.
- Once found, it will drop a hidden file called RICHED20.DLL to any directory which has DOC and EML files.
 - When other users try to open DOC or EML files from these directories, Word, Wordpad or Outlook will execute RICHED20.DLL
 - causing an infection of the PC.
- The worm will also infect remote files if it was started on a server.

- Damage:

- Large scale e-mailing: Uses MAPI to send itself out as Readme.exe (Readme.exe may NOT be visible as an attachment in the email received)
- Modifies files: Replaces multiple legitimate files with itself.
- Degrades performance: May cause system slowdown
- Compromises security settings: Opens the C drive as a network share

- Distribution:
 - Name of attachment: README.EXE (This file may NOT be visible as an attachment in the email received)
 - Size of attachment: 57344
 - Ports: 69
 - Shared drives: Opens network shares
 - Target of infection: Attempts to infect unpatched IIS servers

- Reference Site

- <http://www.europe.f-secure.com/>
- <http://www.symantec.com/avcenter/venc/data/w32.nimda.a@mm.html>

- FreeBSD. Scalper. Worm

- Discovered in Jun. 2002
- Use the Apache HTTP Server chunk encoding stack vulnerability
- Target IP host
 - Hard coded in the worm
 - Randomly generated
 - Scanned incrementally
- Use UDP port 2001 to listen for remote instructions

- Remote instructions perform one of the following functions:
 - Collect email addresses from the infected computer
 - View Web pages
 - Send email messages (spam)
 - TCP, UDP, DNS Flooding **
 - Execution of shell commands
 - Other Denial of Service functions.

- The Infecting process
 - Send port 80 HTTP GET request to target IP computers
 - Use the chunk vulnerability to
 - Execute a remote shell command
 - Simulate a handshake between the infected computer and the vulnerable computer
 - Send UUEcoded worm program to remote computer
 - /tmp/.uua
 - /tmp/.a

- Damage

- Large scale e-mailing:

- Contains the functionality to sent **e-mail spam** to all e-mail addresses found on the infected machines

- Degrades performance:

- performs many port 80 requests which could cause internet degradation

- Releases confidential info:

- allows **unauthorized access** to the infect machine

- Compromises security settings:

- allows unauthorized access to the infect machine

- **Linux. Slapper. Worm**

- Discovered in Sep. 2002
 - Use a flaw in OpenSSL libraries
 - Affect the Linux machine running Apache web server and OpenSSL enabled

- The infected machine can

- remotely be instructed to launch a wide variety DDOS to the Online-commerce, banking, privacy applications

- **Very similar to the Scalper Apache Worm**

- Variant: **Slapper. A**
 - /tmp/.bugtraq.c
 - /tmp/.bugtraq
- Infect process
 - Scan a hard coded class A networks for vulnerable machines
 - Apache port 80
 - Connect to SSL server (port 443)
 - Infect the target by using the vulnerability
 - Contained a **backdoor** listens to UDP port 2002
 - Can be controlled remotely

- Variant: **Slapper.B**
 - /tmp/.cinik.c
 - /tmp/.cinik
 - Copy the .cinik file to other directory
 - listens to UDP port 1978
 - Can be controlled remotely
 - Can **download a copy of its source code** from web site
 - The worm also **added itself to crontab** file to restart the worm hourly

- Variant: **Slapper.C**

- /tmp/.unlock.c
- /tmp/.unlock
- listens to UDP port 4156
- It also sends IP addresses of infected hosts via email probably to the virus writer

- Variant: **Slapper.D**

- listens to UDP port 1812

4. 攻擊訊務的監測

- UDP X-Attack Traffic Measurement
 - 一般骨幹router的封包轉送處理上限僅為 $10^6 \sim 10^8$ pps (packet per-second)
 - X-Attack
 - 瞄準網路processing, buffer資源
 - 快速送出鉅量封包或大量網路連接
 - 達成其耗損資料傳送沿徑的網路設備processing與連線頻寬資源.

