Global Information Assurance Certification Paper

GIAC Advanced Incident Handling and Hacker Exploits Practical Assignment

15 Aug 2000

By

Carlos Carrillo

The following summarizes an incident that took place within my organization some time ago. All of the names and IP addresses were changed for this project.

Executive Summary

At approximately 1732 hours on 18 Sep 99, an unknown individual gained root level access to ***Victim-Alpha*** computer 201.33.24.36 *(dns2.Victim-Alpha.com)*. Victim-Alpha is used as a backup Domain Name Server (DNS) for our organization.

At approximately 1040 hours on 19 Sep 99, an attacker gained root level access *to* ***Victim-Bravo***, the primary DNS server, IP address 201.33.24.3 (*dns1.Victim-Bravo.com)*.

The DNS service is used for translating canonical names such as "www.mycompany.com" to their numeric equivalent "201.33.24.36".

Internet traffic is routed using the numeric IP addresses (201.33.24.36) as opposed to the canonical names (www.mycompany.com). Canonical names exist to relieve users from the task of memorizing numerical addresses.

In this case, the attacker compromised the DNS servers via the BIND NXT vulnerability. BIND is a standard DNS application shipped with most distributions of UNIX/Linux. Both servers were running an older version of Linux (Red Hat version 4.0 kernel 2.0.18) on an Intel platform.

A warning of this vulnerability was posted by the software distributor Red Hat (REDHAT: RHSA-1999:054-01).

During the compromise, the attacker created accounts to access Internet Relay Chat (IRC), and removed logs in an attempt to conceal his/her activity. The attacker also downloaded, compiled, and executed applications on the victim servers. The software was retrieved from another, possibly compromised system. The software downloaded to the victims Alpha and Bravo was used for sniffing network traffic, scanning other systems/networks, facilitating IRC communication, and launching denial of service attacks.

Throughout the incident, the attacker scanned multiple university networks, and captured local traffic. The captured traffic resulted in the compromise of 12 local account usernames and passwords. The evidence collected (logs and server disk images) were tagged and turned over to law enforcement for further investigation and possible prosecution.

On 25 Sep 99, both systems were taken off-line and rebuilt. Each system was loaded with updated versions of the operating system and patched for known vulnerabilities. The DNS tables were restored from known good back-ups.

It should be noted that members of the Incident Response Team (IRT) and local system administrators worked long hours and weekends to resolve this matter. Their outstanding skill and professionalism resulted in minimal system downtime and the collection of valuable evidence to be used for prosecution. Because of their efforts, a potentially embarrassing situation and possible legal action against the company was avoided.

Preparation Phase

The IRT consists of five members. Members of the IRT contribute skills in all of the following areas: network intrusion detection and network monitoring, multi-platform computer forensics, database management, programming, and technical writing. Each member of the IRT helped develop the incident response checklist.

To ensure the checklists are up-to-date, monthly off-site checklist review meetings are held. Counterparts from other companies in the local area are invited to the meetings on a quarterly basis. An invitation is also extended to computer crime investigators from the local area. Top management and the corporate attorney approved the checklist procedures.

Every system in the corporate network has a logon banner. The banner, approved by the corporate attorney, clearly indicates that the system is property of the company and only authorized users can utilize the resource. Furthermore, the banner also indicates the system is subject to monitoring at any time for security and usage compliance purposes.

During an incident investigation, IRT members use PGP email, faxes, and phones (both cellular and land lines) for communication. Prior to deploying to the victim site, the lead member of the IRT selects an individual to consolidate and record (journal) all activities of the team.

The IRT "Jump Bag" or "Fly-Away-Kit" contains nearly everything the team members could need to execute disk imaging, system backups, and network monitoring.

The monitoring/forensic system consists of a custom built luggable computer containing 5 removeable drive bays, and exported power and IDE interfaces for disk imaging. The

hardware for the drive bays consists of: LS-120s, CD-RWs, 4mm tape drives, and multiple large capacity hard drives. The luggable PC also contains and internal 56K modem, and a 10/100 ethernet card. The kit also contains a flashlight, anti-static wrist guard, multi-tool kit, two 10/100 ethernet hubs, crimper, RJ-45 connectors, and 50' of Cat V cable.

