Global Information Assurance Certification Paper

Unlikely Sources of Network Security Risks
Ted McDermott
GSEC Practical Assignment Version 1.4b – Option 1
16 September 2003

SUMMARY
Companies have focused great efforts on proper configuration of firewalls and Internet-facing edge routers as a means of securing enterprise networks. Most server administrators have been diligent to regularly apply OS patches. Desktop administrators have installed anti-virus software to protect PCs from malicious code and viruses. Other network devices, however, typically get very little attention in terms of network security. Printers, scanners and copiers represent up to 20% of the network device population. Yet, these devices are often deployed with default settings, which may bring vulnerabilities onto the enterprise network. Additionally, the growing popularity of video-conferencing has added a whole new category of LAN-based devices. This paper will focus on a popular HP printer, a multi-function system from Xerox, and a pair of Tandberg video-conferencing systems. The purpose is to identify default settings and their associated vulnerabilities, and then to provide tips on maximizing network security by locking down as many vulnerable ports as possible, as well as implementing good password authentication for the remaining services.

XEROX DOCUMENT CENTRE 432
The Xerox Document Centre Multifunction System features the ability to print, scan, email, fax, and copy documents. This powerful behemoth also features a sophisticated suite of web-manageable services, which enhance the capabilities of the system.

KEY OPERATOR CODE
The default key operator code, per the Xerox manual, is "#22222"[1]. While the special "#" key introduces a non-alphanumeric key to the password, it's still not a difficult password to crack. The system allows but does not require the creation of a PIN to override the default password. **The first vulnerability, therefore, is that the operator is not required to set up a unique PIN or password for front-panel access to system configuration. Also, the password is not cryptic enough to foil a persistent key operator.**

WEB ACCESS AND AUTHENTICATION
An Nmap port scan of the Xerox System produced the following output:

Port	State	Service
80/tcp	open	http
139/tcp	open	netbios-ssn
515/tcp	open	printer
631/tcp	open	ipp

After pointing a web browser, at the system's IP address, the user is presented with a straightforward graphical interface with six options with sub-menus which allow significant reconfiguration of not only the system, but also its relationship to and impact on the network.The **second vulnerability is that the web server by default is accessible via port 80 without any kind of authentication**. Although most of the critical sub-menus require that the user authenticate to the system, a would-be intruder could be discouraged from further intrusion attempts by a prompt for a password.

The web-accessible main menu options are: *Services, Queue, Status, Properties, Maintenance, and Assistance*. The initial screen also lists the device type, serial number, DNS name and IP address of the system. Finally, a "Device Index" icon allows another method of accessing and modifying critical functions by alphabetical index-type selection. Xerox provides a User Guide and a System Administration Guide with excellent pictures, graphics and instructions. Additionally, there are a lot of features, such as authentication and IP address filtering capability, which indicate that Xerox has done a good job in offering flexible options for different server and operating systems environments, as well as access security. Unfortunately, the typical end-user organization will not take the time to evaluate the implications of plugging such a system into the network. Thus, the system ends up on the network with mostly default settings, leaving the network vulnerable, especially since the user guide is freely available on the web and has dozens of references to the default administrative password. The web password is "22222". **The third vulnerability is that the administrative password is not only trivial, but is freely available.**

One of the key functions accessible from the "Device Index" icon is, Authentication (also under the Properties option). The system lists five options for authentication:

- Kerberos for Solaris
- Kerberos for Windows 2000
- NDS – Novell 4,5
- SMB – Windows NT 4
- SMB – Windows 2000

Authentication is required for access to the most powerful functions involving Email, Fax Server, and Network Scanning features of the Xerox system. The online Help documentation states, regarding the default domain controller, the "IP address and domain entries are also required when Kerberos is the selected authentication protocol."[2] Unfortunately, these two fields are blank by default, and, though Kerberos for Windows 2000 is the default selected authentication method, it has no effect, since the IP address and domain fields are blank. This is probably not a true vulnerability, since without authenticating, the user would not be able to scan to a network device. Additionally, the Fax Server feature depends on the Network Scanning feature to be operational. Nevertheless, it is confusing

that the sub-menu indicates that Kerberos for Windows 2000 is engaged, when, in fact, it isn't.

Another key function accessible from the "Device Index" icon is Web Server Configuration (also under the Properties option). The Keep-Alive timeout, which by default is set to 10 seconds and Maximum Connections, which defaults to 32, are the only parameters which can be modified in this sub-menu. Once again, commendably, Xerox requires authentication to modify the Keep-Alive timeout or Maximum Connections settings. There is no option, however, to modify the web services port. It is fixed at 80. One potential improvement would be to allow the properly authenticated administrator to modify the web server configuration to use a less common port number. This is a common practice for administrative control of other devices, such as web-caching appliances from Blue Coat. Their Port 80 Security Appliance uses port 8081 for the web management interface.[3]

OTHER FEATURES AND VULNERABILITIES

Here are a couple of other features of this powerful multi-function system which further point out the criticality of securing both the front panel and web access.

