Global Information Assurance Certification Paper

SANS
Global Information Assurance Certification (GIAC)
Program

Advanced Incident Handling and Hacker Exploits

Practical Assignment
v. 1.5c

Incident Illustration

Candi A. Davidson

July 2001

Table of Contents

Executive Summary

On June 8, 2001 a RedHat Linux system version 7.0 running the FTP service version 6.0 was compromised using an FTP Format String vulnerability to exploit the system and deface a web page.

Our organization had spent the past year developing Information Technology (IT) Security Policies and Procedures for developing a strong IT Security program both technically and administratively. The network architecture configurations and the "lock down" was completed first with policy and documentation following.

Incident reporting and response became a focus. The organization had never experienced a true incident. The incident response team was made up of highly skilled IT Security and system administrator personnel across the numerous platforms that are being operated and maintained by MY-COMPANY.COM.

The Incident Response Team was notified of the incident directly by the system administrator. The response to the incident was quick. An analysis of the situation, the damages, and the best course of action were determined rapidly.

Shortly after the discovery of the incident, the system was removed from the network to reduce the likelihood of the compromised system being used to attack other systems. The incident was contained to the one system involved in the incident, the problem eliminated, and the system was restored to service in a more secure manner. Management was kept apprised of the situation at all times.

Phase 1: Preparation

Warning Banners

It is a requirement that all IT systems connected to the corporate network post a warning banner. The requirement includes local access and network connections (i.e. FTP and telnet connections). The following is an example of the warning banner used to notify users they are attempting to log into a system.

> *WARNING! This is a "MY-COMPANY.COM" computer. This system is for the use of authorized users only. By accessing and using the computer system you are consenting to system monitoring, including the monitoring of keystrokes. Unauthorized use of, or access to, this company computer system may subject you to disciplinary action and criminal prosecution.*

Policies and Procedures

Incident Handling policies and procedures were developed prior to the incident. The procedures define the roles and responsibilities of upper, middle, and lower management, IT Security

Officer, Incident Response Team, system administrators, and employees before, during, and after an incident. It has been determined who is to notify law enforcement and when. The procedures also identify how to recognize an incident.

Specific procedures are in place for reporting an incident. Everyone must know how to report an incident or suspected incident. Contact information is provided for all users. Once an incident is reported the Incident Response Team is immediately dispatched.

Local and Corporate-Wide Incident Response Team

Incident Response Teams have been developed for each regional office and at the corporate-wide level. It is considered part of the Incident Response to notify the corporate home office so the other offices can be aware of the problem and monitor their systems for the same activity.

Assignment of Responsibility

Users must sign a statement of responsibility upon account request. The statement of responsibility identifies the rules of account usage, presumption of privacy, information on password construction requirements, and "Rules of the Road". Responsibilities of systems are assigned to system administrators and IT managers, as well.

Annual IT Security Training

All employees are required to attend annual IT Security Awareness training. The types and amount of training received is in direct correlation with the responsibilities.

Users	General IT Security awareness training
IT Managers	General IT Security awareness training IT Managers' Overview Risk Management
System administrators	General IT Security awareness training IT Security for the platform administered (i.e. NT, 2000, UNIX, Linux)
IT Security and Incident Response Team	General IT Security awareness training Risk Management IT Security for all platforms

Onsite technical training for Firewalls, TCP Vulnerabilities, ISS vulnerability scanning, security planning, and platform specific technical training has been provided for system administrators and IT Security Team members.

Network Intrusion Detection

A Network Intrusion Detection system is used to monitor and analyze network traffic. Suspicious activity is collected frequently and sent to the corporate home office for a trend analysis with other corporate offices. RealSecure is currently being used for intrusion detection. Network Flight Recorder (NFR) will be added to the intrusion detection system to compliment the protection. Two or three sensors will be strategically placed on the network for improved protection.

Bulletins, Alerts, and Vendor Updates

As part of the Corporate-wide Incident Response Center's responsibilities, IT Security bulletins, virus alerts, and vendor updates are sent to each local IT Security Team sends all system administrators. The IT Security Team sends all applicable bulletins, alerts, etc. to the local system administrators.