- X-Attack訊務的量測
 - 以 {src_IP, dst_IP} host pair為攻擊訊務量測indexing
 - Communicating partner, flow, session
 - 為躲過firewall的過濾及管理人員的注意
 - 網路攻擊程式
 - 採動態的 src_port, dst_port
 - 動態的攻擊/休眠時間
 - 甚至Spoofed Source IP address

- 首先, 讀取Netflow log 檔
 - 比對/ 累計各source / destination IP pair 所傳送UDP packet count, flow count, , 與 byte count
 - (protocol identifier=17)
 - 存入相關的訊務變量
 - pair_i_udp_flows,
 - pair_i_udp_packets,
 - pair_i_udp_bytes

- 過濾高於threshold的X-Attack 攻擊訊務數據
 - 超高攻擊訊務threshold值
 - pairi_udp_flow / hour > 900、
 - pairi._udp_packet / hour > 1000,000
 - 排序/篩選/顯示單日各小時的超高傳訊數據
 - host_pair
 - netflow log數
 - Packet_Size
 - Packet封包數
 - Bytes總量

- 透過Hypertext Preprocessor (PHP) scripting網頁程式
 - 提供用戶隨時監測定期統計的X-Attack攻擊訊務
 - 於用戶輸入查詢日期後，invoke PHP 程式讀取對應日期的攻擊訊務數據顯示於網頁.
 - Fig. 1顯示 Feb-15-2003 的超量UDP攻擊訊務數據

http://163.25.255.10/~yang/Moe/index_evil.php - Microsoft Internet Explorer

檔案(E) 編輯(E) 檢視(V) 我的最愛(A) 工具(T) 說明(H)

← 上一頁 · → 搜尋 ★ 我的最愛 媒體

網址(🔍) http://163.25.255.10/~yang/Moe/index_evil.php 記錄 移至

UDP Attack Traffic Logs of TAnet-Internet OC3 Link #1

03 月 11 日 SUBMIT

日期:0215-- UDP Attack Logs時

SRC_IP > DST_IP	Flows	pk_size(KB)	Pkts	Total(MB)
=====				
140.123.102.184>61.9.12.150	33	0.042	21069962	864.037
203.68.31.22>80.135.155.194	105412	0.044	267655	11.487
140.136.200.11>200.249.243.249	26	0.028	13273928	367.111
66.250.72.7>203.64.42.192	41	1.096	98314	105.259
218.146.254.203>140.111.84.119	64	1.404	83701	114.751
64.95.80.9>140.128.69.170	57	1.405	82043	112.551
163.13.10.141>61.171.38.242	109	0.129	68932	8.710
61.171.38.242>163.13.10.141	138	0.092	52718	4.737
140.112.250.145>211.162.248.122	32	0.071	64774	4.484
203.242.146.143>203.72.179.12	550	0.544	46458	24.681
61.100.6.66>140.112.233.66	60	1.247	50534	61.561
140.113.146.154>62.94.49.168	7170	1.027	7170	7.193
140.113.146.87>62.94.49.168	7164	1.027	7164	7.187

完成 網際網路

開始 Monitoring_攻... http://163.25.255... 163.25.255.10 - ... 下午 06:56

** Flow Logs of UDP X-Attack-1 Traffic

(scr_ip)	(dst_ip)	(protocol)	(scr_p)	(dst_p)	(pkts)	(bytes)
140.136.200.11	200.249.243.249	17	32773	80	504154	21678622
140.136.200.11	200.249.243.249	17	32773	80	531475	22853425
140.136.200.11	200.249.243.249	17	32773	80	515715	22175745
140.136.200.11	200.249.243.249	17	32773	80	495831	21320733

** Flow Logs of UDP X-Attack-1 Traffic

140.136.192.1	161.69.3.150	17	1086	53	230600	345900000
140.136.192.1	161.69.3.150	17	0	0	445580	603912000
140.136.192.1	161.69.3.150	17	1086	53	229274	343911000
140.136.192.1	161.69.3.150	17	0	0	442218	599481000
140.136.192.1	161.69.3.150	17	1086	53	193822	290733000
140.136.192.1	161.69.3.150	17	0	0	374025	507057000

** Flow Logs of UDP X-Attack-2 Traffic

(scr_ip)	(dst_ip)	(protocol)	(scr_p)	(dst_p)	(pkts)	(bytes)
203.68.31.22	80.135.155.194	17	3541	4766	1	526
203.68.31.22	80.135.155.194	17	3542	4182	1	526
203.68.31.22	80.135.155.194	17	3543	706	1	526
203.68.31.22	80.135.155.194	17	3544	1601	1	526
203.68.31.22	80.135.155.194	17	3545	106	1	526

