Global Information Assurance Certification Paper

GIAC Certified Incident Handler
GCIH Practical Assignment
Version 2.1a

Network Printers: Whose friend are they?

Lorna J. Hutcheson
Washington D.C. SANS 2002

TABLE OF CONTENTS

Part 1: The Exploit 4

Introduction 4

Name 5

Operating System 5

Protocols/Services/Applications 5

Brief Description 6

Variants 6

References 7

Part 2: The Attack 8

Description and Diagram of Network 8

IP Addressing Scheme 8
Components Used 8
Border Router 8
Primary Firewall 9
Internal Router 9
U.S. Marketing Firewall 9
International Firewall 10
Server Firewall 10
VPN 10
Printer/Multifunction Device 10
Access Methods 14
Customers 14
Suppliers 14
Partners 14
ACL Description 14
Firewall Rule Description 15

Protocol Description 16

How the Exploit Works 17

Source Code Description 17
Compiled Code Description 22

Description and Diagram of the Attack 26
Print Job Status/Collection 26
Unauthorized storage 28
Signature of the Attack 29
How to Protect Against It 29
What can we do? 29
What can the vendors do? 30
Part 3: The Incident Handling Process 32
Preparation 32
Identification 36
Containment 40
Eradication 45
Recovery 45
Lessons Learned 46
Extras 52
References 56

Part 1: The Exploit

Introduction

The focus of this paper is to attempt to bring awareness to the issue of network peripheral devices (I.E. printers, faxes, copiers, etc.), specifically printers and their vulnerabilities. Unfortunately, when it comes to these devices, they are oftentimes overlooked and as such can pose a danger to the network. For some reason, people have it in their mind that these devices can do only one thing, and that one thing is what they were originally designed for and nothing more. This paper is going to focus on network printers and their vulnerabilities to narrow down the issue. Doing so is somewhat difficult, because there has not been a lot of emphasis given to this problem.

A problem? What is the problem with printers, they just print, right? This is not the case at all anymore. Printers have become much more than just devices that print. They also include a wealth of other functions. Most offices now have multifunction network printers that do everything. As an example, there is one of Xerox's multifunction office systems: the Xerox 490. It was chosen at random. Below is a look at its capabilities taken from the Xerox website at http://a1851.g.akamaitech.net/f/1851/2996/24h/cache.xerox.com/downloads/usa/en/b/brochure_490.pdf:

- Network Scanning with E-mail
- Scan to PC Desktop Client Software
- Network Fax Server Integration
- Network Accounting Enablement
- Image Overwrite Security
- Foreign Device Interface/RS-232 Port
- Network Connectivity
    - SMart network controller with 433 MHz processor and 128 MB RAM
    - 9.1 GB(minimum) hard disk
    - 10/100 BaseT Ethernet connectivity
    - All major network protocols and operating systems supported

This does not describe your everyday printer as most people think of them. Nowhere in this brochure was security for this device ever mentioned. I know for a fact, that only a Xerox employee is allowed to open and service the device and usually it was monthly and with their laptop. Not only is network security involved, physical security is as well. I don't know many people, even trained security personnel, who could determine what a technician was doing on one of these devices.

The problem is that network peripheral devices have changed and evolved, but without much consideration for their security. We worry about all the computer systems out there, but why don't we hear about these exploits if they are such a risk? Dennis W. Mattison (a.k.a. LittleW0lf) wrote an excellent paper on the subject called "Network Printers and Other Peripherals – Vulnerability and Fixes." This can be found at http://members.cox.net/ltlw0lf/printers/printers.pdf. In this document, he writes to this very question and states, "Well, how can we be so sure that attackers aren't? Very few of the printers actually had logging capabilities, and most of these capabilities were clunky and difficult to configure." (Mattison, 28) I would have to agree, when was the last time you looked at a printer log? Do printer manufacturers even make their logs look at security events, if they log anything? I would submit that the answer is no. I also believe that there is not much talk on these exploits because the attackers do not want to give away an advantage. Why give away a capability that allows such easy access? They now have all the storage and power they need to hide on a network and do whatever they want. But if people had a way to monitor their peripheral devices this situation might just change.

With that little introduction, this paper is going to focus on an exploit that I found interesting. It can be found at http://www.phenoelit.de/hp/docu.html and is called Hijetter.exe.

Name

Hijetter.exe is a program that takes advantage of printers. There is not a CVE or CERT reference that I could find.

Operating System

All Hewlett Packard Printers and indications are other different kinds of printers, but this needs to be verified.

Protocols/Services/Applications

This program specifically looks at port 9100, Printer PDL Data Stream/hp-pdl-datastream. Both of these accept TCP or UDP connections on port 9100. The PCL (Printer Command Language) was created by Hewlett Packard to order to control features of printers across the board. HP states "The PCL Printer language is successful because the following points remain constant at all levels:

1. All HP LaserJet printers implement PCL printer language features consistently.
2. HP printers implement the PCL feature in very cost-effective formatters.
3. HP printers have the ability to ignore most unsupported commands." (HP LaserJet Printers)

Within the PCL are five different phases from PCL 1 to PCL 6. Each of these phases is usually backward compatable. Within the PCL, there are four types of PCL printer commands, which are:

1. Control codes
2. PCL commands
3. HP-GL/2 commands
4. PJL commands

Within this paper we are going to focus on the PJL commands.

Brief Description

It can be found at http://www.phenoelit.de/fr/tools.html. At that site, the description given is as follows "The Hijetter gives you the opportunity to explore printers via their PJL interface. This includes access to the environment variables, the file system and the display of the target." PJL (Printer Job Language) is what makes this possible. This tool makes a connection to port 9100 by default and enables you to then manipulate the printer from there if listening. However, you are not restricted to that port. You may choose whatever port you would like to attempt to connect on.

Variants

I have not found a variant to this exploit; however there are several printer exploits on www.cve.mitre.org as well as www.cert.org that deal with PJL commands and buffer overflows. This is the only one I have found that gives you an interface to manipulate the file system of the printer allowing you to place and delete files.

References

"Attacking Network Embedded Systems." July 2002 URL: http://www.blackhat.com/presentations/bh-asia-02/bh-asia-02-fx.pdf (19 November 2002).

"BoF with FX of Phenoelit." URL: http://www.security.org.sg/webdocs/news/event12.html (18 February 2003).

Computer Security Schweiz. URL: http://www.computer-security.ch/ids/default.asp?TopicID=189 (16 February 2003).

Dennis W. Mattison. "Network Printers and Other Peripherals – Vulnerability and Fixes." 8 July 2002. URL: http://members.cox.net/ltlw0lf/printers/printers.pdf (19 November 2002).

"E-SECURE-DB IT Security Information DATABASE." 21 August 2002. URL: http://www.e-secure-db.us/dscgi/ds.py/ViewProps/File-11389 (16 February 2003).

FtR. "PFT and Hijetter." URL: http://www.phenoelit.de/hp/ (16 February 2003).

"[INFOCON] - OCIPEP Daily Brief Number: DOB02-128 Date: 21 August2002." 21 August 2002. URL: http://www.google.com/search?q=%22hijetter%22&hl=en&lr=&ie=UTF-8&oe=UTF-8&start=10&sa=N (18 February 2003).

PacketStorm Archives. URL: http://packetstorm.decepticons.org/Win/indexdate.shtml (16 February 2003).

"Xerox Document Centre 490 Overview." URL: http://a1851.g.akamaitech.net/f/1851/2996/24h/cache.xerox.com/downloads/usa/en/b/brochure_490.pdf (17 February 2003).

Part 2: The Attack

Description and Diagram of Network

The network design listed below is taken from my previous GCFW practical posted at http://www.giac.org/practical/Lorna_Hutcheson_GCFW.zip. I chose to use this because I feel it is a secure design and I wanted to be able to demonstrate how a secure design can become unsecured based on the introduction of a peripheral device. The first graphic you will see is Figure 1. It is the original network design. I added printers in logical locations for the network, which modifies the first design as seen in Figure 2. I chose to use an HP LaserJet 4100mfp, which is an intelligent multifunction network printer. I will define the capabilities below in the components used section from the firewall practical. The IP Addressing Scheme, components used, access methods and ACL/firewall rules description are all taken from my practical at http://www.giac.org/practical/Lorna_Hutcheson_GCFW.zip.

IP Addressing Scheme

The following addressing scheme will be used in this design. The routable IP addresses are factious.

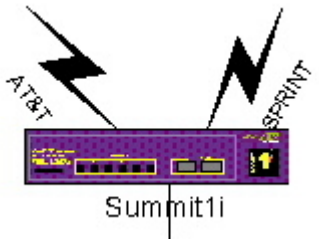
- Border Router:
  External Interface: 153.27.210.10/24
- Primary Firewall:
  External Interface: 153.27.38.20/24
  Internal Interface: 153.27.39.10/24
  Suppliers Services Network: 172.16.20.5/24
  Customers Services Network: 172.16.21.5/24
- Corporate Internal Router:
  External Interface: 153.27.39.15/24
- U.S. Marketing Firewall:
  External Interface: 153.27.39.25/24
  Internal Interface: 172.16.22.5/24
- International Firewall:
  External Interface: 153.27.39.20/24
  Internal Interface: 172.16.23.5/24
- Server Firewall:
  External Interface: 153.27.39.30/24
  Internal Interface: 172.16.24.5/24

Components Used

Border Router

In order to assure customers have access to the web site, two different ISPs will be used. One will be the primary ISP and the second ISP will be the backup. If

one ISP goes down for any reason, connectivity will be maintained through the second ISP. The following diagram shows the two connections.



Brand

Extreme Networks was chosen for the border router. In order to meet the growing needs of GIAC Enterprises, Extreme Networks offers Gigabit throughput and implements layer 2 and layer 3 capabilities at wire speed.

Version

The Summit1i switch was chosen for the border router. It has many security features and offers full layer 2 and layer 3 capabilities.

Primary Firewall

Brand

The Symantec Enterprise Firewall (formally Raptor) was chosen for the primary firewall. It is a proxy firewall, with great flexibility to perform other functions.

Version

The version to be used is 6.5. This version not only provides the same great protection and diverse functionality of the previous versions, but also improves upon the GUI interface and makes managing and configuring easier.

Internal Router

Brand

Extreme Networks was chosen again for the internal router. Since Extreme Networks offers Gigabit throughput and implements layer 2 and layer 3 capabilities at wire speed, it also makes it the perfect internal router to handle the growing needs of GIAC Enterprises corporate headquarters.

Version

The Summit7i switch was chosen for the internal router. It has many security features and offers full layer 2 and layer 3 capabilities.

U.S. Marketing Firewall

Brand

The Symantec Enterprise Firewall (formally Raptor) was chosen for the U.S. Marketing firewall.

Version

The version to be used is 6.5. This version not only provides the same great protection and diverse functionality of the previous versions, but also improves upon the GUI interface and makes managing and configuring easier.

International Firewall

Brand

The Symantec Enterprise Firewall (formally Raptor) was chosen for the primary firewall. It is a proxy firewall, with great flexibility to perform other functions.

Version

The version to be used is 6.5. This version not only provides the same great protection and diverse functionality of the previous versions, but also improves upon the GUI interface and makes managing and configuring easier.

Server Firewall

Brand

The Symantec Enterprise Firewall (formally Raptor) was chosen for the primary firewall. It is a proxy firewall, with great flexibility to perform other functions.

Version

The version to be used is 6.5. This version not only provides the same great protection and diverse functionality of the previous versions, but also improves upon the GUI interface and makes managing and configuring easier.

VPN

Brand

The Symantec Enterprise Firewall also offers VPN capabilities and will be used as the VPN device for the Suppliers and International partners.

Version

The version used will be 6.5 as mentioned above. This allows for multiple encryption capabilities.

Printer/Multifunction Device

Brand

The HP LaserJet 4100mfp was chosen because it is a common printer found in organizations and because many companies are going to multifunction devices.

Version

The version used is a 4100mfp. More information can be found at www.hp.com. This version has many capabilities. It does "automated integration of paper-based documents into key business processes through send-to-email, color scanning, and digital sending capabilities, optional services enable sending to Internet fax servers, network folders and desktop applications." (http://www.hp.com/itrc_pdi/products/pdfs/lj4100mfp.pdf) It is also Internet connected with remote management and a throughput of 4.5MB per second. It has a minimum of a 250 MHz processor, 64 MB RAM, 5 GB hard drive.