Vulnerability Scanning

ISS vulnerability scanning is conducted on a regular basis for all systems. Vulnerability scan reports are distributed to system administrators listing all system vulnerabilities and fixes. Policies have been developed requiring security patches and hot-fixes to be applied to reduce or eliminate the vulnerabilities identified. New systems are scanned for vulnerabilities before they are allowed of out development and into production.

Annual Penetration Tests

Annual Penetration Tests are conducted by a third party. External and internal penetration tests are both performed. The third party assessment team evaluates the firewall from the outside attempting to penetrate any "edge" systems. Internal tests are performed to evaluate the level of security behind the firewall. These tests prove to be extremely valuable in evaluating the true IT Security posture of the network.

SANS Step-by-Step Guides

System administrators have access to the full set of SANS Step-by-Step Guides available. A recent purchase included the SANS Windows 2000 guide. All system administrators are strongly encouraged to use these guides to assist them in the set up of their systems and lock them down.

System Baseline Requirements

Baseline requirements have been created for all systems. The type of information stored on a system categorizes a system. For instance, a system storing personnel and salary information would have more stringent requirements than a public web server. Requirements include items

such as password construction, user account management, information management, encryption, etc.

Phase 2: Identification

Reporting of the Incident

On Friday, June 8, 2001 at 9:35 am, a system administrator reported to the local Help Desk that one of his systems had been compromised. The Help Desk immediately notified each member of the Incident Response Team by pager that an incident had occurred on a RedHat Linux 7.0 system running the RedHat Linux FTP service version 6.0. The Incident Response Team was dispatched to the location of the system with a brief description of the incident.

The incident was discovered by the administrator of the Linux system shortly after the system was brought onto the network. A web page had been altered and it was obvious that a hacker had compromised the system. The page on the system was replaced by the hacker with a statement claiming the system had been compromised and that critical company data had been stolen. The hacker also claimed that the activity was done to inform system owners and administrators of their insecure systems on the Internet.

Response to the Incident

At 9:45 am all members of the Incident Response Team arrived in the office of the system administrator where the compromised system was located. The system administrator explained the accounting of events to the previously assigned, Primary Incident Handler. The system administrator explained it was a new, test system being loaded and there was NO data on the system other than a web page that was about five years old being used solely to test the system. The compromise of the data on the system was of little or no impact to the Corporation or any of its customer base. Reloading the system from scratch would be of no concern to the system administrator.

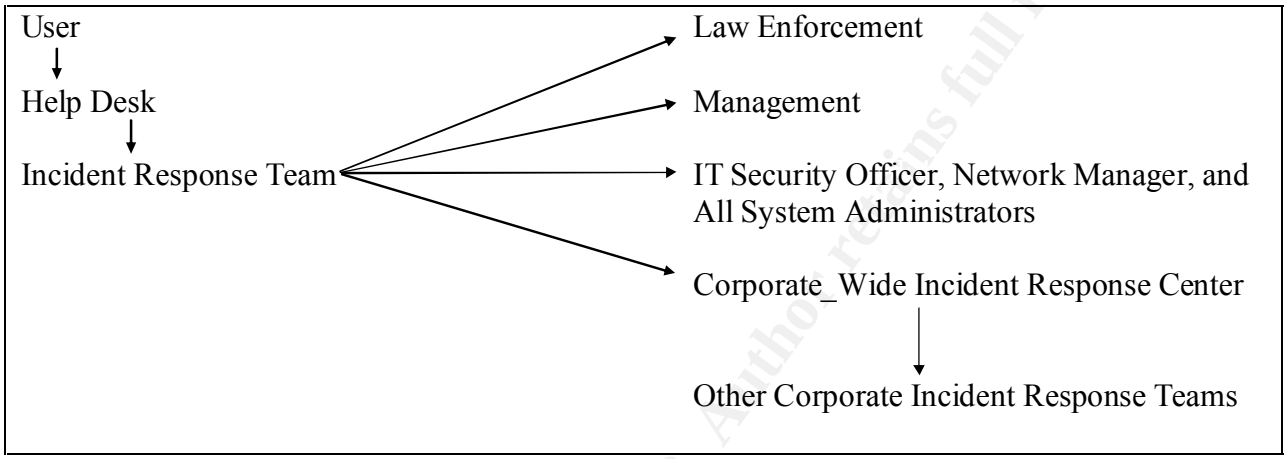
The system administrator was interviewed in an area separate of all activity on the system. A questionnaire was given to the system administrator for a description on "how the incident was discovered", where the system was on the network, and other detailed that may assist in the resolution of the incident. The system administrator was asked to fully document the accounting of events before bringing the system online, how the operating system was installed, what patches were installed, what services where running, any open ports on the firewall to accommodate the functionality of the system. All pertinent information was communicated to the incident handlers working on the system at the time.