- X-Attack UDP 攻擊訊務
 - 140.123.102.184與140.136.200.11
 - 攻擊主機的超大量攻擊封包
 - 每小時可送出高達 $10^7 \sim 10^8$ 的UDP封包
 - 挑戰連網router processing資源, 遲緩其訊務轉送功能.
 - 依據攻擊主機的IP位址 (source IP) 資訊, 回頭過濾 netflow logs
 - X-Attack封包大都針對destination host的80/UDP、8080/UDP、53/UDP 等well-know service port (Fig. 1b), 傳出超大量packets.
 - 逐次調小packet size強化其癱瘓網路設備的威力

- DOS Attack

- 藉快速建立超量UDP flow連接, 耗損destination主機的processing與network資源
- 每小時高達 10^2 - 10^6 flows

- DDOS Attack

- 誘發同一 Class C IP 網段的百餘部主機, 以上百倍的冒充UDP 封包, 擴增對單一destination主機的攻擊威力
- 感染主機的用戶大都未能察覺其攻擊的發動原因
 - 選擇重新安裝系統, 或提高security等級
 - 防患系統再次被寄生病毒.

- 適度調降攻擊訊務threshold值,
 - 監測high-bandwidth MediaPlayer / Game UDP訊務
 - 整體而言, streaming media 封包大小要大於 game或http封包大小. 一般落於300 ~ 1500 Bytes/Packet
 - 163.13.10.141與61.171.38.242 兩Counter_Strike servers (27015/UDP service port)的訊務
 - Game 封包大小約為70 ~ 200 Bytes/Packet
- 218.146.254.203、 64.95.80.9
 - MediaPlayer servers
 - 每小時送出的數十Mbytes的高訊務量
- 203.242.146.143 > 203.72.179.12 flow
 - 為TFtp感染主機持續送出的TFtp封包,
 - mean packet size約為 544 Byte/Packet.
 - 依據主機IP位址再次篩選netflow logs,
 - » 可以發現: 該主機也同時對數部主機的 httpd service port (80/TCP) 發出頻仍的 SYN連接(packet size為 48 Bytes),
 - » 傳訊行為吻合Nimda virus攻擊特徵 [10].

- ICMP攻擊訊務

- 除了ping 與traceroute 網路偵錯訊務外, ICMP並無承載其他網路應用協定封包.

- 惡意的攻擊程式

- 快速傳輸無用的ICMP封包, 或建立大量ICMP連接
 - 挑戰連網設備網路及服務主機的計算資源極限
 - 壅塞, 甚至癱瘓連網訊務或server開放的服務.

- 攻擊host pairs 傳送出的超量ICMP封包
 - 不論destination hosts是否真的存在
 - 巨大的ICMP攻擊訊務都會耗損沿徑數十段國外WAN網段的 routing process及網路頻寬
 - 嚴重干擾destination hosts的開放服務
 - Backbone連網有必要利用蒐集的 router Netflow log轉送訊務紀錄
 - 累計/篩選可能耗損大量網路資源的ICMP 攻擊主機位址及訊務資訊
 - 方便用戶隨時查詢, 以及時修護攻擊主機漏洞
 - 避免昂貴WAN網路資源的持續浪費.

ICMP Attack Traffic Logs of TAnet-Internet OC3 Link #1

02 月 12 日 SUBMIT

日期:0212-- ICMP Attack Logs時

SRC_IP > DST_IP	Flows	pk_size(KB)	Pkts	Total(MB)
02-12 :: 00				
140.125.80.228>66.250.50.55	74	1.456	684399	973.083
140.123.14.149>1.1.1.1	75	1.444	236378	333.325
140.113.2.99>65.61.139.229	64	1.462	222763	318.124
140.125.94.128>1.1.1.1	78	1.456	214989	305.639
140.114.53.144>1.1.1.1	64	1.442	210743	296.858
140.125.240.101>202.24.66.254	38	1.020	12176	12.123
02-12 :: 01				
140.125.80.228>66.250.50.55	36	1.456	366097	520.516
140.114.53.144>1.1.1.1	32	1.450	127305	180.327
140.123.14.149>1.1.1.1	33	1.445	117971	166.522
140.113.2.99>65.61.139.229	32	1.462	109740	156.719
140.125.94.128>1.1.1.1	37	1.457	106950	152.132
140.125.240.101>202.24.66.254	15	1.020	5364	5.341
02-12 :: 02				
140.125.80.228>66.250.50.55	59	1.456	696307	989.983
140.123.14.149>1.1.1.1	59	1.441	232616	327.396
140.113.2.99>65.61.139.229	53	1.462	209786	299.593

完成

網際網路



Sonet高速骨...

http://163.25.2...

