Incident Report for a
Rootkit attack on a
Fedora workstation

GIAC Certified
Incident Handler

Practical Assignment

Version 4.00

Bonnie Norman
Track 4 / Orlando, FL
April 2004

Submitted 09/19/04
Revision 1

Table of Contents

List of Figures

Abstract

The information in this paper documents the evolution of an event into an incident, the technologies/processes used to protect an organization, and the lessons learned from the experience. I will summarize the methodologies available to the organization and the organization's ability to employ them. I chose to present this incident to demonstrate the value of deploying technologies and methodologies to protect an organization. Many times we cannot identify how something happened. Sometimes we are only left with evidence of what did and (sometimes) what did not happen. In this case I was not able to identify exactly what the name of the compromise was. I was only able to determine the most probable method that was used to place the compromise on the system, what it tried to do, how it was discovered, and what was done to contain it. This investigative work is still valuable to learn from the experience and help protect the organization's assets.

Document Conventions

When you read this practical assignment, you will see that certain words are represented in different fonts and typefaces. The types of words that are represented this way include the following:

Link	Blue highlighting and an underline indicate that a http: link is attached to the word or phrase for reference.
Quotation	A citation or quotation from a book or web site is in this style.

Statement of Purpose of the Exploit

The purpose of the exploit is to gather information about the compromised system and network that would allow exporting confidential information to an external site without the knowledge of the compromised organization.

The Exploit

A Rootkit compromise installs itself into the kernel of a Linux system and modifies system files on the system to take control of the activities of the system. In this case the exploit was scanning the compromised network. The system began connecting to external web sites. Reviewing the packets that were sent to these sites revealed that this traffic seems only to be some type of “stay alive”[1] component or a test and no information actually left the organization. I suspect that eventually the compromise would have started sending the discovered information to external http sites but I discovered the compromised system before that stage of the attack.

Exploit Name

The files that would have helped us identify the name of compromise were missing from the system when I conducted the investigation. I suspect that it happened early in the discovery when the root password was changed on the system on the compromised workstation[2]. The investigation was not able to identify exactly what the compromise was but I was able to identify several remaining files on the system that did not pass the MD5 hash check that pointed to the signature of a Root Kit compromise, several suspicious hidden directories, and 3 open security holes that could have been used by the compromise.

Operating System

Fedora Core 2 Linux
http://fedora.redhat.com/

[1] Some exploits will send packets out to confirm that they are still connected to a network, “stay alive”. If the sites they are programmed to reach are not available they then start an event, sometimes the event is to start removing traces of the exploit from the compromised system.

[2] When the machine was retrieved from the user they had rebooted the machine (after the “pull the power plug” request had been requested and completed). He changed his user password and the root password on the system.

Protocols/Services/Applications

Http was used to deliver the initial compromise and some hacking tools for the compromise to use.
Mozilla web browser was used by the compromise to download Nmap, a network scanner from a web site.
Nmap was used to scan the compromised network.

Exploit Variants

I used Rootkit Hunter from http://www.rootkit.nl/projects/rootkit_hunter.html version 1.1.6. This rootkit compromise scanner contained checks for many variants of a rootkit attack[3]. The rootkit compromise scanner[4] that I used scanned for: 55808 Trojan - Variant A, AjaKit, aPa Kit, Apache Worm, Ambient (ark) Rootkit, Balaur Rootkit, BeastKit, BOBKit, CiNIK Worm (Slapper.B variant), Danny-Boy's Abuse Kit, Devil RootKit, Dica, Dreams Rootkit, Duarawkz, Flea Linux Rootkit, FreeBSD Rootkit, Fuck`it Rootkit, GasKit, Heroin LKM, HjC Kit, ignoKit, ImperalsS-FBRK, Irix Rootkit, Kitko, Knark, Li0n Worm, Lockit / LJK2, MRK, Ni0 Rootkit, RootKit for SunOS / NSDAP, Optic Kit (Tux), Oz Rootkit, Portacelo, R3dstorm Toolkit, RSHA's rootkit, Scalper Worm, Shutdown, SHV4, Sin Rootkit, Slapper, Sneakin Rootkit, Suckit Rootkit, SunOS Rootkit, Superkit, TBD (Telnet BackDoor), TeLeKiT, T0rn Rootkit, Trojanit Kit, Tuxtendo, URK, VcKit, Volc Rootkit, X-Org SunOS Rootkit, zaRwT.KiT Rootkit.

Description and Exploit Analysis

The rootkit checker, Rootkit Hunter by Michael Boelen and Stephane Dudzinski, that I used checks for:

MD5 hash compare
Look for default files used by rootkits
Wrong file permissions for binaries
Look for suspected strings in LKM and KLD modules
Look for hidden files
Optional scan within plain text and binary files

[3] Rootkits have been around since the early 90's. There are extensive resources on the internet and in publication on Rootkit compromises. Review the references section of this document for additional information.
[4] Rootkit Hunter's project members are Michael Boelen (Michael) - Project founder / Developer and Stephane Dudzinski (a.k.a. FRLinux) - Tester

The /bin/netstat, /sbin/depmod, /sbin/ifconfig, /sbin/insmod, /sbin/modinfo, files were identified by our rootkit checker as not meeting MD5 known hashes. It also identified several vulnerabilities that also could have been exploited by this compromise were found.

The scanner found hidden directories: /etc/.pwd.lock, /etc/.aumixrc, /etc/.java. OpenSSL was found to be unpatched and vulnerable. Open SSH was found to be unpatched and vulnerable. The scanner identified that remote root login was possible and this was a method of connection that the exploit could have made use of. I found C library references to the use of the directories. /etc/.pwd.lock is used by a C library and used as a lock file, not a directory. I found reference to the file /etc/.aumixrc on bugzilla.redhat.com but not a directory by that name. I found reference to /etc.java as a file in several location but I did not find a reference to a directory by that name. The hidden directories were empty when I conducted the investigation on the machine.

The variant that infected the compromised Linux system, replaced several standard Linux system files, created hidden directories, and removed system logs to mask the compromise. There were no files left in the hidden directories when I reviewed the system.

Unlike many of the exploits I researched the programmer of this exploit was not sloppy. Information that may have helped me identify what type of compromise was placed on the system was not present. From the information I was able to gather from research I believe it was a LKM exploit variant.

Exploit References

I found excellent information on the Internet to help with this investigation.

http://staff.washington.edu/dittrich/misc/faqs/rootkits.faq
Contains excellent information on the files to check and was to get around potentially compromised files.

http://la-samhna.de/library/rootkits/list.html
Contains a list of some of the rootkits that could have compromised the system.

http://www.cs.wright.edu/people/faculty/pmateti/Courses/499/Fortification/obrien.html
Provided some additional history and Cert advisory listings to start the investigation.

http://www.sans.org/y2k/t0rn.htm

Provided an outstanding paper by Toby Miller on the T0rn rootkit compromise. This site helped me identify some the characteristics of the compromise and relate them to a rootkit attack.

http://www.securityfocus.com/guest/4871
This link contains “Analysis of the KNARK Rootkit”, by Toby Miller. This site provided good instructions on how to use Nmap and netstat to identify a compromise and what that compromise was trying to accomplish. Excepts from Toby’s paper:

“This link gives you a play by play analysis on the concepts of developing a rootkit such as KNARK.
http://packetstorm.securify.com/groups/thc/LKM_HACKING.html
If you want to learn more about LKM programming this is the link for you.
http://howto.tucows.com/LDP/LDP/lkmpg
Phrack has some great information on exploiting the Linux Kernel as well as hardening the Linux Kernel.
http://www.2600.com/phrack/p52-06.html
and
http://www.2600.com/phrack/p52-18.html“

The links Toby provided in this paper were also good references of information for my research.