Notification of Management, et al.

At 9:55 am, management was notified by the Incident Response Team that a test system had been compromised. The Incident Response Team would provide periodic updates on the status of the cleanup and a report of the system, network, and/or data damages once the situation was at a point were an Incident Response Team member could offer an update of the situation.

As the figure below depicts, the corporate Incident Response Center, all on-site system administrators, and Network Manager were also notified. Law enforcement was not notified immediately. The notification of law enforcement is the decision of the IT Security Officer. If an incident is relatively small in nature and minimal cost to the company, the IT Security Officer may choose not to involve law enforcement until the incident is complete.

Call tree:



The Corporate Incident Response Center notified all other MY-COMPANY.COM Incident Response Teams to be aware of the compromise and to be prepared in their respective areas. It is a standard that if one location is compromised, all other locations are put on notice. Onsite system administrators were asked to check their system logs for any unusual logging activity for the past few days and look for a particular host name and IP address.

Phase 3: Containment

At 10:00 am, the Network Manager disconnected the system from the network. It was quickly decided that the impact to the other systems could be far greater if the compromised system were left online. Power remained on the system at all times.

The physical area was secured in order to protect any evidence gathered during the containment process. Only the system administrator, the Network Manager, and the Incident Response Team were in the immediate area.

Incident Response "Jump Kit"

The Incident Response Team members have each been provided with an Incident Response "Jump Kit". Each kit includes dual boot laptops, system binaries, large capacity hard drives (SCSI and IDE) with a variety of cables (wide, narrow), small hubs, network cables, power cables, CD burner, CDs, flashlights, extra batteries, company phone books, Incident Response

Team call-out lists, management "need to know" list, writing pens, notepads, and large Ziploc bags.

The team does not have a backup communication plan. Our offices are in a very remote location and the cell phones typically do not work in our area.

Backups

At 10:35am backup of the system began. The system was backed up by the Incident Response Team and the system administrator using the *dd* command. Once the Incident Response Team completed the backup of the system, the system was powered down. The hard drive was removed, labeled, and securely stored. A replacement drive was installed in the compromised system.

The backup command issued was as follows:
 # dd if=/dev/sda of=/dev/st0

Hardware Specifications of the System

The system was a Dell Latitude laptop, 500 MHz with a 10GB Hard Drive and 128 MB Memory.

Chain of Custody

The Incident Response Team made a backup of the original hard disk to tape. The backup with date of backup, time of backup, method of backup, and signatures of those involved in the backup process were sealed in a Ziploc bag and stored in a lockable container. Intrusion Detection Logs, firewall logs, and system memory were gathered as evidence. Each Incident Response Team member confirmed each piece of evidence at the time it was gathered. One Incident Response Team member was responsible for the handling, security, and storage of the system evidence. Documentation was kept on system commands issued. The original hard drive was removed from the system and replaced with a spare.

All records were copied; the originals were signed, sealed, and labeled as evidence and delivered to the IT Security Officer with an evidence letter requiring signature at the completion of the incident.