1:163.25.255...

2:163.25.255...

3:163.25.255...



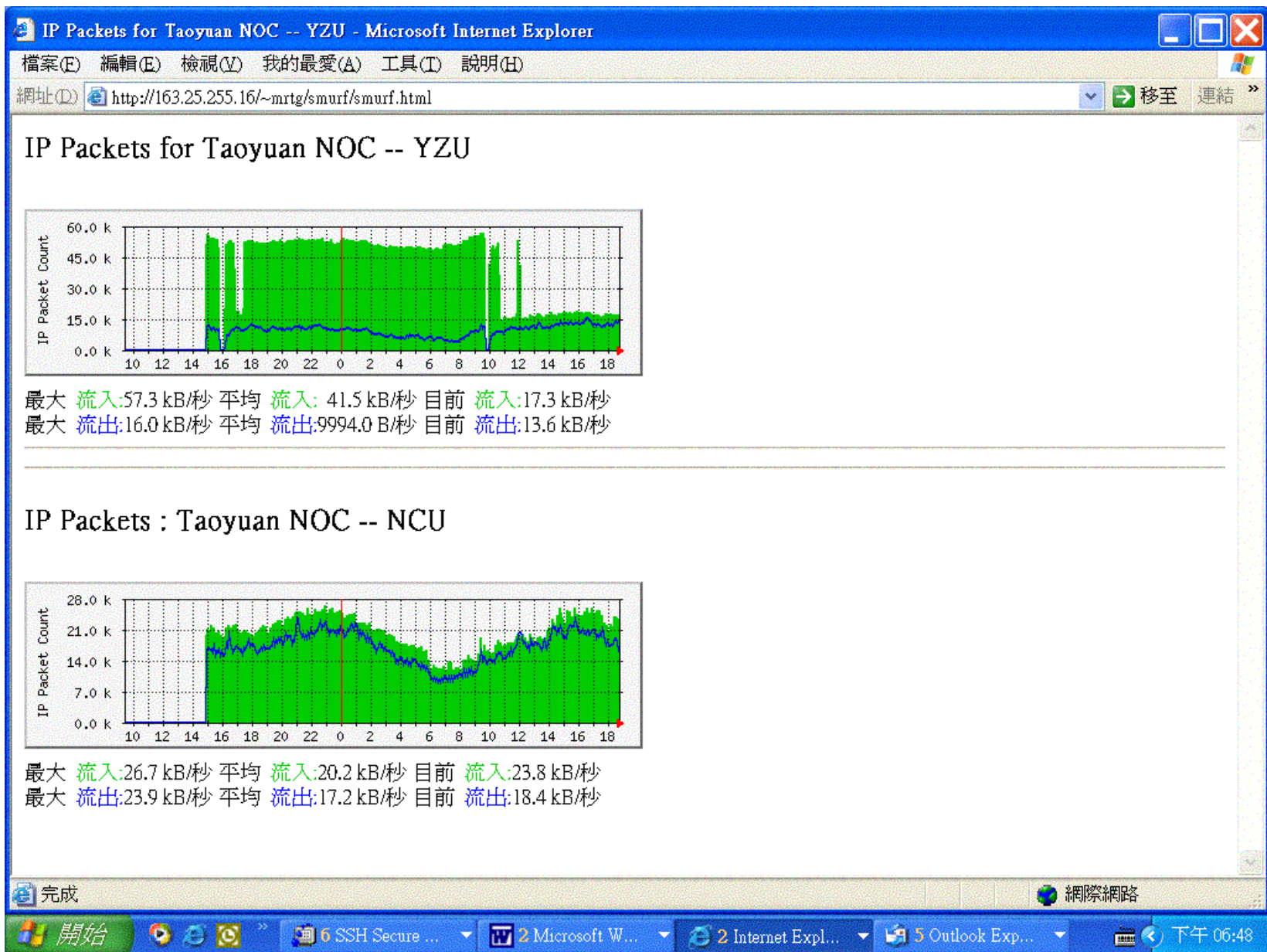
下午 02:08

5. 結語

- 促成超級攻擊訊務迅速成長的原因
 - 開放的Internet 傳輸協定
 - 簡易的socket 程式庫應用
 - 最主要應為:缺乏方便的攻擊訊務監測工具,
 - 協助網路管理者藉由具體的攻擊相關訊務數據,了解網路攻擊途徑, 採取適當的防患策略.
 - 方便用戶隨時查詢, 以及時修護攻擊主機漏洞

- 本研究利用WAN網路閘門位置的優勢,
 - 蒐集轉送訊務紀錄
 - 並針對X-Attack 快速耗損網路資源的特質, 實作X-Attack攻擊訊務的監測網頁
 - Monitoring
 - UDP / ICMP X-Attack Traffic
 - DOS / DDOS Attack Traffic

- Find out the attacking sub-network
 - Monitoring IP Packet Rate MRTG Graph
 - SNMP Interface MIB
 - Identify the attack **hosts** or **reflectors**
 - Improve the vulnerability
 - Campus Network
 - Department sub-network
 - Lab sub-network

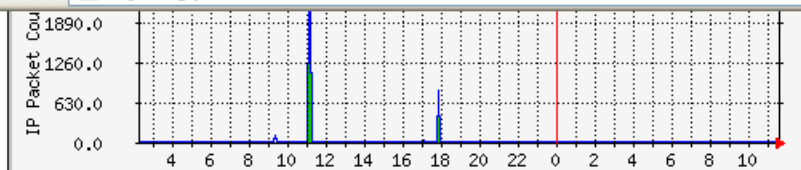


Find out the attacking subnetwork

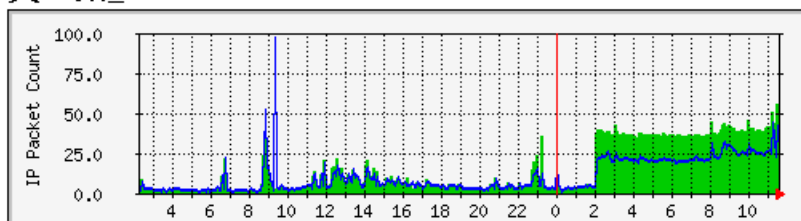
03-25 :: 22

140.138.144.5>146.100.59.82	2	1	0.575	1719	0.989
140.138.144.208>146.100.59.160	2	1	0.587	1662	0.975
140.138.144.51>146.100.59.110	2	1	0.566	1697	0.960
140.138.144.144>146.100.59.160	2	0	0.572	1677	0.959
140.138.144.183>146.100.59.160	2	0	0.562	1705	0.958
