

Survival Acceptability Evaluation and Incident Case Report in Taiwan

Shih-Kun Huang, Nian-Shing Chen, Chia-Mei Chen, and
Biing-Jong Lin

skhuang@cert.org.tw, nschen@cert.org.tw, cchen@cert.org.tw, and
wing@cert.org.tw

Taiwan Computer Emergency Response Team (TW-CERT)

<http://www.cert.org.tw/>

Abstract

Information security is becoming one of the most important issues as our government deploys the national information infrastructure and information policies. The Internet is inherently not a secure communication environment and new vulnerabilities of the Internet computers are continuously reported. However, the emerging technology of the open network attracts more institutes, industries, government agencies, as well as attackers connecting to the Internet. Web servers are often used to provide services, advertise themselves, or make electronic commerce activities before they are ready to protect themselves from the possible threats of the open network – attacker's intrusions or compromise of critical infrastructure.

This paper contains two parts. The first part presents an evaluation of the survival acceptability of the web servers in National Sun Yat-sen University (NSYSU). Based on the preliminary evaluation, we analyze the security level and identify the weakness of the national information infrastructure, and seek solutions to our government. The second part describes our process on an incident case happened in August 1999 in which several government web sites were attacked, from which we learned and practiced the response plan to the information warfare.

Keyword: *computer security, survivability, incident response, vulnerability*

Taiwan Computer Emergency Response Team is an independent agency sponsored by Directorate General of Telecommunications, MOTC, Taiwan, Taiwan Network Information Center (TWNIC), and the Computer Center of National Sun Yat-sen University, Taiwan.

1. Introduction

The Internet is inherently not a secure communication environment and new vulnerabilities of the Internet services are continuously reported. Attackers may facilitate various scan tools and exploit programs to search for target hosts, waiting for the appropriate time to break into the systems. Firewalls and intrusion detection tools may prevent their attempts if properly configured. Survivability is the capability of a system to fulfill its mission, in a timely manner and in the presence of attacks, failures, or accidents. It serves as an index to show the degree of preparation on intrusion resistance and recovery.

There are some existing tools called Network Intrusion Detection System(NIDS), which are available for examining vulnerabilities of a network such as IDIOT [9] and STING [6]. Some tools can even monitor traffics and activities within a network for defending potential threats to computer systems by autonomous agents[7]. We have examined the survivability of the servers in NSYSU, which provide public services to the Internet users based on the proposed method [10]. Based on the preliminary evaluation, we analyze the security level and identify the weakness of the national information infrastructure, and seek to provide solutions to our government.

In the second part of this paper, we describes our process on an incident case happened in August 1999 in which several government web sites were attacked. TW-CERT formed an incident handling team for this matter right after the attack happened. The following actions were taken to response to the incident: (1) monitoring how many sites were attached; (2) tracking the attacker sources; (3) analyzing the vulnerability patterns used for the attack; (4) issuing an incident note and announcing the media the incident case to alert other web site administrators and to avoid further damage. We learned and practiced the incident response plan to the information warfare from this incident.

2. Survivability survey

To evaluate the survivability of a network, we need to know what kind of services running in the network, how many hosts in the network, and the overall network architecture. Intruders are most interested in the public services provided in the target network. Hence, we study the impact of the services and evaluate the survival acceptability on a selected network by the method proposed by [8].

There are several researches on classifying the impact level of vulnerabilities according to different aspects. We propose ours based on [1] for this evaluation as shown in Table 1. The evaluation eliminates the impact level of the “Denial of Service” for maintaining normal services and the testing is done in off-peak for

minimizing the degradation of the network. The campus network of the National Sun Yat-sen University (NSYSU) is our chosen network with 324 server hosts and 2812 services in total.

Category	Item	Description
C1: (Level 0) Security Information	Security Information Leakage	Leakage of administrative related information and the version of the services
C2: (Level 1) Denial of Essential Service	Denial of Service	Resources fully occupied, performance degradation or out of service.
C3: (Level 2) Relay of Internet Attack	Relay of Attacker's Command	Similar to proxy relaying attacker's command.
C4: (Level 3) Remote File Access	Remote File READ	Unprivileged file read through a vulnerability of a network service.
	Remote File WRITE	Unprivileged file update through a vulnerability of a network service.
C5: (Level 4) Remote Command	Remote USER Shell	Command execution as a normal user in the system through vulnerability of a network service.
C6: (Level 5) Execution	Remote ROOT Shell	Command execution as a root user in the system through vulnerability of a network service.
C7: (Level 6) Backdoor / Trojan Horse	Various of Backdoor/Trojan Programs	Backdoor or Trojan program resided in the System

Table 1: Vulnerability category.

At level 0, attackers may perform the following activities such as:

- 1 Grab information by *EXPN/VERY* commands in an SMTP server in which they are not disabled.
- 2 Use *rpcinfo* command to list all services provided by the server.
- 3 Try to log into the target system to see the "LOGIN BANNER"(a.k.a. system footprint).

The results of level 0, information leakage, are shown in Figures 1 and 2. Over half of the server hosts are vulnerable with information leakage. The mail service, SMTP, has the most of level 0 vulnerabilities among the others.