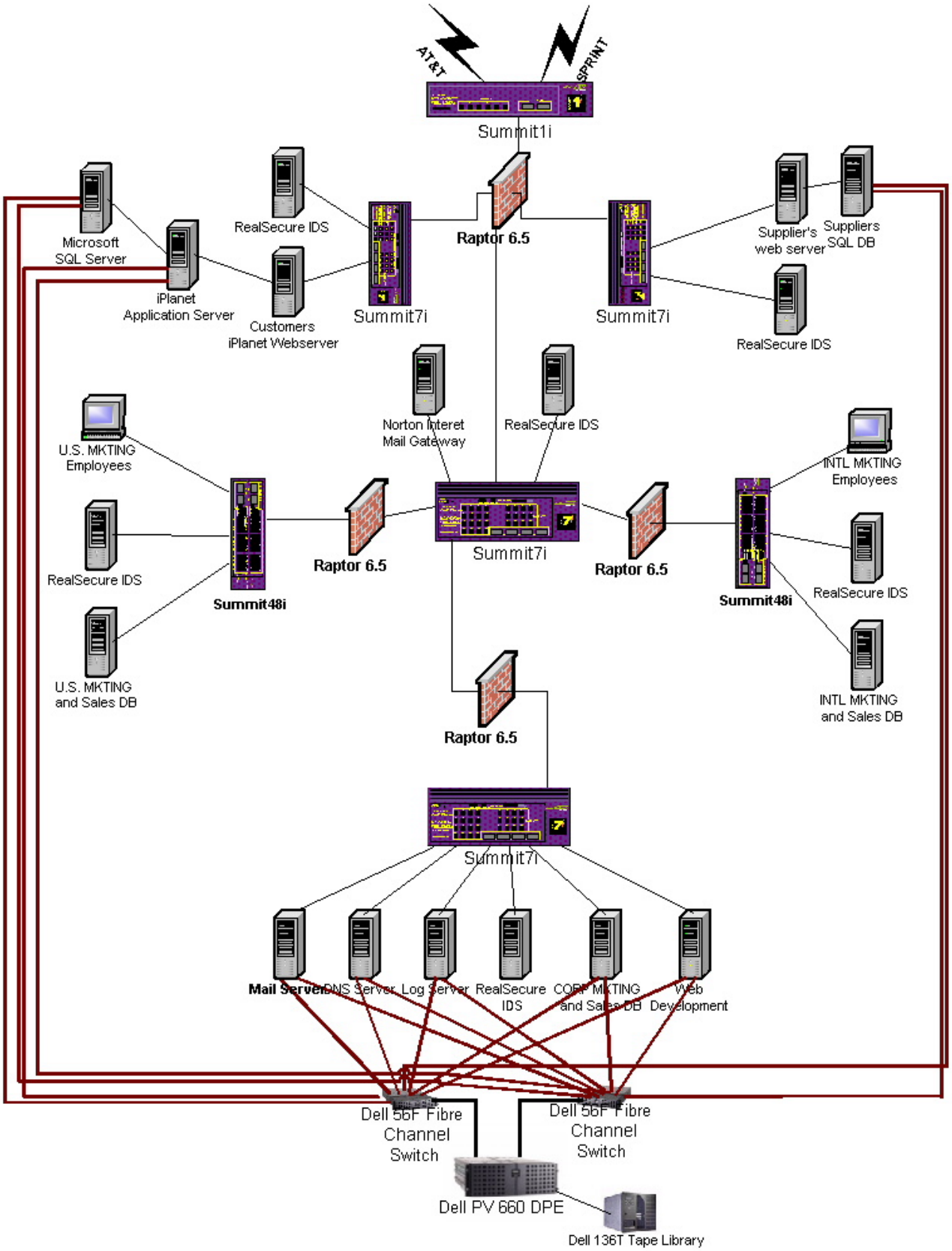


Figure 1

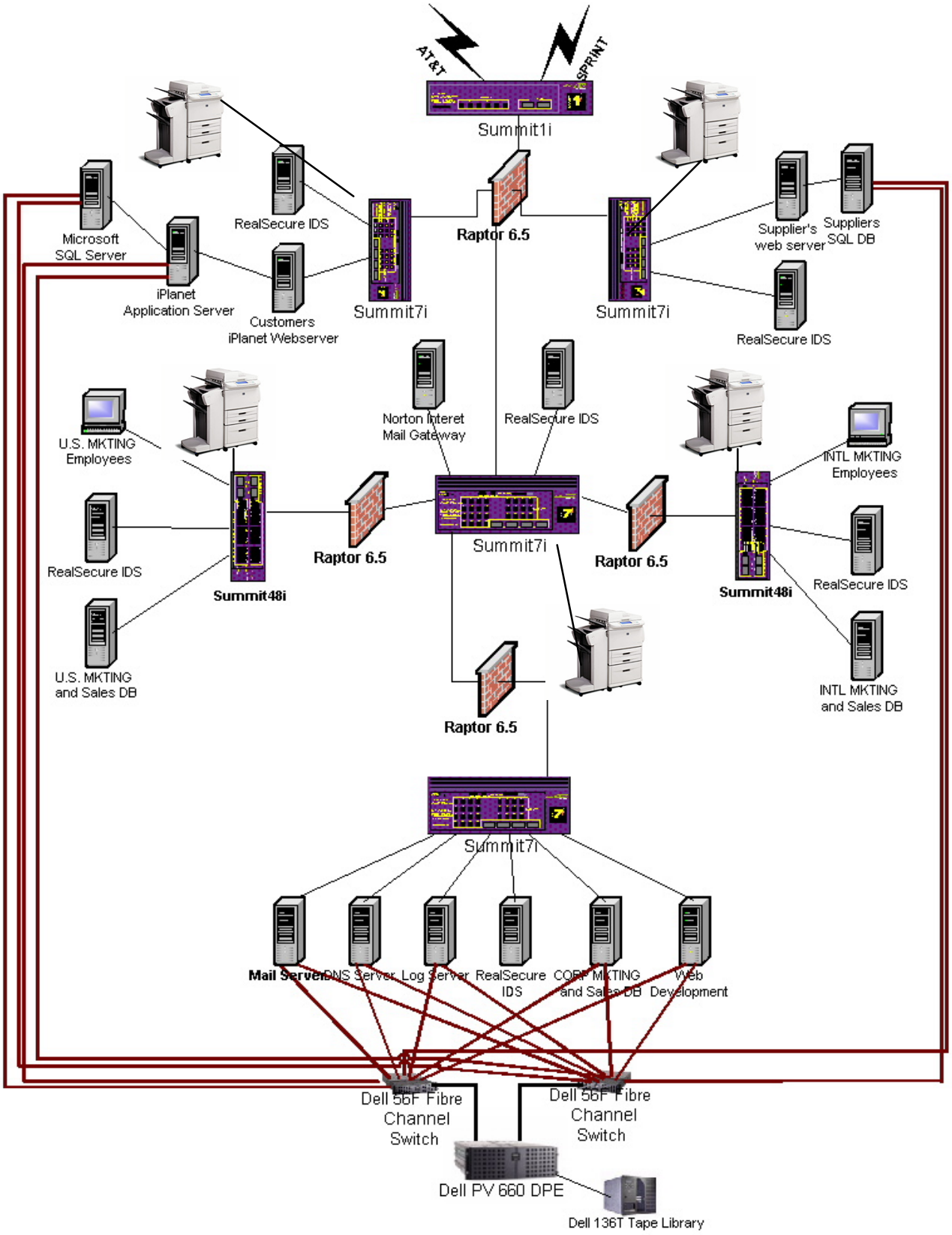


Figure 2

Access Methods

Customers

Customers will have access to only the web server. They will be coming in using HTTPS. This will be enforced by rules set up on the firewall. They will access the web server and, using iPlanet's e-commerce suite, will have a secure method of conducting business.

Suppliers

Suppliers will come in and access a secure web server, which will require them to authenticate before gaining access. User accounts will be created and they will only see their necessary information.

Partners

Partners will gain access by means of raptor mobile and a nested VPN tunnel to the International Marketing Subnet. Any other access to other areas in GIAC Enterprises will require authorization.

ACL Description

Create access-list denyTelnet_23 tcp dest 153.27.38.20/32 ip-port 23 source any ip-port any deny ports any precedence 100 log
(Denies any telnet session to the firewall's external interface and logs it)

Create access-list denyFTP_21 tcp dest 153.27.38.20/32 ip-port 21 source any ip-port any deny ports any precedence 200 log
(Denies any FTP sessions to the firewall's external interface it and logs it)

Create access-list denyRTR ip dest 153.27.210.10/32 ip-port any source any ip-port any deny ports any precedence 300 log
(Denies any attempt to connect to the router and logs it)

Create access-list denyPing icmp dest 153.27.210.10/32 source any type 8 code 0 deny
(Denies any attempt to ping the router. You cannot set precedence on ICMP)

Create access-list denyPrivate_10TF tcp dest any source 10.0.0.0/8 deny precedence 20
(Denies tcp from private addresses)

Create access-list denyPrivate_10UF udp dest any source 10.0.0.0/8 deny precedence 21
(Denies udp from private addresses)

Create access-list denyPrivate_172TF tcp dest any source 172.16.0.0/12 deny precedence 22
(Denies tcp from private addresses)

Create access-list denyPrivate_172UF udp dest any source 172.16.0.0/12 deny precedence 22
(Denies udp from private addresses)

Create access-list denyPrivate_192TF tcp dest any source 192.168.0.0/16 deny precedence 23
(Denies tcp from private addresses)

Create access-list denyPrivate_192UF udp dest any source 192.168.0.0/16 deny precedence 24
(Denies udp from private addresses)

Create access-list denyPrivate_10TT tcp dest 10.0.0.0/8 source any deny precedence 25
(Denies tcp from private addresses)

Create access-list denyPrivate_10UT udp dest 10.0.0.0/8 source any deny precedence 26
(Denies udp from private addresses)

Create access-list denyPrivate_172TT tcp dest 172.16.0.0/12 source any deny precedence 27
(Denies tcp from private addresses)

Create access-list denyPrivate_172UT udp dest 172.16.0.0/12 source any deny precedence 28
(Denies udp from private addresses)

Create access-list denyPrivate_192TT tcp dest 192.168.0.0/16 source any deny precedence 29
(Denies tcp from private addresses)

Create access-list denyPrivate_192UT udp dest 192.168.0.0/16 source any deny precedence 30
(Denies udp from private addresses)

Create access-list allowFW ip dest 153.27.38.20/32 source any permit ports any precedence 500
(allows all other IP traffic to pass to the firewall)

Firewall Rule Description

Rules Required:

1. Rule for suppliers to access web server: Connection in: External NIC; From Source: suppliers group; Destined for: suppliers' web server; coming out: any (Service HTTP and HTTPS)
2. Rule for customers to access the customer web server: Connection in: External NIC; From Source: universe; Destined for: customers' web server; coming out: any (Service HTTP and HTTPS)

3. Rule for employees to access the customer web server: Connection in: Internal NIC; From Source: universe; Destined for: customers' web server; coming out: any (Service HTTP and HTTPS)
4. Rules for E-mail coming in: Raptor has a built in SMTP wizard that will configure your email access for you. It can be modified after creation. It creates all necessary hosts and a rule for mail in and one for mail out. Ensure the mail server is specified as the Norton Mail Gateway IP address. You have to modify the rule for mail going out and change it to be the host entity of the exchange server.
5. Rule for employees to use the Internet: Connection in: Internal NIC; From Source: universe; Destined for: universe; coming out: any (Service HTTP and HTTPS
6. Rule to deny private IPs in: Connection in: External NIC; From Source: Private IP group; Destined for: universe; coming out: any (explicit deny access)
7. Rule to deny private IPs out: Connection in: Internal NIC; From Source: Private IP group; Destined for: universe; coming out: any (explicit deny access)
8. Rule to deny Internal IPs coming in from the outside: Connection in: External NIC; From Source: Internal IPs; Destined for: universe; coming out: any (explicit deny access)

(NOTE: No Rule for DNS is required as we are allowing the primary firewall to act as the DNS proxy. All DNS requests go to it and it goes and gets them for the users.)

Additional rules need to be created to determine who has FTP privileges, Telnet privileges, files that can be downloaded etc. SEF has a vast set of abilities to tighten security.

Protocol Description

The protocol that is being exploited is the Socket API. This allows for TCP connections to port 9100 in order to pass commands to the printer via Printer Job Language (PJL). PJL is a language that was developed by Hewlett Packard in order to facilitate communication between systems and printers. Printers use Printer Command Language (PCL) in order to control different printer features across multiple devices. Within PCL, there are different printer languages used to communicate with the printer and give it the specifics of what it needs to do. This is where PJL comes into play. With PJL, you can tell a printer what you do and even how to configure itself. (http://www.hp.com/cposupport/printers/support_doc/bpl04568.html)

The characteristics of PCL and PJL lend to its weaknesses. Most of Hewlett Packard's (HP) printers all listen on port 9100 by default and they all speak the same language. HP is the originator of this common language and almost all

major printer manufacturers have come on board to establish the same language for ease of use as well as the overall standardization of printers. While this is good for configuration management and ease of use, it lends itself to being a security weakness because all of the printers depend on it and listen to it. (http://www.cruzio.com/~jeffl/sco/lp/printservers.htm)

How the Exploit Works

FtR of Phenoelit developed a tool called Hijetter. According to Phenoelit, "The Hijetter gives you the opportunity to explore printers via their PJL interface. This includes access to the environment variables, the file system and the display of the target." (http://www.phenoelit.de/fr/tools.html) This tool takes advantage specifically of HP printers. Because HP printers are standardized to listen on port 9100 it was only a matter of time before tools were created that had useful/detrimental abilities. FtR has done all of the hard work to establish the socket and verify the printer is listening. Here is the real danger of the tool; it requires no understanding of what is happening underneath in order to make it work.

Source Code Description

For the purpose of this description of the source code, I am not going to go through all of it, but rather the major first pieces, which describe what is taking place. The code would take up over 22 pages and it is not necessary to describe all of it. If you would like to view the source code, go to http://www.phenoelit.de/fr/tools.html to the download section for Hijetter and download the Visual C++ (VC++) source code for a complete package.

The following section is just the standard packages being used within the code. There are UNIX options as well as windows options. Some of the packages are not standard and were written by FtR. They are included in the complete C++ package that you can download.

```
/*
 * PJL File Transfer
 *
 * command line interface to PJLlib functionality
 * is extended as lib grows
 *
 * first attempt
 *
 * $Id: main.cpp,v 1.6 2002/01/30 11:54:16 fx Exp fx $
 */
#include <iostream.h>
#include <stdio.h>                  // cant live without printf() ;)

#ifndef UNIX
// Windows header files
#include <direct.h>                 // _getcwd() ...
#include <io.h>                     // _open()
#include <fcntl.h>                  //  -"-
```

```
#include <sys/types.h>             //  -"-
#include <sys/stat.h>              //  -"-
#include <conio.h>                 // if key pressed _kbhit()
#else
// UNIX header files
#include <stdlib.h>
#include <unistd.h>
#include <signal.h>
#include <sys/types.h>             // open(), close(), write()
#include <sys/stat.h>
#include <fcntl.h>
#endif UNIX

#include "fxstrings.h"
#include "pjlsession.h"
#include "commands.h"

#define SPLASH              "PFT - PJL file transfer\n" \
                        "\tFX of Phenoelit <fx@phenoelit.de>\n"\
                              "\tVersion 0.6 ($Revision: 1.6
$)\n"\
                              "\tPhenoelit INTERNAL Code - DO NOT
DISTRIBUTE!\n"
#define GENERIC_ERROR   "syntax error (try help)"

// commands available in command line
#define CMD_QUIT        "quit"
#define CMD_EXIT        "exit"
#define CMD_HELP        "help"
#define CMD_SERVER            "server"
#define CMD_PORT        "port"
#define CMD_CONNECT           "connect"
#define CMD_CLOSE       "close"
#define CMD_ENV               "env"
#define CMD_ENV_READ          "read"
#define CMD_ENV_PRINT         "print"
#define CMD_ENV_COMMIT        "commit"
#define CMD_ENV_SHOW          "show"
#define CMD_ENV_SET                "set"
#define CMD_ENV_OPTIONS       "options"
#define CMD_ENV_CHANGED       "changed"
#define CMD_ENV_UNPROTECT     "unprotect"
#define CMD_ENV_BRUTEFORCE    "bruteforce"
#define CMD_MESSAGE           "message"
#define CMD_FAILURE           "failure"
#define CMD_VOLUMES           "volumes"
#define CMD_LS                "ls"
#define CMD_CD                "cd"
#define CMD_PWD               "pwd"
#define CMD_CHVOL       "chvol"
#define CMD_RM                "rm"
#define CMD_MKDIR       "mkdir"
#define CMD_LPWD        "lpwd"
#define CMD_LCD               "lcd"
#define CMD_GET               "get"
#define CMD_PUT               "put"
```

```
#define CMD_APPEND            "append"
#define CMD_SESSION           "session"
#define CMD_TIMEOUT           "timeout"
#define CMD_PAUSE       "pause"
#define CMD_PRINTERNAME       "printername"
#define CMD_SELFTEST          "selftest"

PJLsession              sess;
bool                    end_application=false;


// prototypes
void  usage(char *s);
void  read_command(String *s);
void  cmdloop(void);
void  print_help(char *cc);
void  commandline_ident(void);
#ifdef UNIX
void  sighandl(int s);
#endif UNIX


class Program_config {
      public:
            String                  server;
            unsigned int      port;
            String                  pwd;
            String                  pvol;
            String                  lpwd;
            bool              pause;
#ifdef UNIX
            bool              ctrlc;
#endif UNIX
};
```