140.138.144.190>146.100.59.110	2	0	0.578	1656	0.957
140.138.144.106>146.100.59.110	2	0	0.577	1648	0.951
140.138.144.182>146.100.59.160	2	0	0.568	1671	0.950
140.138.144.13>146.100.59.110	2	1	0.552	1714	0.946
140.138.144.20>146.100.59.110	2	1	0.592	1599	0.946
140.138.144.157>146.100.59.110	2	1	0.576	1640	0.944
140.138.144.251>146.100.59.110	2	0	0.573	1641	0.941
140.138.144.193>146.100.59.160	2	0	0.563	1669	0.940
140.138.144.135>146.100.59.110	2	0	0.566	1662	0.940
140.138.144.65>146.100.59.160	2	1	0.549	1711	0.940
140.138.144.183>146.100.59.110	2	0	0.568	1654	0.940
140.138.144.165>146.100.59.110	2	0	0.569	1653	0.940
140.138.144.190>146.100.59.82	2	1	0.553	1696	0.938
140.138.144.143>146.100.59.110	2	0	0.537	1746	0.938
140.138.144.250>146.100.59.82	2	0	0.582	1609	0.937
140.138.144.45>146.100.59.160	2	0	0.585	1602	0.937
140.138.144.111>146.100.59.110	2	0	0.560	1673	0.936
140.138.144.227>146.100.59.82	2	0	0.561	1668	0.935
140.138.144.212>146.100.59.82	2	1	0.564	1656	0.935
140.138.144.237>146.100.59.160	2	0	0.555	1683	0.934
140.138.144.154>146.100.59.160	2	1	0.574	1626	0.934