The rootkit compromise scanner that I used can be found at:
http://www.rootkit.nl/projects/rootkit_hunter.html
Rootkit Hunter by Michael Boelen and Stephane Dudzinski
Link verified 09-19-04

Platforms/Environments

The environment consisted of Windows XP, Windows 2000, and all versions of Linux workstations. The environment also has Windows 2000 and 2003 servers, Linux, Novell, and HP Unix servers. The network is managed with Cisco technologies, VLANs, and firewalls. Internet access is controlled through a proxy server, firewall, DMZ, and a second firewall. Authentication to the proxy server is serviced by NDS (Novell Directory Services).

Victim's Platform

The initial victim is Fedora Core 2 Linux. The exploit, once installed on the Linux workstation, was trying to scan and attach to Windows 2000 servers and workstations from the infected workstation.

Source Network (Attacker)

I reviewed the network traffic that had traveled to and from the compromised workstation. I compared it to other users in the organization's traffic during the same time period. The variances were a connection to a shopping site that redirected the user to a seller's site that did not have the same IP address at the time of the investigation. The IP address that the compromised workstation connected to for the seller did not ping during the duration of the investigation. The IP address that the scanning tool was downloaded from did not respond to http, tracert, or ping requests during the investigation period. The IP address belonged to a third world country. I consulted our law enforcement resources about trying to further determine where the initial traffic came from and was advised that I didn't have enough information or identified that we had endured damages to warrant their involvement.

Target Network

The target network is an Ethernet network. The primary protocol is IP and is a subnetted utilizing the private networking structures of 10.x.x.x and 196.168.x.x. The internal addresses are NAT serviced by leased public addresses. The internal network is connected to the Internet through two tier 2 ISP vendors through a DMZ, Firewall, proxy servers, and VLANs.

Network Diagram

Below is a basic drawing of the compromised part of the network. Components were omitted from the drawing that were identified to be uninvolved in the compromise. This was determined by reviewing IPS sensors logs.

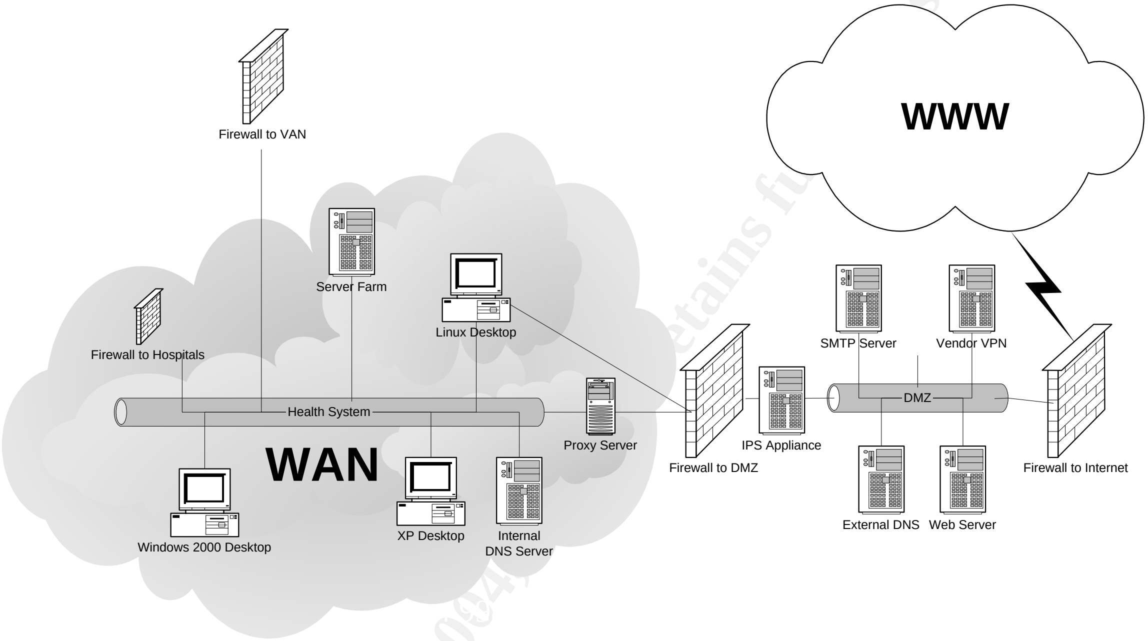


Figure 1: Compromised Network

The Attack Process

My conclusion was the following:

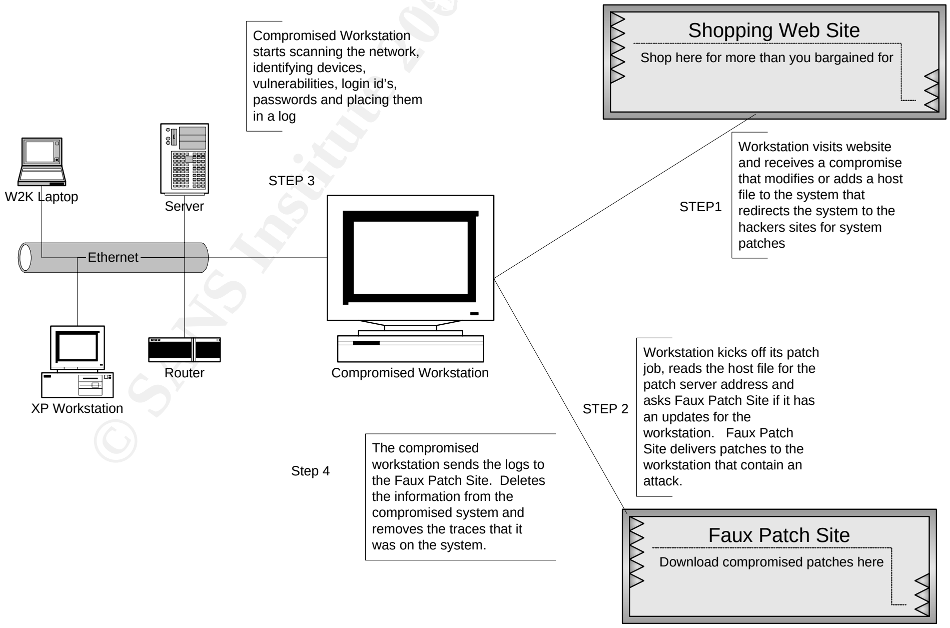
The compromised system received a host file from an external site that redirected the system to an invalid address for a patch. The compromised patches were installed on the Linux workstation by the user. The compromise downloaded a scanner utility and began scanning the network.

How The Exploit Works

The purpose of the attack is to scan the network for systems with vulnerabilities. Exploit discovered vulnerabilities to gain access to the information held on the compromised systems. Export any information of interest to an external location.

Description and Diagram of the Attack

The exploit was accomplished by compromising an internal system. The compromised internal system then began scanning the systems and infrastructure visible to it. It gathered information about the systems and sent the information to an external http site.



Compromised Workstation starts scanning the network, identifying devices, vulnerabilities, login id's, passwords and placing them in a log

Workstation visits website and receives a compromise that modifies or adds a host file to the system that redirects the system to the hackers sites for system patches

Workstation kicks off its patch job, reads the host file for the patch server address and asks Faux Patch Site if it has an updates for the workstation. Faux Patch Site delivers patches to the workstation that contain an attack.

The compromised workstation sends the logs to the Faux Patch Site. Deletes the information from the compromised system and removes the traces that it was on the system.

Figure 2: Diagram of Exploit

Signature of the Attack

MD5 hash checks do not match for system files on the workstation.
Normal system, and activity logs are missing from the system
A workstation's traffic patterns change
A workstation scans a network
A workstation's host file contains a new unknown or wrong address
A workstation's resolv.conf file is pointing to an external address for DNS queries

How to Protect Against the Attack

Build gold images for all servers and workstations standards. In our environment a gold image is the standard image that is built from trusted media, tested to be clean of any compromises, and protected. The master gold image is only accessed, offline from the live network, to build the image server or media all other machines are created from. Only absolutely essential ports and services should be opened/started for the gold image.