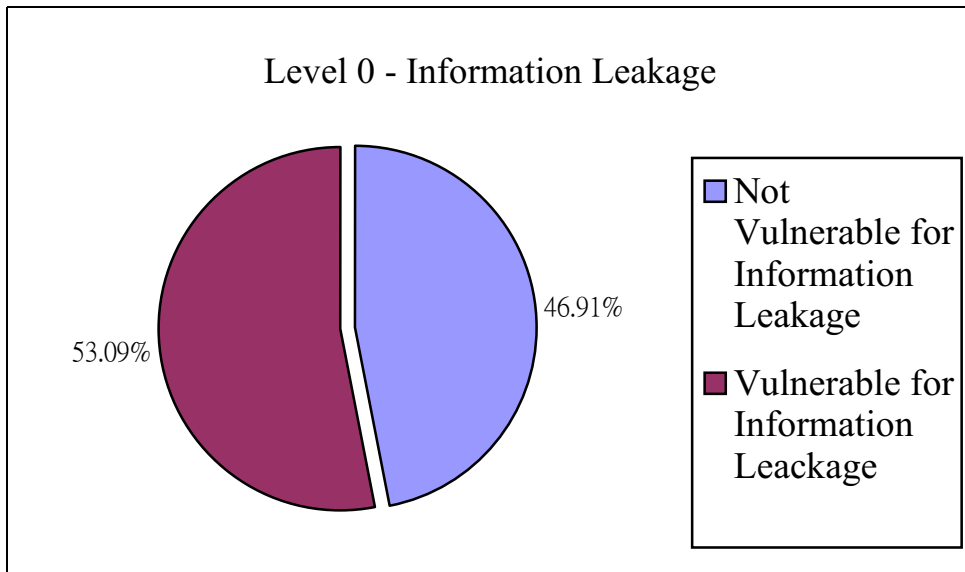


Figure 1: Level 0 affected server hosts.

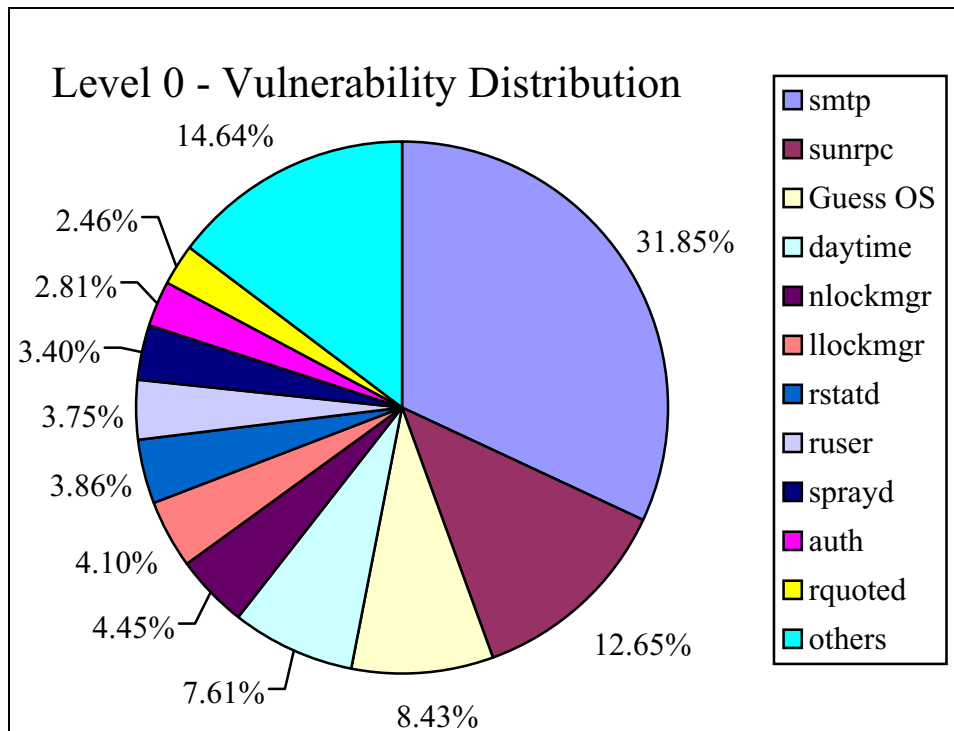


Figure 2: Level 0 vulnerable services.

Servers with level 2 vulnerability may have the following problems:

1. Mis-configured web/gopher servers with the proxy function enabled, so attackers may bypass it to other hosts.
2. Rexecd and fingerd are obsolete, allowing attackers to access other hosts from them.

The results for level 2 are shown in Figures 3 and 4. Only one third of server hosts are vulnerable for level 2 vulnerability, relay of Internet attack, while http service contributes about 50% of vulnerability for services.