The kit contains two preconfigured drives. One drive contains the latest version of Linux and the other is preloaded with Windows NT. Source disks are also contained within the kit. Each operating system is hardened for use on the compromised subnet. In high-risk monitoring, a one-way ethernet cable is used to sniff network traffic. The use of the one-way cable (transmit wires cut) ensures the sniffer's invisibility on the subnet.

Each member of the IRT carries a company issued digital cellular phone and Personal Digital Assistant (PDA). The PDA contains the incident response checklist, reference material for multiple operating systems, forensics and system backup procedures, corporate contact lists, and incident response contact lists.

Additional software contained in the kit include: Safeback, Norton Utilities, Norton Ghost, statically linked binaries of commonly trojanized commands for multiple operating systems.

Lastly, the kit also contains blank 4mm tapes, CDRs, LS-120s, 1.4 MB floppies, and 4 large capacity IDE hard drives.

Identification

On 18 Sep 1999 at 1800 hours the IRT received a call from the DNS server administrators from MyCompany. The administrators believed the server (dns2.Victim-Alpha.com) was compromised based on NID alarms and logs. The IRT advised the system administrators to unplug the ethernet cable from the hub and not touch the suspected compromised system. The IRT also asked the administrators to fax the pertinent NID logs to the IRT office and not to discuss the incident with anyone.

Members of the IRT reviewed the logs and agreed an incident did take place and an investigation should begin immediately. The IRT assembled and deployed to the site of the intrusion.

Upon arrival the next morning, the IRT secured a private work area near the server and introduced the members of the team. The IRT then gathered and reviewed all NID logs and confirmed that at approximately 1732 hours on 18 Sep 99, an unknown individual gained root level access to ***Victim-Alpha*** computer 201.33.24.36 *(dns2.Victim-Alpha.com)*. This system is used as a backup Domain Name Server (DNS). The attacker accessed the computer, and created a new user account "j1*zz*", then logged off the system.

Approximately one hour later the attacker returned and downloaded software to the system (Diagram 1). The attacker's activity triggered an alarm on the NID. The activity triggering the alarm was the string "cat /etc/password". At this point, the NID system began recording the intruder's activity.

NID logs recorded the attacker installing a compressed file named *BitchX*. BitchX is a Internet Relay Chat (IRC) program. This program allows IRC users to connect to IRC servers for chat purposes. The attacker uncompressed and installed additional files. Approximately 340 attacker files and programs were added to the Victim-Alpha.

The attacker ran these programs allowing him to further exploit the computer and obtain information from this system. Review of NID logs indicate the attacker obtained root level access on Victim-Alpha and tried to establish an Internet Relay Chat (IRC) session.

Also during this session, the attacker completely deleted several log files to aid in covering his tracks. The attacker deleted the "/var/log/messages" file.

The NID monitoring system tracked the second logon from start to completion for approximately one hour. The attack on ***Victim-Alpha*** was from 144.31.64.25 *(DIAL-1.ZZ.USNET.NET)*, located in the New Jersey area.

Containment Victim-Alpha

Once the initial assessment was complete, the IRT used the existing external tape drive connected to the server and executed a bit-by-bit image of the drive using the following command: dd if=/dev/hda of=/dev/st0. The tape used to capture the image was new, tagged by an IRT member (2 team member signatures) and locked in an office safe.

The image on the tape would later be restored to disk for forensic analysis.

The IRT consulted with the system owner and legal representatives to go over company policy and determine the next step. The consensus was to bring the system online and establish network monitoring to gather more evidence for prosecution.

Victim-Bravo

At approximately 1040 hours on 19 Sep 99, an attacker gained root level access on a second server, IP address 201.33.24.3 "*dns1.Victim-Bravo.com"*. This system is the primary domain name server for this company. Attackers now had total control over the organizational domain name service.

The attacker exploited this system before team members had a chance to patch it. The attacker was able to access this computer using the login "rewt" which triggered another alarm on the NID system. A review of the NID logs revealed the following information about the intruder's activity.

The attacker achieved complete control over the system (root level compromise—rootkit installation). The attacker remained active on Victim-Bravo for approximately 5 minutes. During this time the attacker transferred a file from a likely compromised university FTP server. On the FTP server, the attacker opened a hidden directory containing a program named "*SMURF.C"* and *"Strobe.C"*. The attacker transferred these programs to Victim-Bravo. ***Smurf*** *(diagram 3)* is a common and effective denial of service program. Smurf denies service or disables victims by generating large volumes of bogus traffic destined for the victim. ***Strobe*** is a port scanner used for pre-attack reconnaissance.