- Scan to Email; Scan to File; Scan to Fax
    - Email address lists can be imported, thus making it possible to scan once and distribute to an entire email recipient list.

- LAN Fax
    - Network users can send a document to the system which in turn can fax it out the phone line to the recipient. This could potentially mask the source of the fax.

Kevin Smith's earlier GIAC GSEC paper on vulnerabilities of the Sharp AR-507 Imager discusses similar features and exposures on that system.[4]

STEPS TO TAKE TO SECURE THE XEROX DOCUMENT CENTRE 432

- Override the default operator key code with a new, unique PIN.
- Set up the hostname and IP address of the authentication server and verify that web users must authenticate in order to gain access to the system for Email, Server Fax, and Network Scanning features.
- Disable all unused protocols. Supported protocols include: IP, IPX, Appletalk, and Banyan Vines. Note that to disable protocols, a password is required, but it is even simpler to guess than the operator key code
- Verify settings after each vendor service call, to make sure that customized security features, including operator key code and web authentication, are still in place.
- Create a step-by-step procedure to install these security settings in the event that the settings are reset to default.

HP COLOR LASERJET 4600 PRINTER

The HP Color LaserJet 4600 is a sleek and powerful workhorse with the additional attraction of color printing capability. Like the Xerox, the HP 4600 also features a sophisticated suite of web-manageable services, which enhance the capabilities of the system.

KEY OPERATOR CODE (NONE)

There is no default key operator code, and all parameters are configurable by pressing the front keys, beginning with the "Ö" button. There is no password protection available for the front panel. Since this is strictly an output device, this is not as big an issue as with the previously discussed Xerox multi-function system. However, an incorrect configuration can still wreak havoc on the local-area network. **The first vulnerability, therefore, is that there is no protection from a user walking up to the printer and modifying configuration settings, including network settings.** There is one password protection service available. Users can lock their print jobs, such that other people cannot see their output before they go and collect it themselves. The user can put a PIN on the print job. Then when collecting the output, the user must key that PIN into the front panel in order for the job to print. [5]

WEB ACCESS AND AUTHENTICATION

An Nmap port scan of the HP 4600 produced the following output:

Port	State	Service
21/tcp	open	ftp
23/tcp	open	telnet
80/tcp	open	http
280/tcp	open	http-mgmt
515/tcp	open	printer
631/tcp	open	ipp
9100/tcp	open	jetdirect

Remote operating system guess: HP JetDirect Card (J4169A) in an HP LaserJet 8150/8550

I was able to both telnet and ftp into the printer, since the HP JetDirect password was not set. **The second vulnerability is that there is no default password protection and the printer is wide open for telnet, http and ftp access.** What is the risk? The printer can be rendered inoperable, by modifying the IP address. Users might access the printer via DNS name. By modifying the static address of the printer, users could no longer access the printer either via its known IP address or by its DNS name. An unwanted intruder could also modify the printer's IP address by changing it to the IP address of another critical device on the same subnet, creating an IP address conflict, and possibly rendering that other device unusable as well.

STEPS TO TAKE TO SECURE THE HP LASERJET 4600 PRINTER

- Set up an “IP Administrator” password for the JetDirect card. This controls web, tcp, and ftp access to the printer. With up to 16 alphanumeric characters allowed, a tough password can be created. [6]
- Set up HTTPS to insure secure web-based administration of the printer.
- Set up an IP access control list of allowed administrators.
- Disable telnet. All configuration can be performed securely and reliably using HTTPS.
- Set up a security password to prevent unauthorized remote configuration of the printer. From the main menu, click on Security, and then enter a password.
- Disable all unused protocols. Supported protocols include: IP, IPX, Appletalk, and DLC/LLC.

TANDBERG 6000 AND 1000 VIDEO-CONFERENCING SYSTEMS

The Tandberg 6000 Video-Conferencing system consists of a camera, monitor, codec, and an optional multi-point control unit (MCU). In addition to the camera and the monitor, there are jacks for connecting other video and audio input and output devices, such as VCRs and auxiliary microphones. This rollabout system also features connectivity for three ISDN lines, dial-in/dial-out line, and an Ethernet 10/100 network interface card. The MCU allows for a multi-point video conference. Up to sixteen different locations can join a conference by way of video and/or audio call either over the LAN or via ISDN or dialup. The MCU can also manage multiple concurrent calls[7].