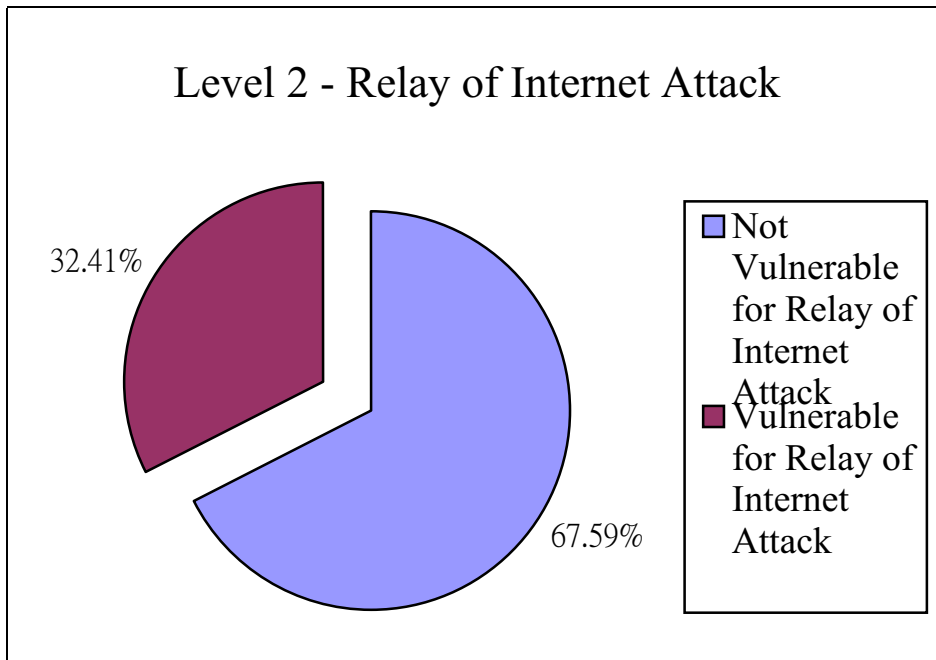


Figure 3: Level 2 affected server hosts.

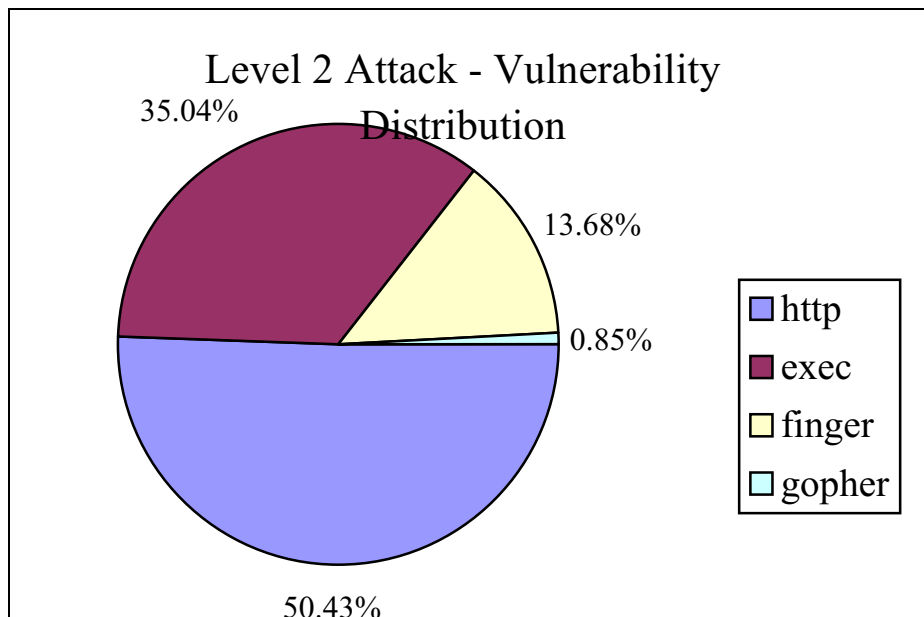


Figure 4: Level 2 vulnerable services.

The common problems at level 3 are:

- 1 Attackers can generate a core file when using the PASV mode in FTP session, and then collect the password information in this core file.
- 2 Attackers may use the *web-dist cgi* program in */cgi-bin* directory to grant the READ privilege of httpd user.
- 3 A vulnerability in *tftpd* could grant attackers access permission.

Figures 5 and 6 illustrate the results. Very few hosts are vulnerable for level 3 attack – remote file READ and two services, ftp and http, are the most vulnerable

services for level 3 attack.

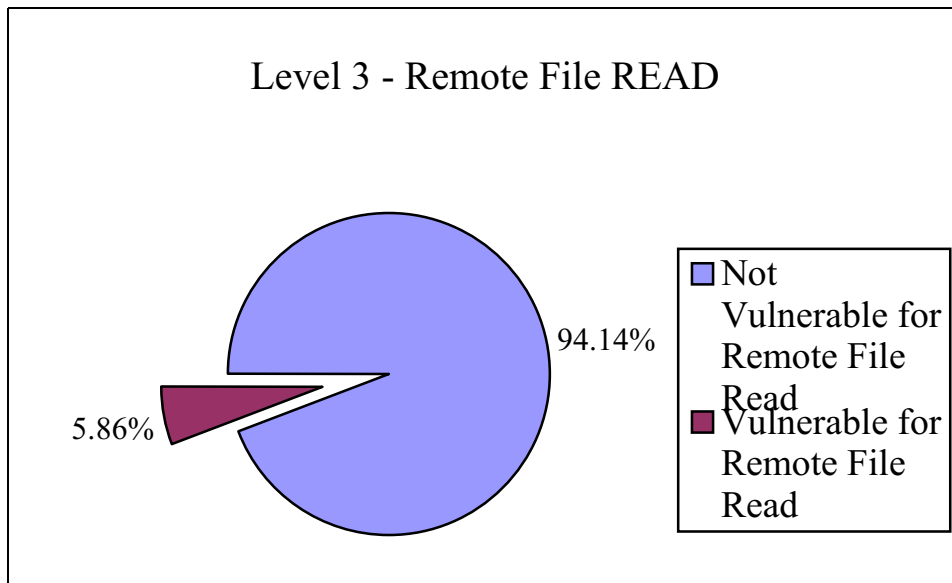


Figure 5: Level 3 affected server hosts.