A representative from the Corporate Incident Response Center arrived locally to receive the evidence from the IT Security Officer. The evidence including the original hard drive was transported backed to the Incident Response Center for forensic analysis.

Intrusion Detection System Logs

Intrusion Detection System logs were checked and analyzed for the system penetration points.

Event Date	Event Name	Source Port	Destination Port	Source Address Name	Destination Address Name	Tag Value	ID
6/8/01 8:43	FTP_Format_String	62252	21	xxx.xx.xx.bad	xxx.xx.xx.xxx	SITE EXEC %x %x %x %x +%x |%x	4872863
6/8/01 9:01	FTP_Format_String	62573	21	xxx.xx.xx.bad	xxx.xx.xx.xxx	SITE EXEC %x %x %x %x +%x |%x	4872897

The Intrusion Detection System was queried for all other instances of the source address or any other suspicious activity.

Firewall System Logs

The firewall logs were checked as well. A query for the target system revealed the following.

```
"14819"  "8Jun2001"  " 6:04:10"  "drop"  ""  " xxx.xx.xx.10"  " xxx.xx.xx.xxx
"  "icmp"  "77"  ""  " icmp-type 3 icmp-code 13"

"99436"  "8Jun2001"  " 7:39:35"  "accept"  "http"  " xxx.xx.xx.10"  "
xxx.xx.xx.xxx "  "tcp"  "38"  "39653"  " len 48"

"101522"  "8Jun2001"  " 7:41:10"  "reject"  "http"  " xxx.xx.xx.10"  "
xxx.xx.xx.xxx "  "tcp"  "0"  "39653"  " message SYNDefender warning: SYN ->
SYN-ACK -> RST"

"156578"  "8Jun2001"  " 8:18:14"  "accept"  "http"  " xxx.xx.xx.10"
"xxx.xx.xx.xxx"  "tcp"  "38"  "1436"  " len 60"

"162555"  "8Jun2001"  " 8:22:51"  "accept"  "ftp"  " xxx.xx.xx.10"
"xxx.xx.xx.xxx"  "tcp"  "38"  "62252"  " len 60"

"162559"  "8Jun2001"  " 8:22:51"  "drop"  ""  " xxx.xx.xx.10"
"xxx.xx.xx.xxx"  "icmp"  "77"  ""  " icmp-type 3 icmp-code 13"

"162676"  "8Jun2001"  " 8:22:59"  "accept"  "http"  " xxx.xx.xx.10"
"xxx.xx.xx.xxx"  "tcp"  "38"  "1437"  " len 60"

"162822"  "8Jun2001"  " 8:23:09"  "accept"  "http"  " xxx.xx.xx.10"
"xxx.xx.xx.xxx"  "tcp"  "38"  "1439"  " len 60"

"175754"  "8Jun2001"  " 8:32:52"  "accept"  "ftp"  " xxx.xx.xx.bad"
"xxx.xx.xx.xxx"  "tcp"  "38"  "62332"  " len 60"

"175761"  "8Jun2001"  " 8:32:52"  "drop"  ""  " xxx.xx.xx.10"
"xxx.xx.xx.xxx"  "icmp"  "77"  ""  " icmp-type 3 icmp-code 13"

"178830"  "8Jun2001"  " 8:35:18"  "accept"  "http"  " xxx.xx.xx.10"
"xxx.xx.xx.xxx"  "tcp"  "38"  "1440"  " len 60"

"182496"  "8Jun2001"  " 8:37:51"  "accept"  "http"  " xxx.xx.xx.10"
"xxx.xx.xx.xxx"  "tcp"  "38"  "1441"  " len 60"

"186770"  "8Jun2001"  " 8:40:37"  "accept"  "ftp"  " xxx.xx.xx.bad"
"xxx.xx.xx.xxx"  "tcp"  "38"  "62573"  " len 60"
```

```
"186775"  "8Jun2001"  " 8:40:37"  "drop"  ""  " xxx.xx.xx.10"
"xxx.xx.xx.xxx"  "icmp"  "77"  ""  " icmp-type 3 icmp-code 13"
```

The firewall logs were checked, searching for any other instances of the source IP. Activity of the systems in the same subnet as the compromised system was queried as well. Incoming and outgoing traffic was actively monitored.

