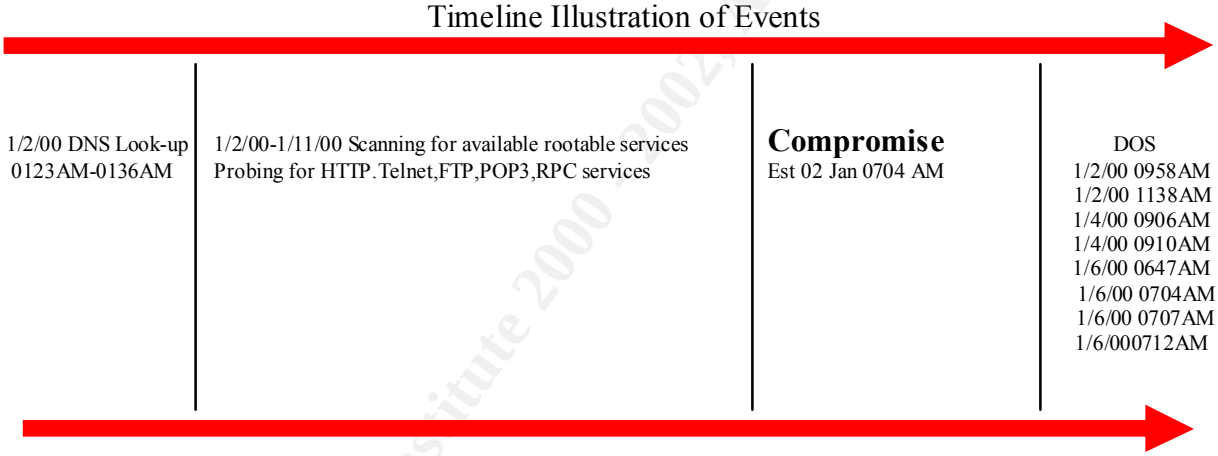
Global Information Assurance Certification Paper

SANS GIAC PRACTICAL

Hacker Exploits and Vulnerabilities
SANS Conference, December 2000 - January 2001
Rhonda Maluia

Executive Summary: The following incident was observed during real-time monitoring of both ISS RealSecure and NetRanger intrusion detection systems. The target networks do not fall under the monitoring organizations administrative control. No immediate action can be taken to prevent the destination network (s) from compromise or denial of service. The only action the analyst can take is to attempt contact with system administrator and report the incident to the proper authorities. The following incident serves as an example of an attack that illustrates network reconnaissance and the valuable network information that is gathered through such activity. Post analysis and site administrator confirmation, affirmed that this network was compromised at the root level and participated in activity against other networks. The log files have been sanitized and fictitious network names are used throughout this paper when referencing the targeted organization.

Timeline Illustration of Events



Source: Indonesia, INDONET

Whois
Reference: APNIC
202.159.72.18
inetnum 202.159.72.0 - 202.159.80.255
netname CADANG-INDONET-ID
descr Segment for Small Customer country ID
admin-c SS112-AP, inverse tech-c ED1-ID, inverse rev-srv ns1.indo.net.id rev-srv ns2.indo.net.id rev-srv ns3.indo.net.id remarks none notify dbmon@apnic.net, inverse mnt-by MAINT-INDONET-ID, inverse changed hostmaster@indo.net.id 19960202 source APNIC

202.159.51.145
inetnum 202.159.50.0 - 202.159.51.255
netname NETURA-INDONET-ID
descr IndoInternet - Bandung country ID
admin-c SS112-AP, inverse tech-c ED1-ID, inverse rev-srv ns1.indo.net.id rev-srv ns2.indo.net.id rev-srv ns3.indo.net.id remarks none notify dbmon@apnic.net, inverse mnt-by MAINT-INDONET-ID, inverse changed hostmaster@indo.net.id 19960202 source APNIC

202.159.120.196
inetnum 202.159.101.0 - 202.159.127.255
netname INDONET-ID
descr Reserved for other use country ID
admin-c SS112-AP, inverse tech-c ED1-ID, inverse rev-srv ns1.indo.net.id rev-srv ns2.indo.net.id rev-srv ns3.indo.net.id remarks none notify dbmon@apnic.net, inverse mnt-by MAINT-INDONET-ID, inverse changed hostmaster@indo.net.id 19960202 source