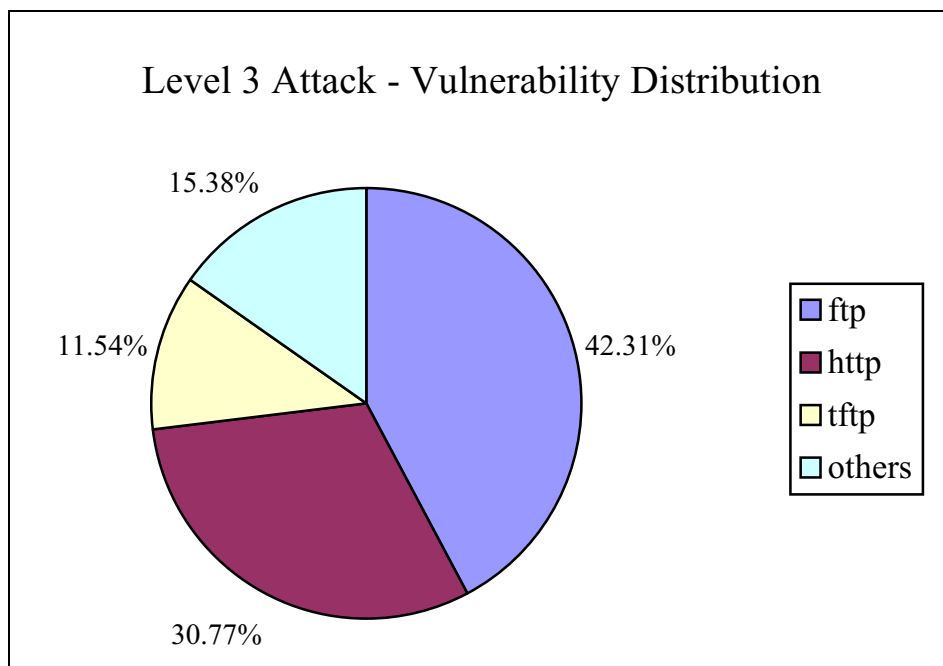


Figure 6: Level 3 vulnerable services.

The common problems at level 4 are:

- 1 All hosts can do R/W access to the NFS server.
- 2 Remote user can upload any file to any directory in FTP service.

From the results shown in Figures 7 and 8, few hosts are vulnerable to such level of attacks and NFS is the most vulnerable service with respect to level 4

attacks.

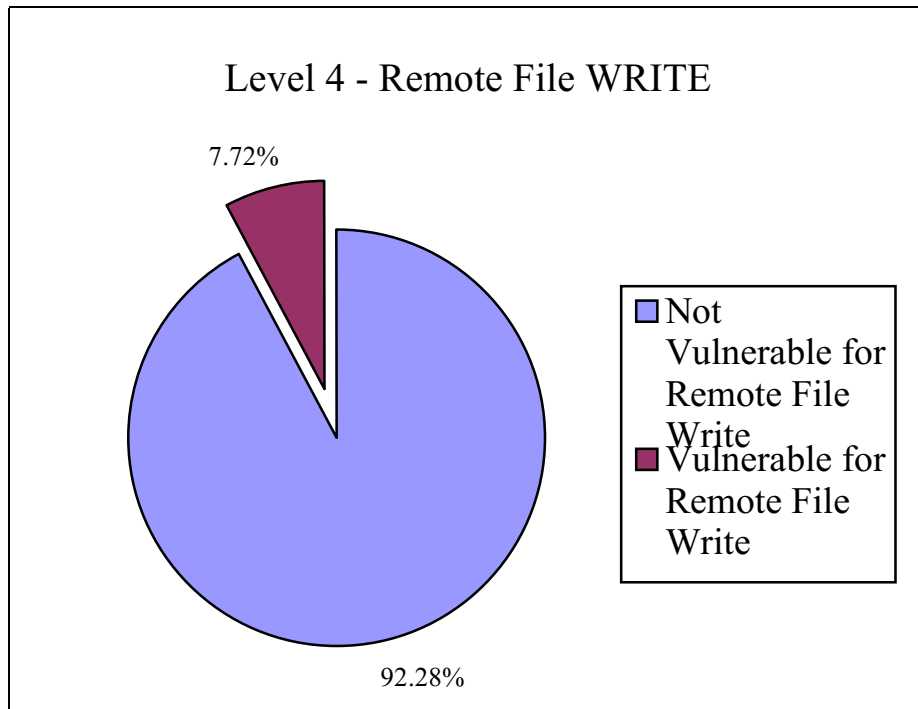


Figure 7: Level 4 affected hosts.