IP Block

Once a source ID was identified by the Intrusion Detection System logs, the IP address was reported to the Corporate Incident Response Center as "Hostile" and the IP Address was immediately blocked at the firewall by the Network Manager. The Corporate Incident Response Center maintains a database of "Hostile" IP addresses. Information from each Corporate location is compiled into one centralized database for trend analysis by the Corporate Incident Response Center. All information held at the Incident Response Center is made available at the local level if necessary.

FTP_Format_String Description

A description of the FTP_Format_String exploit was researched to better inform the Incident Response Team of the full impact and possibilities of the exploit. A description of the vulnerability, type of systems affected, and removal of the vulnerability was found on the RealSecure web site.

FTP server command contains format string (FTP_Format_String).

RealSecure Network Sensor:

This signature detects an FTP protocol command with an argument that contains a "printf()-style" format specifier. This event is highly indicative of an attempt by an attacker to crash or otherwise execute code on a vulnerable FTP server, although it does not indicate whether or not the attack was successful. The command executed will be listed in the Command information field, along with its arguments.

False positives:
RealSecure Network Sensor: No false positives are known for this signature.

False negatives:
RealSecure Network Sensor: No false negatives are known for this signature.

Default risk level:
High

Sensors that have this signature:
RealSecure Network Sensor: MU 2.2

Systems affected:
FTP

Type:
Suspicious Activity

Vulnerability description:
FTP is the File Transfer Protocol, a TCP-based protocol for transferring files between systems. Many FTP servers, such as earlier versions of wu-ftpd (Washington University FTP daemon), are vulnerable to format string attacks. In a format string attack, a remote attacker sends printf()-style format specifiers as arguments to certain commands. When a vulnerable FTP server attempts to process data that contains such format strings, the data can overwrite or corrupt portions of the stack. This type of attack could lead to system failure or allow an attacker to execute arbitrary code on your FTP server.

How to remove this vulnerability:
Not all FTP servers are vulnerable to format string attacks. Contact your FTP server's vendor to determine if your system is vulnerable to a format string attack. Upgrade to the latest version of your FTP server software, and apply any patches or updates that correct format string vulnerabilities.

Phase 4: Eradication

The host name and IP address were "borrowed" from another to set up the Linux system. The system administrator had recently removed the original host from the network, but had never notified the Network Manager of the system removal. The Network Manager is responsible for allowing and disallowing of open ports through the firewall. The borrowed host name and address was listed in the firewall rule base allowing access to ports *tcp 80 http* and *tcp 21 ftp*. The attacker used the open FTP port and gained access to the system and compromised a test web page. Fortunately, the web page was an extremely old page that was loaded on the system for testing purposes only. No immediate damage or disclosure of critical data resulted from the compromise.

The Network Manager removed the firewall rule from the firewall rule base. The system host name and IP address are now retired and have removed from the DNS system as an allowable host.

Other systems in the subnet were analyzed and scanned for vulnerabilities and a network vulnerability analysis was conducted. The analysis resulted in a “Very Low” risk likelihood for further network damage and/or data compromise.

Phase 5: Recovery

Being that the system was a new test system, there were no backups, no data, and no loss. This makes the recovery phase quite simple. By 2:00 pm the same day, the operating system was

reloaded onto the system and all patches were applied, a system risk and vulnerability assessment was performed on the system.

Typically, an incident would involve the restoration of data. Backup policies have been developed requiring all systems be backed up daily, weekly, monthly, etc. Policy also requires offsite storage as well as current system documentation made available to all members of the Incident Response Team.

Baseline configuration requirements for the type of system are followed upon recovery. An audit was performed on these requirements.

The system administrator and IT Security Team monitored the system heavily for any abnormal activity or traffic for several days.