The Tandberg 1000 is a smaller, all-in-one integrated desktop system. The monitor, camera, microphone, and speakers are in one ergonomic unit that easily fits on even the most crowded desktop. The 12" monitor is not as viewable as its larger 6000 cousin. This unit offers ISDN, LAN, and even wireless connectivity, making it a very portable, user-friendly solution for both executive offices, and also for adhoc usage in small conference rooms with groups of a half-dozen or less.

WEB ACCESS AND AUTHENTICATION

An Nmap port scan of the Tandberg 6000 System produced the following output:

Port	State	Service
21/tcp	open	ftp
23/tcp	open	telnet
80/tcp	open	http
1720/tcp	open	H.323/Q.931

Remote operating system guess: Alcatel Advanced Reflexes IP Phone, Version: E/AT400/46.8

An Nmap port scan of the Tandberg 1000 System produced the following output:

Port	State	Service
21/tcp	open	ftp
23/tcp	open	telnet
57/tcp	open	priv-term
80/tcp	open	http
1720/tcp	open	H.323/Q.931

Remote operating system guess: Alcatel Advanced Reflexes IP Phone, Version: E/AT400/46.8

Like the Xerox and the HP systems, the http service allows immediate access to the system. The friendly graphical menu allows all aspects of call management as well as system configuration. Although the manual states that the system

would prompt for a default password ("TANDBERG", which is case-sensitive), not only was there no prompt, but there was no graphical means of setting the password on the evaluated software release (software version e1.2 NTSC, boot SW release Rev. 1.23, 2002-08-16). By telnetting to the system, a password can be set to restrict web, telnet and ftp access. The system requires a combined total of eight alphabetic and numeric characters, and is case-sensitive. The delivered evaluation system came without password authentication enabled. **The first vulnerability (once again) is that the web server by default was accessible via port 80 without any kind of authentication.** This is apparently not the factory setting, but the Tandberg Sales team delivered the evaluation product in this state. What's the risk? Plenty!

Call Management

Under the Call Management menu, the operator can initiate a call to virtually any other reachable video conferencing system. Typically, the operator need look no farther than the Connect sub-menu, where various video-conferencing systems throughout the network are listed by name and IP address. Because these systems are usually located either in executive offices or board rooms, there is a significant risk of disrupting critical business meetings. When auto-answer is set on the remote end, there is also a very real potential for eavesdropping and leaking of confidential corporate information. The web operator also has the capability to disconnect a current call, thus disrupting an ongoing meeting. The operator could also edit the directory information for other video-conferencing systems on the network, thus rendering the unit temporarily inoperable.

System Configuration

From the "IP settings" sub-menu, the operator can revise IP address, gateway, SNMP community strings and trap hosts, as well as Ethernet network interface card speed. The "WLAN" settings" sub-menu allows modification of the SSID field, community and keys[8]. The "H.323 settings" sub-menu allows modification of the E.164 alias and the H.323 prefix. Other settings sub-menus include configuration options for audio control such as volume, and auto-answer, which defaults to "on". One could argue that it is a security risk to allow a video-conferencing system to be set in auto-answer mode, but the convenience and usability of the system is far easier if it doesn't require any action on the remote end. One obvious observation is that it could take even a knowledgable operator hours to recover from unwanted tampering with the above information. Video conferences are usually tightly scheduled. Any long-lasting setup problems would effectively cancel the conference call. Therefore, it is vital that the system configuration be carefully protected by strong password authentication.

The port scan of both Tandberg units indicated that several unexpected services were open with the units, including ftp, telnet and priv-term. With the capabilities of the web-based configuration and call management menus, these services should be unnecessary. In addition, the wireless LAN option for the Tandberg 1000 portable unit further heightens the vulnerabilities posed by leaving these

ports opened. Finally, the lack of password authentication even further compounds the security exposure of the system, leaving it ripe for an attack.

STEPS TO TAKE TO SECURE THE TANDBERG 6000 and 1000 VIDEO-CONFERENCING SYSTEM

- Put a password on the system, using the “ippassword <password>” command [9].
- Turn off unnecessary but vulnerable ports, especially on the extremely portable, and potentially wireless 1000 model using the command, “services <telnet/ftp/http/h323/remote-software> <enable/disable>”.
- Keep the rollabout (6000) system under lock and key, except during usage.
- Ensure that fixed configuration video-conferencing rooms are secure.
- Distribute the menu and submenu settings to a small group of well-trained individuals who will be responsible for the setup and maintenance of the systems.
- Practice placing the variety of point-to-point, multi-point, audio, ISDN, and LAN-based calls which may be required.
- Practice setting up the unit after changing all of the settings to default, following a procedure. The procedure should include the IP address and host name of all other video-conferencing units on the network for reference.
- Time how long it takes to set up the call. This is important, since pressure (and productivity loss) is high when dozens of users are waiting for a call to begin.