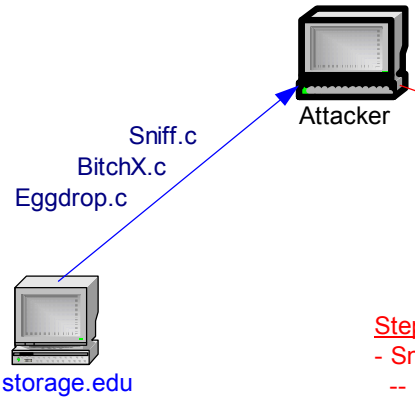
The attacker successfully compiled both programs on Victim-Bravo but only used the port scanner (Strobe) against several universities. Our belief is that he was saving the Smurf tool for retaliation against other IRC users.

The attack on the Primary DNS system was from 138.62.57.14 (DIAL-2.YY.EASTCOAST.NET), located in Massachusetts.

Containment Victim-Bravo

Victim-Bravo, the primary DNS server, was configured identically to Victim-Alpha. Upon completing the initial assessment, the IRT used the existing tape drive connected to the server and executed a bit-by-bit image of the drive using the following command: "dd if=/dev/had of=/dev/st0". The tape used to capture the image was new, tagged by an IRT member (with 2 team member signatures), and locked in an office safe with the Victim-Alpha evidence tape.

Significant Activity
18 Sep 1999
Backup DNS Server Compromised



Step 1: Transfer the tools from repository
- Attacker uses "drichie" login (likely sniffed)
  -- Files contained in "sploits" hidden directory
- 1st file transferred is "Sniff.c"
- 2nd file transferred is "BitchX.c"

Step 2 Compilation and Program Execution
- Sniff.c transferred and compiled on victim
  -- "Sniff.c" is a network monitor/wiretap
  -- Sniffer configured to capture first few bytes of packet (targeting logins and passwords)
  -- Sniffer compiled and launched on victim
     --- sniffer output saved to "/var/ ../.snifferout"
- Attacker creates account "Jizz" on victim
- Attacker compiles BitchX
- Attacker compiles Eggdrop
- Attacker uses "Jizz" account and logs onto IRC
- Attacker copies "/etc/password" file
  -- Passwords not shadowed
  -- Attacker cracks and logs in with "mhughes" account