202.159.32.16
inetnum 202.159.32.0 - 202.159.35.255
netname INTERNAL-NOC-INDONET-ID
descr Indonet's Internal Network country ID
admin-c SS112-AP, inverse tech-c ED1-ID, inverse mnt-by MAINT-INDONET-ID, inverse changed sanjaya@indo.net.id 19991109 source APNIC

202.159.65.30
inetnum 202.159.64.0 - 202.159.67.255
netname BACKBONE-INDONET-ID
descr IndoInternet's backbone country ID admin-c SS112-AP, inverse tech-c ED1-ID, inverse rev-srv ns1.indo.net.id rev-srv ns2.indo.net.id rev-srv ns3.indo.net.id remarks none notify dbmon@apnic.net, inverse mnt-by MAINT-INDONET-ID, inverse changed hostmaster@indo.net.id 19960202 source APNIC

202.159.71.6
inetnum 202.159.68.0 - 202.159.71.255
netname WASANTARA-INDONET-ID
descr PT. Pos Indonesia country ID
admin-c SS112-AP, inverse tech-c ED1-ID, inverse rev-srv ns1.indo.net.id rev-srv ns2.indo.net.id rev-srv ns3.indo.net.id remarks none notify dbmon@apnic.net, inverse mnt-by MAINT-INDONET-ID, inverse changed hostmaster@indo.net.id 19960202 source APNIC

Destination IP addresses:

Myfriendsnet.com (ficticious)
All networks beginning with letters belong to the above.

Network Reconnaissance

Log File: ISS RealSecure

Event Date/Time	Event Name	Source Port/Name	Destination Port/Name	Source Address	Destination Address
1/2/00 0123:09AM	DNS_Zone_High_Port	8244	53/DNS-Xfer	202.159.72.18	Y.Y.1.34
1/2/00 0131:51AM	DNS_Zone_High_Port	6471	53/DNS-Xfer	202.159.72.19	X.X.84.99
1/2/00 0132:03AM	DNS_Zone_High_Port	7239	53/DNS-Xfer	202.159.72.20	X.X.84.99
1/2/00 0132:50AM	DNS_Zone_High_Port	10066	53/DNS-Xfer	202.159.72.21	X.X.84.99
1/2/00 0134:17AM	DNS_Zone_High_Port	12372	53/DNS-Xfer	202.159.72.22	X.X.84.99
1/2/00 0134:51AM	DNS_Zone_High_Port	14970	53/DNS-Xfer	202.159.72.23	X.X.84.99
1/2/00 0135:46AM	DNS_Zone_High_Port	16985	53/DNS-Xfer	202.159.72.24	X.X.84.99
1/2/00 0136:14AM	DNS_Zone_High_Port	18771	53/DNS-Xfer	202.159.72.25	X.X.84.99

Alarm Definitions and Criteria: The following definitions and descriptions are provided by ISS RealSecure and can be accessed by right clicking on the alarm and selecting "what's this." It is important that the analyst know how the intrusion detection system defines the alarms and criteria in order to more effectively identify suspicious activity.

DNS Zone Transfers from High Ports
Type: Pre-attack probe.
Console Name: DNS_Zone_High_Port
Technical description: This decode detects a zone transfer being made between your DNS server and what appears to be a client system using a DNS client program such as nslookup. The source port number is a non-privileged port number (above 1024) which indicates a client process.
Why this is important: Zone transfers contain a list of the systems on your network. This is a list of potential targets for an attacker.
False positives: None.
Systems affected: Any DNS server.
What to do: Observe the source address. Watch for additional events originating at that address.

How to remove this vulnerability: Configure your DNS server to disallow zone transfers from systems other than the peer DNS servers it must participate with, or at least from non-privileged port numbers. If it is a standalone DNS server, disallow zone transfers entirely.

Reference: ISS RealSecure console

Associated Vulnerabilities: http://cve.mitre.org/
Name **CVE-1999-0024**
Description: DNS cache poisoning via BIND, by predictable query IDs.
Name **CVE-1999-0101**
Description: Buffer overflow in AIX and Solaris "gethostbyname" library call allows root access through corrupt DNS host names.
Name **CVE-1999-0274**
Description: Denial of service in Windows NT DNS servers through malicious packet which contains a response to a query that wasn't made.