Every machine on the production network must use the standard gold image to start with. As a workstation is customized changes must be documented. Special builds are only allowed on a test, segregated network (no access to the live network)!

Deploy workstation image control technologies policies (Windows or Novell) to force a workstation's security settings everytime it logins to the network for services.

Deploy a proxy server to protect the workstations on your network.

Frequently conduct internal scans for machines that have ports open that they should not have open.

Deploy IPS (Intrusion Protection Systems and Sensors) technologies to protect the network. Deploy as many firewalls as they will pay for.

Manage your VLANs to keep "need to see" traffic bundled together. It's not just a performance issue any more you also gain a little more security.

Check the validity of all patches, quarantine them, keep extensive patch management records and copies of all patches. If you don't have automated technologies (IDS "Intrusion Detection System" or IPS "Intrusion Prevention System") then closely watch all systems for at least 7 days after patches are applied. Watch the logs and scanner traffic if you have it.

Get the staff that has superuser rights on board with security. Involve them in the planning and protection process. If they help develop and monitor security they are less likely to ignore the policies and procedures.

If possible eliminate all non-business related surfing. If they won't let you disable all external non-business surfing start with lobbying for blocking the highest risk sites. Demonstrate Steganography to the executives. Show them what can be hidden in those picture jokes that are being sent out of the organization via email or pulled into the organization from web sites. Pull traffic (bandwidth usage and hours spent surfing, productivity is usually a hot button) and risk reports. This may inspire them to let you block some. The decision-makers may let you turn non-business traffic off little by little when you continually show them their risks.

If possible eliminate all personal email account access from within the business network.

Provide employee education classes to teach them how to protect their computers at home. Really, this works. When they start caring about who's in their home computer they start caring about who's in their work computer too. If they are going to be dishonest and steal from you those people are going to learn how without your class. The people that do things in error cause more problems and expense to the organization than the intentional criminal.

The Incident Handling Process

The organization uses the SANS 6 Primary Phases +1 incident handling Process. These steps are:

- Preparation
- Identification
- Containment
- Eradication
- Recovery
- Lessons Learned
- Regulatory Reporting (this is the organizations extra step)

Preparation Phase

Policy

Warning Banners:

The organization has deployed warning banners on NDS, all severs, and all applications. Warning banners must be accepted to complete workstation login, authentication into the network, and access to an application. Warning banners must be accepted to access secured areas of applications. An example of this would be accessing the psychiatry notes area of a medical record. The user may have the authority to access that information but they must also have the necessity for the care plan that they are reviewing the record for. The warning banner prompts them to consider if they need to access this part of the medical record.

Response Strategies:

The organization is a large non-profit healthcare system. There are extensive regulatory and certification (accreditation and licensor) requirements for incident response from a clinical and operational perspective. The response strategies have executive committee sponsorship and ownership by Corporate Compliance with a Vice President as its steward.

A draft organizational information technology compromise incident response policy and procedure had progressed through 3 generations of revisions. No deadline had been set for final adoption of a policy and procedure. Procedures and methodologies have been implemented by the organization from the requirements of these drafts. The drafts were modified to include policy/procedure needs that were discovered through any lessons learned from the incidents that had been experienced by the organization to date.

The organization has established, tested, and implemented, response policy and procedures for all other disciplines of the organization. In all of these policies and procedures there is a "downtime" component of their plan should they ever be impacted by any incident that changed their normal operations protocols. This includes any loss of access to information through technology. Their plans hold short and long term plans for "downtime".

Each established and drafted policy/procedure contains a documented communications plan and a list of decision-makers component. Each document holds extensive lists of identified potential events. These event plans included a decision tree for when law enforcement will be brought into the event.

The organization employs community, state, and federal, law enforcement officers during their off hours from their agencies as a major portion of the physical security arm of the organization. Many of the other members of the organization's security force are retired members of these agencies. These employees are part of most response team so involvement of law enforcement is usually an early part of most events.

Corporate Compliance is an active member of the local chapter of HTCIA. Response team members have completed Kennesaw State University education offerings from the Southeast Cyber Crime Institute, SANS, Microsoft security training, Unix security training, Novell security training, and regulatory requirement education.

Peer Notification

The organization is an active member of the Atlanta Healthcare Security Counsel. This organization shares information with each other to help identify and deploy best practice services and technologies for their respective entities. Best practice is a required but undefined component of the HIPAA Privacy and Security regulation that each of the member health systems must operate under.

Extranets

The organization has established the requirement to execute a Business Associate Agreement or a Trading Partner Agreement[5] with every external entity that may have access to the information entrusted to the Healthcare System. Prior to establishment of either one of these agreements a complete security survey and review of the applying organization is conducted by Information Technology and Corporate Compliance divisions. A component of this review is a review of the applying organization's incident policies/procedures and response team. A component of the executed agreement is the requirement to provide, and maintain current, response team and reporting methodologies (and to report!). The HIPAA Regulation does not require the organization to monitor the associate or partner but they are responsible to the Federal Government for the actions of the associate/partner. The agreement holds the associate/partner responsible to healthcare system. The agreement also identifies the healthcare system as the decision-maker with regard to any event involving protected health information received from or gathered on behalf of the healthcare system.

The organization does not allow confidential or protected health information to leave the organization without encryption or a point to point connection that is firewalled at each end. This is controlled by policy, education, monitoring, and deployed technologies.

Application Service Provider (ASP) models are not permitted by the organization. All applications used by the organization are housed within the organization. All electronic information entrusted to the organization is protected by VLANs, Routers, Firewalls, Proxy Servers, DMZ, VPNs, Encryption, and Point to Point Connections. IPS sensors are deployed at all points of egress/ingress.

Management Support

Weekly summary of events reports are submitted to executives of Corporate Compliance. Monthly reports of Internet Usage, Exception to Policy Requests/Approvals, Policy Violations, and Security Events are presented to executives of Information

[5] Business Associate Agreement and the Trading Partner Agreement, is a requirement of the HIPAA Privacy Regulation (sample Business Associate Agreement available at http://www.hhs.gov/ocr/hipaa/contractprov.html, sample Trading Partner Agreement available at http://www.cms.hhs.gov/providers/edi/cob_tpa.asp?)

Management Counsel, Corporate Compliance, Information Technology, and Clinical Initiatives.

Building a Team

Incident Response Team has core members of Vice President of Corporate Compliance and Risk Management, Director of Corporate Compliance, Corporate Security Officer, Corporate Privacy Officer, Compliance Investigator, System Security Engineer, System Security Administrator, Director of Information Systems, Director of Physical Security, Director of Human Resources, or their delegates. Event driven team members are Corporate Counsel, Director of Clinical Initiatives, Divisional Vice Presidents of the affected or involved organizational team, Director of Facilities Management, Marketing/Public Affairs Representative, Business Associate or Trading Partner Representative/Response Team.

Command posts are permanently established at each organizational major site for all types of events. Minor site command centers are established in the site manager's office or conference room. A Central Command center for information compliance/security incidents is located in Corporate Compliance/Risk Management. Pre-identified potential events were defined with risk weights. The Vice President of Compliance/Risk Management weights new events during the initial discovery of the event. This risk weight determines the frequency of status reports and to what level of the organization these reports are delivered. Command center deployment is tested twice a year at every major site and annually at minor sites with mock drills.

Checklist and Team Issues

System check lists only existed for systems that had gone through an audit 2 years prior to the event. Check lists for new or changed systems since the last audit only existed in the minds and note pads of the system administrators.

Response team shift staggers and comp time are built into HR policies.

Emergency Communication Plan

Emergency Communications Plans are established and tested during mock events at major and minor sites. Core response team members have current communications information with them at all times. Designated Site Coordinators hold an offline copy of the response plan (which includes communications) that is reviewed and updated quarterly.