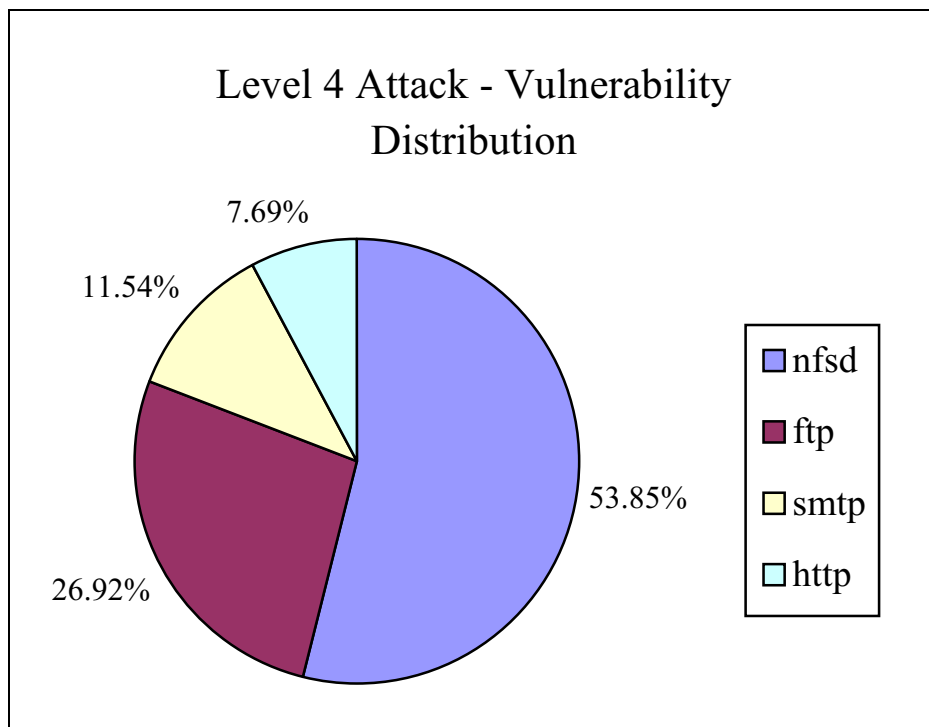


Figure 8: Level 4 vulnerable services.

The common problems at level 5 are:

- 1 Users choose simple passwords which can be easily guessed.
- 2 Some ftp daemons have buffer overflow problem.

3 CGI programs could be misused by running commands remotely.

The results in Figures 9 and 10 show that over one fourth of hosts are vulnerable for such level of attacks and telnet is the most dangerous service if passwords are not properly chosen.

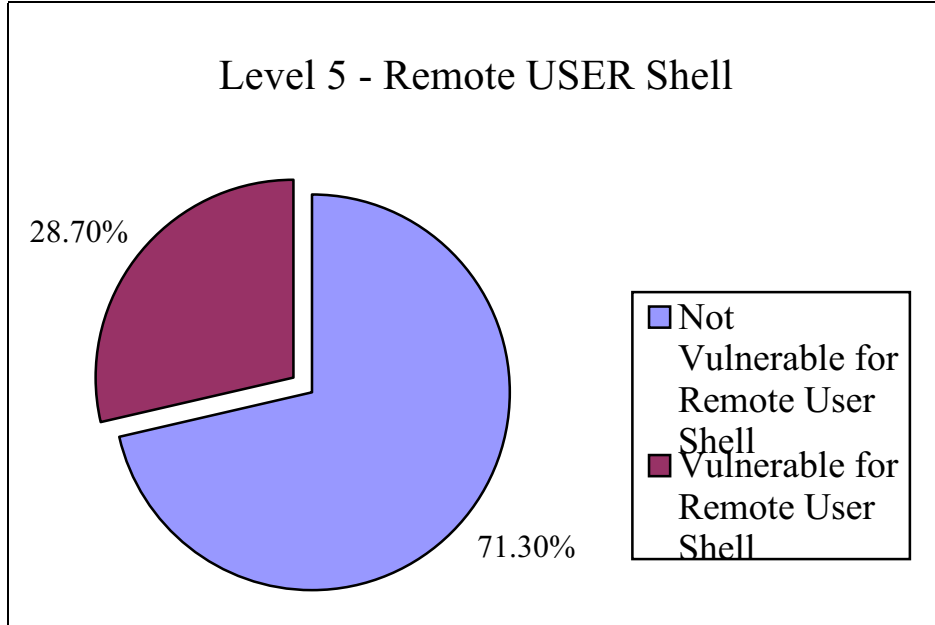


Figure 9: Level 5 affected hosts.

