Global Information Assurance Certification Paper

GIAC Level Two Advanced Incident Handling and Hacker Exploits

Practical Assignment for SANS Certification

Material submitted by G.M. Howard

Attended: Capitol SANS 2000

Date Submitted: February 19, 2001

Contents

Abstract

There is a growing tendency from computer software and hardware manufacturers to incorporate HTTP based management capabilities to its network-enabled products. The information technology era adds a full load of unusual appliances like printers and copiers that now support this feature along with more traditional networked devices like routers, file servers and workstations. Most of these HTTP-enabled devices provide poor security features, allowing the occurrence of several dangerous scenarios to its networks and ultimately affecting the performance of its company.

This paper documents my experience identifying HTTP-enabled devices on the corporate network under my responsibility as security specialist, implementing immediate measures to protect such devices, and developing procedures to prevent future similar situations while coordinating with LAN managers. HTTP-enabled devices like Cisco routers and switches, Hewlett-Packard printers, Compaq workstations, Novell file servers and Intel print servers will be used as examples through out this GIAC practical assignment. The emergency action planned to improve the situation included the SANS six steps for incident handling: preparation, identification, containment, eradication, recovery, and lessons learned.

Executive Summary

In November 2000, our information security office ran a port scan over the entire TCP/IP enabled group of devices in our organization's computer network. The objectives were simple: to take a 'snap-shot' of our network (determining how many hosts were up during our scan, the operating system they were running, and what they were used for), while looking for possible sources of exploits. Using a jump-kit based on the popular security tool nmap [FYO98], the port scanning included all the TCP and UDP ports available and would try to determine the OS of each device.

After the scan was finished, came the opportunity to analyze all the data gathered. One quick fact that caught our attention was that nmap listed more than four hundred (400) devices listening to TCP port 80. According to our records there were only one (1) web server: our corporate Intranet (internal use only). Such disparity required an additional investigation, which later assured us that all these web servers were HTTP-based management utilities for our file, print and communication devices. We decided to handle this as an incident when we later confirmed that very few administrators were aware of such tools and their deficient protection provided.

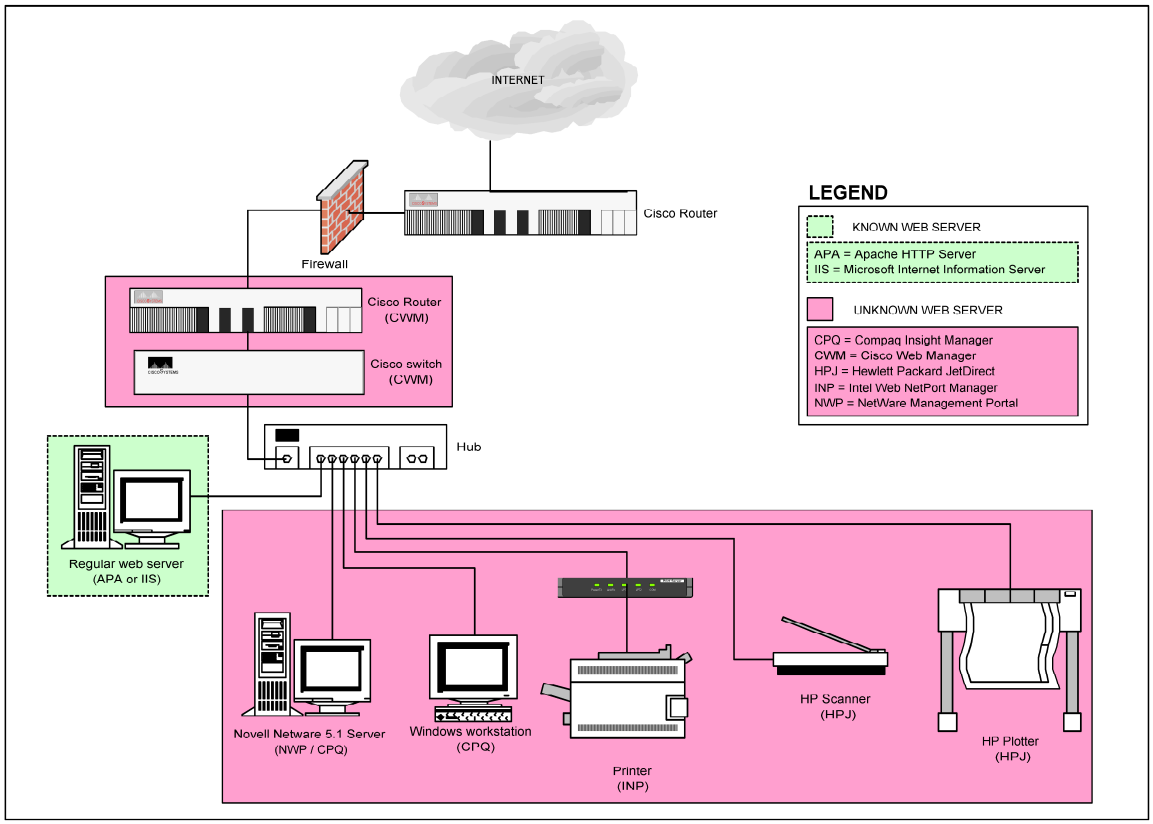
The group of HTTP-enabled devices was composed by five systems: Novell file servers, Cisco routers and switches, Compaq remotely managed servers and workstations, Intel NetPort print servers, and Hewlett-Packard print servers. It was necessary to assess each system separately, look for its vulnerabilities and produce countermeasures.