Name **CVE-1999-0275**
Description: Denial of service in Windows NT DNS servers by flooding port 53 with too many charactersCERT® Advisory CA-2000-03 Continuing Compromises of

CERT Advisory CA-2000-03 Continuing Compromise of DNS Servers.
Original release date: April 26, 2000
Last revised: April 26, 2000
Source: CERT/CC
Systems Affected: Systems running various vulnerable versions of BIND (including on machines where the system administrator does not realize a DNS server is running)
Overview: This CERT Advisory addresses continuing compromises of machines running the Domain Name System (DNS) server software that is part of BIND ("named"), including compromises of machines that are not being used as DNS Servers. The Advisory also reports that a significant number of delegated DNS servers in the in-addr.arpa tree are running outdated versions of DNS software, and urges system and network administrators to ensure that they are up-to-date with DNS security patches and workarounds.

DNS Overview: The DNS directory service consists of DNS data, DNS servers, and Internet protocols for retrieving data from servers. Resource records, located DNS directory, are divided into zone files. Zones are located on authoritative servers which answer queries according to DNS network protocols. Caching servers query the authoritative servers and cache replies. Most servers have a dual function and are authoritative for some zones and perform a caching function for all other DNS information. It is not a difficult task to acquire domain names. There are numerous whois databases (ARIN, Apnic, Ripe) available on the web. A whois utility is built into UNIX and nslookup is also available on most operating systems. One can

also traceroute (UNIX) or tracert (NT) to the destination address and obtain domain names and route information. Example:
C:\>tracert 202.159.51.175

Tracing route to ip-mjk-114.indo.net.id [202.159.51.175] Domain was automatically given.
over a maximum of 30 hops:

```
  1   100 ms   100 ms   111 ms  154-042.sybercom.net [209.96.154.42]
  2   100 ms   110 ms   111 ms  nn-t1-gw.vabch.com [209.96.154.1]
  3   100 ms   120 ms   120 ms  eth32.core1.Norfolk.visi.net [206.246.204.5]
  4   110 ms   110 ms   110 ms  hssi31.core1.Richmond.visi.net [206.246.247.137]
  5   110 ms   111 ms   120 ms  hssi31.core1.WashDC.visi.net [209.96.135.53]
  6   110 ms   110 ms   110 ms  fe7-4.core2.wdc.cais.net [63.216.1.37]
  7   110 ms   120 ms   120 ms  sl-gw27-pen-5-1-0.sprintlink.net [144.232.191.17
  8   120 ms   111 ms   120 ms  144.232.5.193
  9   120 ms   110 ms   121 ms  sl-bb20-pen-12-0.sprintlink.net [144.232.16.193]
 10   180 ms   180 ms   170 ms  sl-bb20-stk-12-0.sprintlink.net [144.232.18.46]
 11   181 ms   170 ms   180 ms  sl-bb22-stk-14-0.sprintlink.net [144.232.4.237]
 12   250 ms   241 ms   250 ms  sl-gw1-prl-3-0.sprintlink.net [144.232.8.174]
 13  ^C
C:\>
```

Note: The operator stopped the trace. The trace was unable to reach 202.159.51.175, however, it did reach 202.159.51.89. Domain names of routers along the route are also a valuable source of information. An attacker can conceal themselves by compromising a box along the route that has a trust relationship with the destination IP address.

Analyst Action: This type of activity is often one of the first phases of reconnaissance. An incident ticket was generated for these alarms and a query of the database for previous activity from the source IP address was conducted. A query was also performed for prior alarms generated against the destination IP addresses. No prior activity was noted. The alarms were logged into the intrusion detection watch log and passed to the oncoming section. An E-mail was generated to the network administrator and point of contact for the destination network. Due to the time of the alarms, a network administrator at the destination site was unavailable. The main point of caution here was the source of the alarms (Indonesia). The organization had no affiliation or reason to conduct activity against the destination IP address's organization. Additionally, the alarms were generated against several networks that fall under the same domain. This type of alarm is considered to be a high level alarm on both NetRanger and ISS RealSecure. It is difficult to determine the objective of the attacker at this point. However, a review of vulnerabilities indicates a possible denial of service or an attempted compromise. While this may be a simple lookup. The worst case scenario should be considered and investigated. The prudent analyst should always ask "what if?" This IP address was placed on a watch list and monitored closely for additional activity.