Here is the main program for Hijetter. It sets a variable for the default printer IP address and the default port. It also sets two other control variables. It initializes the array pointer and gets the present working directory if compiled and run on Unix, Otherwise it gets the current working directory.

```
Program_config          cfg;

int main(int argc, char **argv) {

      cfg.server="10.1.1.16";
      cfg.port=9100;
      cfg.pause=true;
#ifdef UNIX
      cfg.ctrlc=false;
      signal(SIGINT,&sighandl);

      {
```

```
            char  cwdb[2048];
            cfg.lpwd=getcwd(cwdb,2048);
      }
#else
      cfg.lpwd=_getcwd(NULL,0);
#endif UNIX
```

Here is the code that takes the input from the command line. If there are more than three arguments, it returns a usage message and then exits.
If there are two arguments, it assigns cfg.server the IP address of the printer it is to look at and drops out of the if statement to the rest of the program. If there are three arguments, it takes the IP address and then gets the device ID and exits.

```
      if (argc>3) {
            usage(argv[0]);
            return(-1);
      } else if (argc==2) {
            cfg.server=argv[1];
      } else if (argc==3) {
            cfg.server=argv[1];
            commandline_ident();
            return 0;
      }
```

After entering the correct syntax, it puts a message on the screen about the Hijetter program and then drops down to the cmdloop while waiting on input from the user.

```
      cout << SPLASH << endl;

      cmdloop();

      return 0;
}


// function implementation
#ifdef UNIX
void sighandl(int s) {
      cfg.ctrlc=true;
}
#endif UNIX
```

Here is a partial look at the loop. This basically controls all of the options that you have. From here you can run a multitude of different commands. If you look back at the top of the program each of these are defined with a #define and will give you a general idea of what you can do. Basically, while not the end of the application, keep looping and doing what the user wants. You can set your port and then run a connect command to establish a socket with the printer on your port of choice. For our purposes we will be using port 9100. Once a socket is established you can execute commands on the printer.

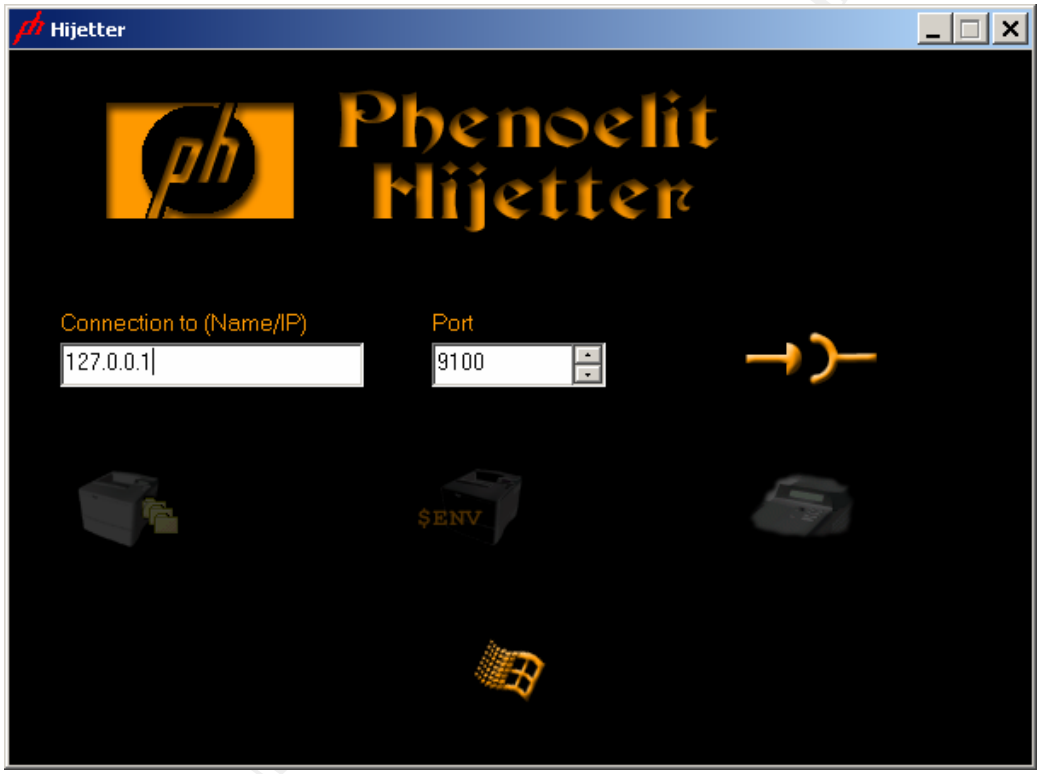
```
void cmdloop(void) {
      String                  cmd;
      String                  basecmd;

      while (!end_application) {
            cout << "pft> ";
            read_command(&cmd);
            cmd.chomp();
            //cerr << "DEBUG >>>>" << cmd.get() << "<<<<" << endl;

            // catch single command lines
            if (cmd.token(' ',0)==NULL) {
                  basecmd=cmd.get();
            } else {
                  basecmd=cmd.token(' ',0);
            }

            // user requested end of communication ;)
            if (basecmd==CMD_QUIT) {
                  end_application=true;
                  continue;
            }

            // user wants to end talking but with the wrong cmd ;)
            else if (basecmd==CMD_EXIT) {
                  cout << "Did you try 'quit'?"<<endl;
                  continue;
            }

            // user want help
            else if (basecmd==CMD_HELP) {
                  print_help(cmd.token(' ',1));
            }

            // user wants to set the server
            else if (basecmd==CMD_SERVER) {
                  if (cmd.token(' ',1)==NULL) {
                        cerr << GENERIC_ERROR << endl;
                        continue;
                  }
                  cfg.server=cmd.token(' ',1);
                  cout << "Server set to " << cfg.server.get() << endl;
            }

            // user wants to set port
            else if (basecmd==CMD_PORT) {
                  if (cmd.token(' ',1)==NULL) {
                        cerr << GENERIC_ERROR << endl;
                        continue;
                  }
                  cfg.port=atoi(cmd.token(' ',1));
                  cout << "Port set to " << cfg.port << endl;
            }

            // user would like to connect
            else if (basecmd==CMD_CONNECT) {
```

(snip)

The code itself is not very difficult to understand and the command lines are relatively simple. For our convenience, FtR has put this into a nice Windows GUI that allows point and click access to the commands. You will get a better understanding of the capabilities from the windows description below, especially for all of the non-command line individuals!

Compiled Code Description

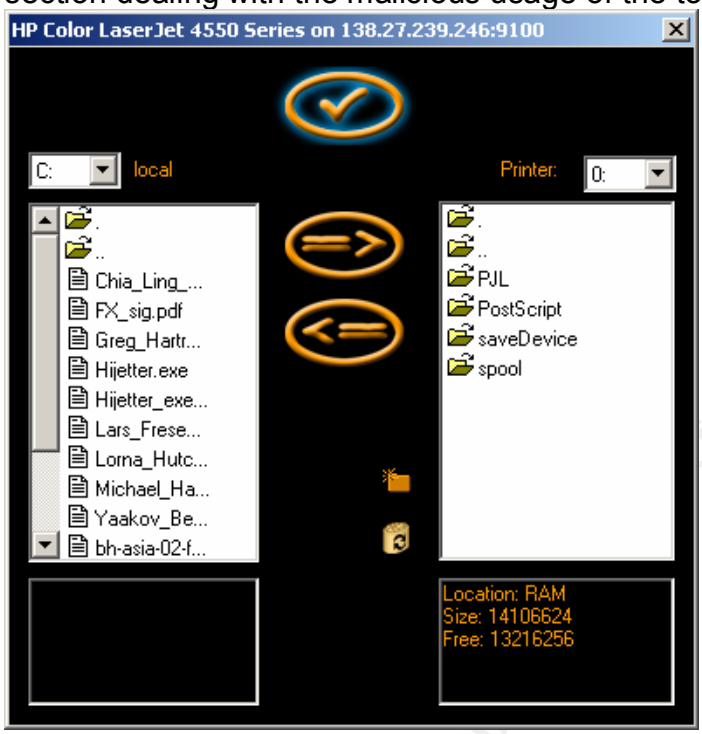
First, enter the IP address of the printer you wish to establish a connection with and choose your port. If your printer doesn't listen on port 9100 or it has been changed, no problem, just select the port you wish to connect to.



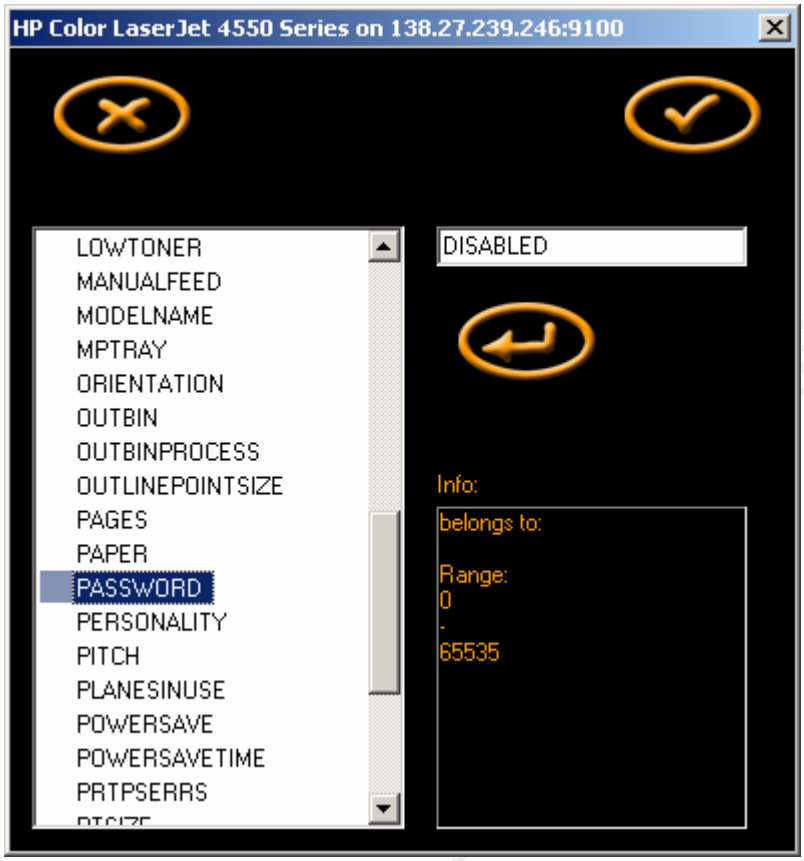
To the right of the IP address box and the Port box, you see an object that looks like it should fit together. If you click on this or just hit enter, Hijetter will attempt to establish the connection.

Once the connection is established, you will get a screen that gives you three options as seen below and each will be discussed. The printer on the left takes you into the file system of the printer and lets you transfer files on and off the printer. The middle printer with the $env on it allows you to set the printer's environment variables. The last icon on the right that looks like a fax allows for you to change the display. Each of these is discussed below.

First off, you have the ability to move files onto or off of the printer. This function only works as long as the printer has a hard drive and is not write protected. The majority of the printers do have a write enabled hard drive. As you see in the following screen, it is extremely easy to use and requires no effort. However, the implications of this ability are staggering. These will be discussed in the next section dealing with the malicious usage of the tool itself.



Now, you have the option to setup the printer however you wish. It will give you all of the options available on that printer and allow you to set them. This can have very bad implications as you can very well imagine.



Last, but not least, you can choose to change your display message. If the message type is display, it just changes the displayed message, which is usually "Ready." However, if you click failure, all the lights come on and people get really excited. Hitting the "Online" button will reset it, however FtR says, "The fun starts if you disable the printer buttons via the environment variables first." Once again, it has scary implementations.

Description and Diagram of the Attack

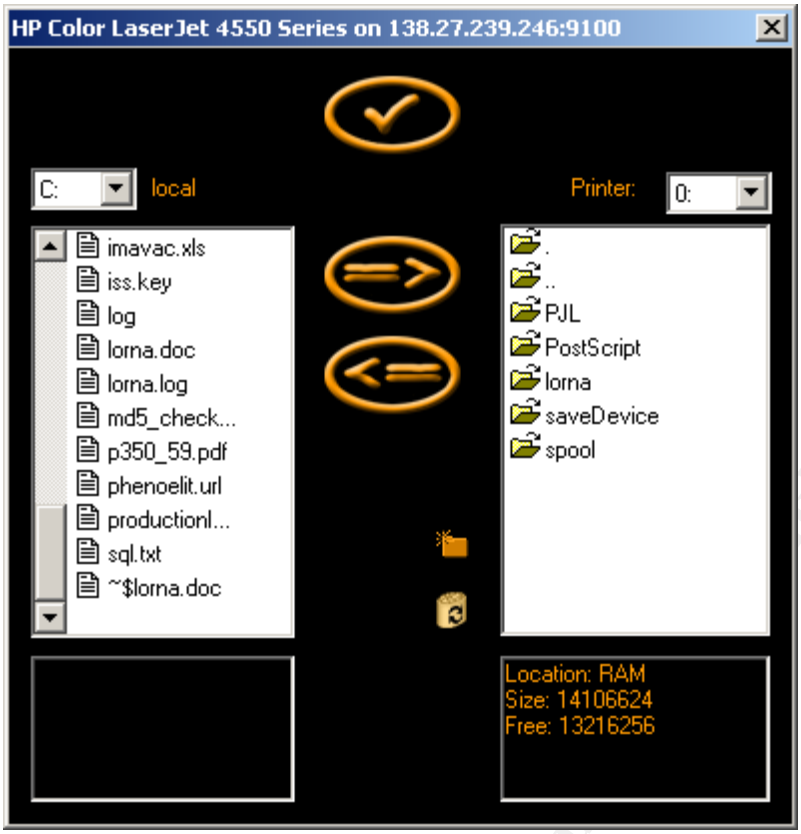
The attack itself is one that could be carried out from inside or outside of the firewall, depending on the purpose/motive of the individual. Many people today, in order to facilitate access, place their printers on the outside of the firewall and then remotely manage them. They not only do this, but they also allow access to internal printers. After all, it just prints right? For the purposes of our example and theoretical network, the printers have all been placed in logical areas. Each of the major departments has multifunctional units and folks from the outside only have access to facilitate transactions or to print information that someone else needs. They all also have remote management ability.