Two members of the IT security office provided guidelines and procedures to change the default configurations found on most of the devices and a checklist as well to make sure administrators were aware of the security implications of installing web servers on devices like those found above. General documentation from each vendor on how to deal with these issues was also provided.

We decided to organize two separate meetings: one for file and print administrators and the other for the networking support unit. It allowed us to provide only the information necessary to each group. Both teams agreed to implement all the recommendations made in four days, at the latest. Each

departmental coordinator sent back a signed list with all the changes made, along with a feedback of their impressions on the incident.

WEB SERVERS FOUND IN CORPORATE NETWORK



During our assessment, we searched for any vulnerability posted publicly on leading security sites that was related to any of our HTTP-enabled devices. Several exploits were found and documented, allowing us to update the advisories we sent to the departmental coordinators and the networking support unit.

After the departmental reports arrived, we started a new security assessment on the HTTP-enabled devices. The result was a reduction of more than 7/8 of the previous population of devices found. The networking unit took the opportunity to snif the behavior of our scan for learning purposes.

Several reports were produced after the incident. Both included the experiences and opinions of all the personnel involved in this incident. A copy was presented to the Chief Information Officer and his staff.

The incident showed several shortcomings on our network and allowed us to learn better communication skills for future similar situations. It allowed us to work on a field where few people have had previous experience. This will be valuable when we start the CERT implementation project.

During the incident one issue that was discussed extensively was the importance of mitigating enumeration capabilities on the network. The SANS six steps [SAN98] provided a methodical procedure to convince personnel who were not really sure in the initial stages of our response.

Although our response was not the fastest possible [LAN00], it will be used as a comparison for future similar incidents. The experience provided a good learning environment, thanks to the goodwill of the personnel involved. We felt this overcome several of the shortcomings we faced early during the incident.

Preparation

Several years ago, our organization created an information security (IT) office with the main purpose of promoting adequate IT security awareness among all of our employees. A lot of preparation work has been done: creation of policies and procedures, implementation of security mechanisms to protect resources, and the education of regular users and support personnel. Nevertheless, there are still many opportunities for improvement. The nature of our business and recent important changes to our organization's operational objectives and procedures has created somehow this situation. Working in IT security at our organization should still be fun for some time to come.

Policies have been our constant work during the last four years. Thanks to the support of upper management, policies have been created and disseminated among employees. In 1998, the Chief Information Officer and the Information Security Officer created an information systems security program, subject to the review and approval of the Information Systems Management Steering Committee, which includes members from non-IT departments. Since then, this has been our starting point for any consequent security policy our office has created. Examples of such policies are computer systems, electronic mail, password management

and control, backups, virus management, incident handling, software disposal, and electronic access termination policies.

Our security office has also setup a security awareness program dedicated to all the computer systems users. The new employees have the opportunity to attend a monthly security orientation talk to introduce them to our policies and procedures. Regular users receive advisories and guidelines through our Intranet, electronic mail and/or normal mail system.

Training has been provided to both regular and administrative users, including special courses for management personnel. Last year we celebrated the ACM Computer Security Day (http://www.home.gs/a4csd), which turned out to be a big success. Our corporate Intranet includes an IT security section, updated by our office, to provide a repository of security policies, procedures, advisories and guidelines.

The anti-virus system includes all our Novell file servers and Windows-based servers and desktops. The corporate e-mail server farm offers anti-virus protection to provide a centralized management point in case of virus outbursts. Our handling team includes several units of the IT department that provide around the clock support, monitoring newly detected viruses and their impact on our systems. Every week, advisories and updates are sent to users to make sure all systems are properly configured.

As in any organization, our firewall is a very important asset to the security infrastructure. It controls communication to/from our internal network and the Internet servers. Our networking unit has also setup an intrusion detection system (IDS) that monitors our switched network and several important servers. A switched network helps control non-authorized communication sniffing. The IT security office provides auditing support to both the firewall and the IDS.

For the last year and a half we have performed several vulnerability assessments on our systems, with the help of COTS software like Network Associates CyberCop [CYB01] and freeware like Nessus [NES99]. Meetings with system administrators have been organized to discuss the data

gathered and its implications. Such meetings have helped promote the use of security configuration guidelines such as SANS Step-by-Step handbooks or Microsoft Security Checklists (http://www.microsoft.com/technet/security/tools.asp).

Recently we have started a vulnerability assessment procedure that will be run periodically over our network. The purpose is to detect situations not handled by other security procedures or mechanisms, known as the 'layers' of the security system. With the help of the popular port scanner *nmap* and the vulnerability tools mentioned above, the assessment should be run every three months. After the data from the nmap scan had been analyzed by the IT security office, a consensus is reached as to what should be assess next. The following steps of this document, provide information from the first time we implemented this security layer.