Knock….Knock

Event Date/Time	Event Name	Source Port/Name	Destination Port/Name	Source Address	Destination Address
1/2/00 0222:17AM	IPHalfScan	4/ tcp, udp echo AppleTalk Echo Protocol	80/HTTP	202.159.72.18	X.X.84.39
1/2/00 0222:17AM	IPHalfScan	5/ tcp, udp rje Remote Job Entry	80/HTTP	202.159.72.18	X.X.84.39
1/2/00 0222:18AM	IPHalfScan	4	80/HTTP	202.159.72.18	X.X.84.40
1/2/00 0222:19AM	IPHalfScan	5	80/HTTP	202.159.72.18	X.X.84.40
1/2/00 0222:19AM	IPHalfScan	4	80/HTTP	202.159.72.18	X.X.84.66
1/2/00 0222:19AM	IPHalfScan	5	80/HTTP	202.159.72.18	X.X.84.66
1/2/00 0222:21AM	IPHalfScan	5	80/HTTP	202.159.72.18	X.X.84.43
1/2/00 0222:21AM	IPHalfScan	4	80/HTTP	202.159.72.18	X.X.84.43
1/2/00 0222:23AM	IPHalfScan	5	80/HTTP	202.159.72.18	X.X.84.78
1/2/00 0222:23AM	IPHalfScan	4	80/HTTP	202.159.72.18	X.X.84.78
1/2/00 0222:33AM	IPHalfScan	4	80/HTTP	202.159.72.18	X.X.84.157
1/2/00 0222:33AM	IPHalfScan	5	80/HTTP	202.159.72.18	X.X.84.157
1/2/00 0222:33AM	IPHalfScan	4	23/Telnet	202.159.72.18	X.X.84.99
1/2/00 0222:33AM	IPHalfScan	5	23/Telnet	202.159.72.18	X.X.84.99
1/2/00 0222:39AM	IPHalfScan	5	80/HTTP	202.159.72.18	X.X.84.166
1/2/00 0222:39AM	IPHalfScan	4	80/HTTP	202.159.72.18	X.X.84.166
1/2/00 0222:54AM	PmapDump	617/ tcp udp sco-dtmgr SCO Desktop Administration Server	111/Portmap	202.159.72.18	X.X.84.99
1/2/00 0224:23AM	IPHalfScan	5	80/HTTP	202.159.72.18	X.A.98.189
1/2/00 0224:23AM	IPHalfScan	4	80/HTTP	202.159.72.18	X.A.98.189
1/2/00 0224:31AM	PmapDump	930	111/Portmap	202.159.72.18	X.A.98.189
1/2/00 0225:35AM	IPHalfScan	4	110/POP3	202.159.72.18	X.B.67.52
1/2/00 0225:35AM	IPHalfScan	5	110/POP3	202.159.72.18	X.B.67.52
1/2/00 0229:48AM	IPProtocolViolation	1477/ tcp, udp ms-sna-server ms-sna-server	23/Telnet	202.159.51.175	X.X.84.99
1/2/00 0229:51AM	IPProtocolViolation	1477	23/Telnet	202.159.51.175	X.X.84.99
1/2/00 0232:44AM	IPProtocolViolation	1477	23/Telnet	202.159.51.175	X.X.84.99
1/2/00 0233:08AM	IPHalfScan	4	23/Telnet	202.159.72.18	Z.Z.11.80
1/2/00 0233:08AM	IPHalfScan	5	23/Telnet	202.159.72.18	Z.Z.11.80
1/2/00 0233:43AM	FTP_Syst	1479	21/FTP	202.159.51.175	X.X.84.99
1/2/00 0236:02AM	IPHalfScan	5	80/HTTP	202.159.72.18	Y.Y.1.34
1/2/00 0236:02AM	IPHalfScan	4	80/HTTP	202.159.72.18	Y.Y.1.34
1/2/00 0245:43AM	IPProtocolViolation	1477	23/Telnet	202.159.51.175	X.X.84.99
1/2/00 0249:54AM	FTP_Syst	1514/ tcp udp fujitsu-dtcns	21/FTP	202.159.51.175	X.X.84.99
1/2/00 0252:47AM	IPProtocolViolation	1477	23/Telnet	202.159.51.175	X.X.84.99
1/2/00 0252:50AM	IPProtocolViolation	1477	23/Telnet	202.159.51.175	X.X.84.99
1/2/00 0308:47AM	IPProtocolViolation	1477	23/Telnet	202.159.51.175	X.X.84.99
1/2/00 0317:57AM	IPProtocolViolation	1477	23/Telnet	202.159.51.175	X.X.84.99
1/2/00 0321:59AM	IPProtocolViolation	1477	23/Telnet	202.159.51.175	X.X.84.99
1/2/00 0337:24AM	IPProtocolViolation	1477	23/Telnet	202.159.51.175	X.X.84.99
1/2/00 0936:30AM	IPProtocolViolation	1057	23/Telnet	202.159.51.158	X.X.84.99

