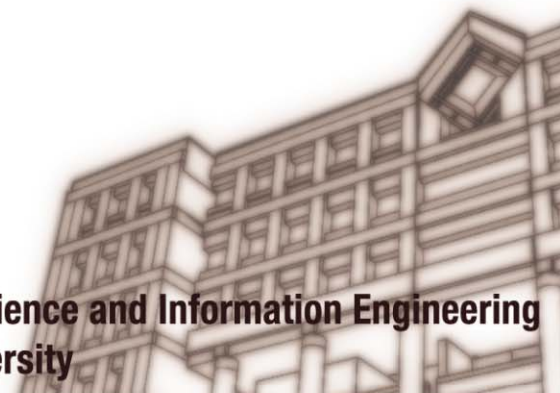
Worm Detection

Kudo@CCUCSIE

kudo@cna.ccu.edu.tw



Department of Computer Science and Information Engineering
National Chung Cheng University

What is Worm？

- A computer program that replicates itself and is self-propagating. Worms, as opposed to viruses, are meant to spawn in network environments. The Internet worm of November 1988 is perhaps the most famous;
- From： http://www.wwwebfx.com/

Why detect worm ?

- Bother others !
- Zombie packets make network slow !
- No one wants to be infected !
- How about the influence in CCU ?

Famous Worm --- Blaster

- Reboot and reboot again !
- Attempt to attack others by DCOM hole though port 135

Famous Worm --- Sasser

- Reboot and reboot again !
- Attempt to attack others by LSASS hole though port 445/9996/5554

The first method to detect

- Analyze the log from tcpdump, ipfw, or something like that in NON-Windows Host.
- Easy to do.
- But may be miscarriage
- It is now used in dorm@CCU.

How about the better method ?

- Oh ! Ya ! That's Netflow
- （but also sflow…etc）

What's Netflow

- A technology to analyze flow in network.
- Produce by Cisco.
- Information include SrcIP/DstIP, SrcPort/DstPort, packet numbers, packet sizes, time … blah blah

How to detect worm by Netflow ?

srcIP	dstIP	prot	srcPort	dstPort		octets	packets
140.121.131.26	140.123.243.228	6	4196	135		96	2
140.121.131.26	140.123.243.229	6	4197	135		96	2
140.121.131.26	140.123.243.206	6	4173	135		96	2
140.121.131.26	140.123.243.207	6	4174	135		96	2
140.121.131.26	140.123.243.209	6	4175	135		96	2
140.121.131.26	140.123.243.238	6	4211	135		96	2
140.121.131.26	140.123.243.239	6	4212	135		96	2
140.121.131.26	140.123.243.241	6	4213	135		96	2
140.121.131.26	140.123.243.242	6	4216	135		96	2
140.121.131.26	140.123.243.243	6	4217	135		96	2
140.121.131.26	140.123.243.230	6	4199	135		96	2
140.121.131.26	140.123.243.231	6	4200	135		96	2
140.121.131.26	140.123.243.232	6	4201	135		96	2

How to detect worm by Netflow？（Cont.）

srcIP	dstIP	prot	srcPort	dstPort	octets	packets
140.123.232.22	140.123.241.188	6	2561	445	96	2
140.123.236.43	140.123.9.122	6	3806	445	96	2
140.123.234.197	140.123.241.97	6	4868	445	96	2
140.123.234.102	140.123.9.206	6	2101	445	96	2
140.123.221.107	140.123.9.81	6	3011	445	96	2
140.123.238.207	140.123.241.196	6	4028	445	96	2
140.123.237.112	140.123.226.91	6	2537	445	96	2
140.123.232.22	140.123.241.18	6	2609	445	96	2
140.123.220.218	140.123.241.234	6	2579	445	96	2

How to detect worm by Netflow？（Cont.）

- One SrcIP and DstPort
- Many and many DstIP
- Flow data import in MySQL
- SELECT COUNT(DstIP) + GROUP BY SrcIP

More about Netflow

- Port Scan Detection

srcIP	dstIP	prot	srcPort	dstPort	octets	packets	
140.123.214.91	140.123.220.5	6	60476	240	46	1	
140.123.214.91	140.123.220.5	6	60476	47557	46	1	
140.123.214.91	140.123.220.5	6	60476	2018	46	1	
140.123.214.91	140.123.220.5	6	60477	708	46	1	
140.123.214.91	140.123.220.5	6	60477	1103	46	1	
140.123.214.91	140.123.220.5	6	60477	2028	46	1	
140.123.214.91	140.123.220.5	6	60477	599	46	1	
140.123.214.91	140.123.220.5	6	60475	1497	46	1	
140.123.214.91	140.123.220.5	6	60475	2026	46	1	
140.123.214.91	140.123.220.5	6	60475	285	46	1	
140.123.214.91	140.123.220.5	6	60475	1006	46	1	
140.123.214.91	140.123.220.5	6	60475	390	46	1	

More about Netflow（Cont.）

- One SrcIP, DstIP
- Multiple DstPort
- SELECT COUNT(DstPort) + GROUP BY SrcIP

More about Netflow（Cont.）

- More accuracy
- But need more time and space

Other method ?

- IDS !
- Worm packets might have the similar fingerprint.
- Yes ! It's a idea, a todo.
- Performance ?
- And other difficulties ?

Moreover ？ It’s time to discuss

- Fake worm ?
- Unknown worm ?
- Performance ？ Accuracy ？
- Other technology ?