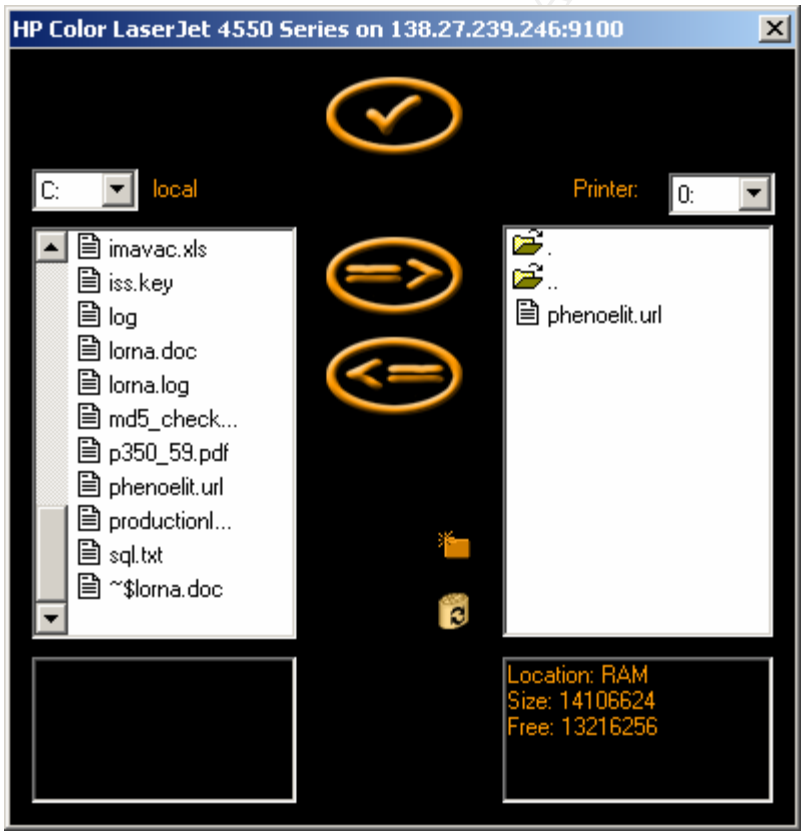
There is more than one usage for this type of attack/vulnerability. We are going to look at a couple of different scenarios and how the printer compromise could be utilized.

Print Job Status/Collection

This is an undocumented exploit that is completely theoritical as of this time. I can find no documentation that it has occurred, but it seems feasible and I am not the only one who thinks so. Dennis Mattison addresses this same issue in his paper entitled "Network Printers and Other Peripherals-Vulnerability and Fixes." He writes about the concept of print job forwarding. Having a copy sent to an alternate IP address in addition to printing it. I would like to look at it a little differently and see what the print job spooler is leaving on the hard drive of the printer, especially the multifunctional devices which do scanning, emailing, etc. of files. The HP 4100 we are looking at (remember, it was chosen at random) describes in the User's Guide that it has a "Hard disk (for job retention)." (User Guide, 19) It also describes what is called Job Retention. This is where a copy of the job is able to be saved on the printer (you even get to name it) and be accessed for later usage. (User Guide, 67). With the multifunction device you do not even need a computer to access email or the network.

Since I do not have a HP 4100 available I am unable to test or attempt some of the scenarios posed in the theory. However, I do know that I can copy to and from an HP printer's hard drive and as such, I have access to the entire file structure on the system. I did substitute a regular HP 4550TN and experimented with it. The pictures below provide a look at the file structure on the printer. As you can see I created a directory on the printer named "lorna." This was done through the nice little graphic interface of Hijetter. I also then moved one of my files, "phenolit.url" over to the printer. I can take files from the printer as well. Because of this, if I have free access to the hard drive, I should be able to pull anything off of the multifunction device that is stored there as well. If I run into trouble, I can just access the environment variables, through Hijetter, and change them to get me what I need. Remember, this is considering people deploy the printer pretty much out of the box and with full functionality.





By default, the web server and email capability are enabled on the printer. I can access what I need/want on the printer. As more and more files get stored on the printer for convenience, the risk associated with them goes up drastically. Think about it for a minute, you now have key pieces of the organization's data traffic going through your multifunction device. This information will be available to whoever has access to the printer. Consider those entities from our network design that have access to the printer. In order for them to have bi-directional communication, port 9100 will have to be allowed through the firewall for them. Now, the network design that you worked so hard on to secure just got a hole in it by a printer. The international folks have access to only the international multifunction printer, but who else uses it. How many of the other sections send data to this device? How hard would it be to connect and pull off stored jobs every so often? I have checked the documentation and can't find logging capabilities or security features other than a password to access the web server. This theoretical exploit, while not complicated, may give a whole to meaning to corporate espionage.

Unauthorized storage

While this is not a typical exploit, you can use a printer's storage capability for something other than its intended purpose. As I have stated, most security personnel who secure a network, perform an assessment, monitor a network, etc. never look at the printers. As a matter of fact, I am not sure I have ever heard printers discussed as a concern. What is to stop someone from our suppliers group from accessing the printer and storing their child pornography on there or something else that they don't want to get caught with? How about a pickup and drop off location for data that they are trying to hide? The lists of possibilities are endless if no one is looking at the file system. Hackers have a great use for printers. Why leave your tools where they cannot be found? Just store them on a printer somewhere and access them as needed. What an easy way to transfer files, unnoticed, onto an unsuspecting network. At the last DefCon in Las Vegas, a briefing was given by FX and kim0 on "Attacking Networked Embedded Systems." (http://www.blackhat.com/presentations/bh-asia-02/bh-asia-02-fx.pdf) Part of this topic was on HP printers and their vulnerabilities. If, as security professionals, we believe that these devices are insignificant, we need to think again.

Notice I did not spend a lot of time looking at the network configuration of our theoretical design and how to worm our way through it. This was for a reason. As I said before, the game was over when access to the printer was granted from the outside. But, think about the internal threat for a moment. There is just as much danger from the inside threat as well. All of the well-positioned firewalls are not going to protect against this when access to the different multifunctional devices are granted. Even if we didn't have this tool, the ability to send PJL commands to the printer is available. Hijetter just made it point and click.

Signature of the Attack

How do we begin to determine if a printer has been attacked? In most cases it is very difficult. Since printers and multifunctional devices have long since been viewed a just a basic function, the security aspect is severely weak. Even when it is addressed, it typically does not reflect the standards that one expects from other devices. The logging capability is more for the usage information such as paper, ink, number of jobs etc. There is nothing that logs accesses, attempts, or other issues that you normally on other networked devices with the equivalent capabilities. Mr. Mattison provided examples of several attempts to work with the manufacturers to fix vulnerabilities. He summarizes up the problem accurately. "Most vendors don't understand the implications, and thus will deny a problem exists, will threaten the vulnerability researcher with legal action if the vulnerability is exposed, or will downplay its threat or discredit its importance. To most of these companies, security is a new issue, and one that they haven't planned for, so getting them to work with you on a security issue is difficult and frustrating." (Mattison, 28) As a result, printers, multifunctional devices and other peripheral pieces of equipment go uncared for and certainly not watched for vulnerabilities.

As of now, I have been unable to find any signature that will detect unauthorized access to a printer or specifically the Hijetter software in an IDS signature. This does not surprise me as the number of folks that are concerned about peripheral devices are few and far between. As a matter of fact, some of my co-workers thought I had lost my mind doing my paper on printer exploits. Most people seem to feel it would be a waste of time to watch a printer for an exploit. After all, what can you do but maybe a buffer overflow, change the display, and print all the paper out of it. It is just a printer, right?

How to Protect Against It

Now comes the hard question, how do we fix the problem. There are definitely two sides that it will take to fix the issue. One side resides with us as security professionals and the other side rests heavily on the vendor. Without efforts from both sides, the problem will not be addressed.

What can we do?

In the mean time, what can be done? Here are a few suggestions, but each organization will have to decide what is right for them.

1. First off, we need to turn off unwanted services. Do we really need the web browser? What about the telnet, FTP and email services? Each organization is going to have to make some informed decisions about what is the acceptable risk level by leaving those services active. An informed decision will entail understanding the risk to the organization, not just the printers, if the services are left active.

2. Second, we need to make sure the firmware stays up to date. Ensure that the latest firmware updates and patches are applied to the peripheral devices.
3. If at all possible, turn on all logging that is available. You may be able to see trends in production increases, disk size shrinkage, etc.
4. Monitor the hard drives of the printers. KNOW what the file system should look like and ensure that it does not change.
5. If there is a way to password protect a feature, do it. Also ensure that the user has what they need to do their job and nothing more. Remember the concept of least privilege.
6. Ensure the users understand and are properly trained on the devices. Make sure they know if they store a print job, others could potentially access it. User awareness if very key.
7. Place your printers or peripheral devices behind the firewall and do not allow access from the outside in to them. Internal monitoring is going to be a different issue with regard to the insider threat.

In all fairness to HP, they do have a document (however buried and difficult it is to find) at http://www.hp.com/cposupport/networking/support_doc/bpj05999.html that deals will ways to lock down their printers. Some are discussed above; others depend on what you need for your organization. Whatever the case, security professionals are going to have to become more aware and broaden their knowledge base.

What can the vendors do?

Here is the real crutch of the matter: what the manufacturer's can do. There is not a simple answer. Manufacturers build devices to perform specific functions. Unfortunately the devices were never meant to need security. As such, building logging for a printer/multifunctional device has never been an issue. They do not understand, nor realize that when they connect it to a network it becomes more than a printer. The above quoted SANS Security News Letter states, "In August, four network printers at the University of New Mexico were employed in a denial of service attack." (SANS Security Alert, 3) Many people seemed shocked that a printer could do such a thing. But think about the characteristics of the multifunctional device I described at the beginning. Does that sound like just a printer? Manufacturers are going to have to become aware of and understand the vulnerabilities they introduce every time they expand the capabilities of their devices. However, this is not just going to happen and hence our vicious circle has begun. Why implement something that cost money if no one is complaining? If they industry does not hear cries from the security community, nothing will ever change.

What are some things that manufacturers can do if we lived in the perfect world and they would do them without being forced into it? I am going to look at some of the bare basics and not get too elaborate.

1. A good logging system is needed. The logs need to reflect accesses, from whom, what protocol, time, IP Address, changes in file system, etc. Knowing the status of your printer and its supplies is good, but that is not all that should be logged. If some one was on your printer at 0300 in the morning and no one is at the office at that time, wouldn't you want to know it? If your hard drive suddenly had a Gigabit of storage used in a day, which would be useful to know. As it stands now, we do not have that capability.
2. Access control lists are a very much-needed feature. Some of the newer devices are implementing limited ability to use access control lists. It would be great to control what users can do what on the printer, as well as logging it.
3. Providing greater control over the services offered. Some of the manufacturers and models of the peripheral devices do not allow you to turn off the functionality. You are just stuck with the services running whether you want them to or not.
4. Implementing a better, more secure method for access the printers for configuration. Many printers just use telnet, FTP or web administration for the remote configuration of the systems. They are not even encrypted in their communications, or, if they are, it is not a secure method of encryption.

Until manufacturers are held accountable for their devices and something major occurs using one of them, our chances of getting things fixed are not really good. Something is going to have to occur that raises the sensitivity level to these peripheral devices and force the manufacturers to build more secure devices.

Part 3: The Incident Handling Process

This practical is based on a theoretical network design and attack. As such, the Incident handling process will be modeled after that network. All areas discussed in here were taken from what I view a normal network would look like. If something is not what you would normally find, I treat it as such in the scenario. The network from the firewall practical is part of GIAC Enterprises, a company who sells fortune cookies. They have different business areas internal to the company that is sectioned off by firewalls such as the U.S. Marketing section and the International Marketing section. There are two service networks, one of which is for the customers who come to the company to place orders and the other is for the suppliers drop off fortunes for the cookies. Because of the need to streamline and consolidate, it was decided that multifunctional devices would be the ideal solution for the company's needs. These data centers would reduce the number of individual devices and provide a way for greater production and a much greater expansion of abilities. A multifunctional device was bought for each of the major areas mentioned above. Now each of the areas can send print jobs, faxes, scanned data, etc. to other areas without having to physically go there or try to send it via another method. Because of the need for the multifunctional devices to be used by other areas and for management of the devices, each division is allowed to use each other's devices. As we walk through this scenario, all things that were done incorrectly or recommendations will be address in the lessons learned section.

Preparation

-Existing Countermeasures/Policy

GIAC Enterprises has very good policy in place dealing with network security. All operating systems have security lockdown settings (see Figure 3) that were kept up to date. There was a written firewall policy (See figure 4) governing what could and could not leave the network and actions that were to be taken. All users had a user manual (See Figure 5) that they were required to keep and sign, acknowledgeing their understanding of the contents. Each of the systems was required to have warning banners before access was attempted. They are also using RealSecure IDS on all of the major network segments. However, nothing in the policy addressed printers and their usage. As a rapidly growing forture 500 company, the concentration of effort was on securing data that was their livelihood and keeping up with the consumer demands. The addition of the multifunctional devices did not raise any flags for the security team. After all, they were just printers right?