Management was notified that the Incident Response Team has evaluated the situation, removed the system from the network, eliminated the problem on the compromised system and returned the system to service. The level of damage was reported as “Very Low” and the data compromised was reported as "None". The system was involved was reported as a non-productive system with no data being stored. It was that reported there were no other systems involved in the incident. A full report was issued giving full details of the incident within three days.

Phase 6: Lessons Learned

Summary Report

Incident Report Summary Report was developed and sent to management by the Incident Response Team. As a follow-up session, a meeting was held for the Incident Response Team to discuss the incident and what could have been done differently. The purpose of the follow-up session was not to assign blame and point fingers, but to determine what could be done differently to prevent another incident from occurring again. Policy, administrative controls, technical controls, network configuration, and the IT Security architecture were all reviewed as part of the follow-up.

Follow-up with Corporate Incident Response Center

Before any follow-up assessments and reports had begun, the Corporate Incident Response Center was called and asked for a quick assessment of the activities at our location that led up to the incident and the activities during the incident. We wanted to know from them how we handled the situation.

The Corporate Incident Response Center is considered to be the experts in our organization for the simple reason is that they deal with incidents day-in and day-out. They are fully trained experienced professionals whose sole job is to respond to incidents across the country.

Their assessment of the activities included:

- The use of a Demilitarized Zone (DMZ) which we have, but have not fully implemented to avoid a hacker from getting in and wreaking havoc on the network. At least this way, the system would be cornered off.
- The use of *Safeback* as an incident response backup solution as opposed to the *dd* command or Ghost. Safeback is the product of choice for the following reasons (http://www.forensics-intl.com/safeback.html):
    - Safeback provides a detailed audit trail of the backup process for evidence documentation purposes.
    - Safeback copies all areas of the hard disk drive.
    - Safeback is an excellent method of backup with a priority of evidence preservation technology.
    - Safeback creates a non-compressed file that is an exact and unaltered duplicate of the original. This feature eliminates legal challenges concerning the potential alteration of the evidence.
    - Safeback is fast and efficient. Depending on the hardware configurations involved, the data transfer rate can exceed 50 million bytes per minute during the backup process.

Evaluation of the Incident Response Team

The Incident Response Team responded well to the incident. Only half of the members of the team have actually experienced an incident within a two to three year period. A small, relatively easy incident gave the team the needed practice. More importantly, everyone remained calm and careful in his or her actions. Many recommendations resulted in the follow-up evaluation and assessment.

The cost of the incident was estimated and reported to home office for corporate-wide analysis and reporting. The only cost realized was actual labor, which was estimated at approximately 40 hours for all members of the team. The cost of the incident did not meet the corporation's minimum amount to involve law enforcement. Otherwise, law enforcement would have been notified of the incident.

The Incident Response Team agreed unanimously about the backup procedures being changed to the use of Safeback. Though there were no problems experienced with backing up in this incident, the team sees the potential for problems. Standardizing on a product that can be used in conjunction with a drive duplicator makes the evidence collected rock-solid. Based on the recommendations from the Corporate Incident Response Center, Safeback will be used for future incidents.

The Incident Response Team also felt that each team member should have access to each of the types of systems (or at least somewhat representative of the population) for which we must respond. The team would like having an isolated location for testing response capabilities and staging war games. There should be a place to actually test these exploit scenarios in an area off of the network.

Documentation

During an incident, the documentation seemed to get the least amount of attention. This is probably an area that should first and foremost in order for the Corporation to pursue any legal avenues.

The last thing anyone wanted to do during the incident was slow down so the team member documenting all actions could catch up, especially knowing management would be wanting to know quickly what is going on. This process seemed to put more pressure on everyone involved in the incident. Essentially, the process had not been tested. We had the best responding to the incident from a systems standpoint. We had a fully capable system administrator responsible for documenting every command, every event, and every aspect of the incident. Forms had been created that would make certain items "Fill in the Blank". The process did not work 100 percent to no fault of anyone.