Access to Systems & Data

By established policy and procedure, the Corporate Security Officer and the Compliance System Security Engineer hold the superuser id's and passwords for all systems, firewalls, switches, routers, proxy servers, web servers, applications, and databases. All superuser id's and passwords are changed every 90 days or when a workforce member that had knowledge of the ID or password changes roles, or leaves the organization. These passwords are also changed after usage of the superuser id and password for an event. Documentation of these Ids and passwords are securely delivered and vaulted in Corporate Compliance. Policy and procedure requires that breaking of the seal on the secured documents be witnessed and signed off on.

Point of Contact and Resources

Policy and Procedures for established points of contact, etc. are outlined in, Building A Team, above. Secure communications are established and tested with mock events. Supplies are maintained in Corporate Compliance and at established major site command centers.

Reporting Facilities

New employees are trained on all policies and procedures through e-learning methods and initial orientation. Employees have mandatory etraining annual reviewing all policies/procedures and introducing them to any new or modified documents. Reporting methodologies that are provide to them is a 7x24 help desk, a 7x24 confidential compliance hotline, and a 8-4, M-F, Live HIPAA Help Line. Calls to the compliance hotline are not recorded and the caller has the option to remain anonymous.

Establish A War Room

Response centers are established at each major site and in Corporate Compliance. All of these rooms are internal rooms, badge access controlled, entrance to the room is monitored by video camera and the security command center for the facility 7x24. Rooms are equipped with full multi-media, white boards, flip charts, general office supplies, recording media, 4 data jacks, quad data jacks on all 4 walls that are supported by site generators (at the major sites). Data switches, VCR, Video Camera, Digital Camera, DVD Player, DVD Recorder, TV, Tape Recorders, and Forensic Investigation Technologies are also available for deployment from the Corporate Compliance command center,

Train the Team

Response Teams practice twice a year at every major site and annually at minor sites with mock drills.

System Admin. Relationships

Daily business events intertwine the core response team members and they have good relationships well established.

Jump Bag

All investigators maintain jump bags. The jump bags include:

Dual OS Laptop (Windows 2K and Redhat Enterprise Workstation)	Laptop has: 10/100 NIC, wireless NIC, Cellular Modem, Standard modem, CDRW, DVDRW+
1-100 ft RJ45 Cat5 Ethernet Straight Through Cable	5-25 ft RJ45 Cat5 Ethernet Straight Through Cables
2-25 ft RJ9 Phone Cables	Original Media for all OS versions in the organization
Bundle of assorted zip ties	25 spindle of CDRW disks
25 spindle of DVDR+ disks	256MB USB Thumb Drive
USB Hard Drive	5 port 1/100 Hub
25 box of 1.44 floppy disks	2-10 ft RJ45 Cat5 Crossover Cables
PC Anywhere	Bi-directional Parallel cable
10 Investigation Notebooks	10 Automatic Pencils
10 Pens	10 pack of post-it flags
20 pack of 2x2 post-its	5X10 High Gloss White Oil Cloth (portable whiteboard)
Whiteboard marker kit (includes eraser)	1 roll of duct tape
5 sharpie markers	Norton Ghost
Digital Camera	Digital Voice Recorder
Blank media for camera and recorder	Penguin Sleuth Kit
Windows 2000 Resource Kit	Windows XP Resource Kit
Win98 boot disk with basic disk utilities	Cell phone
Extra cell phone batteries	Large Zip Lock Evidence Bags
Static Free Evidence Bags	Stapler
Box of staples	Box of small and large paper clips
Box of small and large alligator clips	24 Desiccants for handling moisture in bags

2 Copies of current policies and procedures	10 Copies of Incident Handling Forms - Security Incident Report - Chain of Trust Labels and Log
Phone message pads	Scotch tape
Screw driver set	Wire cutter/stripers
Scissors	Flashlight
Battery operated CD Player/Radio	8 triple A batteries
8 double A batteries	8 D batteries
5 Female-to-female RJ-45 connectors	1 Female-to-female RJ-9 connectors
25 business cards	Company phone directory
Compliance department emergency contact lists	Company Emergency Plan Binder
The Corporate Compliance Division holds the tools:	
SF-5000, Forensics Investigative/Cyber-crime Hard Drive Cloning Device	Encase Enterprise Investigation System
Forensics Examiners Tool Kit	3 CPUs for use with forensic copies
5 HD for use to make forensic copies	1000 piece tool kit

Existing Incident Handling Procedures

The organization has extensive handling procedures for all types of incidents and disasters. For this incident the procedures were:

Identify an event
Verify an incident
Review With Security Officer
Contain
Investigate Risk Factors
Set Risk Level
Set Communication Schedule
Establish Incident Team
Establish Response Team
Establish Document/Evidence Controls
Respond to Incident
Perform Investigation
Review Evidence with Incident Team
Develop Action Plan
Execute Action Plan
Review Incident (Lessons Learned)
Develop new Policies and Procedures
Develop Plan of Corrective Actions
Complete Required Compliance Documentation

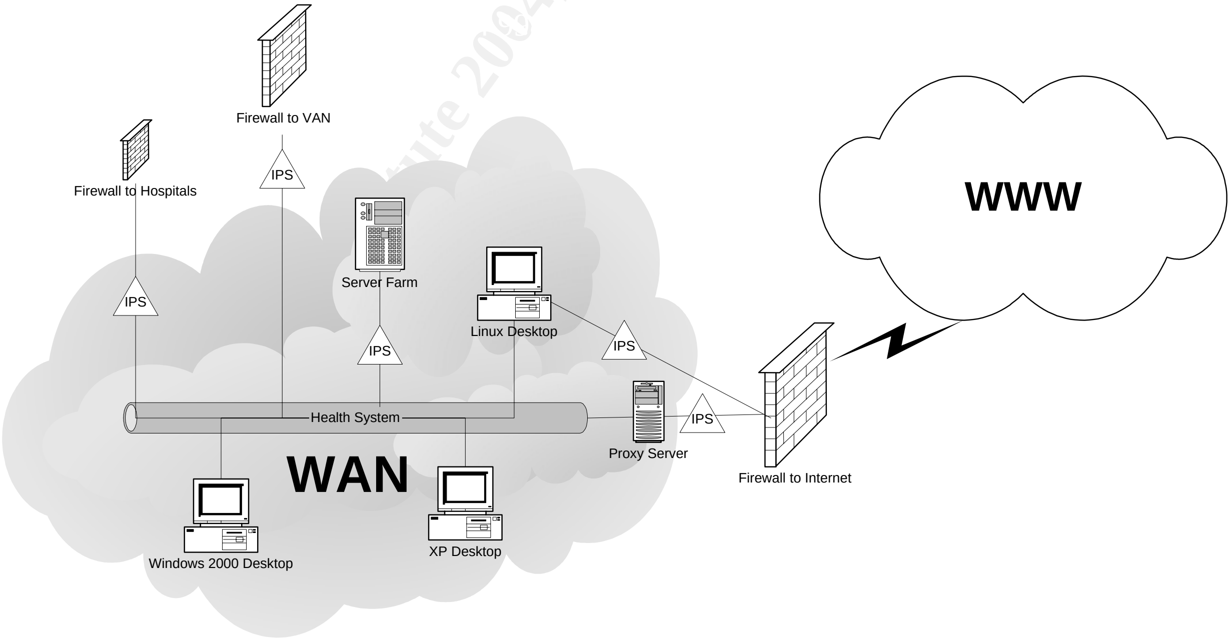
Existing Countermeasures

The organization utilizes an Asset Inventory Database, Directory Services Auditing, IPS system (Intrusion Protection System), a proxy server with complete logging and filters, an Internet traffic pattern monitoring system, a full packet reconstruction system, Firewalls, Proxy Servers, VLANs, Network Infrastructure Monitoring Tools. These systems have smtp notifications turned on to notify the monitoring staff (investigators) that review the alerts for what these systems feel are high threats. The monitoring staff also reviews the other priority system alerts twice a day.