Figure 3: GIAC Enterprises Security Lockdown Settings for Operating Systems

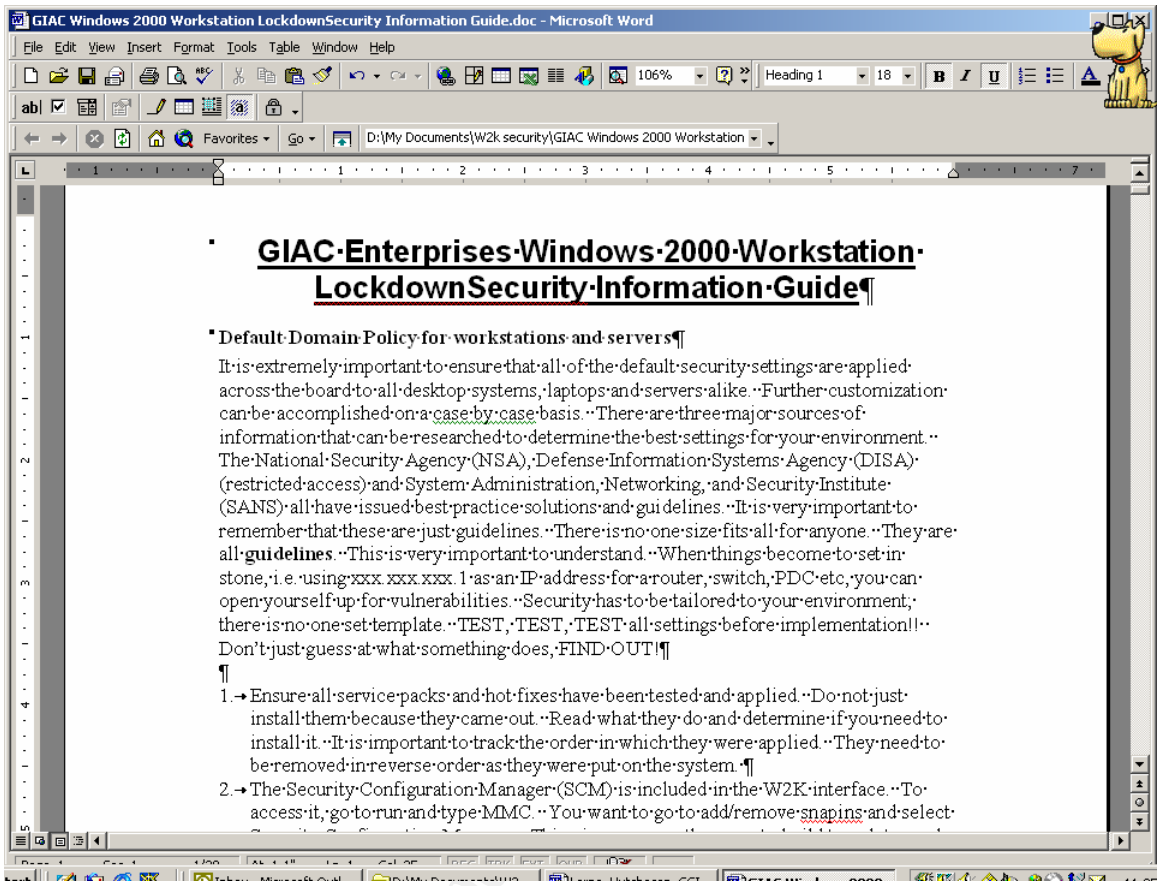


Figure 4 GIAC Enterprises Firewall Policy Table Of Contents

GIAC Enterprises Firewall Policy

6.1. Background and Purpose 3
6.1.1. Roles and Responsibilities 3
6.1.1.1. Information Assurance Program Manager (IAPM) . 4
6.1.1.2. Information Assurance Security Officer (IASO) . 4
6.1.1.3. Firewall Administrator . 4
6.2. Authentication 6
6.3. Routing Versus Forwarding 6
6.4. Firewall Architectures 6
6.4.1. Multi-homed host . 6
6.4.2. Services Network . 6
6.5. Firewall Administration 7
6.5.1. Qualification of the Firewall Administrator . 7
6.5.2. Remote Firewall Administration . 7
6.5.3. User Accounts . 7
6.5.3.1. Firewall Backup 8
6.6. Network Trust Relationships 8
6.7. Virtual Private Networks (VPN) 8
6.7.1 International Marketing Group . 8
6.7.2 U.S. Marketing Group . 8
6.8. DNS Resolution 9
6.9. System Integrity 9
6.10. Documentation 9
6.11. Physical Firewall Security 10
6.11.1. WINDOWS: 10
6.11.2. WALLS: 10
6.11.3. CEILING: 10
6.11.4. DOORS: 10
6.11.5. COMPUTER ROOM: 11
6.11.6. FIREWALL: 11
6.12. Firewall Incident Handling 11
6.12.1. Reporting Chain of Command: 12
6.12.2. Report Format 13
6.13. Restoration of Services 14
6.14. Upgrading the firewall 14
6.15. Revision/Update of Firewall Policy 15
6.16. Logs and Audit Trails (Audit/Event Reporting and Summaries) 15
6.17. GIAC Enterprises Access Policy 15
6.18. Service-Specific Policies 17
6.18.1 Managerial Level Policy 18
6.18.2 Technical Policies 22
6.18.2.1. GIAC Enterprises to Universe Policy 22
6.18.2.2. Universe to Services Network Policy 25
6.18.2.3. Services Network to GIAC EnterprisesPolicy 27
6.18.2.4. Firewall Scan Policy 28

Figure 5: GIAC Enterprises User's Guide Table of Contents

1.0 INTRODUCTION 1-1

1.1 PURPOSE 1-1
1.2 SCOPE 1-1
1.3 DOCUMENT ORGANIZATION 1-1

2.0 SYSTEM RULES OF BEHAVIOR 2-1

2.1 WHAT ARE RULES OF BEHAVIOR 2-1
2.2 WHY RULES OF BEHAVIOR ARE NEEDED 2-1
2.3 GENERAL PRINCIPLES 2-1

3.0 SYSTEM SECURITY OVERVIEW 3-1

3.1 SYSTEM PHILOSOPHY OF PROTECTION 3-1
3.1.1 Security Policies 3-2
3.1.2 Access and Privilege Control 3-2
3.1.3 Workstation Restrictions 3-2
3.2 SYSTEM LEVELS OF PROTECTION 3-3
3.3 TRUSTED FACILITY OPERATIONS 3-3
3.4 SITE COMPOSITION 3-3
3.5 MALICIOUS LOGIC 3-4
3.5.1 Indications of System Infection 3-4
3.5.2 Virus Attack Response 3-4
3.6 COUNTERMEASURE PROCEDURES 3-4

4.0 USER SECURITY GUIDANCE 4-1

4.1 LOGGING ON TO THE SYSTEM 4-1
4.2 USER I&A 4-1
4.3 PROFILES 4-1
4.4 LOGGING OFF THE SYSTEM 4-2
4.5 FILE SYSTEM GUIDANCE 4-2
4.6 DISCRETIONARY ACCESS CONTROL 4-2
4.7 SECURITY ROLES AND RESPONSIBILITIES 4-4
4.7.1 Information Assurance Security Officer (IASO) Roles and Responsibilities 4-4
4.7.2 Information System User Roles and Responsibilities 4-5

5.0 PERSONAL LIABILITY 5-9

6.0 ACKNOWLEDGMENT. 6-10

-Incident Handling process

GIAC Enterprises had grown so rapidly, that a team was not in place yet for handling incidents. The rapid growth of the company and the implementation of a new network design had left the IT and Security folks exhausted. All efforts went into securing the computers, servers, switches/routers etc. They went to great lengths to establish these lockdowns and to ensure their network's security. As such, they had not yet considered how to handle an incident. Having a true incident handling team had not yet been part of the preparation. As such, there was much confusion and debate on how to handle the issue and if it should even be called an incident. No one was even sure whom to call and if they should contact authorities. After all, that would bring bad press upon the company and they were just starting to see their potential. Because no one had experience and because there was no one in charge of this area, a lot of things were done incorrectly.

Identification

-Incident Detection

The detection of this incident did not occur because of some network security device that was in place or an IDS that triggered an alert. It was found because of good policies and procedures. Part of the policies and procedures involve regular random network scans and war dialing. The tool of choice for vulnerabilities was Nessus. However, a simple batch process detected this incident. The security team randomly scanned the network with different policies and procedures looking for anything unusual and watching for anything unauthorized. At this particular time, they were scanning with a procedure to look at running processes. A batch file was run as an administrator account that goes out and queries the network and looks at services, processes, listening ports, etc. One of the tools that was used in the batch file was called PULIST.exe and can be found at http://www.microsoft.com/windows2000/techinfo/reskit/tools/existing/pulist-o.asp. This tool enables you to query remote systems for runningprocesses and find out who is running them. After systems are scanned, the data is fed into a database and the security team is able to look at what is running on the network and who is doing it. The scan results picked up an executable that no one was familiar with called Hijetter.exe on a Windows 2000 box. Here is what the output showed:

Process	PID	User
Idle	0	
System	8	
SMSS.EXE	140	NT AUTHORITY\SYSTEM
CSRSS.EXE	168	NT AUTHORITY\SYSTEM
WINLOGON.EXE	164	NT AUTHORITY\SYSTEM
SERVICES.EXE	216	NT AUTHORITY\SYSTEM
LSASS.EXE	228	NT AUTHORITY\SYSTEM

SVCHOST.EXE	408	NT AUTHORITY\SYSTEM
lexbces.exe	432	NT AUTHORITY\SYSTEM
SPOOLSV.EXE	468	NT AUTHORITY\SYSTEM
lexpps.exe	496	NT AUTHORITY\SYSTEM
defwatch.exe	560	NT AUTHORITY\SYSTEM
dklog.exe	576	NT AUTHORITY\SYSTEM
SVCHOST.EXE	600	NT AUTHORITY\SYSTEM
mdm.exe	624	NT AUTHORITY\SYSTEM
rtvscan.exe	672	NT AUTHORITY\SYSTEM
nvsvc32.exe	256	NT AUTHORITY\SYSTEM
regsvc.exe	724	NT AUTHORITY\SYSTEM
mstask.exe	740	NT AUTHORITY\SYSTEM
vsmon.exe	788	NT AUTHORITY\SYSTEM
minilog.exe	832	NT AUTHORITY\SYSTEM
MSGSYS.EXE	1020	NT AUTHORITY\SYSTEM
explorer.exe	284	BADUSER\evildoer
SynTPLpr.exe	1212	BADUSER\evildoer
SynTPEnh.exe	1236	BADUSER\evildoer
DadApp.exe	1252	BADUSER\evildoer
dadtray.exe	1272	BADUSER\evildoer
prpcui.exe	1280	BADUSER\evildoer
realplay.exe	1068	BADUSER\evildoer
vptray.exe	1308	BADUSER\evildoer
EM_EXEC.EXE	1320	BADUSER\evildoer
rsMenu.exe	1336	BADUSER\evildoer
CasAgnt.exe	1348	BADUSER\evildoer
LMpdpsrv.exe	1372	BADUSER\evildoer
CTFMON.EXE	1380	BADUSER\evildoer
LEX125SU.exe	1420	BADUSER\evildoer
QWDLLS.EXE	1436	BADUSER\evildoer
zonealarm.exe	1456	BADUSER\evildoer
IXApplet.exe	1468	BADUSER\evildoer
QDCTray.exe	1476	BADUSER\evildoer
MSOFFICE.EXE	1496	BADUSER\evildoer
OUTLOOK.EXE	1028	BADUSER\evildoer
DLLHOST.EXE	1584	BADUSER\evildoer
WINWORD.EXE	1608	BADUSER\evildoer
WINMINE.EXE	1740	BADUSER\evildoer
IEXPLORE.EXE	800	BADUSER\evildoer
CMD.EXE	1596	BADUSER\evildoer
AcroRd32.exe	1764	BADUSER\evildoer
Hijetter.exe	**1760**	**BADUSER\evildoer**
msiexec.exe	1636	NT AUTHORITY\SYSTEM
pulist.exe	1192	BADUSER\evildoer

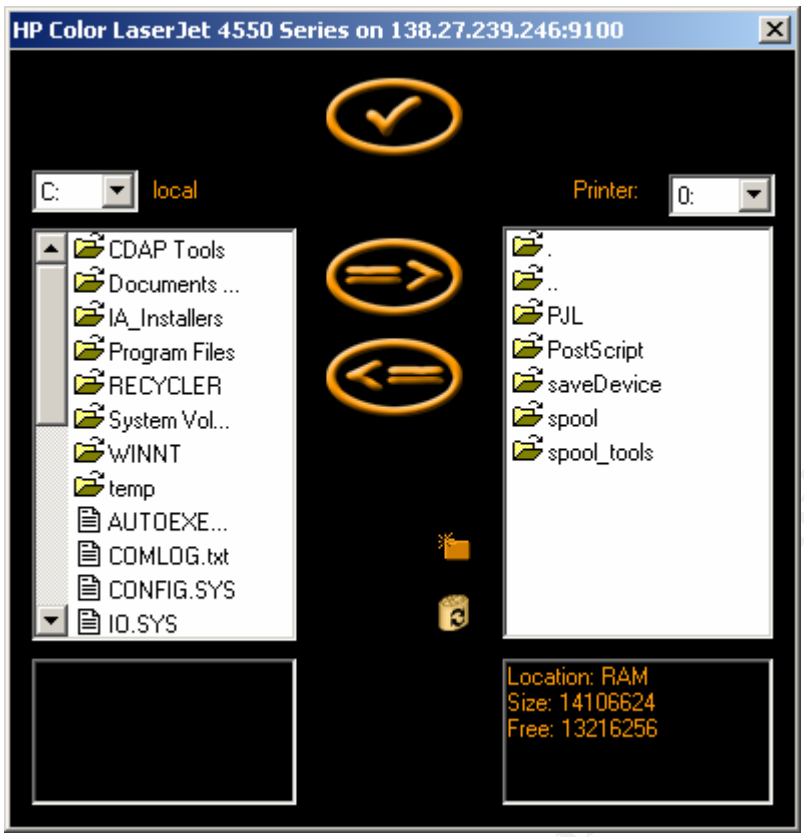
Because no one was familiar with the program, a google search was done that lead them to an interesting discovery, the program is used to access HP printers over port 9100/TCP. After reviewing the programs abilities, a level of concern was raised and they decided it should be elevated higher to the rest of the security team.