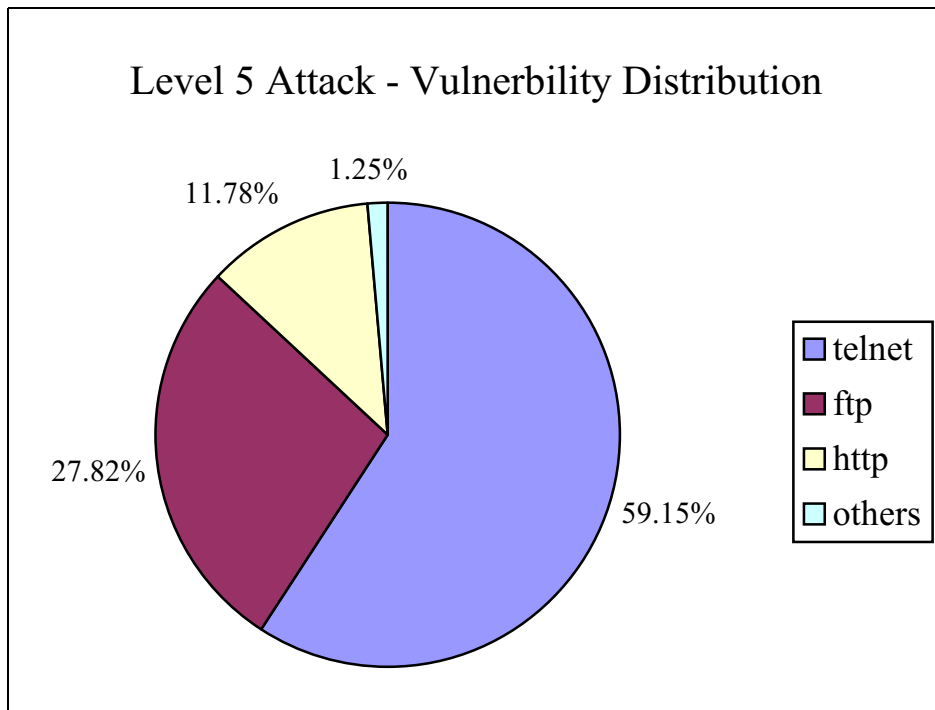


Figure 10: Level 5 vulnerable services.

The common problems at level 6 are:

1. Attackers may utilize the buffer overflow problem in *mountd*, *ftpd*, and

imapd.

2. Attackers may use redirection with pipeline on sendmail program.
3. Attackers may facilitate the vulnerabilities on RPC.
4. The buffer overflow problem in BIND reverse query could be another choice for attackers.

From the results in Figures 11 and 12, over one fourth of hosts are vulnerable for such level of attacks and mountd is the most vulnerable.

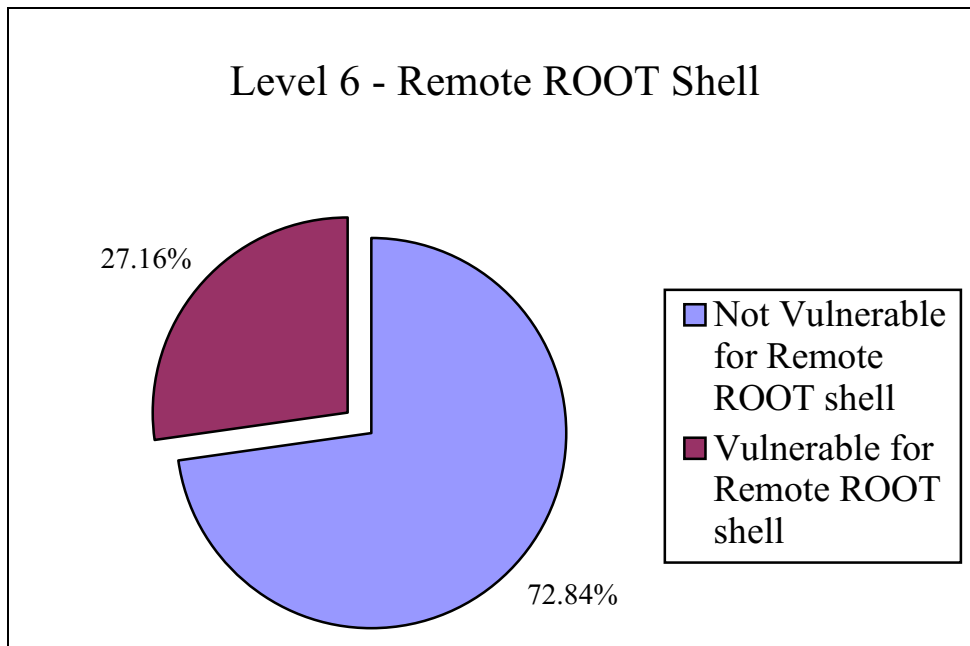


Figure 11: Level 6 affected hosts.

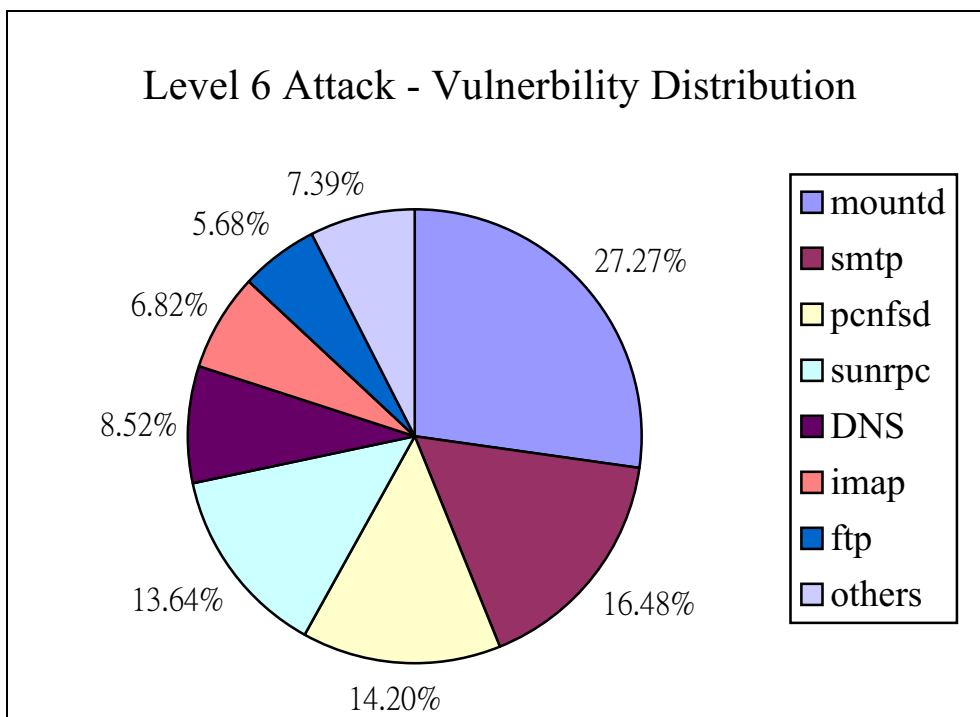


Figure 12: Level 6 vulnerable services.