The IPS system will ignore, alert, or block traffic based on predefined rules or patters of behavior that it notices on the network. If a workstation has always just gone to one system and now starts trying to connect to all systems it will block that traffic and send an alert to the investigator. It will also log it as a high priority threat in the system logs for review.

The full packet reconstruction system captures all IP information on the segment it monitors and reconstructs the traffic based upon the sending or receiving IP address for the reconstruction request.

Figure 3: Sensors



The Internet traffic pattern monitoring system has several classifications of threats that it monitors packets for. This monitoring system will look inside of a packet and review the words contained in it, determine if it meets the criteria for one of the monitoring filters, capture the packets that would allow it to re-assemble the screen that is being presented to the screen of the computer receiving the information, log the IP address, the category of the filter, and the date/time information of the event.

Incident Handling Team

The incident handling team consisted of two wan engineers, a system security engineer, application security engineer, Information Security Officer, Director of Information Services, physical security representative, executive committee sponsorship, and ownership by Corporate Compliance with the Vice President as its steward.

The incident response team consisted of a system security engineer, application security engineer, and Information Security Officer.

Policy Examples

Extensive policies and procedures have been established for remote access, vendor access, information encryption, telecommuting, as well as, information classification, destruction, protection, and controls.

Appropriate use policies and procedures have been established for hardware, software, email, network access/use, and Internet access/acceptable use. Appropriate access, and need to know, policies and procedures have been established for every data element as well as for each system that holds or has access to that information in the organization, or is held by their Business Associates/Trading Partners.

Many of the policies and procedures were refined to meet the requirements of the HIPAA regulation. The HIPAA regulation may either contain a component that requires a technology that the organization has deployed or has identified it as addressable by technology safeguards or by some other methodology. Some policies and procedures that the organization has deployed are defined and required by JCAHO. JCAHO accreditation is crucial to the success of the organization. Meeting and exceeding the HIPAA and JCAHO requirements help the organization provide world class service to their patients.

Identification Phase

I was reviewing the Internet traffic pattern monitoring system when I noticed in the hacking threat filter logs that traffic for a workstation had downloaded netstat and Nmap[6]. I then pulled all Internet activity for the workstation and saw consistent traffic for the workstation to normal sites for 30 days until 3 days prior. At that time normal activity ended. The activity just prior was to the change was a YUM generated event that downloaded updates to the machine. Early the next morning, before staff usually arrived, the logs reflected that someone or some process downloaded netstat and Nmap onto the machine.

I reviewed the logs from the IPS system that resided between the identified desktop and the server farm. The identified workstation had been scanning the network holding the server farm for two days. But alarms had not been tripped.

I ran Superscan against the identified workstation and the workstation did not reply with a host name. The organization's standard requires a host name set to serial number of the workstation. Superscan reported PCanywhere remote control host mode was running on the workstation (This turned out to be VNC). I then reviewed the asset database for the assigned location of the workstation based upon the IP address. There was no record in the asset database for the workstation by name or by IP address. I then contacted the LAN/WAN team and requested that they locate the IP address via switch port traffic. The workstation was identified as a Linux OS workstation being used by one of the system superusers it was his development machine.

I contacted the superuser's manager and requested that the power plug for the workstation be pulled for a hard shut down and advised him that an investigator would be at the location shortly to secure the machine. There was an Application Security Engineer on site at a meeting where the compromised box was located. He was contacted to retrieve and secure the machine.

The Security Officer, Director of Compliance, CIO, Director of Network Services, and the VP of Compliance/Risk Management were advised of the event. Progress updates were then provided to them, at a minimum, every 4 hours, via voice mail and email, until the completion of the recovery plan. By policy, the response investigation team for this type of incident was defined as the Director of Compliance, the Security Officer, a

[6] Nmap is a network-scanning tool commonly used by hackers to perform reconnaissance on a network. Netstat is a utility that is a standard file on Linux. The netstat file that was downloaded was part of the compromise that would report inaccurate information to an administrator if they ran netstat.

Network Security Engineer, and an Application Security Engineer. Each team member initiated a numbered page journal for the event and labeled the books with the event number, the start date, their name, and initialed the cover of the journal. A master investigation binder was established and stored in the investigation vault. A Bates Stamp code was initiated and used on all discovery documents created from the investigation.

When the investigator arrived to secure the machine it was unplugged from the power as requested. The investigator was advised that the machine was configured with a power-on password and a non-standard administrator password. The password was requested. The user did not want anyone to have his password. The user powered on the workstation and changed the administrator password. When he tried to launch the GUI for the workstation it failed so he had to change it manually. He advised the investigator that the workstation had been acting like this for the last 3 days. The investigator was advised that there were two more machines, a Windows XP OS and another Linux machine that was assigned to the same person. The user had already changed his password on these machines and they had already been turned off and disconnected. They had been shut down gracefully, using the system shutdown command. The two other machines were offered for investigation and secured by the investigator. The investigator completed chain of custody documents for the equipment and moved the workstations to the Investigation War Room.

I pulled a full packet reconstruction event from the full packet capture system for all devices that communicated with the suspected compromised workstation (Linux workstation). There was very little traffic until 24 hours prior. The system reflected scanning of all the systems in the server farm by the Linux workstation and http traffic to external addresses that the workstation had not communicated with before. Reconstruction of the packets to these external sites did not reflect any information being sent to/from these sites but a normal request for the home page and delivery of that normal home page to the compromised workstation.

I pulled the Proxy server logs for the Linux workstation and compared to the full packet reconstruction system traffic logs. They did not match. There were two different accounts used for Internet traffic for this IP address in the logs. Traffic for the first account was traveling through the proxy server and traffic for the second account was passing directly out to the Internet through the firewall without proxy. Traffic that traveled in/out of the proxy server to the external addresses was a generic account usually locked to kiosk workstations for Internet access. Traffic that was travelling directly in/out through the firewall was using the login id of the assigned user of the Linux workstation.

I pulled Proxy server logs and full packet reconstruction events for all devices that showed up in the scan and a repetitive job of this report was built to deliver every morning to all investigation response team for the next fourteen days. The systems that the Linux workstation scanned were servers that normally would have no Internet traffic, in or out bound. The reports did not reflect any change in the servers traffic patterns, scanning by the servers, or any attempt to connect to the WWW or be connected to by the WWW. A firewall entry was added to block the IP addresses that the http traffic that had been established to from the compromised Linux workstation.

I forensically cloned the disk for all workstations retrieved were using a Forensics Investigative/Cyber-crime Hard Drive Cloning Device. During the cloning process the cloning machine reported a hardware error for the second Linux workstation's hard drive and no clone could be created. The assigned user for the workstations was contacted and he advised the investigation team that the machine had not booted in 3 weeks and that he had been seeing hardware errors for months. I sealed and labeled the original drives and secured them in the investigation vault.

I placed the clone drive from the Linux workstation in the Linux workstation chassis. I booted the Linux workstation with the Penguin Sleuth Kit to review the hard drive in read-only mode. I reviewed the system to try to determine what had most recently happened on the machine. I reviewed the system for user information. The only user directories I found on the system were for root, the assigned user, and the kiosk account that was seen in the proxy server logs. I looked for network configuration files and activity logs. Secure and messages files in /log were empty. The access.log file in /log/cups was empty. The host file contained entries to external sites holding addresses in third world countries and the resolv.conf DNS configuration pointed to an external DNS source IP address located in a third world country.

I used a formatted floppy a clean install Linux workstation and placed the floppy in the drive of the Linux workstation that was being investigated. I placed the most current kernel rootkit checker (found by searching through threads on freshmeat.net) on a USB drive. I mounted the floppy drive and the USB drive and ran the rootkit checker on the machine. I saved the rootkit checker log to the floppy drive. I started an investigation CDRW and placed a copy of the log files from all systems collected to-date on the disk and added the disk to the evidence held in the master investigation binder.