One area that needs our attention, is the creation of a computer emergency response team (CERT). A good foundation is in place because of the existence of an on-call support team that provides emergency response to our computer systems and its users. Recent attendance to SANS and the Forum of Incident Response and Security Teams (FIRST) conferences by several of our employees have also risen the awareness of such need. In the coming months, the IT security office will develop a plan to create our CERT team, how to incorporate several existing security 'layers', and provide training to personnel involved.

Identification

Our incident occurred a couple of months ago when we decided to run periodically a port scan over the network, trying to determine hosts or situations that would need an investigation or assessment. As much as we believe in all the security layers we had placed so far in our network, there was a strong feeling that a more proactive security measure needed to be taken. Besides the already deployed intrusion detection system, we decided it was necessary to run several times per year a complete port scan over our network.

A good source on how to set up a port scanning system was John Green's nmap course [GRE00]. It was easy to decide on

nmap as our starting tool but as he said, it is necessary to create the complete 'vulnerability assessment toolbox' or 'jumpkit' to provide a methodical process to help assess the network's security posture. We installed Linux RedHat 6.2 on a pentium-based computer with:

- nmap: the network mapper
- nlog: nmap log files management tool [NLO00]
- nmap-web: web-based interface for nmap tool [KOM00]
- tcpdump: network packet sniffer
- nessus: vulnerability scanner and penetration tester with scripting language capabilities to create own attacks.
- Cybercop: another vulnerability scanner, from Network Associates. Also includes own scripting language.

The first time we ran the port scan, it took three (3) days to finish. We limited our scan to regular working hours to include as many live hosts as possible, along with all UDP and TCP ports available (more than 130,000) for each of the hosts in our network. We coordinated with network administration to let them know of the activity we would be generating. It was very helpful since it allowed them to turn on their sniffers to record our toolkit behavior for later study.

Once the port scan was finished, we used nlog to analyze all the data produced. A very quick fact jumped out: there were more than three hundred (300) web servers in our network. That was unexpected since we were only aware of our internal web server (Intranet).

We ran nmap again to only scan hosts with TCP port 80 open and the OS identification option: *nmap -O -p 80 <subnet address>.* It showed us that 70% of those web servers were print servers, Intel NetPort and HP JetDirect, while 25% were Cisco devices, routers and switches. We determined another 5% as Novell file servers just by using our web browsers and pointing to those IP addresses.

While we were scanning the first time, we had a casual talk with the networking support unit. They let us know about their project to install Compaq Management Agents, a web-based management utility to monitor hardware on Compaq servers and workstations. This utility uses TCP port 2301 and can be accessible from a web browser. After another nmap

scan, it increased the number of web servers to more than 400.

We were very concerned with this situation since all these networked devices provided some kind of information without any authentication and/or could have other security risks such as denial of service, which are always inherent to any computer system. The real problem was that our support people were not aware of this. To our IT security office this was an incident that required all our effort, time and resources to fix it promptly.

There are several reasons as to why this was an incident, even though no hacker or malicious user was present. The most important to us was that our file, print, routing and switching systems could have been disrupted thanks to mostly unused management tools with very little security provided. Some security publications have discussed the risks involved and possible scenarios [HIG01]. It is very well known that most attacks and security breaches occur from inside the networks [CSI00], thanks (most of the time) to consultants, temporary, or disgruntled employees.

Other reasons as to why we handled this as an incident were the training of our support personnel in unforeseen situations and to help determine potential support members from other departments to our emergency response team. Finally, we wanted to raise awareness among our colleagues of the growing tendency by computer software and hardware manufacturers to incorporate http-based management tools to network devices and their inherent security risks.

Here is a generalized description of the devices we found with http communication enabled on our network:

Novell NetWare file servers

Novell NetWare servers, version 3.x and higher, include Novell Management Portal. Simply known as Portal, it is an http-based management utility that provides server health monitoring, diagnostic and debugging capabilities. It can be accessed from a remote workstation running at least Netscape Navigator 4.5 or Microsoft Internet Explorer 5. It is SSL-enabled.

Portal's default installation allows a non-authenticated

user to determine the server's memory and operating system health that could be used by a malicious user during the 'reconnaissance' stages of his/her attack or to determine how effective is his attack. For example, such attacker could determine how effective a denial of service attempt might be against a Novell server.

Compaq Servers and Workstations

Compaq provides system remote management to several servers, workstations, desktop, and even portables models through the installation of the Compaq Management Agents on those machines. System administrators control the agents through own web interfaces or by using the Compaq Insight Manager utility. Both tools provide fault, configuration, and performance management of hardware and operating system. Current versions of Compaq Management Agents and the Insight Manager software are http-enabled, using TCP port 2301.

The agents' default configuration allows anonymous web users to gather important information from its servers and workstations, such as memory, operating system, and storage parameters. The administrator account also comes with a default password (also administrator).

Cisco routers

Several versions of the Cisco IOS allow routers configuration and monitoring through a web server, installed with the OS. Such http-based remote access allows the same control as access through the router console.