REMAINING EXPOSURES

Clear-text passwords remain an issue with all of the above systems, except for the HP 4600 printer, which offers HTTPS. On local-area networks, this presents a serious vulnerability. For example, the manufacturers of a competitive video conferencing system, the ViewStation from Polycom, acknowledged this exposure before announcing a system upgrade to combat several vulnerabilities. Most notably, a sniffer device could easily determine the administrative password of a video conferencing system. This would allow an intruder to take control by connecting or disconnecting calls at will, eavesdropping on rooms, and even broadcasting video conferences over the Internet. [10].

To combat this intrusion, third parties such as Navastream, are offering front-end gateways and stand-alone devices to encrypt the video conference administration and transmission into IPSec and and digital certificates to encrypt the traffic, thus warding off password sniffing[11]. Depending on the number of video conferencing systems in an enteprise, this could be an expensive proposition. Video conferencing manufacturers like Polycom and Tandberg will probably soon have these security features built into their native software, saving

the end-user from the headache and expense of deploying yet another box on the network.

Perhaps, the best recommendation is to seriously weigh the risks and benefits of web access and administration of these devices. It might just be easier, and certainly safer, to use the remote controller or the trusty front panel, and shut down all unnecessary IP ports. It could save everyone some very embarrassing moments!

REFERENCES

[1] XEROX. “Document Centre 440/432/420 System Administration Guide”. November, 2000. URL: http://a1851.g.akamaitech.net/f/1851/2996/24h/cache.xerox.com/downloads/world/d/dc440_432_425_SAG_en.pdf http://docushare.xerox.com/Get/File-22367/DC_440_Setup.pdf.

[2] XEROX. “Document Centre 440/432/420 User Guide”.November, 2000. URL: http://a1851.g.akamaitech.net/f/1851/2996/24h/cache.xerox.com/downloads/world/d/dc440_432_425_UG_en.pdf

[3] Blue Coat Systems. “Blue Coat Systems Port 80 Security Appliance Configuration and Management Guide” . April, 2003. URL: http://www.bluecoat.com/downloads/manuals/SGOS_CMG_Guide_2-1-07.pdf

[4] Smith, Kevin “Do You Copy? Security Issues with Digital Copiers,”, SANS Institute 2000-2002, As part of GIAC practical repository. (16 Sept 2000)

[5] HP “hp color LaserJet 4600 series printer User Guide”. April, 2002. URL: http://h200005.www2.hp.com/bc/docs/support/SupportManual/bpl11903/bpl11903.pdf

[6] HP “hp jetdirect administrator’s guide”. July, 2003. URL: http://h200005.www2.hp.com/bc/docs/support/SupportManual/bpj07248/bpj07248.pdf

[7] Tandberg “Tandberg 2500 User Manual”. September 16, 2002. URL: http://www.tandberg.net/sendFile.asp?FileID={AAA87CA8-9373-486F-8F0F-00EDB11D5A36}&Extension=.pdf

[8] Tandberg “Tandberg 6000 User Manual”. September 16, 2002. URL: http://www.tandberg.net/sendFile.asp?FileID={38FF71AF-0DBD-409E-9773-66594C704C99}&Extension=.pdf

[9] Tandberg “Tandberg-API (Dataport User Guide) Software Version E1/B6” Tandberg D11943 Rev 12

[10] Wired News “Video-Conferencing Hole Exposed”. September 16, 2002. URL: http://www.wired.com/news/technology/0,1282,55145,00.html

[11] Navastream “NAVASTREAM SECURES REMOTE MANAGEMENT VULNERABILITY IN POLYCOM VIDEOCONFERENCING PRODUCTS” September 13, 2002. URL: http://www.navastream.com/Press_Releases_Polycom.shtml

Last Updated: July 24th, 2017

Upcoming Training

SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
Community SANS Omaha SEC401*	Omaha, NE	Aug 14, 2017 - Aug 19, 2017	Community SANS
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
Community SANS Trenton SEC401	Trenton, NJ	Aug 21, 2017 - Aug 26, 2017	Community SANS
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
Community SANS Pasadena SEC401 @ NASA	Pasadena, CA	Aug 23, 2017 - Aug 30, 2017	Community SANS
Mentor Session - SEC401	Minneapolis, MN	Aug 29, 2017 - Oct 10, 2017	Mentor
SANS San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
Mentor Session - SEC401	Edmonton, AB	Sep 06, 2017 - Oct 18, 2017	Mentor
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS New York SEC401	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Boise SEC401	Boise, ID	Sep 25, 2017 - Sep 30, 2017	Community SANS
Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Oct 02, 2017 - Oct 07, 2017	Community SANS
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
Mentor Session - SEC401	Arlington, VA	Oct 04, 2017 - Nov 15, 2017	Mentor