Global Information Assurance Certification Paper

I’m from headquarters, and I am here to help!

By Shawn Roberts

Submitted to complete the practical requirement for the course:

Incident Handling and Hacker Exploits

Assignment: Document an Incident

Executive Summary:

This incident will illustrate the initial compromise of a dual boot system in a network and the subsequent compromise of three additional systems. This compromise occurred at our company's research and development subsidiary Alpha Research. My information was gathered from interviewing both the incident handlers at the company headquarters CERT and a brief interview of Alpha's uncooperative security officer. The incident reports did not include any logs of the incident nor were any maintained at the site. Security at the site appears to be an afterthought. The site has had numerous security incidents and continues to be hammered. I will attempt to illustrate the incident via the six-step incident response process with the provided information and point out how the incident could have been handled better. In addition, I will attempt to illustrate the other half of the battle I discovered. There is some disdain for those involved in information systems security no matter how polite and cooperative they attempt to be. My warm words of, 'I'm from headquarters, and I am here to help,' just did not do the trick.

This incident occurred in the fall of 2000. A Pentium system running dual-boot Windows NT 4.0 SP5 and Red Hat 5.2 was compromised by who is believed to be a script kiddie while Linux was running. The box was compromised via the WU-FTPD Remote Format String Stack Overwrite Vulnerability.

WU-ftpd stands for the Washington University ftp dameon. This dameon is included as part of many versions of the Linux and UNIX operating systems. The SITE EXEC implementation allows for remote attack of the system. This attack is similar to a buffer overflow but is actually an input validation problem. The user input goes directly into a format string for the *printf function. This input overwrites data on the stack. The function can jump into shellcode pointed to by the overwritten eip and execute arbitrary commands as root.

After this box was compromised IRC and a sniffer were installed. Utilizing the sniffer the intruder was able to learn the passwords for three additional computers and gain root access. The initial compromise was discovered upon review of the IDS logs at the site, a copy of these logs was not maintained for further analysis. The subsidiary does not operate a firewall, due to its relationship with the education community and the misconception that it is a hindrance to their work.

No research data was believed to be compromised, however this cannot be verified and is likely an erroneous assumption, a case of wishful thinking, due to the nature of the incident. Upon completion of this event, sixty-eight man-hours were expended to clean and restore the compromised systems.

Despite the passage of time and the subsequent resolution of the incident, there is the remaining defensiveness exhibited by the subsidiary and those involved in the incident. I was an outsider. The continuing occurrence of incidents at their site has brought them under some scrutiny from the executive levels.

Informing the members that I was merely researching a previous incident toward my certification and that I would change the names (and any IP addresses to protect the innocent) resulted in the initial 'you need to talk to this other person circle' It did literally end up being a circle as I was directed back to the man I originally contacted for information. I did receive a phone call from one of the subsidiary's executives questioning my intentions. I informed him that I was purely interested in the technical aspects of the incident and was not out to lambaste the subsidiary or any of its members by name. In defense of the subsidiary, I will say that I was invited to come to visit and possibly speak to those involved; however, the word 'ambush' did come to mind.