By default, the routers have the web server enabled. Such configuration is dangerous since the "enable" password is used for authentication. Such password is sent in clear text over the wire. Potential security risks such as buffer overflows and denial of service could also exist.

Hewlett Packard print servers

Hewlett Packard (HP) JetDirect series of print servers include an embedded web server, for any firmware version x.07.03 or above (except A.0x.xx). The web server allows the same type of configuration capabilities as any other mechanism provided by HP: telnet, JetAdmin or Web JetAdmin

management software or even the front panel of the printer. This situation is also true for any other JetDirect-enabled device, including scanners and plotters.

The default configuration of the embedded web server has no password. If the administrator does not change this situation, any modification to the device is allowed without authentication.

Intel print servers

Any Intel Netport print server with firmware version 4.40 or above provides an embedded web server. The Web Netport Manager allows directly changing the print server configuration, monitoring the server's status, and even resetting the server to factory's default.

As with the HP JetDirect print servers, the Netport server comes with no configuration password by default.

It is important to mention that we found a big number of web services without passwords on print servers and remote management agents. Such issue plus the fact that several administrators were not even aware of the existence of the web servers (and its inherent vulnerabilities), made us believe strongly that this situation should be handled with the priority of an incident. Check Appendix B for examples of web servers described above, except Cisco servers.

Containment

The IT security office assigned two staff members to work on the following stages of this incident. As a member of that group, I was responsible for producing the technical procedures and guidelines to help the system and networking administrators set up properly the devices' configuration. We also included steps to remove the web services, in cases where the tools were not necessary. It took us two days to produce such documents for the five systems involved.

Several steps were recommended in our documents to improve the security of the devices. Here is a generalized list of such recommendations:

- Uninstall the web server: Part of our goal is to

always keep management as simple as possible (KISS rule). Any administrator that would not use the web server should uninstall it.

To uninstall the web server on Cisco equipment, the following configuration line should exist: **no ip http server**. Novell servers should not have loaded the PORTAL.NLM (for NetWare Management Portal) and/or CPQ*.NLM (for Compaq Management Agents). Windows machines can uninstall the Compaq agents with the Add/Remove Programs option in the Control Panel.

HP JetDirect print servers can disable its web service by making a telnet session and typing: **ews-config: 0** (also make sure you have set up a telnet password).

- Check configuration: This was necessary since unauthorized users may have used an access point not monitored. Print servers found without password may have changes in their configuration so administrators needed to check. It also happened to Compaq agents with default administrator password.

  For Novell administrators, we asked to make sure SSL (secure socket layer) protocol was enabled on the servers to provide encrypted communication with remote browsers. The following lines have to be commented out in the server's AUTOEXEC.NCF file:

  load nile.nlm
  load httpstk.nlm /SSL /keyfile:"SSL Certificate IP"
  load nicisdi.xlm
  load sasdfm.xlm
  load sas.nlm
  load pki.nlm

- Restrict Access: If the devices require remote access, it should only be available to administrators. One way to help control the access is by restricting the number of hosts or subnets that can establish HTTP communication with the devices.

  On Cisco devices, it is possible to control HTTP

access by specifying the IP addresses allowed with the **ip http access-class** *list* command. For JetDirect print servers using DHCP, it is possible to store an allow list through TFTP. Netware Management Portal requires the installation of Support Pack 1 to restrict HTTP access, also using IP addresses.

- Change password: It was made necessary to change all passwords on print servers. Compaq machines needed to change default administrator password. Cisco equipment also needed to change its password since it hadn't been changed in several months. Novell servers were not affected by this recommendation since there was a password policy in place that requires changing password frequently.

- Add Warning Banner: Option available to Novell and Cisco equipment. Here is our sample banner:

  You have reached a private node, do not attempt to login if you have not been authorized to do so. If you access it without previous authorization, you are violating federal laws and could be prosecuted.

  To include the banner in the Portal main page, it is necessary to create an HTML file named PRTLANNC.HTM and placing it in the server's SYS:\LOGIN directory. To establish the banner on Cisco routers, you have to use the command **banner login**

- Backup the system: All Cisco equipment and Intel and Hewlett Packard print servers should have a hard copy of its configuration. Each Novell server has a backup system installed, so we asked to have all tapes updated.

- Keep systems updated: Any system has to be updated often. Our documents asked for print servers to have latest firmware versions, use latest Compaq Management Agents and Insight Manager versions, keep a recent Cisco IOS version installed on equipment, and install support pack on Novell servers.

  Novell 5.1 Support Pack 1 was particularly important

to our effort since it would allow restricting the amount of information it provides to anonymous users and control HTTP access by host addresses. We had to contact the Novell Support Team to actually find out about this new feature, since there wasn't any indication of the new capabilities in the documentation provided with the support pack. A recently released Support Pack 2a provides more improvements to the Portal tool.

- General security documents: In order to improve awareness of security issues we also included documents from each vendor we felt would help educate our constituency.