1/2/00 0938:03AM	IPProtocolViolation	1060/ tcp udp startron STARTRON	2345 202.159.51.158	X.X.84.99
1/2/00 0940:57AM	IPProtocolViolation	1063/ tcp udp kyocerantdev KyoceraNetDev	2345 202.159.51.158	X.X.84.99
1/2/00 0941:29AM	IPProtocolViolation	1064/ tcp udp jstel JSTEL	2345 202.159.51.158	X.X.84.99
1/2/00 0956:59AM	IPProtocolViolation	1073	2345 202.159.51.158	X.X.84.99
1/2/00 0958:41AM	IPProtocolViolation	1075	2345 202.159.51.158	X.X.84.99

Logon ID created at 0704 AM by unknown intruder!!!

Alarm Definitions**:** Obtained from ISS RealSecure console**.**

FTP SYST Command Decode
Type: Pre-attack probe
Console Name: FTP_Syst
Technical Description: This decode detects a SYST command being issued to a FTP server. This command causes the FTP server to return a response indicating the host operating system of the server.
Why this is important: Knowing the host operating system allows an attacker to customize their attack to exploit other vulnerabilities likely to be present.
False positives: Some FTP clients (such as Macintosh clients) issue a SYST command on every connect to determine if the server supports certain desirable FTP extensions.
Systems affected: Any host running an FTP server which supports SYST.
What to do: Pay close attention to other activity on the target system following the SYST request.
How to remove this vulnerability: If it is a non-anonymous FTP server, make sure your FTP server requires users to log in prior to honoring a SYST request. If anonymous access is allowed, you may be able to disable the SYST command. Consult the documentation of your FTP server.
Reference: ISS RealSecure console

Associated Vulnerabilities: CVE-1999-0017
Description: FTP servers can allow an attacker to connect to arbitrary ports on machines other than the FTP client, aka FTP bounce.
References: RFC 959
http://cve.mitre.org/

CERT Advisory CA-1999-03 FTP Buffer Overflows
Original issue date: February 11, 1999
Last revised: July 7, 1999
Updated information for Silicon Graphics, Inc. (SGI).
Source: Netect, Inc.
Topic: Remote buffer overflows in various FTP servers leads to potential root compromise.

Affected Systems: Any server running the latest version of ProFTPD (1.2.0pre1) or the latest version of Wuarchive ftpd (2.4.2-academ[BETA-18]). wu-ftpd is installed and enabled by default on most Linux variants such as RedHat and Slackware Linux. ProFTPD is new software recently adopted by many major internet companies for its improved performance and reliability. Investigation of this vulnerability is ongoing; the below lists software and operating systems for which Netect has definitive information.
Overview: Software that implements FTP is called an "ftp server", "ftp daemon", or "ftpd". On most vulnerable systems, the ftpd software is enabled and installed by default. There is a general class of vulnerability that exists in several popular ftp servers. Due to insufficient bounds checking, it is possible to subvert an ftp server by corrupting its internal stack space. By supplying carefully designed commands to the ftp server, intruders can force the server to execute arbitrary commands with root privilege. On most vulnerable systems, the ftpd software is installed and enabled by default.
Impact: Intruders who are able to exploit this vulnerability can ultimately gain interactive access to the remote ftp server with root privilege.
Solution: Currently there are several ways to exploit the ftp servers in question. One temporary workaround against an anonymous attack is to disable any world writable directories the user may have access to by making them read only. This will prevent an attacker from building an unusually large path, which is required in order to execute these particular attacks. The permanent solution is to install a patch from your Vendor, or locate one provided by the Software's author or maintainer.