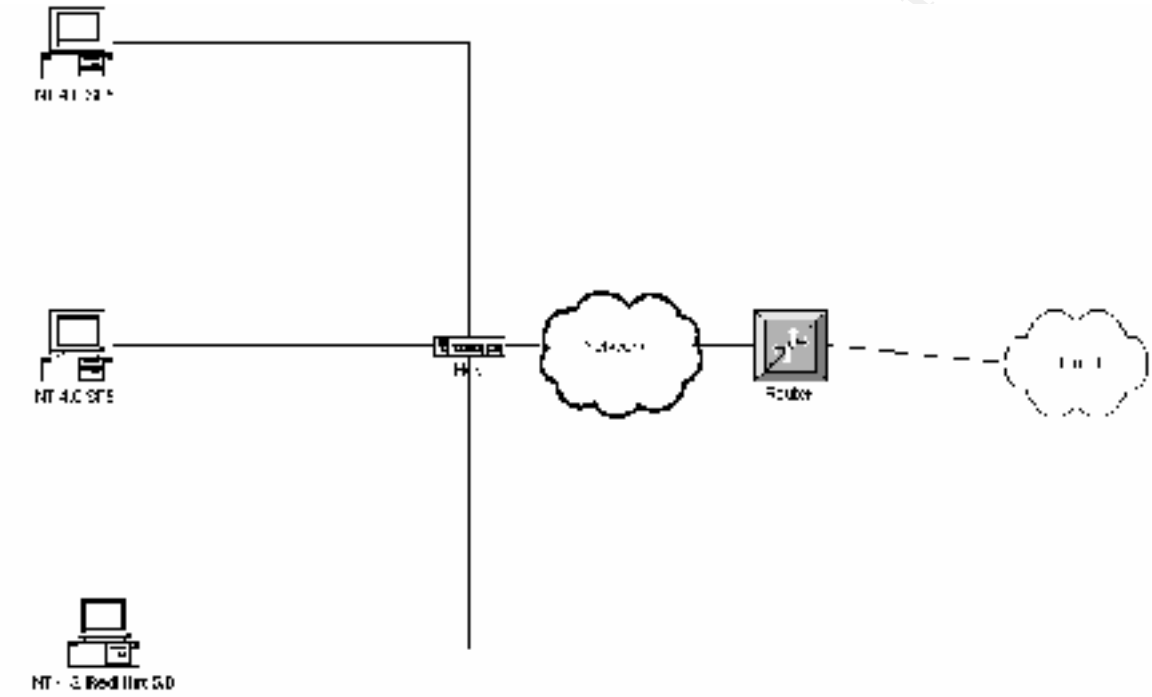

Figure 1. Network configuration of research subsidiary

Incident Handling:

A wise man once said to me 'How do you eat an elephant? Answer: One piece at a time. So to is the process of handling a computer incident.

Incident handling is divided into six stages: preparation, identification, containment, eradication, recovery and follow up. Each stage is further subdivided into additional steps. Some are chewier than others.

Preparation:

It is during this phase in which you have time think. Do not count on such a luxury during an actual incident. You must prepare your site and its personnel as well as the incident handling team. Preparation is probably the most significant of the six steps. It will determine success or failure in the handling of an incident. This stage should occur long before an incident occurs. Preparation includes several facets:

1) Policy
2) People
3) Data
4) Software/hardware
5) Communications
6) Supplies
7) Transportation
8) Space for personnel to operate
9) Power/environmental controls
10) Documentation.

A well-written policy should be concise and easy to understand. It must be short enough so there is a reasonable expectation of it being read. Warning banners should make clear the policy on any expectations of privacy. The bite size chunks idea comes into play here.

The company has an overall information security policy. Realizing that a wide variety of system requirements exist throughout the company the company instruction is general. Each site manager is expected to develop and implement his own security policy specific to his site. At Alpha Research there is a policy. It is contained in two three-inch binders and it is not widely promulgated. No reasonable expectation of it being read exists. The site does use warning banners all users see as they log on.

People: includes the system administrators, incident handlers and most importantly the users (employees). The personnel at the subsidiary are dominated by scientists and academians. The population is very fluid as visiting scientists arrive and leave to work on different projects. The employees must be more than aware of information systems security they must be educated on the security policies of the company. Several employees at the subsidiary are aware there is a security policy, but do not know what it says. If an employee is unaware of the security policy it is not worth the paper it is written on.

The incident handlers made no real preparation efforts. Like many companies the IT staff is overworked and undermanned. There are three incident handlers for over 10,000 computers in several buildings at this site. The incident handlers do not have any type of jump bag to handle an incident. The site meets company guidelines by having a contingency plan, but it is not maintained and is untested.

Communications: The incident handlers should be able to communicate effectively. A cell phone is ideal. It ensures connectivity after business hours, allowing handlers to report back to a coordination center and contact each other if they are spread out over a large site.