-Notify Appropriate Officials

The discovery was brought to the attention of the rest of the network/security team. Every one had their own idea on what should be done. Some felt it should be immediately brought to the attention of management, while others felt they should wait till they could find out more. Not worrying management if nothing has really occurred became the ultimate decision. This was made by majority consensus and not by someone who understood how to handle an incident. As such, it was agreed to investigate further to see if something serious had occurred.

-Signs of An Incident

The security team decided to download a copy of Hijetter and see what it did. They placed a copy on one of their Windows 2000 boxes and then made a connection to one of their printers. They realized that they were able to see the entire file system and manipulate the settings. As such, they decided they needed to check all of the printers to see if there was anything strange added. They did find one printer that appeared to have an unusual directory on its hard drive. Since no one was familiar with what the file system of the printers looked like, they were not sure if the folder was supposed to be there. It was the only printer that was different from the others. The folder called “spool_tools” appeared on the printer file system.



- Chain of Custody

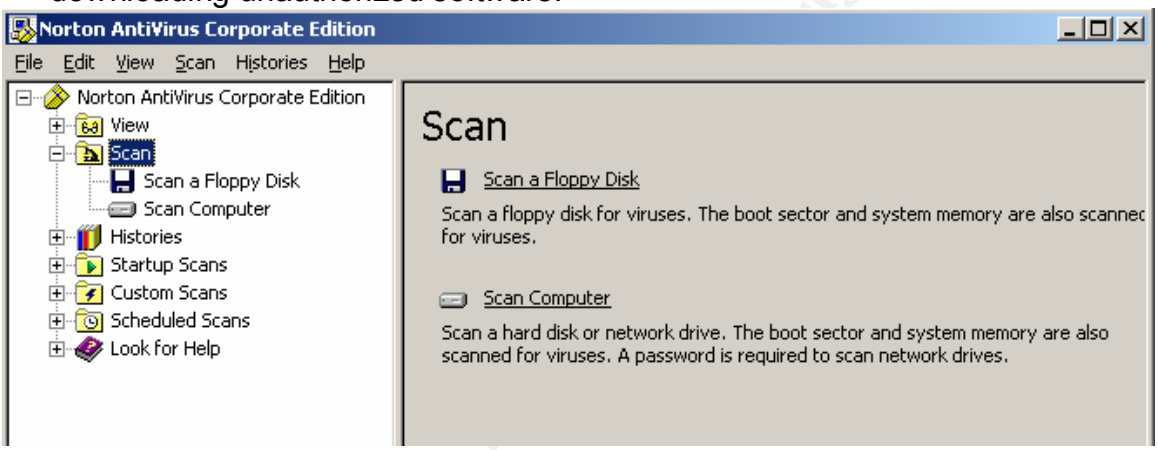
Once it was established that there appeared to be something going on that warranted further investigation, no one was quite sure how to proceed. They decided to let management know what they had found and request permission to search the hard drive of the user in question. Once permission was granted, they logged onto the system to see if there was anything on the hard drive that might indicate the intentions of the individual. They looked around on the hard drive and found several different tools that could be considered to have malicious purposes. When questioned about the tools, the individual said they were just experimenting. The Hijetter program was found and the individual gave the same answer. They also stated they did not put/create anything on any printer. During the inspection of the hard drive, nothing was preserved or kept for future usage. It was decided to let management handle the discipline for the unauthorized tools on the system.

Containment

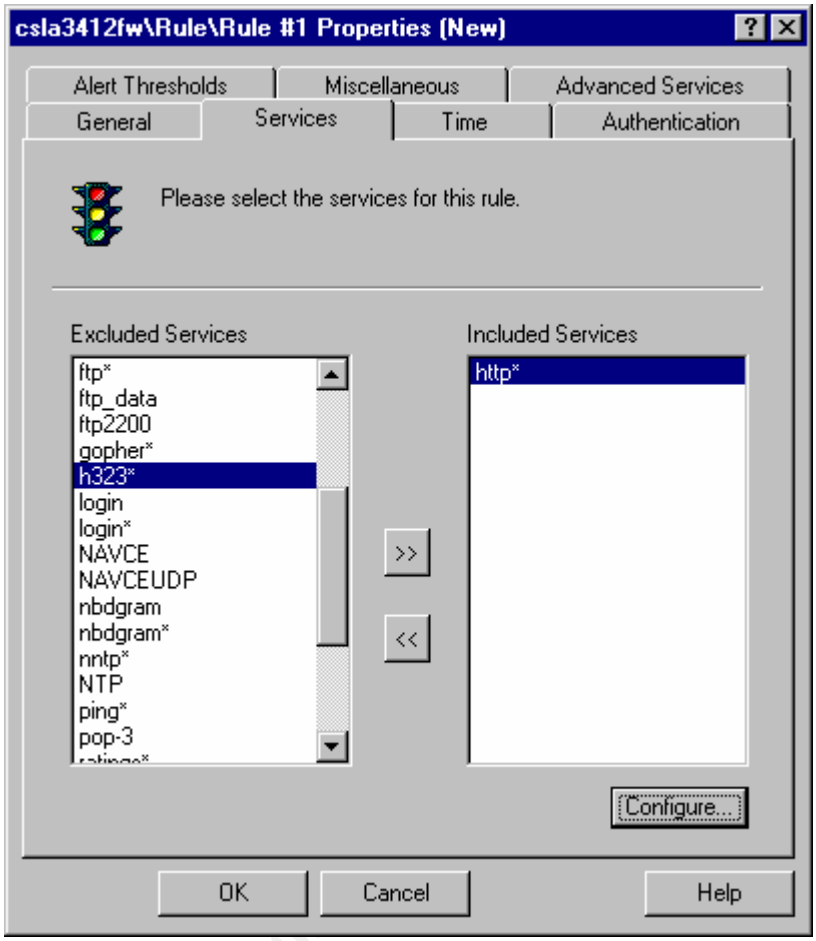
-Methods Used

Since the unauthorized software appeared to be isolated to one specific box, these are the steps taken by the team to ensure that nothing could potentially affect the rest of the network.

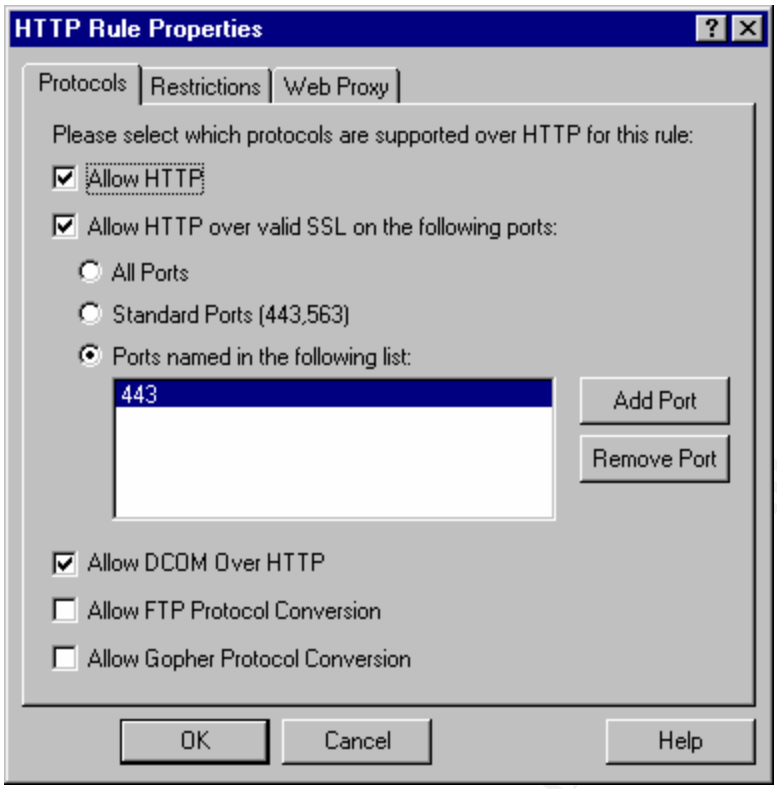
1. The security team decided that it was best to remove the system from the network by unplugging the NIC card. They did not back up the system before they first touched it. This was mainly due to inexperience.
2. They decided that they needed to first scan the hard drive to ensure that there were no viruses on the system. Since the user was obviously downloading unauthorized software.



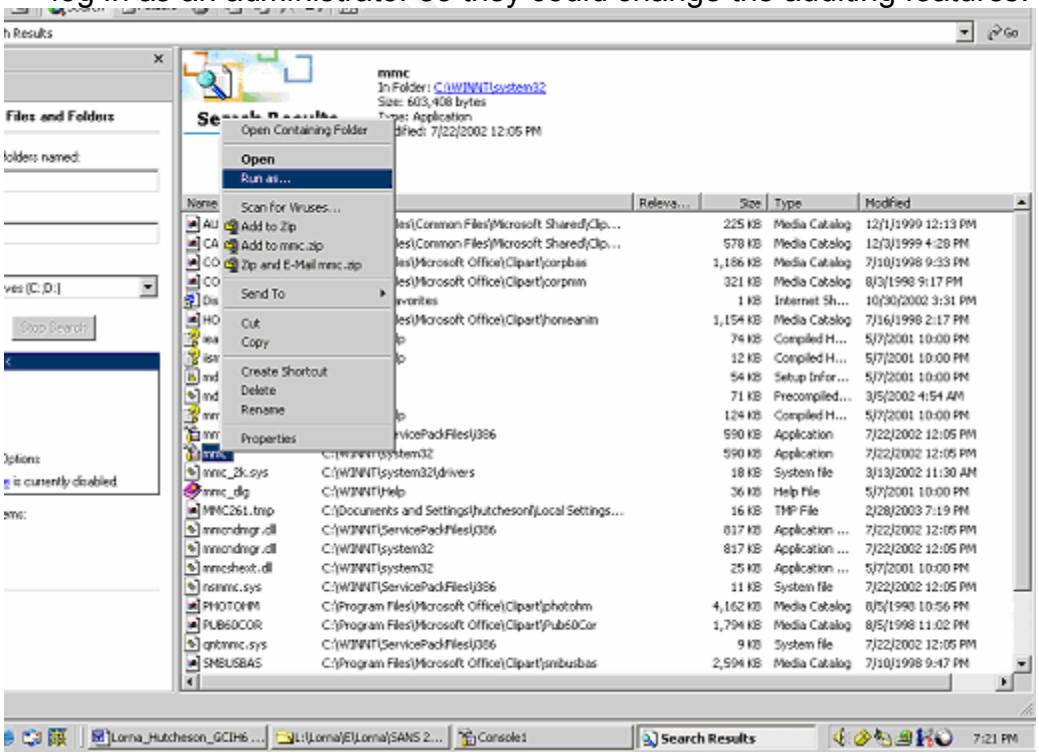
3. They also decided that the firewall rules needed to be modified. Now instead of access being granted from each division to the other for use of the printer, the divisions were only allowed access to their own printer. At least this meant that access attempts to the other devices would be detected. This was immediately put into place until management could be reached and they could make a final decision.
4. The firewall rules were also modified to prevent the users from downloading certain file extensions. To do this, you click the services tab to determine which services this rule will allow through. We are going to allow HTTP and then configure the HTTP service. (NOTE: Raptor has several proxy services that allow easier configuration. Ensure the HTTP proxy service is enabled in the Raptor in the Access Control proxy service.



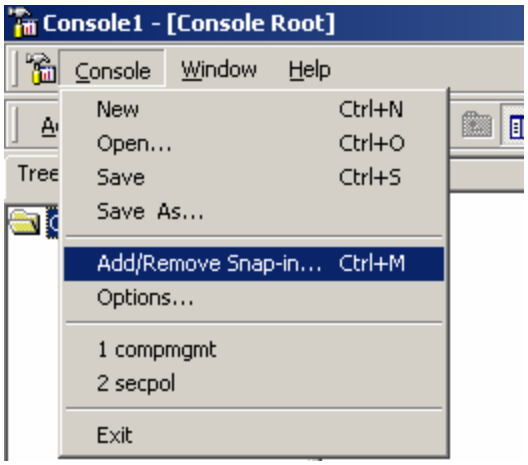
After this you click on the configure button at the bottom, you will be given the option of how to configure the service. We are going to allow normal web access, but also click the tab for restrictions and add in those file extensions that we want to be allowed to pass through. Remember, ONLY those listed will be allowed to pass through. This is a major pain because of all of the mime types, however it will stop users from downloading certain file types, to include .exe files. After a while, you get a nicely tailored list. However, you must remember that if the connection is an SSL, you will NOT be able to see what is passing on the firewall and restrict it. It will take a while to work out all of the file extensions that are needed, but the results are very good and stop a lot of unauthorized activity since a request has to be made to allow an extension through.