Diagram 1

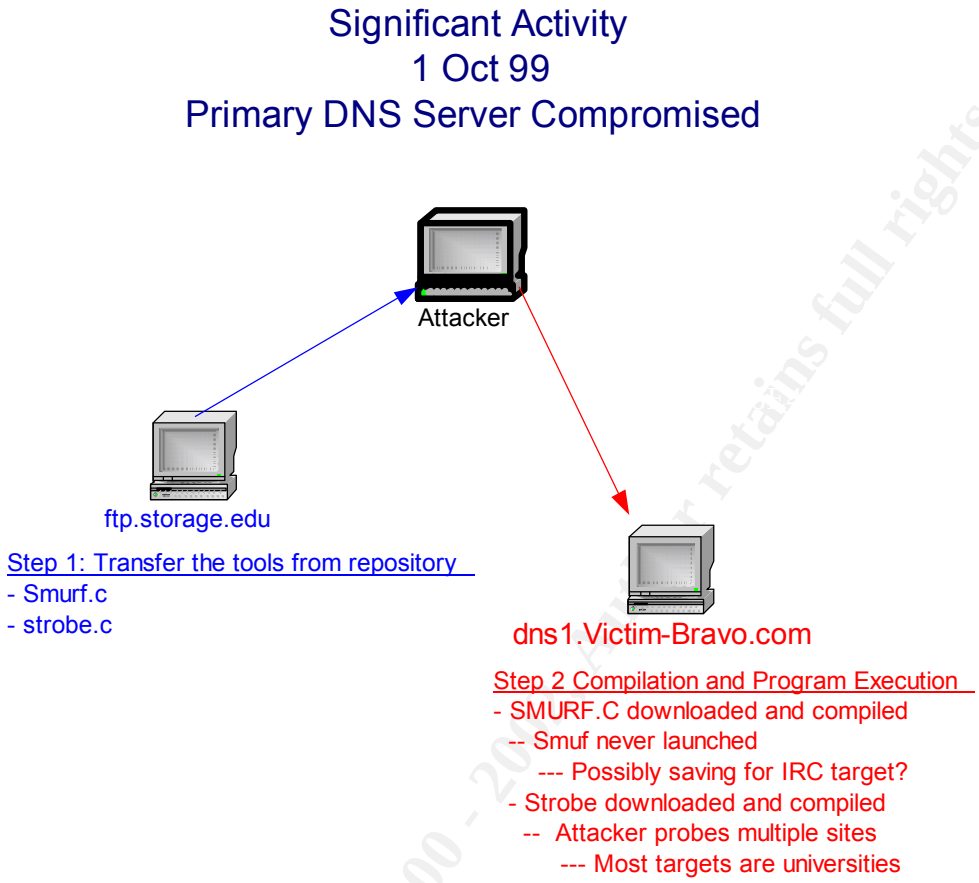


Diagram 2

Attacker Activity Profile (Victims Alpha and Bravo)

- Logs in using "rewt"
- Runs "w" command to see others active users
- Switches to user "j1zz" prior to IRC logon
- Keeps sniffer in hidden files and directory within /var
  - At times forgets where he places file
- No high port activity (strictly port 23 telnet)
- Frequently scans other networks (full sequential port scans 1-7000 big footprints)
- Conceals activity on system logs by totally deleting logs
- No on-the-fly scripting or programming

Source IP addresses and activity profiles seem indicate we are dealing with the same person on each compromised system. The attacker in this case exhibits poor activity

concealment skills. He does not use automated tools to remove his activity from logs. Instead, he totally deletes the logs. Any competent system administrator would know something is just not right on the system. Also noted is the attacker's fondness of full-blown sequential port scans. NID logs reveal the attacker ran vanilla TCP scans against multiple universities (ports 1-7000).

This type of probing activity indicates carelessness and inexperience. The attacker also likes to access the victims via the telnet port (23) as opposed to high-port access. Access via telnet is extremely careless.

Lastly, the attacker's IP indicates a dynamically assigned IP from a dial-up account (big clue is the word "dial-up" in the IP address).

Based on the monitored IRC sessions and overall activity, the consensus among the team members is that the attacker is a teenager located in the U.S.

Eradication and Recovery

The systems administrators decided to upgrade the operating systems. They opted for the current version of Red Hat Linux, applied all patches. Since the attacker ran a sniffer, all personnel on the affected subnet reset their passwords.

The system administrators requested a vulnerability scan of all machines on the network. The IRT complied with their request and found no known holes on any machines on the subnet, but did recommend disabling all unessential services (ftpd, telnetd, smtpd, httpd, etc.) on all systems. The IRT also recommended using secure shell (ssh) instead of telnet.

The IDS was also reconfigured to include an updated signature database.

The IRT continued network monitoring for 30 days. The network monitoring revealed no further suspicious activity. The IRT also conducted an unannounced system vulnerability test 60 days after the incident. The vulnerability test again revealed no known holes in the network.

Follow Up and Lessons Learned

After terminating the investigation, members of the IRT discussed the incident from start to finish. Using the incident journal as a reference, each member of the IRT was asked for feedback on key events. Each member was asked what could we have been done better or differently. After the meeting, the recorder consolidated the meeting notes and incident journal into a comprehensive report. The IRT team chief briefed the incident to senior management.