A common problem for level 7 is that attackers normally will implant backdoors or Trojan programs into the victims for their future access. From the results in Figures 13 and 14, we can see that most hosts can resist such level of attacks. However, two most commonly used services in campus, finger and ftp, are the most vulnerable for such attacks. A summary result of the conducted survey on the NSYSU campus network is shown in Table 2.

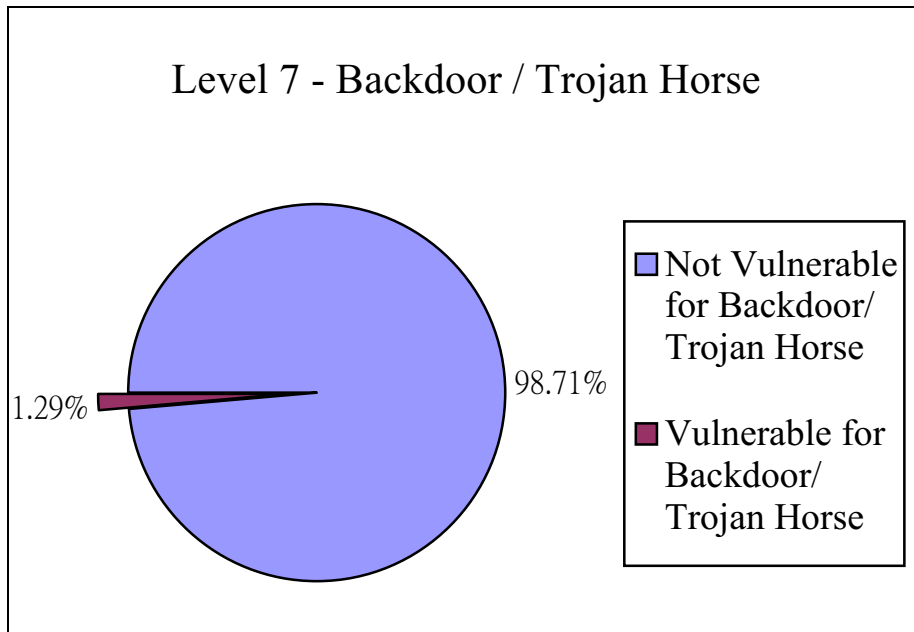


Figure 13: Level 7 affected hosts.

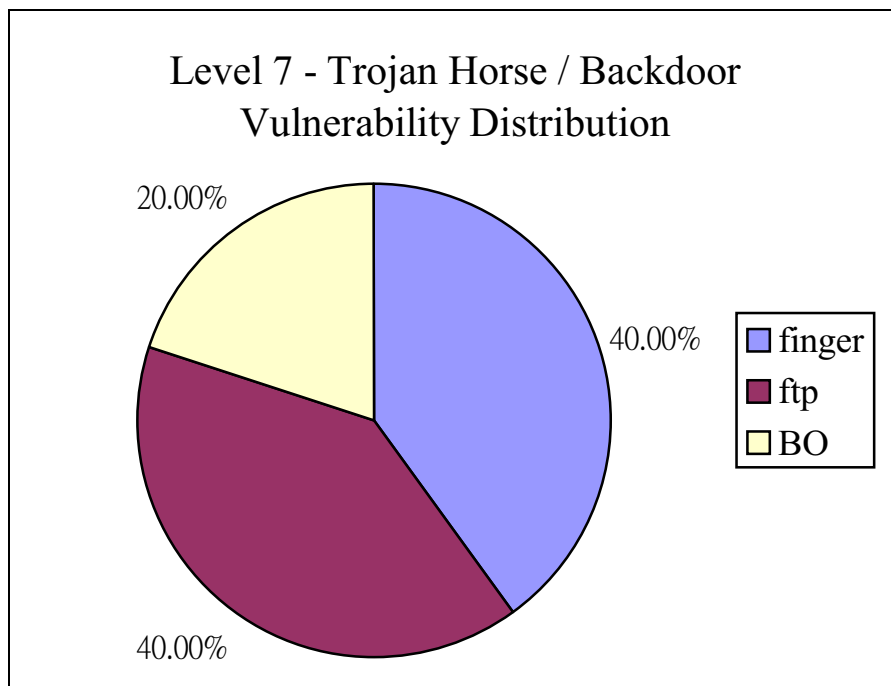


Figure 14: Level 7 vulnerable services.

Attacking level	Affected hosts	Survivability ratio
Level 0 – Information Leakage	172	46.91 %
Level 1 – Denial of Service	N/A	N/A
Level 2 – Relay of Internet Attack	105	67.59 %
Level 3 – Remote File READ	19	94.10 %
Level 4 – Remote File WRITE	25	92.28 %
Level 5 – Remote USER Shell	93	71.30 %
Level 6 – Remote ROOT Shell	88	72.83 %
Level 7 – Backdoor / Trojan Horse	4	98.71 %

Table 2: Survival ratio of WEB sites in NSYSU.