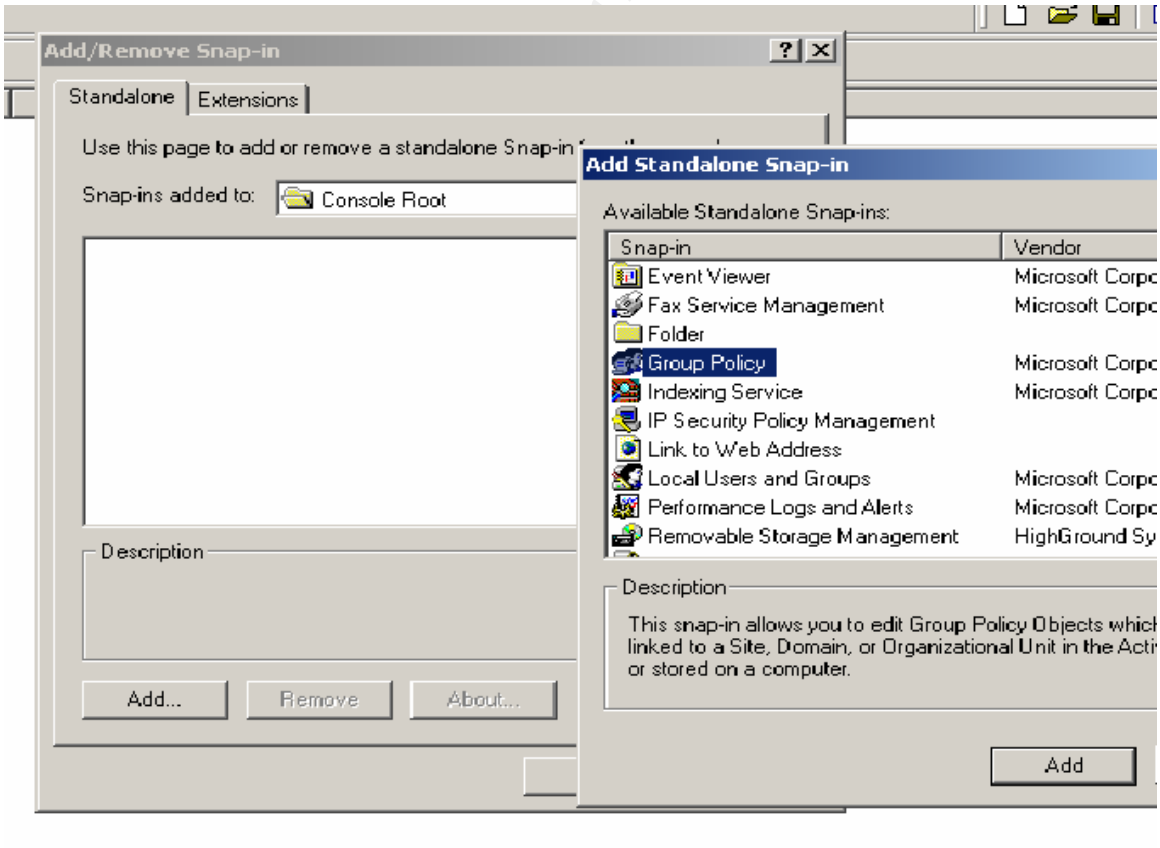
5. The user's privileges were also audited more intensely than the other users. As no user has administrative rights, the security team did a shift "runas" on the MMC console (Microsoft Management Control) this let them log in as an administrator so they could change the auditing features.



Once the MMC was up, the snap-in for the group policy was loaded by selecting the console clicking add/remove Snap-in from the selection.

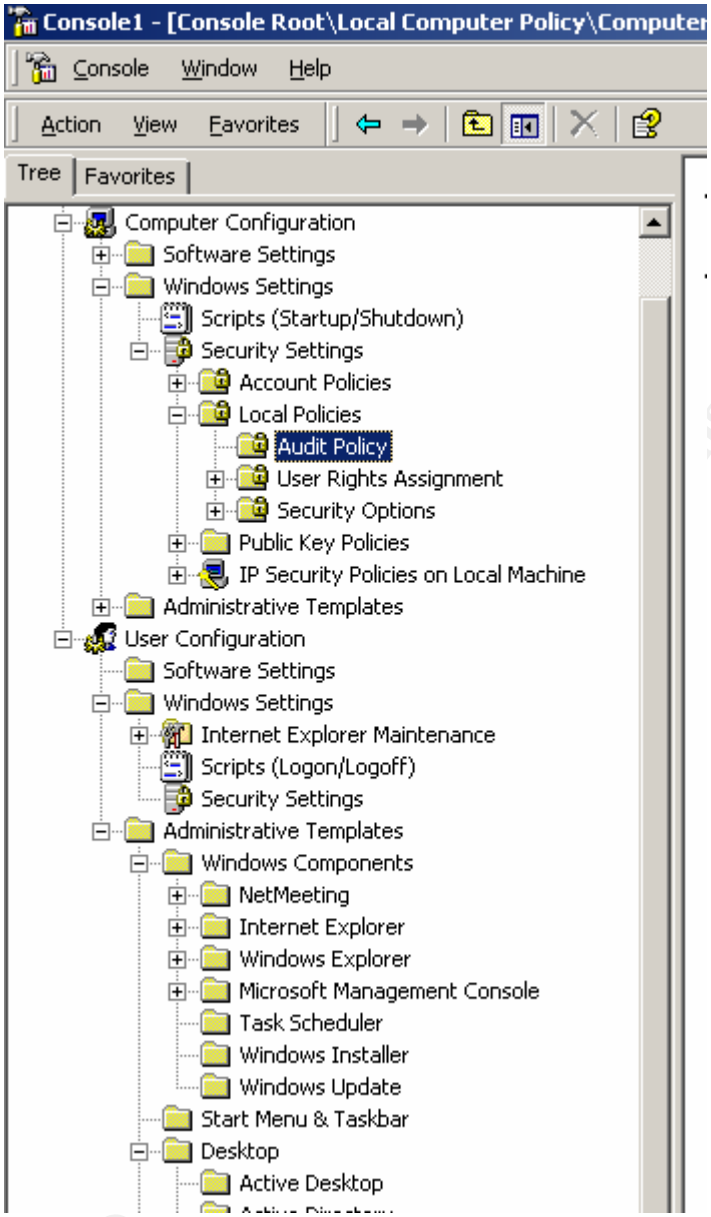


At the next screen they clicked Add at the bottom and then chose group policy as your selection.



Once in the group policy you are going to see two major categories called "Computer Configuration" and "User Configuration." Please keep in mind that

the computer configuration affects the settings on the computer for all users and the user configuration affects what they can and cannot do on that system such as what they see on their desktops etc.



What we want to do is select Audit Policy and ensure that we are auditing everything that we want to be able to monitor for activity.

6. The final step was to ensure that any logging capability was enabled on the multifunctional device. Unfortunately, this was very limited and dealt more with the status of the printer.

-Tools Used

The tools on hand suddenly became very important to the security team. They had some things they needed, but they did not have everything in one central location. This will be discussed further in the Lessons Learned. What they did have to use was a zip disk, which they copied the Hijetter program onto and also the logs were copied off of the system. They also made copies of all the unauthorized tools.

-Update System Owners

The security team briefed management after the search of the system and let them know what they had found and the actions taken. They also briefed them on their recommendations for the firewall configurations and the other changes they had made. The final decision would be given to the security team after management had a chance to talk things over.

Eradication

-Removing Malicious Software

Deleting the unauthorized files from the hard drive completed removal of the software. The Hijetter program makes no modification of the hard drive, registry or file system. It is a self-contained executable. The other questionable tools were deleted as well. The Hijetter program was also ran against the multifunctional device in question and the unknown directory was deleted off of it after checking with HP about its existence. It is amazing to think that the time required and the resources used to figure this out were caused by the observation of an unknown process running on a system.

Recovery

-Restore Operations

Once the files were deleted, the security team debated on how to return the system to the network. The security team wanted a new build on it and the network team argued there was no reason since the files in question were deleted. Not to mention the individual in question said they were just experimenting. This caused a severe debate that finally was won by security team. Mainly because they were going to put it in writing that the network team refused to reload and have the team chief sign it. Once this happened, the network team grudgingly decided they would take the time and reload the system. It was not a hard procedure since they were using a product called INODE, which can be found at http://www.persystent.net/. This program gave them the ability to push out an image using PXE without having to do much effort. They did have to backup the user's files and ensure that auditing was turned on as the security requested. The issue came from lack of understanding on the SA side as to the security implications and the need to reload.

-Monitor

The biggest remaining question was how to monitor against this type of issue in the future. It was decided that continual monitoring was appropriate. They also decided building a better list of what is normal for the systems must be established. This will be addressed further in the Lessons Learned section.

Lessons Learned

This section is extremely important. The scenario above, although fictional, had several bits of true-life experience combined into it. What we need to do is learn from our mistakes. GIAC Enterprises learned the hard way about how important preparation and procedure was before an incident occurred. Fortunately, for the best they can tell, nothing too malicious took place. However, it was a real eye opener for the security team. The realization that they needed an incident handling process was very obvious. They decided to have three meetings to rectify the issues. The first one was a lessons learned session conducted amongst the security team. It was decided they needed to brainstorm first about what would take place. Next they wanted to meet with the network team and present their ideas and findings to them. They did not want more problems or disagreements like what happened before, so they want to get them to buy off on it. The last meeting was going to be with management and the security team chief as well as the network team chief and get them involved with what they determined needed to happen. Here is a look at the security teams analysis of what happened or in this case, didn't happen.

-Security Team Meeting

The security team members decided they needed to walk through the incident and evaluate it against a criterion. After a little research they found at a document from SANS Institute that appeared to be the guidance they needed. It was called "Incident Handling Step by Step: Unix Trojan Programs - Version 2.1" and can be found at http://www.sans.org/y2k/DDoS.htm. This document became the pattern for their meeting and analysis of the event. Even though it was for UNIX, the pattern was still there for what they needed immediate guidance on. Here are the results of their self-analysis of the events:

1. Preparation Phase.
   a. Management Support: The security team knew they were not prepared for the incident and especially not a serious one in the future. They also knew that what they came up with had to be something that management would buy off on due to cost and resource issues. It was decided that the best approach was to layout the seriousness of the issue and then present them their two options of doing nothing or being prepared. They decided to do a cost analysis of what GIAC Enterprises stood to loose if the network were taken down for any length of time compared to doing things correctly. As a rapidly growing company, GIAC Enterprises stood to loose a lot if down for long periods since their business was web based. They had already invested good time and money in security tools, now they just needed to be convinced they needed to carry that one step farther and be prepared. It did not appear to be a hard sell, since management had been supportive all along. Also, management, with advice from legal, needed to determine how to handle issues with the International Marketing group. Legal guidance was needed for establishing policy and procedure in this area.

b. Establish an Incident Team: Since there was not a distinct function in this area assigned to anyone, they needed to establish a team. This was definitely missing in the incident that just happened and no one was in charge. Everything was done by group consensus. Due to the nature of the business being 24 hours and the possibility of multiple occurrences, it was decided to have two teams that did the investigation. One team would be primary and one would be backup. Each of these responsibilities would rotate on a monthly basis. This is did not eliminate their normal job functions; it was just an added responsibility. In case of an emergency, the secondary team would fill in for the primary team. Each team would answer to the security chief. He/she would have an alternate to fill in off of the security team. The team was going to consist of people from the network side as well as the security side of the house. There would be a primary security person in charge of the team as it conducts its mission. Supporting this individual would be a Windows subject matter expert (SME), a Unix SME and a web server SME. They also wanted to address how to handle the legal and public affairs. Their recommendation was to have someone on call that could advise in these areas.
c. Checklists. It was clear that steps needed to be developed for the handling of incidents. This would cut down on arguing and allow for fewer mistakes when things were going hot and heavy. In this last incident, there were no guidelines present for what to do and many mistakes were made. It was decided that the following checklists and procedures needed to be written. System backup procedures for both UNIX and windows platforms were a must. It was soon realized that a duplicate of the hard drive needed to be made before anything was done on it. Procedures for each server and each type of workstation on how to bring it down and rebuild it need to be developed. It never fails that the actual SA is out when you need them most. It should be documented clear enough that anyone can do it. Also, each of the server books should have a log section that identifies what has been done to the system, when and by whom. This should eliminate unknowns if you can look and see if a program was installed by one of the SAs and no one realized it.
d. Communication. This was a very big issue. When things are going hot and management is yelling and it's usually at you, that is when everyone needs to remain cool. Communication is key. Everyone needs to have a small pocket Point of Contact (POC) list that has each team member's name, number and a way to reach him or her when they are not home. It was also decided that GIAC Enterprises should pay for pagers for each of the team members to ensure they can be contacted at any time. It is also very important that the security team and network team communicate and know the roles of the other and the privileges the incident team has. It is very important the incident team does not abuse the privileges. Not only is communication important for the teams, but with the user as well. ALL users need to be trained on what to look for and how/to whom something

gets reported. Most users just don't know what to look for. It was realized that users need to be educated and acknowledged for doing things right. Most users want to help, they just don't know what they are looking for. Training was going to be key.

e. War Room. This is one of the most critical in my opinion. The security team has to have a central location to monitor network security at all times. If one person does it over here and another over there, there is no graceful way to transition between people and have things go on business as usual. If someone gets sick and you have to fill in for him or her, how do you know what was going on. The war room would also contain all of the reports and a central location of all security issues, policies, procedures, checklists etc. When an incident occurs, everything is ready and the network's current security status is continually being checked. Everything is there and ready.
f. Training. This one is very key as well. Each person should be trained on their responsibilities AND cross-trained to perform another function. If the primary windows SME got in an accident on the way in and the back up SME is in the hospital, who is going to fill in? Everyone person needs to understand how the team works and be good in at least one additional area. Then, no matter what happens, someone is always ready to step up and take over. A training plan needs to be established for each year and for each person. This needs to be done and submitted for the budget to be planned for. Without training, the team will not be ready for what is coming at them. It is also important to do internal training for the team conducted by team members (also known as "Train the Trainer"). Just as essential, is training for the user. Mandatory yearly responsibilities were already in the policy, but it was realized that it needed to be conducted more regularly. A training plan needed to be established for the user population.
g. Jump bag. There were some basic things that they realized needed to be centrally located and accessible. These items were compiled into a list and were to be developed as they went. A good list of things to have was found at CHIHT – Clearing House for Incident Handling Tools (http://chiht.dfn-cert.de/). A list of items that were needed for GIAC Enterprises was to be developed.

2. Identification Phase.
   a. Identify Chain of Command. This is very important. Everyone has to know who is in charge and what the reporting order is. This should be identified and distributed to each of the team members. Remember, if anything happened to the head person, someone has to step up. During the incident at GIAC Enterprises, group vote was what made decisions and everyone milled around, but no one was in charge. This has to be put into place. Only one trained person should be making the decisions at one time. Popular vote is NOT the way to go. ALWAYS keep the chain of command informed! Do not let them be blind sided by something you did

wrong, an incorrect call, or pertinent information about the incident. It is not the way to do business, nor is it good for your career to fail to be up front, honest and responsible for your actions.

b. Initial Assessment. Not everything that happens is an incident and the whole team needs to respond. No one knew what was going on at GIAC Enterprises or how to make the determination. Guidelines need to be in place as to what constitutes an incident. This cannot be a definite list, but it can guide the handler as to what should be called an incident. For example, are viruses considered incidents? What about unauthorized use of the Internet or unauthorized software? It is important that some guidance is in place. The handler has to have the ability to make the call, however, based on pure gut instinct and experience as to the call and how to handle it.
c. Notification of Appropriate Personnel. Who do you call? This needs to be established up front and management needs to be involved in this process. How the incident is handled can be crucial to an organization. For a young company like GIAC Enterprises, it could severely hurt business if a security breech occurred. What about an incident that turned out to be nothing? If it was published first and then tried to be taken back, there are still consequences to the actions. GIAC Enterprises has to determine what to report and to whom. This will eliminate any guesswork when the time arrives.
d. Chain of Custody. Document, document, document. It cannot be emphasized enough that courts will not accept into evidence that which cannot be reliably proven not to have been tampered with. The recent event at GIAC enterprises is an example of realization after the fact. The only thing the team realized they had was based on their word. They wiped the system, deleted the tools, deleted the folder and had nothing to prove it with except a zip disk with the copies of the tools on it. Who can prove where they came from, who put them there, who had access to it, etc? Chain of custody is extremely important and must be treated as such. Document everything and backup everything BEFORE you do anything. Also, keep a record of everything done and keep all evidence in your possession. Ensure that if turned over to law enforcement, they sign for it.