  - NetWare Management Portal Utility Guide. Available at http://www.novell.com/documentation/lg/nw51/pdfdoc/10412391.pdf
  - Improving Security on Cisco Routers. Available at http://www.cisco.com/warp/public/707/21.html
  - Making HP JetDirect Print Servers Secure on the Network. Several links available: http://www.hp.com/cposupport/docindex/j3111a_set_main1.html
  - Controlling Printer Access. Available at: http://www.intel.com/network/tech_brief/printer_access.htm

- Logging capabilities: Finally, it was important to us to mention how little logging capabilities these devices provide. Therefore a bigger chance for malicious users to launch their attacks through the web services without getting caught. The conclusion was simple: if not needed, don't use it.

We felt it was neither necessary nor possible to disrupt the devices since that would have meant shutting down most of our file, print and TCP/IP communication services. Since all those machines were currently operational and we didn't have evidence of intrusion on any of the systems, we decided to start improving the assurance on our equipment with the measures from above.

According to our policies, the first point of contact to each department for IT-related issues is the office automation (OA) coordinator. We met to let them know of our findings and the importance that such matter would be solved promptly. They either designated a person from their

department to coordinate the follow-up or took the incident personally. This meeting was beneficial to us since the OA coordinators appreciated our interest to be proactive and offered to help as much as needed.

We provided a detailed departmental list of all the devices found to each OA coordinator. It included: IP address, device name, type (Novell server / Compaq agent / Intel print server / HP print server / Cisco equipment), and a small description. At the meeting we all agreed to give three (3) days to fix the situation.

The same day, a separate but similarly productive meeting occurred with the networking unit to work on the Cisco communication equipment situation. On both cases, we agreed on meeting four (4) days later to assess the incident again.

Eradication

Up to this point, we had not checked for any devices' vulnerabilities or exploits reported on any security portal or mailing list like Security Focus [SFC01] or Bugtraq [BTQ01], respectively. Since we had already established several objectives in the previous meetings and a timetable to accomplish them, my colleague and I went back to the office to do the research.

Our findings confirmed the existence of several vulnerabilities on several of the http-based management tools. Thanks to web sites like Security Focus, ISS' XForce team [ISS01], and Securify's Packetstorm [PSM01], it was feasible to gather alerts and advisories on the different devices.

A very important source of information to us is the NIPC CyberNotes [NIP01], which summaries every two weeks the vulnerabilities, attacks, Trojans, viruses and exploits discussed on leading security forums. The CyberNotes allows us to introduce new personnel to the type and load of information found in those leading forums without the burden of handling the daily flow of messages received. The CyberNotes help get comfortable with the information one can receive through the forums before you subscribe to such lists.

We created a list of the recent vulnerabilities found in the CyberNotes from the last twelve months, applicable to the HTTP-based management tools we found on our network (see Appendix A for details). We also included certain vulnerabilities related to the respective operating systems, to make sure everybody understood that these devices were not free from regular security risks.

Several vulnerabilities were also found to the Hewlett-Packard Web JetAdmin management utility. This tool can be installed as a web server on an administrator's machine to configure and monitor JetDirect devices. Web JetAdmin uses TCP port 8000 for its default configuration. Although is had not been widely used on our network, we added the vulnerabilities information found to the JetAdmin advisory we released.

An additional advisory was sent to all OA coordinators with the vulnerabilities information gathered and making sure everybody knew the web links to current devices updates. We didn't extend the implementation period because of the new findings, sticking to the original four (4) days agreed. All the vulnerabilities could be fixed by applying latest firmware/software version, a recommendation already made.

Recovery

We started receiving the departmental lists signed by each OA coordinator to act as an acknowledgement that the changes required were made. Along with the lists, hard copies of the entire devices configuration were included. We recommended each departmental team as well to write down their impressions on this incident.

Several OA coordinators contacted our office during the implementation period to discuss further and in private their particular situations. One of the most interesting discussions was with the financial department and the protection of the printers responsible for printing checks. Several additional mechanisms were implemented to protect those printers. During the discussions, several teams even talked about the occurrence of past incidents inside their own constituencies.

After the implementation period was over we immediately

started a new audit with our jumpkit: the nmap port scan was restricted to the TCP ports known from the incident: 80, 2301, and 8000. It took only an hour and a half since we had ready a list of IP addresses for all the devices. The total number of HTTP-enabled devices came down to less than a eigth of the original number.

Finally, the networking unit tuned their IDS and sniffers to collect the behavior of several subnets during the implementation period and our recovery port scan. Along with them, we established new protection mechanisms to sub-networks that were detected as very important to our organization's operations.

Follow-up

A technical report was created by the security office and sent for review to all the OA coordinators, who also distributed it among their personnel involved in the incident. Their response was positive. They made several interesting comments, specially related on how to improve the communication channels from/to the security office. It became particularly important to us to learn from the people closer to the core business of our organization.

Another comment provided by the OA coordinators was the need to include the security office during the development of our organization's IT projects. Since this incident, there has been an increase in the number of projects where our office has been involved.

Several system administrators made a request to our security office to organize (technically-oriented) security talks. For the last year we had been focusing mainly on the administrative employees training, so we accepted their request with pleasure.