The rootkit checker log reflected 5 files that did not meet the md5 hash from their expected results.

I concluded from the results of the rootkit checker, the hidden directories, the missing user files, the missing logs, the missing GUI, and the unique network configuration files that the system kernel had been compromised by a rootkit. The organization had pre-established a reciprocal arrangement with other local organization's security investigators to confidentially review each other findings and hypothesis. I sent my findings and hypothesis to 2 external references for analysis confirmation. The two external sources confirmed the conclusion.

The cloned drive of the XP OS workstation was a FAT drive, the cloning device reported this file type during the cloning process. I booted the XP workstation with a DOS bootable floppy disk. There were no notable findings on this machine.

Incident Timeline

Event Day		Event Day	
Day 1	Event Identified	Day 1	System Identified
Day1	System Shutdown	Day 1	System Secured
Day 1	Forensic Tools Gathered	Day 1	Disk cloned
Day 1	Logs from Proxy Server reviewed	Day 1	Records from full packet reconstruction engine reviewed
Day 1	Logs from Policy Scanner reviewed	Day 1	Logs from Firewalls reviewed
Day 1	All privileged account passwords changed on all systems, applications, databases, and infrastructure		
Day 1	Logs from Internet Traffic Monitoring system reviewed	Day 2	Forensic Analysis conducted on disk
Day 3	Logs from other Linux uncompromised systems logs reviewed	Day 3	Traffic from other Linux uncompromised systems reviewed for same time period
Day 4	Administrators interviewed	Day 5-40	All systems forensically scanned
Day 6	Lessons learned meeting	Day 7-40	Policy/Procedure development for implementation of patches

Event Day		Event Day	
Day 10	System wiped, rebuilt, and redeployed (new name & IP address)	Day 41	Compliance Documentation Completed and electronic investigation files burned to DVD

Countermeasures Assessment on Effectiveness

Initial discovery was opportune. If the exploit had traveled beyond the compromised box, at the time of the compromise the IPS systems were not deployed in a pattern that would have adequately protected the organization. The firewall rules blocked the queries to external DNS servers so only the host file modifications were available to the exploit. The packet monitoring systems lost reconstruction information because the hub they connected to the spanning port with was only 10mb and the network was bursting well past 10mb of traffic so at times, fortunately not when the exploit ran, full packet reconstruction was being lost. The traffic was still being recorded but not all images on all screens and all parts of the packets for files passing on the segment it was scanning were captured. At times only the packet headers were available for retrieval.

The IPS did not stop the traffic or the scan because the MAC and IP address of the compromised system was entered into the IPS system as a privileged system in use by a superuser. The exception had been created because of so many previous false positives from the various system administrator's workstations. All of their workstations were entered into the exception table in bulk.

Chain of Custody

The compromised system was downed hard but turned on again by the user to change their password. Control of the device and investigation information was lost during that event. Serial number of the CPU and hard drive was documented and signed by two investigators. The compromised system was removed to investigation war room, labeled, vaulted, and logged. Hard drive and CPU of compromised machine was removed from vault, logged, and two investigators confirmed serial numbers. A forensic clone was created of the hard drive, logged, and signed by two investigators. The serial number of the original hard drive was confirmed and it was sealed, logged, and signed by two investigators. The sealed drive was returned to the investigation vault and logged in to the vault. After completion of forensic investigation the original hard drive was verified and signed out of the vault, returned to original CPU, sealed, signed by two investigators, secured in cage, and logged into the vault. The clone hard drive of the compromised Linux system that the investigation was conducted on was signed by two investigators, sealed, placed in the investigation vault, and logged into the vault.

Containment Phase

Containment Measures

The Login ID Account for the assigned user of the compromised system was disabled throughout all systems and applications. All root passwords and administrator passwords were changed. All interface and database passwords were changed. The passwords were changed for privileged accounts on all routers, switches, proxy servers, web servers, and firewalls.

All system administrators were interviewed. No notable findings were discovered from these interviews. The manager of the department was interviewed to determine what guidelines he had in place for his workforce. The staff member assigned to the compromised Linux box was interviewed. From that interview I discovered:

The Linux workstation had been "acting funny" for 3 days prior to the incident discovery.
The GUI disappeared from the workstation 2 days prior to the incident.
The staff member assigned to the compromised Linux workstation used YUM to apply RPM's.
The staff member had been assigned to work with Linux 3 weeks prior to the incident.
The staff member had been personally using Linux for a couple of years.
The staff member felt that they are a subject matter expert on Linux
The staff member was not aware of all policies and procedures.
The staff member did not follow software change management procedures.
The staff member did not perform MD5 checks on files on a regular basis and could not remember the last time that they performed one.
The Linux workstation was not a standard, approved build.
The staff member did not document the special build configuration.
The staff member hard coded the kiosk login id into Mozilla on the compromised Linux workstation to avoid having to type their password in each time they wanted to access the internet from the Linux workstation.

The staff member used many of the test ids for various connections to the internet, some business, some personal, does not remember which ids were used.
The staff member used two different browsers on the compromised Linux workstation. The second browser used the staff member's login id and did not go through the proxy server to access the Internet.
The staff member did not know the Linux workstation was compromised.
The staff member had installed VNC on the compromised workstation to provide remote control of the workstation when they were not at their desk.
The staff member left the security privilege of root remote login enabled because is made it easier for him to perform his support services.
There were no backups created of the Linux or XP workstation to restore from.

Jump Kit Components or Division Tools Used in Investigation

Disk clone system
Spare drives for cloning
Penguin Sleuth Kit
Floppy disks
USB Drive
Investigation Logs
Bates Stamps
Static Free Evidence Bags
Seal Tape
Sharpie Markers
Printer
Paper
DVD Burner
DVD R+ Media

Detailed Backup of a Victim System

I Cloned the drive with Forensics Investigative/Cyber-crime Hard Drive Cloning Device. The backup process required me to remove the hard drive from the compromised machine. Place a like drive in the chassis of the cloning device. Connect the hard drive from the compromised system to the Cloning Device's external IDE controller interface with a standard IDE ribbon cable. The cloning device has an LED menu. I selected to clone the external drive, exact copy, normal speed, and with verification. The compromised hard drive was 40GB and it took about 1 hour for the copy and verification to complete. I sealed the compromised drive in a static free bag and placed it in the evidence vault.

Eradication Phase

Performed wipe disk on compromised system and reinstalled OS/applications. Performed forensic evaluation of all like OS systems in enterprise. Developed monitor watch filter for all systems that the administrator of compromised system had administrative privileges on.

The Linux workstation was rebuilt with media disks to standards specifications and hardened to CIS Linux Security specifications. All unnecessary services are disabled. All patches were obtained and confirmed with MD5 hashes from two trusted sites and then applied to the system. The IP address for the system was not configured for DHCP. A new IP address was assigned to the Linux workstation and hard coded in the configuration files. A gold image was created for the system and burned to DVD. A copy of the image is held in Corporate Compliance.

All machines in the server farm and in the same VLANs as the compromised Linux workstation were inventoried for OS, version, patch level, and applications.