Supplies: Build a jump bag to allow for rapid deployment of an incident handling team. This forgoes the rapid search and seizure that would occur as they try to find everything required to handle an incident at their office.

Transportation: A method must be established for the team to reach the site in the most expeditious and economical means available.

Power/Environmental controls: This aspect is more apparent when attempting to recover a site from an act of God, but is also a consideration if teams are being sent overseas where the power distribution system differs.

Documentation: Build worksheets to fill in so the questions do not have to be remembered during a time of stress. This also provides continuity for other incidents should they occur and a manageable chain of custody.

Recommendations for this site:

1) Hire more staff to handle the workload.
2) Break down the Alpha Research's security policy into bite size pieces and promulgate it.
3) Set up an actual training program of all of the employees as they check in to ensure that they are educated on the security policy.
4) Build a jump bag of all of the necessary supplies to handle an incident:
A jump bag should include:
a) Spare HDD's to make backups.
b) Software: The latest drivers and software loaded on the machines
c) Latest Anti-virus signatures
d) Notebooks –The pages cannot be easily torn out.
e) A Micro Tape recorder (remember batteries)
f) A camera to take pictures of the scene.
g) Cell Phones with charged batteries.
h) HDD duplicator
i) Forms: Forms should be planned out during this phase so someone just has to fill in the blanks. It also is a good memory aid to ask the intelligent questions. Under stress you may forget some vital piece of information.
j) Toolkits-Do not trust the toolkits on a compromised machine. Bring your own.
k) Forensic software
l) Phone list of people to contact
m) Laptop computer
n) Hub
o) Binary backup software

A company wide incident response policy is utilized by the company CERT. This policy establishes the CERT and requires the reporting of any and all incidents at its' different subsidiaries.

Our company's incident response policy distinguishes between vulnerabilities in to two types, technical and administrative. A technical vulnerability is a hardware,

software, firmware or design deficiency that leaves a system open to compromise. An administrative vulnerability is weakness that is the result of incorrect or inadequate implementation of a system existing security features. Implementation of published patches would fall under this type of vulnerability. This incident was due to an administrative vulnerability.

The first network probe occurred six days after the tool that was used *wu-lnc.c* was posted on the hacker site www.hack.co.ca.

The Washington University ftp vulnerability has been repeatedly documented previous to this incident: Red Hat issued RHSA-2000:039-02 on 2000-6-23, CERT Advisory CA-200-13 Two Input Validation Problems in FTPD was first issued on July 7, 2000. and as a candidate for inclusion on the CVE list as CAN-2000-0573. This vulnerability was fixed by adding bounds checking by passing the status strings through %s.

Identification:
Identification is the notification that something is amiss.

The first stage of the identification phase is the notification of the appropriate officials. The appropriate official may be a troubledesk or a company CERT as in this case. The users must know who and how to report a possible incident.

The types of notifications that are applied to intrusion detection systems can easily be applied here to incident reports and identification. The four types of notifications that occur: true incidents, false positives, false negatives and subversion. False positives should be utilized as training opportunities for the incident responders. You should never admonish a user who reports an incident that is a false positive. There is no faster way to lose the cooperation of the user community. The next time a possible incident occurs they will not report it to the incident handlers until it is too late. A false negative is the more dangerous of the two. An incident is ongoing and it is not detected. Subversion occurs when the intruder has modified the systems logging capabilities and alarms so his activities in the system go unnoticed thus becoming a false negative.

Two probes from the source IP were detected the week before the incident. These probes scanned the entire network. No action was taken. These probes were overlooked until after the incident. They were discovered upon review of the IDS logs post incident.