After the incident it was decided a tape recorder would be added to each of the Incident Response Jump Kits as a mechanism for documenting an incident. Having seen the importance of the documentation and the difficulties experienced in recording the activities. Had this been a much larger incident, our documentation had some holes in it.

The Primary Incident Handler would call out each step in the process and those working on the system(s) would call out each command entered into the system. The forms will still be used as a mechanism to collect data. It was noted that they were very helpful and organized. Each team member is responsible for making certain his or her activities are documented thoroughly and properly.

What Happened?

The system administrator was setting up a test system to be used in a production environment. The system administrator loaded RedHat Linux 7.0 onto the laptop using *the SANS Securing Linux: Step-by Step Guide*. Towards the end of the day, the system administrator decided to take the system home and complete the configuration and the installation of the patches. He mistakenly left the RedHat Linux 7.0 CD at work but had a 6.0 version at home and decided to load the FTP service from the version 6.0 CD. The installation of all of the patches was not complete.

The following day, the system administrator brought the system up on the network and requested the IT Security group perform a full ISS vulnerability scan on the system.

The combination of using an older, more vulnerable FTP service and borrowing IP addresses from retired systems made the Corporation and its networks more vulnerable to external and internal threats.

No warning banner had been installed on the local machine or for the FTP service running on the system. Policies are in place requiring Warning Banners be installed on all systems and connection services. The policy was not followed. If the incident have had more of an impact to the Corporation, there would have been no legal recourse.

Formalized policies and procedures are not in place, however, for requesting a port opening on the firewall. Nor is there any indication when a host name and IP address is no longer being utilized by a system administrator. Policies are being created and technical controls are being investigated. The system administrator is responsible for notifying the Network Manager when the system is no longer being used or the system will not be in production. System Administrators of the "Edge" systems should be especially aware and diligent of their responsibilities.

We have used this incident to bring awareness to other system administrators that it only takes a minute on the Internet with an unprotected system. The system was online for a short period of time before it was attacked. The system administrator asked that it be scanned for vulnerabilities once it was on the network. The system had already been compromised. The ISS vulnerability scan was relatively clean. See the Appendix for the Host Vulnerability Summary Report. Scanning of new systems should be done in an isolated environment before systems are brought on the site network.

It was later determined that Nessus would be used as a vulnerability scanner in addition to the standard vulnerability scanning software, ISS, used by the Corporation. This would be an attempt to identify all vulnerabilities on a system before the system went online instead of depending on one vendor product.

Overall, we have gained far more than we have lost in this experience. The Incident Response Team is more prepared, system administrators are more aware, policies are being developed, and our procedures have changed as a result.

Appendix

Host Vulnerability Summary Report

6/8/2001

Report Description
This report displays summary information detailing the organization's susceptibility to attack in relation to its policy and vulnerability conditions. Specifically, this report identifies network vulnerabilities and suggests corrective action.

Vulnerabilities are classified as high, medium and low. High-risk vulnerabilities are those that provide unauthorized access to the host, and possibly, the network.

Session Name:	Session1	**Session ID:**	108
File Name:	Session1_010608	**Template:**	Full Scan (No DoS)
Comment:		**Termination Status:**	Finished

Scan Summary Information

Hosts Scanned:	1	**Scan Start:**	2001/06/08 09:25:46
Hosts Active:	1	**Scan End:**	2001/06/08 09:55:33
Hosts Inactive:		**Elapsed:**	00:29:47

Host IP Address	DNS Name	Operating System	Vulnerability Name	Severity
xxx.xx.xx.xxx	www.mycompany.com	Red Hat Linux		
			HTTP proxy detected	Low
			ICMP timestamp requests	Low
			Traceroute can be used to map network topologies	Low

References

"Incident Handling: Step by Step, Version 1.5." The SANS Institute, 1998.

"Linux Security: Step by Step, Version 1.0." The SANS Institute, 1999.

http://www.redhat.com

ISS X-Force: http://xforce.iss.net/static/6182.php

http://www.RealSecure.com

http://www.nfr.com

Safeback Software: http://www.forensics-intl.com/safeback.html