Smurf Attack Diagram

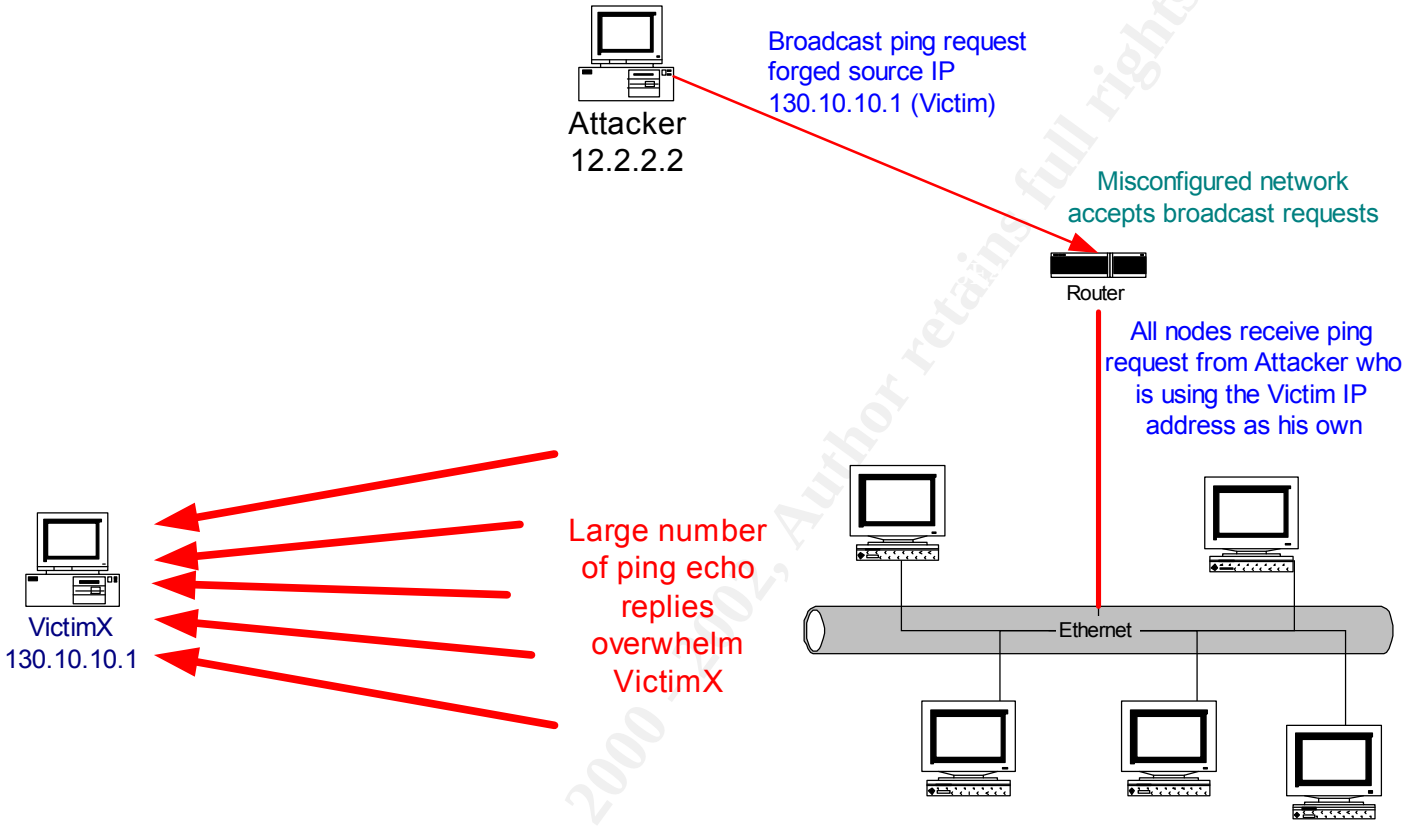


Diagram 3

Glossary of Terms

Domain Name Service (DNS)
The Domain Name System translates easy to remember "canonical" names to numerical addresses required for routing traffic across the Internet. Example: www.sans.org is the canonical name whereas 167.216.133.33 is the actual address.

Internet Relay Chat (IRC)

> IRC (Internet Relay Chat) provides a way of communicating in real time with people from all over the world. It consists of various separate networks (or "nets") of IRC servers, machines that allow users to connect to IRC. The largest nets are EFnet (the original IRC net, often having more than 32,000 people at once), Undernet, IRCnet, DALnet, and NewNet.
>
> Generally, the user (such as you) runs a program (called a "client") to connect to a server on one of the IRC nets. The server relays information to and from other servers on the same net. Recommended clients:
>
> - UNIX/shell: ircII
> - Windows: mIRC or PIRCH
> - Macintosh: Ircle
>
> Be sure to read the documentation for your client!
>
> Once connected to an IRC server on an IRC network, you will usually join one or more "channels" and converse with others there. On EFnet, there often are more than 12,000 channels, each devoted to a different topic. Conversations may be public (where everyone in a channel can see what you type) or private (messages between only two people, who may or may not be on the same channel). IRC is not a "game", and I highly recommend you treat people you meet on IRC with the same courtesy as if you were talking in person or on the phone, or there may be serious consequences.

Reference: http://www.irchelp.org/irchelp/new2irc.html#what

Secure Shell (SSH)
SSH is the secure version of Telnet. SSH sessions use IDEA and RSA encryption.

Telnet
Telnet is utility (originally UNIX) which allows you to log on as a user on a remote system.