It was during this phase that a telephone call was placed to the CERT reporting the incident. I will have two elephant burgers and super size it please. The initial phone report differred from the final report. The differences between the two reports are not a shortfall by the reporting entity. The report should be as quick and expeditious with as much of the facts or what is believed to be the facts as possible. The initial

report is just that an initial report. As an investigation commences more evidence is gathered and the facts are clarified. I

No logs from the actual incident are available for review. If the logs of the target machine were available they might have been similar to what, George Bakos a Systems engineer for EWA-IIT found when he reviewed the script and wrote to BugTraq on his findings:

Possible log entry on target box in var/log/messages:

```
Sept 28 02:46:25 drteeth ftpd[14989]: ANONYMOUS FTP LOGIN
FROM grover.tester.org [192.168.222.1],

      ?


                                        1À1Û1É°FÍ€1À1ÛC‰ÙA°?
Í€ëk^1À1É ^^A^F^Df¹ÿ^A°'Í€1À ^^A°=Í€1À1Û ^^H‰C^B1ÉþÉ1À ^^
H°^LÍ€þÉuó1À^F^I ^^H°=Í€þ^N°0þÈ^F^D1À^F^G‰v^H‰F^L‰ó N^H
V^L°^KÍ€1À1Û°^AÍ€è ÿÿÿ0bin0sh1..11
```

Mr. Bakos states that: The parent service inetd is not affected by this vulnerability. This lack of indicator could allow the attack to go undetected. There is no buffer overflow so no process will exit unexpectedly.

The source IP was initially reported to be from Switzerland. Upon further review and analysis, it was determined that the source IP was from Bulgaria. The final determination of the point of origin was made by reviewing the IRC chatter.

Containment

The goal of containment is to prevent the problem from spreading to the rest of the network.

A *team of incident handlers should be deployed* to the site to take the initial survey of the incident. Once the initial team has surveyed the site it can determine if reinforcements are required and what skill sets are needed. Ensure that the skills and number of handlers meet the needs of the incident. The team should physically secure the area. This prevents an inadvertent user from possibly making a bad situation worse or damaging the evidence on the machine. One consideration that should be remembered is that a company still has conduct business with their customers. The team should take the information developed during the identification phase and begin to build upon it.

Maintain the evidence: It is during this phase in which any evidence will be collected to turn over to law enforcement. A backup should be made of the affected systems before any modifications are made by the incident handlers. This is to protect the evidence should this go to a court of law. It is wise to have a standard operating procedure formulated as to how the backup shall be made before the incident. In addition the means (i.e. spare HDD's) should be available to make these backups (During the Preparation phase). No backups were made of the affected systems.

Lock them Away: Once the backups are made they should be stored and secured accordingly. A chain of custody should be instituted for all evidence gathered. If law enforcement arrives on the scene, ensure that they sign for any and all materials you turn over to them. This avoids finger pointing later on when no one can find the HDD with the missile designs on them. (Suggestion: Look behind the copier) The original HDD should be locked away too. Analysis should be performed on the backup. This eliminates the possibility that the evidence could be corrupted and additional backups can always be made in the future.

The system logs should be reviewed on all neighboring systems to determine if they are affected. At Alpha Research three additional boxes were found to be compromised. The compromise of the three additional boxes was via a group login and password that was the same on all of the boxes. This shows that a poor password policy was implemented at the site. This reality is contrary to the written security policy of the site that requires that passwords be changed every 90 days and group logins are *prohibited*.

The passwords and user logins were changed on all of the affected boxes. Despite the fact that a sniffer was installed on the dual boot system, the site did not implement a site wide password change. How many passwords and user logins were compromised by the sniffer cannot be accurately determined. Alpha Research's team handled the incident. They simply removed the affected boxes from the LAN by physically disconnecting them.

Incident handlers should remain low key as not to arouse the suspicions of the intruder whether he be sitting next to them in the next desk or monitoring the box from some distant machine. Once the intruder finds out that he has been discovered, all of the evidence can vaporize quickly before the handler's eyes. The intruder may have installed a booby trap as well. If the incident handler sets off the bomb and it nukes the HDD, then another backup can be made from the original and the evidence is still intact.