Server Name	**OS**	**Version**	**Patch Level**	**Application**
Healthcare1	HPUX	11.11	Current	Patient Care
Healthcare2	HPUX	11.11	Current	Patient Care
Healthcare2	HPUX	11.11	Current	Patient Care
Financial1	AIX	5.1	-1	Accounting
Financial2	HPUX	11.11	Current	Accounting
Purchasing1	HPUX	11.11	Current	Purchasing
Purchasing2	AIX	5.1	-1	Purchasing
Records1	HPUX	10.20	-1	Medical Records
Records2	AIX	5.1	-1	Medical Records
Dietary1	HPUX	11.11	Current	Dietary Planning
Imaging1	AIX	4.3	-2	Document Imaging
Interface1	AIX	4.3	-2	Interface Engine
Lab1	AIX	4.3	-2	Lab Orders
Pharmacy1	AIX	4.3	-2	Pharmacy Orders
Dictation1	HPUX	11.11	Current	Clinical Dictation
Practice1	Red Hat Linux	7.3	Current	Practice Management
Practice2	Red Hat Linux	Enterprise Server	Current	Practice Management
Identity1	Suse Linux	9	Current	Credentials Management
Identity2	Suse Linux	9	Current	Credentials Management

Print1	Linux	2.2	Current	Printing Services
Admin1	Linux	2.4	Current	Facilities Management
Admin2	Redhat Linux	7.3	Current	Physical Security Management

The tapes for each system were ordered from the vault for 30 days and 60 days prior to the suspected compromise date and tested (verified that they could be read) in preparation for the potential need to restore the OS from tape. Unit Downtime procedures were reviewed and updated in preparation for possible extensive downtime for a system.

An external Linux security expert was retained to perform evaluation of all systems to determine if they had been compromised and develop recommendations for managing and maintaining these systems. A calendar for scan/patch was developed for each system.

Server Evaluation Calendar

Sunday	**Monday**	**Tuesday**	**Wednesday**	**Thursday**	**Friday**	**Saturday**
	1	**2** Healthcare1	**3** Purchasing2	**4** Financial1	**5** Dietary-1	**6** Print1
7 Identity1	**8**	**9**	**10** Dictation1	**11** Records1	**12**	**13** Practice1
14 Interface1	**15** Imaging1	**16** Admin1	**17** Purchasing2	**18** Financial2	**19** Health-care2	**20** Pharmacy1
21 Identity2	**22**	**23**	**24**	**25** Records2	**26**	**27** Practice2
28 Lab1	**29**	**30** Admin2	**31** Healthcare3			

The calendar was developed to minimize the impact on the workgroup that used the application(s) provided by a server and other projects that were scheduled for the organization.

Recovery Phase

The workstations were rebuilt from known good media. Current patches were retrieved, MD5 hashes were checked for the patches with reference from two known reliable sites. Current patches were applied. Systems were booted with Penguin Sleuth Kit. USB drive mounted. Check Rootkit utility was run against the rebuilt workstations and no anomalies were reported by the utility. The Linux workstations were hardened per recommendations from the Center for Internet Security (CIS) for implementing the steps necessary for CIS Level-I security. The XP workstation was re-imaged to the corporate standard.

All other Unix and Linux systems in the organization were inventoried. Linux Systems were booted with Penguin Sleuth Kit. Other Unix version systems were booted with read only media for that OS. USB drives were mounted on each Linux system to install the rootkit checker utility. If the system could not accept a USB drive the kit was mounted into memory by using a secondary CD drive. If no rootkit checker was available for the OS the system and configuration files were individually reviewed and MD5 hash checks comparing the original media or patch that was on the system with the systems current files were run against all files that were compromised on the Linux workstation and files that had known vulnerabilities for that OS. Manufacturers of the applications running on the systems were contacted and hardening recommendations were requested from them. The machines were hardened to the specifications of the application vendor. If an application vendor would not allow the systems to be hardened then the server was placed in a segmented network that was protected by an IPS and firewall. All measures taken to protect the organization from another compromise were documented to meet JCAHO and the HIPAA Security Regulation requirements.

No system or infrastructure compromises were found. IPS systems were installed in each server group VLAN and scanning event filters were escalated to high events. All workstations that had access to the Internet were removed from the exception list for the scanning filters.

Lessons Learned Phase

Developed policy and procedure for application of all patches and download site authentication process.

The information gathered from the incident lead me to conclude that the Linux workstation was compromised. The box was built from media 6 weeks prior to the incident. YUM was implemented on the Linux workstation 5 days prior to compromise. Patches were applied the evening before the compromise. The logs that could help me pinpoint what the exact compromise of the system were deleted from the system. The modified system files, scanning behavior, and external communications seen from the machine point to a rootkit compromise.

The monitoring group had received many false alarms from the administrator/superuser workstations in the past so their workstations had been filtered out. Known superusers used the compromised Linux workstation so this address was filtered out. The Linux workstation had direct access to the Internet because it used to be used to administer the servers in the DMZ. When this system's roles changed it's privileges did not. Policies and procedures were established for changing roles of workstations. Auditing procedures and calendars were established to review the roles of privileged workstations.

During the initial stages of the investigation the Linux workstation was not listed in the inventory database. It was determined that the database is prone to human error and oversights. Policies and procedures were developed that require a workstation to hold authority to connect to the network with a custom written token that is placed on each workstation. This token can only be obtained from the inventory system.

Because the compromised workstations host file was modified, a seemingly innocent patch download delivered a compromise that could have brought the network down or exposed confidential information. Policies and procedures were established for machines that needed to access the Internet for downloads. These machines will now be used for no other purpose. These machines are required to be isolated to a restricted VLAN. An IPS sensor is located in the VLAN with these machines.

File validation procedures were developed. MD5 hash verifications are required whenever possible from two trusted sources. A trusted source list was developed and the same sites cannot be used sequentially. Alternative validation procedures were developed ranging from patch quarantine procedures, application vendor shipped CD/Tape, or legacy modem communications to obtain patches.

The investigation identified that there was no deployment of a centralized log or patch management server. A patch management server and log management server were developed and deployed. Manpower resources were assigned to review the information gathered by these systems twice a day.

The investigation team concluded that if the compromise had escaped into the server farm and into the network a catastrophic breech could have occurred. At the time of the Linux workstation compromise IPS devices were only deployed at perimeter and in the server farm. Additional IPS devises were deployed in all VLANS, all sites. 7x24 monitoring was established.

During the initial stages of the investigation the compromised system was logged into by the assigned user to change the superuser password and the user's password on the system. I speculate that evidence was destroyed by the compromise when this happened. In future investigations users will be required to surrender their passwords and only investigators will be allowed to work with a machine after an event is identified.

The closing process turned into a challenge when a brand/model of hard drive found in the XP system would not clone to the brand/model of hard drive that I had on hand. The investigation inventory was expanded to hold 3 of each type of brand/model of hard drive that was deployed in 80% of the workstations in the organization and 1 each of the remaining 10%.

There are very few Linux workstations in the organization. Prior to the compromise it was judged that a breech from a hack of a Linux workstation was highly improbable. At the time of the incident the investigator's investigation tools were updated monthly for Windows and Novell systems. The Linux investigation tools were 3 months old. The team had to scramble to obtain current forensic tools for Linux. The Linux investigation tools were added to the monthly update schedule with the Windows and Novell system tools.

References & Research for Incident

Citings for Printed Works (Books)

Skoudis, Ed. Incident Handling Step-by-Step and Computer Crime Investigation, Volume 4.1, Version 12.03. United States of America: SANS, 2004. 11-111

McClure, Stuart; Scambray, Joel; Kurtz, George. Hacking Exposed, Fourth Edition. United States of America: McGraw-Hill/Osborne, 1993. 60-68, 265-334, 555-591, 593-629, 683-693

Petersen, Richard L.; Haddad, Ibrahim. The Complete Reference Red Hat Enterprise Linux & Fedora Edition, United States of America: McGraw-Hill/Osborne, 1994. 67-210

Citings for information reviewed at web sites

Trying to determine what type of compromises and exploits the workstation in the this investigation was hit with led to a great deal of surfing and searching through references that had previously been referred to in other investigations and classes. The following sites were notable to me. I may or may not have not cited the sites for their information in this paper but they at least refreshed information previously learned or gave me insight to information that did not relate to this investigation but were well worth my time for reference.