Analyst action: The policy implemented by our organization categorizes this alarm as a low-level alarm. This type of alarm does not pose a direct threat to network integrity. If numerous alarms, in conjunction with medium or high level alarms and targeting multiple hosts, are observed from the source IP address (as is the case) caution is raised. All factors combined, necessitates that the event to be logged in the watch log and added to the incident ticket. Additionally, a query of the all incident and intrusion detection databases should be conducted. Both of these actions were taken at the time of the alarms.

IP Half Scan
Type: Pre-attack probe
Console Name: IPHalfScan
Technical Description: A standard TCP connection is established by sending a SYN packet to the destination host. If the destination is waiting for a connection on the specified port, it responds with a SYN/ACK packet. The initial sender replies with an ACK packet, and the connection is established. If the destination host is not waiting for a connection on the specified port, it responds with an RST packet. Most system logs do not log completed connections until the final ACK packet is received from the source. Sending an RST packet instead of the final ACK results in the connection never actually being established, so no logging takes place. Because the source can identify whether the destination host sent a SYN/ACK or an RST, an attacker can determine exactly what ports are open for connections, without the destination ever being aware of probing.
Why this is important: A stealth scan is dangerous because it allows an intruder to determine which services are running on a given host. Stealth scans are designed to pass through stateless firewalls and to avoid generating a log entry on the scanned host.

False positives: It is possible that a keep-alive timer for certain "internet push" technologies might trigger this signature.
Systems affected: Every system can be stealth scanned.
What to do: Log the address of the scanning entity. Contact the domain administrator of the source domain to verify the address and the intent behind the scan. Pay close attention to the log files of scanned hosts. If appropriate reconfigure your firewalls to inhibit traffic from the source of the scans.
How to remove this vulnerability: Upgrade your firewall to a system that understands the state of TCP connections and rejects stealth scan packets.

Reference: ISS RealSecure console

Associated Vulnerabilities: http://cve.mitre.org/
Name CAN-2000-0324 (under review)
Description: pcAnywhere 8.x and 9.x allows remote attackers to cause a denial of service via a TCP SYN scan, e.g. by nmap.
Name **CVE-1999-0116**
Description: Denial of service when an attacker sends many SYN packets to create multiple connections without ever sending an ACK to complete the connection, aka SYN flood.
Name **CVE-1999-0415**
Description: The HTTP server in Cisco 7xx series routers 3.2 through 4.2 is enabled by default, which allows remote attackers to change the router's configuration.
Name **CVE-1999-0416**
Description: Vulnerability in Cisco 7xx series routers allows a remote attacker to cause a system reload via a TCP connection to the router's TELNET port.

Name **CVE-1999-0494**
Description: Denial of service in WinGate proxy through a buffer overflow in POP3.

Name **CVE-1999-0168**
Description: The portmapper may act as a proxy and redirect service requests from an attacker, making the request appear to come from the local host, possibly bypassing authentication that would otherwise have taken place. For example, NFS file systems could be mounted through the portmapper despite export restrictions.

Half Open Scanning Overview : (AKA TCP SYN Scan). A TCP connection is attempted by first sending a SYN packet to a server. A SYN-ACK is sent back indicating that the port is listening. If the port is not listening then a RST is sent . The client then replies with an ACK. The problem occurs when the server system has sent an acknowledgment (SYN-ACK) back to client but has not yet received the ACK message. This is what we mean by half-open connection because a full TCP connection is not established. If the SYN-ACK is received out of order, the kernel sends a RST, denying the connection. The anomalous flag combination is often utilized to evade detection by the router or firewall. SYN scanning is performed by utilizing the -s option of nmap.

Analyst Action: Due to the probing of rootable services, these alarms are of great concern. The attacker has stepped up the inquiries and has probably utilized NMAP against the network. This tool can be downloaded free from www.insecure.org. The alarms and new logs should be added to the incident ticket and an additional e-mail should be sent to the point of contact and network administrator for the affected system. It is now more likely that the attacker is attempting to gain access through known rootable services. A denial of service attack is not as likely, though should still be held in consideration. The system administrator of the network needs to be informed of this activity.