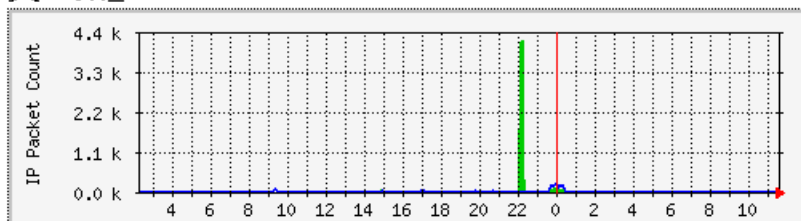
完成



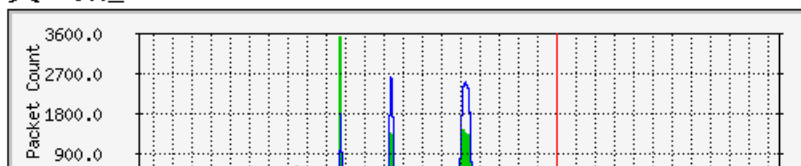
資工系_7



資工系_8



資工系_9



IP Packets for CSE_8 -- YZU - Microsoft Internet Explorer

檔案(E) 編輯(E) 檢視(V) 我的最愛(A) 工具(T) 說明(H)

← 上一頁

→

✖

↺

🏠

🔍 搜尋

★ 我的最愛

🌐 媒體

🔄

✉

🖨

🔗

📁

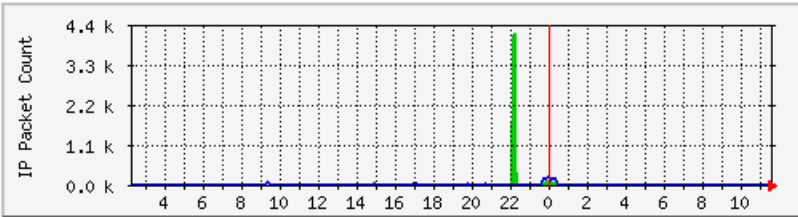
網址(D) http://log.yzu.edu.tw/smurf/cse/smurf_cse_8.html

移至 連結 >>

IP Packets for CSE_8 -- YZU

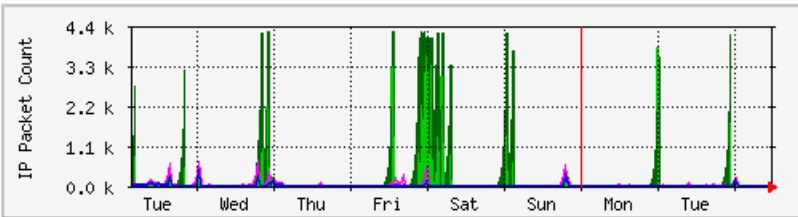
上次統計更新時間: 2003 三月 26 日, 星期三, 11:35,
設備名稱 'CSE-1305', 已運作時間(UPTIME): 59 days, 16:08:51.

每日 圖表 (5 分鐘 平均)



最大 **流入**:4197.0 B/秒 (0.0%) 平均 **流入**:45.0 B/秒 (0.0%) 目前 **流入**:18.0 B/秒 (0.0%)
最大 **流出**:244.0 B/秒 (0.0%) 平均 **流出**:17.0 B/秒 (0.0%) 目前 **流出**:14.0 B/秒 (0.0%)

每週 圖表 (30 分鐘 平均)



最大 **流入**:4287.0 B/秒 (0.0%) 平均 **流入**:156.0 B/秒 (0.0%) 目前 **流入**:18.0 B/秒 (0.0%)

完成

開始

IP Pac...

7 M...

Windo...