Intruder Detection Checklist
http://www.cert.org/tech_tips/intruder_detection_checklist.html
Copyright Carnegie Mellon University 1999
Revision History Oct 03, 1997
Feb 12, 1999
Jul 20, 1999
Initial Release
Converted to new web format
Converted ftp:// URL's to http:// URL's
Link verified 09-19-04

Reverse WWW Tunnel Backdoor
http://www.sans.org/resources/malwarefaq/rwww_shell.php
Author: van Hauser
© 2002-2004 The SANS™ Institute
Link verified 09-19-04

Security Focus
Vulnerabilities list
http://www.securityfocus.com/bid
Copyright © 1999-2004 SecurityFocus
Verified link 09-19-04

http://www.atmosp.physics.utoronto.ca/SX5/docs/g1ab02e/getspent.3c.html
SUPER-UX Programmer's Reference Manual
Copyright 1999 - NEC Corporation – No individual author credited
UNIX is a registered trademark of The Open Group.
NFS is a trademark of Sun Microsystems, Ins.
Link verified 09-10-04

http://staff.washington.edu/dittrich/misc/faqs/rootkits.faq
Contains excellent information on the files to check and was to get around potentially compromised files.
Author: dittrich
Revision: 1.5 - Date: 2002/01/05 00:58:14
Link verified 09-19-04

http://www.cs.wright.edu/people/faculty/pmateti/Courses/499/Fortification/obrien.html
Provided some additional history and Cert advisory listings to start the investigation.
Abstract: The article is by David O'Brien published in Sys Admin www.samag.com 5(11) (November 1996), pp. 8-20.
Copyright © 2004 CMP Media LLC
Link verified 09-19-04

http://www.securityfocus.com/guest/4871
Analysis of the KNARK Rootkit
by Toby Miller
Page last updated Mar 12 2001 6:00PM GMT
Link verified 09-19-04
This link contains "Analysis of the KNARK Rootkit", by Toby Miller. This site provided good instructions on how to use Nmap and netstat to identify a compromise and what that compromise was trying to accomplish. Excepts from Toby's paper:

"This link gives you a play by play analysis on the concepts of developing a rootkit such as KNARK.
http://packetstorm.securify.com/groups/thc/LKM_HACKING.html
If you want to learn more about LKM programming this is the link for you.
http://howto.tucows.com/LDP/LDP/lkmpg
Phrack has some great information on exploiting the Linux Kernel as well as hardening the Linux Kernel.
http://www.2600.com/phrack/p52-06.html
and
http://www.2600.com/phrack/p52-18.html"

The links Toby provided in his paper were also good references of information.

© 2002-2004 The SANS™ Institute
Link verified 09-19-04

http://www.atlhtcia.org/
Atlanta HTCIA Chapter
Link verified 09-19-04

http://www.kennesaw.edu/coned/sci/index.htm
Kennesaw State University – Southeast Cybercrime Institute
Link verified 09-19-04

http://www.sans.org
The SANS (SysAdmin, Audit, Network, Security) Institute
© 2002-2004 The SANS™ Institute
Link verified 09-19-04

http://www.hhs.gov/ocr/hipaa/
http://www.hhs.gov/ocr/hipaa/contractprov.html
http://www.cms.hhs.gov/providers/edi/cob_tpa.asp?
Office of Civil Rights or the United States Department of Health and Human Services
Links verified 09-19-04

CERT® [7]
Ensure that the software used to examine systems has not been compromised
http://www.cert.org/security-improvement/practices/p093.html
Copyright 2000 Carnegie Mellon University.
CERT® and CERT Coordination Center® are registered in the U.S. Patent and Trademark office.
This page was last updated on October 18, 2000.
Link verified 09-19-04

CERT®
Identify data that characterize systems and aid in detecting signs of suspicious behavior
http://www.cert.org/security-improvement/practices/p091.html
Copyright 2000 Carnegie Mellon University.
CERT® and CERT Coordination Center® are registered in the U.S. Patent and Trademark office.
This page was last updated on October 18, 2000.
Link verified 09-19-04

[7] The CERT® Coordination Center is part of the Software Engineering Institute. The Software Engineering Institute is operated by Carnegie Mellon University for the Department of Defense. CERT and CERT Coordination Center are registered in the U.S. Patent and Trademark Office by Carnegie Mellon University

CERT®
Monitor and inspect network activities for unexpected behavior
http://www.cert.org/security-improvement/practices/p094.html
Copyright 2000 Carnegie Mellon University.
CERT® and CERT Coordination Center® are registered in the U.S. Patent and Trademark office.
This page was last updated on October 18, 2000.
Link verified 09-19-04

Linux Forensic Tools
http://www.linux-forensics.com/links.html
Copyright © 2003. Ernest Baca
Link verified 09-19-04

http://fedora.redhat.com/
Copyright © 2003-2004 Red Hat, Inc. All rights reserved.
Fedora is a trademark of Red Hat, Inc.
The Fedora Project is not a supported product of Red Hat, Inc.
Red Hat, Inc. is not responsible for the content of other sites.
This page last modified at: 2004/09/13 17:17:46

http://www.rootkit.nl/projects/rootkit_hunter.html version 1.1.6.
Rootkit Hunter by Michael Boelen and Stephane Dudzinski,
Copyright Rootkit.nl 2003-2004 - All rights reserved
Link verified 09-19-04

http://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=119130
Reporter: Tim Waugh – Assigned to: Mike A. Harris
Copyright © 2003-2004 Red Hat, Inc. All rights reserved.
Link verified 09-10-04

http://la-samhna.de/library/rootkits/list.html
Contains a list of some of the rootkits that could have compromised the system.
Copyright © 2002 by Rainer Wichmann
Link verified 09-19-04

http://www.sans.org/y2k/t0rn.htm
Provided an outstanding paper by Toby Miller on the T0rn rootkit compromise. This document helped me identify some of the characteristics of the compromise and relate them to a rootkit attack.
© 2002-2004 The SANS™ Institute
Link verified 09-19-04

http://www.webopedia.com/TERM/S/steganography.html
Definition for Steganography
Copyright 2004 Jupitermedia Corporation All Rights Reserved.
Link verified 09-19-04

http://linux.duke.edu/projects/yum/
Yum updater
Copyright © 2003-2004 by Duke University
Updated: Jul-27-2004

http://www.faqs.org/docs/linux_network/x-087-2-iface.netstat.html
Linux Network Administrators Guide
By: Al Longyear, Alan Cox, Andres Sepúlveda, Ben Cooper, Cameron Spitzer, Colin McCormack, D.J. Roberts, Emilio Lopes, Fred N. van Kempen, Gert Doering, Greg Hankins, Heiko Eissfeldt, J.P. Szikora, Johannes Stille, Karl Eichwalder, Les Johnson, Ludger Kunz, Marc van Diest, Michael K. Johnson, Michael Nebel, Michael Wing, Mitch D'Souza, Paul Gortmaker, Peter Brouwer, Peter Eriksson, Phil Hughes, Raul Deluth Miller, Rich Braun, Rick Sladkey, Ronald Aarts, Swen Thüemmler, Terry Dawson, Thomas Quinot, and Yury Shevchuk.
Link verified 09-19-04

http://www.insecure.org/nmap/
Nmap download and refernce site
By fyodor@insecure.org
Link verified 09-19-04

http://www.batesstamp.com/
Site to obtain bates stamps.
Link verified 09-19-04

http://www.linux-forensics.com/downloads.html
Penguin Sleuth Kit by Ernest Baca
Link verified 09-19-04

http://freshmeat.net/
Great threads to learn from
Link verified 09-19-04

http://www.rpm.org
Copyright © 2002
R P Herrold fbo the RPM community
Columbus OH
herrold+rpm@owlriver.com
Maintained by Owl River Company -- Comments to: rpm editor, please.
Link verified 09-19-04

http://www.realvnc.com/download.html
Copyright © 2002-2004 RealVNC Ltd RealVNC and the RealVNC logos are trademarks of RealVNC Ltd
Link verified 09-19-04

http://www.cisecurity.org/bench_linux.html
© 2003, the Center for Internet Security.
Link verified 09-19-04