AHHH…Denial of Service….wait……..who are these people not of our network???!!!!

Event Date/Time	Event Name	Source Port/Name	Destination Port/Name	Source Address	Destination Address
1/2/00 1037:17AM	Echo_Denial_of_Service	7/Echo	7/Echo	202.159.120.196	195.184.38.255
1/2/00 1046:38AM	IPProtocolViolation	1099/ tcp udp rmiregistry RMI Registry	2345	202.159.51.158	X.X.84.99
1/2/00 1048:55AM	IPProtocolViolation	1101	2345	202.159.51.158	X.X.84.99
1/2/00 1138:33AM	Echo_Denial_of_Service	7/Echo	7/Echo	202.159.32.16	209.221.200.255
1/2/00 1236:48AM	IPProtocolViolation	1236	2345	202.159.51.183	X.X.84.99
1/2/00 1531:13PM	IPProtocolViolation	1497	2345	202.159.51.183	X.X.84.99
1/2/00 1046:06PM	IPProtocolViolation	1518	2345	202.159.51.143	X.X.84.99
1/3/00 1206:05AM	IPProtocolViolation	1541/tcp udp rds2	2345	202.159.51.181	X.X.84.99
1/3/00 0126:32AM	IPProtocolViolation	1602/ tcp udp inspect	2345	202.159.51.135	X.X.84.99
1/3/00 0807:29AM	IPProtocolViolation	1070	23/Telnet	202.159.51.188	X.X.84.99
1/3/00 0812:46AM	IPProtocolViolation	1073	23/Telnet	202.159.51.188	X.X.84.99
1/3/00 1333:55PM	IPProtocolViolation	1071	2345	202.159.51.137	X.X.84.99
1/3/00 1333:55PM	IPProtocolViolation	1071	2345	202.159.51.137	X.X.84.99
1/3/00 2341:28PM	IPProtocolViolation	1098/ tcp udp rmiactivation RMI Activation	23/Telnet	202.159.51.174	X.X.84.99
1/3/00 2341:29PM	IPProtocolViolation	1098/ tcp udp rmiactivation RMI Activation	23/Telnet	202.159.51.174	X.X.84.99
1/3/00 2342:05PM	IPProtocolViolation	1098	23/Telnet	202.159.51.174	X.X.84.99
1/3/00 2342:37PM	IPProtocolViolation	1101	23/Telnet	202.159.51.174	X.X.84.99
1/3/00 2342:45PM	IPProtocolViolation	1101	23/Telnet	202.159.51.174	X.X.84.99