A final version of the report was presented at the following OA coordinators meeting, which by coincident took place a week later. An executive report was produced and presented by the security officer to the chief information officer and his staff on their following weekly meeting. Their positive comments to our proactive mechanisms provided the confidence necessary by management to start several security projects that were on hold for a while.

Because of the incident, we found out there weren't adequate procedures to update our intranet's security section. The website was an efficient channel to provide general, public documentation during the incident. We had since coordinated with the Webmaster to improve the update procedure.

Since our first port scanning, we have automated it using the **cron** command and developing some shell scripts. We had organized internal *nmap* courses so more members of our office are trained. The security officer can now assemble several teams to audit different systems on our network.

Most importantly, the incident proved to be a learning experience to the security office and the IT support personnel. The procedures documented here have been changed thanks to more experiences from the last few months. This incident became a necessary start to improve the security of our file, print and communication services. This incident also helped to start our CERT project. But most importantly, more people are now aware of the changing nature of security and the inherent need to be proactive.

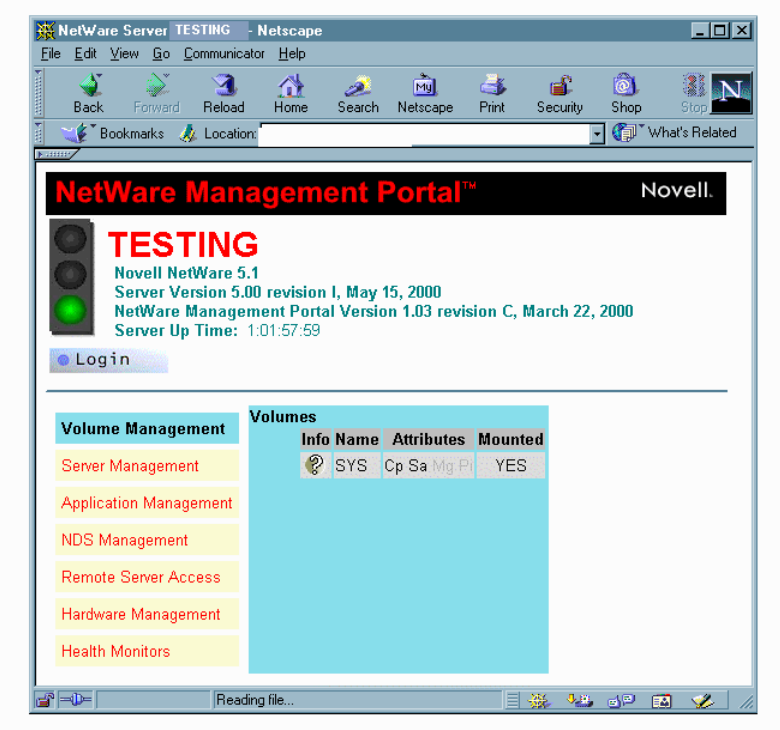
© SANS Institute 2000 - 2005 Author retains full rights.

APPENDIX A. List of Vulnerabilities related to HTTP-enabled devices.

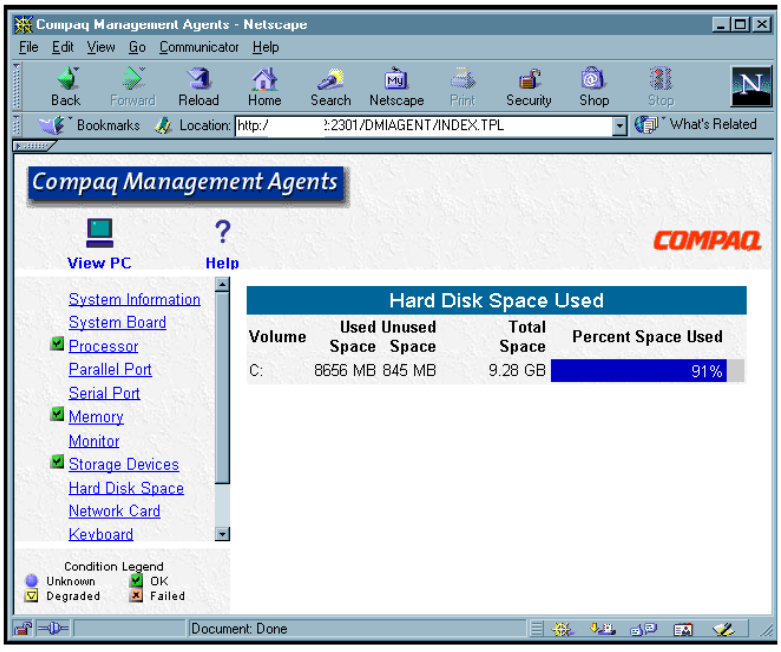
Vendor/Operating System	Software Name	Vulnerability/Impact	Patches/Workarounds/ Alerts	Common Name	CyberNotes Date	Risk
Cisco	Cisco IOS versions 12.0-12.1	Denial of Service vulnerability exists if the IOS HTTP service is enabled and the enable password in known.	Complete advisory CSCdr91706 available at http://www.cisco.com/warp/public/707/ioshttpserverquery-pub.html	Cisco IOS "?/" HTTP Request Denial of Service	11/6/2000	Low
Cisco	IOS 11.0, 11.2x, 11.3x, 12.0x	Denial of Service vulnerability exists if HTML interface is enabled	Complete advisory CSCdr36952 available at http://www.cisco.com/warp/public/707/ioshttpserver-pub.shtml	Cisco IOS HTTP Denial of Service	05/10/2000	Low /High
Hewlett-Packard	JetDirect x.08.04, x.08.05, x.08.20	Multiple buffer overflow vulnerabilities related to FTP, telnet and LPD services	Upgrade available at http://www.hp.com/cpsupport/networking/software/allhpjd3.exe.html VIGILANTE Advisory: VIGILANTE-200014 (available at Bugtraq)	JetDirect Multiple Denial of Service	10/23/2000	Low
Hewlett-Packard	Web JetAdmin Version 5.6	Malicious user is allowed read access to any file on the web-published filesystem	Upgrade available at http://www.hp.com/net_printing/ppss/wja_overview.html	JetAdmin Directory Traversal Vulnerability	06/05/2000	Medium
Hewlett-Packard	Web JetAdmin Version 6.0	Denial of Service by accessing TCP port 8000	Upgrade available at http://www.hp.com/net_printing/ppss/wja_overview.html	JetAdmin Remote Denial of Service	06/05/2000	Low
Hewlett-Packard	JetDirect J3111A rev. A.08.06, G.05.35, G.07.02, G.07.03, G.07.17, G.08.03, JetDirect rev.G.08.04, G.08.20, H.08.05, H.08.20	Denial of Service vulnerability due to FTP service	Upgrade available at http://www.hp.com/cpsupport/networking/software/allhpjd3.exe.html VIGILANTE Advisory: VIGILANTE-200004 (available at Bugtraq)	JetDirect Invalid FTP Command Denial of Service	07/31/2000	Low