3. Containment Phase
   a. Deploy the Team. In the case of an actual incident, the incident team needs to be deployed and start their job of containing the event. However, this should not be done with guns blazing. It should be done discreetly for many reasons. If the incident is an insider, you tip them off that someone is on to them and they can cover their tracks. If it is a user who is the victim, you don't want to subject them to unnecessary comments and criticism (yes, adults can be mean). Know who is doing what job when you get on the ground. Remember, one person is in charge.

b. Backups. After the GIAC Enterprise incident, the team realized that they needed to save the evidence and preserve the originals. A backup needs to be made of the hard drive. It is advisable to make two copies, one to keep as the original and one to analyze and perform forensics on.
c. Keep a Low Network Profile. In addition to discreet deployment on site is just as important to be discreet on the network. Under the past event, everything was done on the spot, to the original and with the user standing there. It should be done where it is low profile, even what is happening on the network. Learn and keep a list of network tools for the system that are discreet and won't alert and intruder that they have been found out. Try not to make your efforts to figure out what is going on visible to someone who may be watching the network.
d. Follow Procedure. Ensure that a checklist of things to look for and do is composed. This list would have helped out GIAC Enterprises with their investigation. As such, it was very disorganized and randomly completed. It is easy to forget in the heat of the moment what to look for. What if you are sick? That can make things worse. A list of things to look for and the order to do them in can be very beneficial. As you handle more incidents, the procedures should be refined and updated. All of the policies, procedures and checklists should be living documents.

4. Eradication Phase
   a. Determine Attack Characteristics and Implementation. Before you can eradicate an incident, you have to understand it. If you don't understand what caused it and how it worked, who is to say it won't happen again once you fix everything. Looking at log files, files on the system, research on the Internet, etc may accomplish this. One of the best methods is experience. The more you do your job, the better you will become and start to know what to look for. If you learn to not quit till you understand all you can about it, you will be a better handler and it will get easier.
   b. Defense Analysis and Modification. Once you determine how an attack occurred, you have to understand and determine how to defend against it. This is extremely important part so that it doesn't happen again. The problem with GIAC Enterprises is that it is a new concept dealing with multifunctional devices and learning how to protect against attacks on them. Good protection is not going to happen until manufacturers start to build it in to the devices. The security team did a good job here of making modifications to the defensive posture of the network.
   c. Removal of the Culprit. This is where you have to decide how to get rid of your problem. Do you rebuild the hard drive or just delete the files. Is either of them the best method. If the incident can be identified with a known name or exploit, it is beneficial to do some research as to what you should do. Lessons learned from other folks can help you not to make mistakes. If you don't execute the removal correctly, you may not get rid of your problem. If you are going to do a restore, make sure the backups are not corrupt as well. In the case of GIAC Enterprises, INODE makes

an image whenever you want. GIAC Enterprises keeps base images with the correct security settings for all the systems. These just need to be pushed out to bring the system back functional.

d. Vulnerability Analysis. It is important that you identify whom else this can happen to. Has it already happened to someone else? GIAC Enterprises failed to do this area. They just looked at the one system found and did not bother to look at other systems. Hijetter was only detected because it was running at the time of the scan. What if it is still sitting out there waiting to be used? Handler's need to identify who else is/could be vulnerable and make sure they have not been compromised as well.

5. Recovery Phase
   a. Validation Checklist. How do you know the system is back up and running properly? One-way to look at the server/workstation book for the configuration of the system. The other way is to develop checklist for your server and workstations with test procedures to ensure functionality. It's great to say you got rid of the vulnerability, but not so great if the system can't be used again. This is critical to GIAC Enterprises. For them to have down time for an unidentified loss of functionality means a loss of financial profit. That does not go over well with management. If checklists are developed and procedures implemented, this can all but be eliminated.
   b. Restoration of Operations. Ensure that you have clear guidance on when to put the systems back operational. For GIAC Enterprises, the management is going to want them back up as soon as possible. What if it were a critical system and they did not want to have it down the time you deemed it needed to be or they weren't willing to wait for the process the be completed. The ultimate decision rests with management. GIAC Enterprises made a good call and that was to implement the changes and then advise what had been done. Sometimes it is better to beg forgiveness than ask permission. Implement that concept at your own risk, however.
   c. Monitor. Once the system is back up, do not assume all is well. If the attacker is really good, who is to say there aren't multiple backdoors or you fixed a decoy? Do you really know what is going on or are you making educated guesses. As such, never think you know it all and can say anything with 100% confidence. Trying to think like a hacker is only an attempt to get into someone's psyche. Be willing to know you can be wrong. As such, monitor the network for future occurrences of the event or watch it more closely for unusual behavior. For GIAC Enterprises, they determined they needed to increase the scan frequency and make it more random to help monitor the network. They also increased the auditing to watch the individual. He/she said it was just curiosity, but are you sure and how did that folder get on the printer then? Never let your guard down.

6. Lessons Learned
   a. Frequency. It was determined that the meeting was a huge success and they were well on their way to making a strong incident handling team and would not be caught unaware again. As such, it was decided that the lesson's learned meeting would occur after every incident or major event. Whether or not it was an incident an AAR needed to be conducted.
   b. Policies and Procedures. All policies and procedures would be evaluated for improvement/modification at the meetings. These are living breathing documents and need to be treated as such. If checklists were found lacking or out of date, it needs to be raised as an issue. If everyone is not imformed of changes, someone may not know the new policy or not even know it was changed.
   c. Attendance. Attendance is mandatory for all members of both security teams. The Network chief will be invited to attend to keep continuity and to help him/her guide their team if they need to modify their own procedures. Remember that communication is key. If not careful it can turn into an us versus them mentality and that is not a good working environment.

Extras

Here are some of the known peripheral device vulnerabilities. This is not an all inclusive list.
CVE/CAN listings for printers from the link: http://www.cve.mitre.org/cgi-bin/cvekey.cgi?keyword=Printer

Name	Description
CVE-1999-0353	rpc.pcnfsd in HP gives remote root access by changing the permissions on the main printer spool directory.
CVE-2000-0184	Linux printtool sets the permissions of printer configuration files to be world-readable, which allows local attackers to obtain printer share passwords.
CVE-2001-0353	Buffer overflow in the line printer daemon (in.lpd) for Solaris 8 and earlier allows local and remote attackers to gain root privileges via a "transfer job" routine.
CVE-2001-0668	Buffer overflow in line printer daemon (rlpdaemon) in HP-UX 10.01 through 11.11 allows remote attackers to execute arbitrary commands.
CVE-2001-0670	Buffer overflow in BSD line printer daemon (in.lpd or lpd) in various BSD-based operating systems allows remote attackers to execute arbitrary code via an incomplete print job followed by a request to display the printer queue.

CVE-2001-1177	ml85p in Samsung ML-85G GDI printer driver before 0.2.0 allows local users to overwrite arbitrary files via a symlink attack on temporary files.
CAN-1999-0061	File creation and deletion, and remote execution, in the BSD line printer daemon (lpd).
CAN-1999-0564	An attacker can force a printer to print arbitrary documents (e.g. if the printer doesn't require a password) or to become disabled.
CAN-1999-0741	QMS CrownNet Unix Utilities for 2060 allows root to log on without a password.
CAN-1999-1061	HP Laserjet printers with JetDirect cards, when configured with TCP/IP, can be configured without a password, which allows remote attackers to connect to the printer and change its IP address or disable logging.
CAN-1999-1508	Web server in Tektronix PhaserLink Printer 840.0 and earlier allows a remote attacker to gain administrator access by directly calling undocumented URLs such as ncl_items.html and ncl_subjects.html.
CAN-1999-1563	Nachuatec D435 and D445 printer allows remote attackers to cause a denial of service via ICMP redirect storm.
CAN-2000-1062	Buffer overflow in the FTP service in HP JetDirect printer card Firmware x.08.20 and earlier allows remote attackers to cause a denial of service.
CAN-2000-1063	Buffer overflow in the Telnet service in HP JetDirect printer card Firmware x.08.20 and earlier allows remote attackers to cause a denial of service.
CAN-2000-1064	Buffer overflow in the LPD service in HP JetDirect printer card Firmware x.08.20 and earlier allows remote attackers to cause a denial of service.
CAN-2000-1065	Vulnerability in IP implementation of HP JetDirect printer card Firmware x.08.20 and earlier allows remote attackers to cause a denial of service (printer crash) via a malformed packet.
CAN-2001-	Multiple buffer overflows in Lexmark MarkVision printer driver programs allows local users to gain privileges via long

0044	arguments to the cat_network, cat_paraller, and cat_serial commands.
CAN-2001-0369	Buffer overflow in lpsched on DGUX version R4.20MU06 and MU02 allows a local attacker to obtain root access via a long command line argument (non-existent printer name).
CAN-2001-0406	Samba before 2.2.0 allows local attackers to overwrite arbitrary files via a symlink attack using (1) a printer queue query, (2) the more command in smbclient, or (3) the mput command in smbclient.
CAN-2001-0817	Vulnerability in HP-UX line printer daemon (rlpdaemon) in HP-UX 10.01 through 11.11 allows remote attackers to modify arbitrary files and gain root privileges via a certain print request.
CAN-2001-1039	The JetAdmin web interface for HP JetDirect does not set a password for the telnet interface when the admin password is changed, which allows remote attackers to gain access to the printer.
CAN-2002-0529	HP Photosmart printer driver for Mac OS X installs the hp_imaging_connectivity program and the hp_imaging_connectivity.app directory with world-writable permissions, which allows local users to gain privileges of other Photosmart users by replacing hp_imaging_connectivity with a Trojan horse.
CAN-2002-1055	Buffer overflow in administrative web server for Brother NC-3100h printer allows remote attackers to cause a denial of service via a long password.

CVE/CAN listings for fax from the link: http://www.cve.mitre.org/cgi-bin/cvekey.cgi?keyword=fax

Name	Description
CAN-2000-0691	The faxrunq and faxrunqd in the mgetty package allows local users to create or modify arbitrary files via a symlink attack which creates a symlink in from /var/spool/fax/outgoing/.last_run to the target file.
CAN-2002-0129	efax 0.9 and earlier, when installed setuid root, allows local users to read arbitrary files via the -d option, which prints the contents of the file in a warning message.
CAN-2002-	Buffer overflow in efax 0.9 and earlier, when installed setuid root, allows local users to execute arbitrary code via a long -x

0130	argument.
CAN-2002-1392	faxspool in mgetty before 1.1.29 uses a world-writable spool directory for outgoing faxes, which allows local users to modify fax transmission privileges.

Links:
Printer Vulnerabilities & Exploits Tektronix Printer Vulnerabilities:
http://members.cox.net/ltlw0lf/printers.html

References

Andress, Mandy. "Printer Protection." URL: http://archive.infoworld.com/articles/op/xml/02/04/01/020401opsecurity.xml (18 February 2003).

"Attacking Network Embedded Systems." July 2002 URL: http://www.blackhat.com/presentations/bh-asia-02/bh-asia-02-fx.pdf (19 November 2002).

"Chapter 11. Printer Communication and Protocols." (17 January 2003) URL: http://www.lprng.com/LPRng-HOWTO-Multipart/socketapi.htm (23 February 2003).

Dennis W. Mattison. "Network Printers and Other Peripherals – Vulnerability and Fixes." 8 July 2002. URL: http://members.cox.net/ltlw0lf/printers/printers.pdf (19 November 2002).

"HP LaserJet 4100MFP Guide." 2001. URL: http://h200002.www2.hp.com/bc/docs/support/SupportManual/bpl11450/bpl11450.pdf (25 February 2003).

"Hp LaserJet 4100mfp intelligent multifunction network printer." URL: http://www.hp.com/itrc_pdi/products/pdfs/lj4100mfp.pdf (21 February 2003).

"HP LaserJet 4100 User's Guide." URL: http://h200002.www2.hp.com/bc/docs/support/SupportManual/bpl10335/bpl10335.pdf (25 February 2003).

"HP LaserJet Printers - PCL (Printer Command Language)." URL: http://www.hp.com/cposupport/printers/support_doc/bpl04568.html. (23 February 2003).

Liebermann, Jeff. 17 May 2000. "Print Server Port Numbers for Netcat." URL: http://www.cruzio.com/~jeffl/sco/lp/printservers.htm (23 February 2003).

Northcutt, Stephen; Cooper, Mark; Fearnow, Matt; Frederick, Karen. Intrusion Signatures and Analysis. Indianapolis: New Riders, 2001.

Northcutt, Steven. IDS Signatures and Analysis, Parts 1 and 2. 2002.

Northcutt, Steven; Novak, Judy. Network Intrusion Detection An Analyst's Handbook. Indianapolis. New Riders, 2001.

"Printer job LANGUAGE (PJL) command for the control of (HP) printers." 2002. URL: http://translate.google.com/translate?hl=en&sl=de&u=http://www.uni-

kiel.de/rz/ausgabe/pjl/&prev=/search%3Fq%3D%2522PJL%2522%26start%3D20%26hl%3Den%26lr%3D%26ie%3DUTF-8%26oe%3DUTF-8%26sa%3DN (18 February 2003).

"Printing with Netcat." URL: http://www.tkrh.demon.co.uk/netcat.html (23 February 2003).

"SANS Security Alert." January 2001. URL: http://weather.ou.edu/~laufers/docs/SAC_0101.pdf (25 February 2003).

Slobotron. "Understanding, Reversing, and Hacking HP Printers." February 2002. http://www.searchlore.org/realicra/hp_slobo.htm (18 February 2003).

Zirkle, Laurie; Dittrich, Dave; Drake, George. "Incident Handling Step by Step: Unix Trojan Programs - Version 2.1." URL: http://www.sans.org/y2k/DDoS.htm (28 February 2003).