小算盤

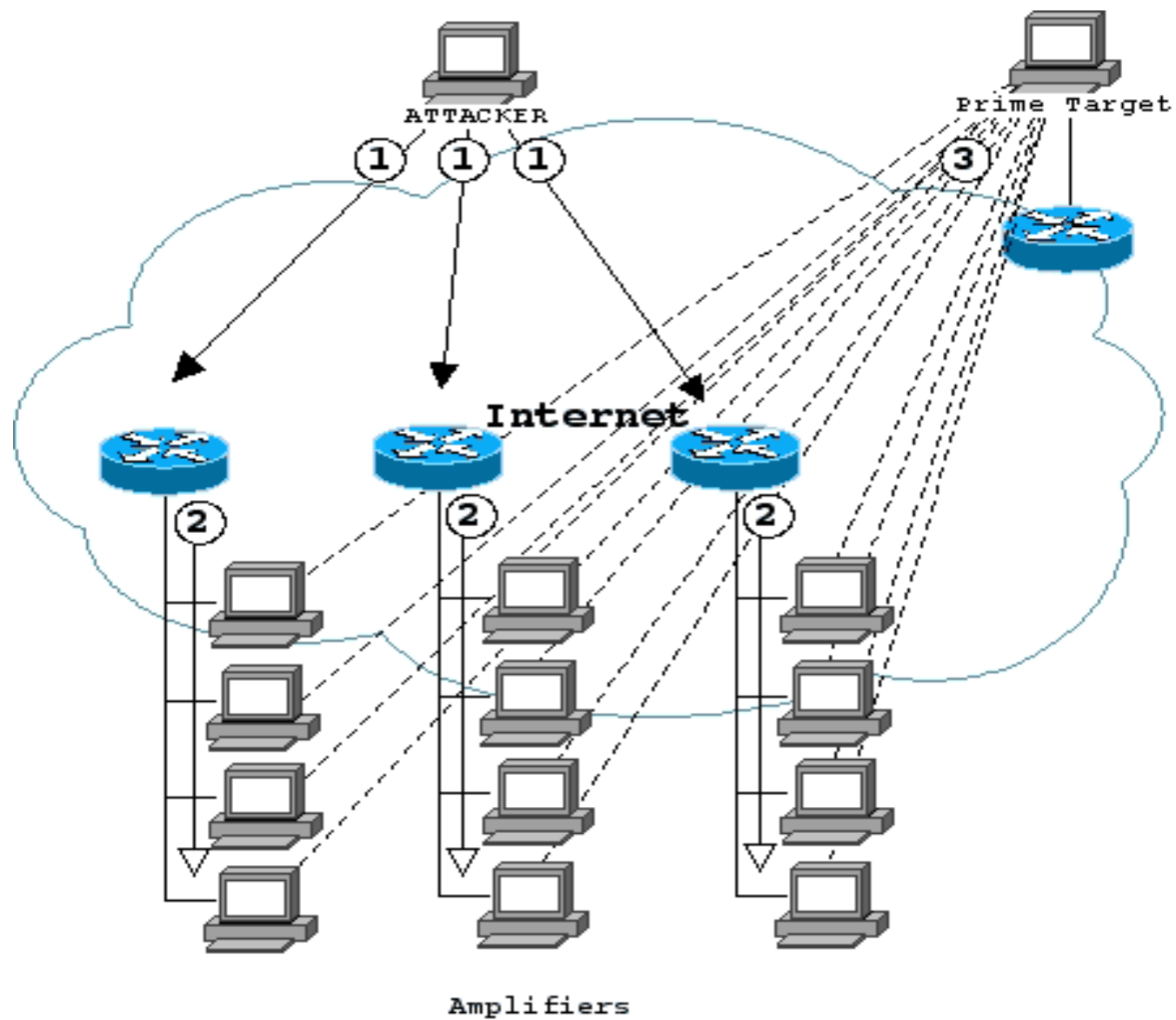
2 M...

3 S...

收件...

上午 11:38

- Spoofed source IP的攻擊訊務
 - Smurf UDP/ICMP flood
 - 需snoop LAN traffic log
 - Tcpdump the transportation logs over the single collision segment
 - Analyze & find out the compromised machine
 - Launch the attack
 - Notice the owner
 - Help patch the system



- 防駭網頁
 - The X-Attack traffic Measurement and Monitoring
 - Contact Information
 - RWHOIS service
 - Trace the patch processing Record
 - Share the experience