3. Incident Response Practice

TW-CERT received several related incident reports on 7th and 8th of August 1999. The intruders broke into the web sites of some government agencies and academic institutes in Taiwan and replaced their web pages. According to our investigation, the first intrusion event started at the midnight of 7th of August, and the target site was recovered within half hour by the corresponding hostmaster. Later on, we received twelve incident reports with the same intrusion pattern.

TW-CERT acted as a coordination agency, helping the victim sites recover and prevention furthermore. We take the following procedures in response of the sequence of the incident events.

1. Monitor the Internet and advise the victims

TW-CERT technical members have monitored the sites since the first intrusion case was reported. We collected the possible victim lists from local news groups and related BBS boards, verifying the real victims and advising the corresponding hostmaster by emails or hotlines. Like most of intrusion cases, the intruders took action in a long weekend when most employees were off and made us repair in time hard.

2. Issue an incident note to prevent further damage

An incident handling team was organized in TW-CERT eight hours after the first incident report. Part of the team members collected and analyzed the intrusion patterns; the rest of them worked on recovery and prevention solution. With the collaboration of the team, an incident note [12] was issued in a timely and efficient way. Key points of the incident note include:

- ♦ The victim sites should disconnect from the Internet network immediately

to prevent further damage. The corresponding hostmasters need to patch the broken services and vulnerabilities. If patching cannot be done for any reason, the machines should be shutdown until the problem is fixed.

- ♦ The intrusion patterns are similar -- aiming at well-known vulnerability holes of RPC services, such as *ToolTalk* [4] and *rpc.cmsd* [2]. The corresponding hostmasters should patch the vulnerabilities as soon as possible and refer to the related advisories of CERT/CC[3,5].
- ♦ The administrators need to keep the latest system logs to trace the intrusion source.
- ♦ TW-CERT provides a hotline offering technical advice, helping victims trace the intruders.

3. Analyze the intrusion pattern

The intrusion patterns of the related incident reports are alike and lead us enough evidence to proof who they are and how they did. They used the same vulnerability holes to break into the system, such as *ToolTalk*, *rpc.cmsd*, or *rpc.ttydbd* services. CERT/CC and TW-CERT have the corresponding advisories for the vulnerabilities. Most of the victims are SunSPARC workstations, and Sun has released the related patches for the vulnerabilities as well [11].

Another common point for all the incidents is that the intruders were from a dial-up network, leading us several IP addresses to trace on. Furthermore, they left logs on some victim servers as a good line for finding out who they are. Later on, we helped the Computer Crime team of the Bureau of Investigation, Ministry of Justice (MJIB) investigate their case when we announced to the media.

4. Announce to the traditional and Internet media

One and half days after the first incident, TW-CERT announced the incidents and the response process to both the conventional and Internet news media for catching attentions of administrators and for preventing further damage. The media includes the press, computer magazines, online E-magazines, news groups, BBS, and the mailing lists of TW-CERT.

4. Conclusion

In this paper, we evaluate the survivability of the servers in NSYSU with 324 server hosts and 2823 public services provided for the Internet users. The results show most system administrators do not upgrade or patch system regularly and that they should improve the security level and survivability of the servers. We also present our experience on an incident response practice, a real case happened in August 1999 in

which several governmental web sites were intruded.

To evaluate and improve the network security level of Taiwan networks, we will develop scan tools and report generator for large scale scan for evaluating security level of Taiwan networks. Besides, we will propose and develop an auto-patch scheme and tools for improving system security.

References

- [1] Anonymous. "Maximum Security – A Hacker's Guide to Protecting Your Internet Site and Network," *Sams.net Publishing*, 1997
- [2] CA-99-08 - Buffer Overflow Vulnerability in rpc.cmsd (<http://www.cert.org/advisories/CA-99-08-cmsd.html>)
- [3] CA-99-05 - Vulnerability in statd exposes vulnerability in automountd (<http://www.cert.org/advisories/CA-99-05-statd-automountd.html>)
- [4] CA-98.11 - Vulnerability in ToolTalk RPC Service (<http://www.cert.org/advisories/CA-98.11.tooltalk.html>)
- [5] CERT(R) Incident Note IN-99-04 : Similar Attacks Using Various RPC Services(http://www.cert.org/incident_notes/IN-99-04.html)
- [6] CyberCop STING of NAI. (http://www.nai.com/asp_set/products/tns/ccsting_intro.asp)
- [7] Defending a Computer System using Autonomous Agents, Technical Report No. 95-022. COAST Lab, CERIAS in Purdue University. 11 March, 1994.
- [8] Freiss ,M. "Protecting Networks with SATAN," *O'Reilly & Associates, Inc.* 1998.
- [9] IDIOT, intrusion detection system from COAST Lab, CERIAS in Purdue University. (<http://www.cerias.purdue.edu/coast/coast.html>)
- [10] Lin, Biing-Jong "System Security Evaluation for Computer Networks," Master thesis of Information Management Department, NSYSU, Taiwan, 1999.
- [11] Patch List of SunRPC Service.(<http://sunsolve.sun.com/pub-cgi/show.pl>)
- [12] Taiwan Computer Emergency Response Team Incident Notes, Documentation Number : TW-IN-1999-001 (<http://www.cert.org.tw/advisory/199908/TW-IN-1999-001.txt>)