Vendor/Operating System	Software Name	Vulnerability/Impact	Patches/Workarounds/ Alerts	Common Name	CyberNotes Date	Risk
Hewlett-Packard	JetDirect J3111A rev. G.08.03, G.07.17, G.07.03, A.08.06	Denial of Service in JetDirect cards	Upgrade available at http://www.hp.com/cpsupport/networking/software/allhpjd3.exe.html	JetScan Portscan Denial of Service	04/26/2000	Low
Compaq / Netware	Compaq Management Agents for Netware 2.28	Vulnerability in default installation, allowing a malicious user access to system files	Advisory available at http://www5.compaq.com/proeducts/servers/management/security.html IXsecurity Advisory: iXsecurity.20001107.Compaq-wbm.a	Compaq Management Agents for Netware Plaintext Password	11/20/2000	High
Compaq / Windows NT4/2000, Unix	Several management agents and Insight Manager versions and Compaq platforms	Buffer overflow vulnerability, allowing arbitrary code execution with system administrator privilege level	Patch available at http://www5.compaq.com/products/servers/management/agentsecurity.html	Compaq Web Management Agents Buffer Overflow	01/29/2001	High

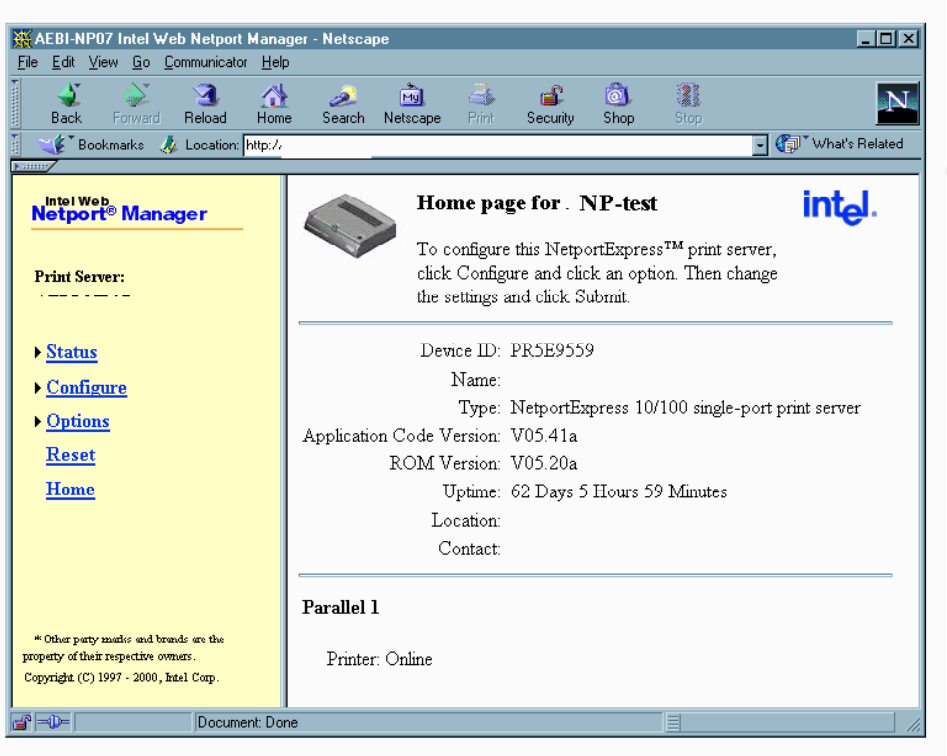
APPENDIX B. Figures of HTTP-enabled devices with default configuration.