Eradication:
The goal of eradication is the removal of all malicious code from the compromised boxes. Eradication consists of five steps:
1) Determine the cause of the incident

2) Improve the defenses of the compromised systems and or networks
3) Perform a vulnerability analysis of the systems
4) Remove the cause of the incident
5) Utilize the most recent clean backup

This can be a daunting process that is dependent on the skill level of the intruder and his/her ability to hide backdoors in your system once it has been compromised. The incident handler must determine what configuration made the system vulnerable to an exploit. Once this vulnerability is determined it must be closed. Just to remove the hacker tools (i.e. sniffer, rootkits etc.) and install the system back on the network guarantees that it will be hacked again shortly. The *cause of the incident* was the default install of Red Hat and the failure to install the patch to fix the vulnerability. One suggestion to *improve the defenses of the network* would be to install a firewall to prevent the network from possibly being scanned and penetrated. The site does not have a firewall, and has not installed one to this day. The company CERT offered to perform a *vulnerability analysis* of the network, but was rebuffed**.** *Remove the vulnerability*: The security officer chose to completely remove Red Hat from the box, eliminating the need to install a patch. The sniffer, and IRC were removed as well. *Utilize the most recent clean backup*: No backups of the local machine existed. This eliminated the possibility of rebuilding the boxes from the last known clean backup. Instead it would have required to rebuild from scratch. The security officer determined that completely nuking the boxes would be overkill.

Recovery:
Recovery is the placement of the compromise machines back in to service. The system must be validated before it is placed back online. The machine should be monitored for at least twenty-four hours prior to placing it back on the network to ensure that it is stable. The incident handler should get the owner/operator of the machine to agree and sign to the fact that system in question is operating normally. This is to ensure that the incident handler is not blamed if the machine has problems at some future point. The system owner must decide when to reintroduce the system back into a network. Even after the owner decides to place the machine back online, it should be monitored closely for several days to ensure that some malicious code or vulnerability was left undetected. The machines were placed back on the network four days later. It is not clear who made the final decision to place the systems back on the network. One week after the systems were placed back on line another probe was detected from the same source IP.

Follow-Up:
The goal of the follow up is to document what occurred in an effort to prevent the same thing from occurring again. The key to the follow-up report is good notes by the incident handlers as the investigation progresses. The incident handlers should come to a consensus as to facts of the events. No two people will testify the same after observing the same incident. By having a united front to present to management or to a court no dissenting opinion will add to the defense attorney's case.

A database of previous incidents and solutions reduces the likelihood that the solution will have to recreated with every incident. The lessons learned are not just for the incident handlers and their method of doing business, but for the users and management. Recommendations on any required modifications or changes that need to be made should be forwarded to management and implemented. A final report was submitted to the company CERT in accordance with the company incident-reporting manual. The report stated that the logs would be mailed within a week. No logs ever arrived. I requested the logs and was informed that they no longer exist. No lessons learned or policy changes were suggested or implemented to my knowledge by Alpha Research.

Conclusion:

Alpha Research viewed this incident as nuisance. The fact that I contacted them and started asking questions of what happened and what was done in light of my recent Incident Handler training was viewed as a threat. A true irony of this situation is the fact that Alpha Research consciously does not install a firewall for fear that it might impede the free flow of ideas, but this free flow hits a major dam when it came to providing logs and information about an incident that occurred at their site. Several shortfalls in security are quickly identifiable. Recommendations:
Install software patches. The failure to install the Red Hat patch is just a symptom that there are probably several software patches that have not been installed. Install a firewall on the network. Check the IDS logs more often. Cooperate with the Company CERT and provide timely and accurate information. Break down the site security policy into bite size chunks and adhere to it.

References:

1. www.redhat.com/support/errata/RHSA-2000-039-02.html
2. www.cert.org/advisories/CA-2000-13.html
3. www.securityfocus.com
4. http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2000-0573
5. www.hack.co.za
6. www.security-focus.com/archive/1/136096
7. www.securityfocus.com/bid/1387