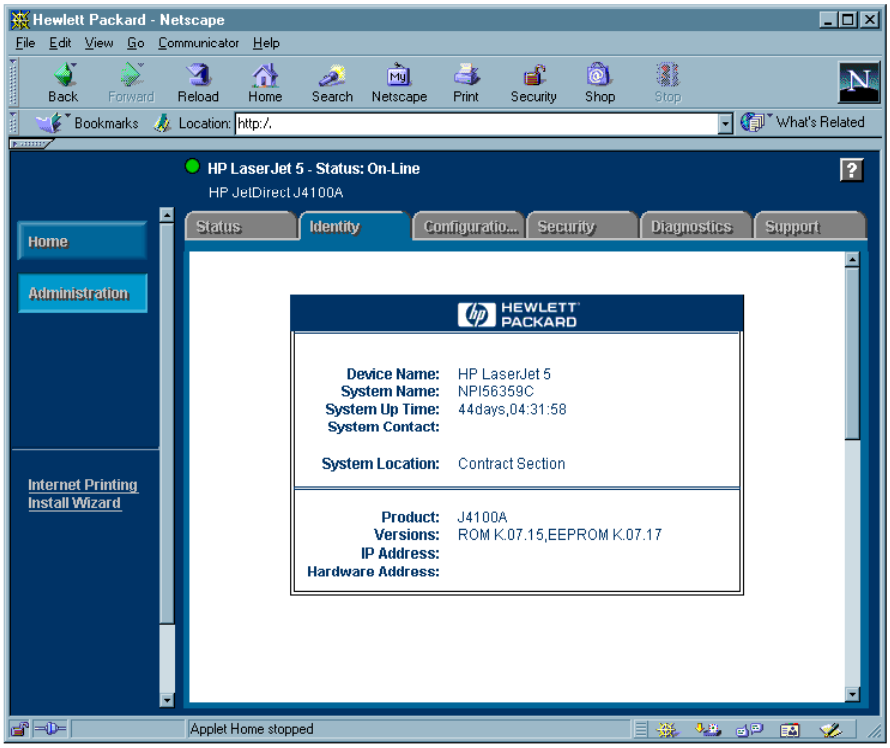
Netware Management Portal v1.03 tool running on a Novell NetWare version 5.1 server



Compaq Management Agent v4.70 running on a Compaq workstation with Microsoft Windows NT4



Intel Web Netport Manager running on a Netport print server v5.41a



HTTP interface for JetDirect J4100A network card installed on a HP LaserJet 5 printer

References

[BTQ01] Bugtraq Security Mailing List. Available at http://www.securityfocus.com

[CSI00] Computer Security Institute. Computer Crime and Security Survey. Spring 2000.

[CYB01] Network Associates CyberCop, network vulnerability assessment tool. Available at http://www.pgp.com/products/cybercop-scanner/default.asp

[FYO98] NMAP, Network Mapper. Created by Fyodor. Available at http://www.insecure.org/nmap

[GRE00] Green, J. Using nmap to Map Your Network and Test for Vulnerabilities. SANS Network Security 2000. Monterey, California, October 2000.

[HIG01] HIGHLIGHTS. National Infrastructure Protection Center. Issue 1-01. January 18, 2001. Available at http://www.nipc.gov/publications/highlights/highlights.htm

[ISS01] Internet Security Systems. X-Force Security Team Website. Available at http://xforce.iss.net

[KOM00] Komarnitsky, A. Nmap-web: Port scanning Made Easy. SYSADMIN Magazine. October 2000. Tool available at http://www.komar.org/komar/alek/ → Misc. Tech Stuff → nmap-web

[LAN00] Private meeting with LAN Administrators. December 2000.

Liebing, E. Beyond the Basics: Configuring the Netware Management Portal Utility in NetWare 5.1. Novell AppNotes. March 2000.

[NIP01] National Infrastructure Protection Center. Cybernotes. Bi-weekly publication available at http://www.nipc.gov/cybernotes/cybernotes.htm

[NES99] NESSUS, Network vulnerability scanner. Available at http://www.nessus.org

[NLO00] NLOG. Created by H.D. Moore. Available at

http://www.digitaloffense.net/nlog/

Northcutt, S. & Novak, J. Network Intrusion Detection: An Analyst's Handbook. Second Edition. New Riders Publishing. September 2000.

[SAN98] The SANS Institute. Incident Handling: Step by Step. Version 1.5. May 1998.

Scambray, J., McClure S., & Kurtz, G. Hacking Exposed: Network Security Secrets & Solutions. Second Edition. Osborne / McGraw-Hill. 2001.

[SFC01] Security Focus, IT security portal. Available at http://www.securityfocus.com

The SANS Institute. How To Eliminate the Ten Most Critical Internet Security Threats: The Experts' Consensus. Version 1.31. December 28, 2000.