1/4/00 1257:40AM	IPProtocolViolation		1134		2345	202.159.51.174	X.X.84.99
1/4/00 1257:58AM	IPProtocolViolation		1135		2345	202.159.51.174	X.X.84.99
1/4/00 0842:10AM	IPProtocolViolation		1318	21/FTP		202.159.51.176	X.X.84.99
Event Date/Time	Event Name	Source Port/Name		Destination Port/Name		Source Address	Destination Address
1/4/00 0906:03AM	Echo_Denial_of_Service	7/Echo		7/Echo		202.159.65.230	208.236.130.255
1/4/00 0910:07AM	Echo_Denial_of_Service	19/Chargen		7/Echo		202.159.71.131	192.115.234.0
1/4/00 2131:56PM	IPProtocolViolation		1031		2345	202.159.51.148	X.X.84.99
1/5/00 2039:36PM	IPProtocolViolation		1042		2345	202.159.51.145	X.X.84.99
1/5/00 2040:30PM	IPProtocolViolation		1042		2345	202.159.51.145	X.X.84.99
1/5/00 2040:32PM	IPProtocolViolation		1042		2345	202.159.51.145	X.X.84.99
1/5/00 2040:35PM	IPProtocolViolation		1042		2345	202.159.51.145	X.X.84.99
1/5/00 2041:31PM	IPProtocolViolation		1042		2345	202.159.51.145	X.X.84.99
1/5/00 2041:47PM	IPProtocolViolation		1042		2345	202.159.51.145	X.X.84.99
1/5/00 2042:49PM	IPProtocolViolation		1042		2345	202.159.51.145	X.X.84.99
1/5/00 2043:54PM	IPProtocolViolation		1042		2345	202.159.51.145	X.X.84.99
1/5/00 2118:34PM	IPProtocolViolation		1042		2345	202.159.51.145	X.X.84.99
1/5/00 2128:49PM	IPProtocolViolation		1042		2345	202.159.51.145	X.X.84.99
1/5/00 2137:06PM	IPProtocolViolation		1102		2345	202.159.51.145	X.X.84.99
1/5/00 2138:12PM	IPProtocolViolation		1103		2345	202.159.51.145	X.X.84.99
1/5/00 2140:05PM	IPProtocolViolation		1108		2345	202.159.51.145	X.X.84.99
1/5/00 2141:41PM	IPProtocolViolation		1109		2345	202.159.51.145	X.X.84.99
1/5/00 2151:16PM	IPProtocolViolation		1114	23/Telnet		202.159.51.145	X.X.84.99
1/6/00 0236:45AM	IPProtocolViolation		1776		2345	202.159.51.185	X.X.84.99
1/6/00 0352:19AM	IPProtocolViolation		1803		2345	202.159.51.186	X.X.84.99
1/6/00 0353:30AM	IPProtocolViolation		1808		2345	202.159.51.186	X.X.84.99
1/6/00 0541:00AM	IPProtocolViolation		1947		2345	202.159.51.150	X.X.84.99
Event Date/Time	Event Name	Source Port/Name		Destination Port/Name		Source Address	Destination Address
1/6/00 0647:52AM	Echo_Denial_of_Service	7/Echo		7/Echo		202.159.71.6	208.236.130.255
1/6/00 0704:35AM	Echo_Denial_of_Service	7/Echo		7/Echo		202.159.71.6	202.8.226.255
1/6/00 0707:29AM	Echo_Denial_of_Service	19/Chargen		7/Echo		202.159.71.6	24.48.36.255
1/6/00 0712:05AM	Echo_Denial_of_Service	19/Chargen		7/Echo		202.159.71.6	210.79.254.255
1/6/00 0725:44AM	IPProtocolViolation		1981		2345	202.159.51.147	X.X.84.99
1/6/00 0756:53AM	IPProtocolViolation		2044		2345	202.159.51.147	X.X.84.99
1/6/00 0759:30AM	IPProtocolViolation		2048		2345	202.159.51.147	X.X.84.99
1/6/00 2149:51PM	IPProtocolViolation		1040		2345	202.159.51.175	X.X.84.99
1/6/00 2000:54PM	IPProtocolViolation		1068		2345	202.159.51.180	X.X.84.99
1/7/00 1240:58AM	IPProtocolViolation		1493		2345	202.159.51.180	X.X.84.99
1/7/00 0330:17AM	IPProtocolViolation		1539		2345	202.159.51.153	X.X.84.99
1/7/00 0435:09AM	IPProtocolViolation		1582		2345	202.159.51.153	X.X.84.99
1/7/00 2353:11PM	IPProtocolViolation		1419	23/Telnet		202.159.51.175	X.X.84.99
1/8/00 1207:40AM	IPProtocolViolation		1029		2345	202.159.51.175	X.X.84.99
1/8/00 1232:32AM	IPProtocolViolation		1413		2345	202.159.51.175	X.X.84.99
1/8/00 1254:33AM	IPProtocolViolation		1029		2345	202.159.51.175	X.X.84.99
1/8/00 0840:08AM	IPProtocolViolation		1037		2345	202.159.51.179	X.X.84.99
1/8/00 1236:03PM	IPProtocolViolation		1072		2345	202.159.51.153	X.X.84.99
1/8/00 1236:32PM	IPProtocolViolation		1077		2345	202.159.51.153	X.X.84.99
1/8/00 1250:22PM	IPProtocolViolation		1083		32345	202.159.51.153	X.X.84.99
1/8/00 1258:07PM	IPProtocolViolation		1085	23/Telnet		202.159.51.153	X.X.84.99
1/8/00 1259:18PM	IPProtocolViolation		1087	23/Telnet		202.159.51.153	X.X.84.99
1/8/00 1301:29PM	FTP_Syst		1088	21/FTP		202.159.51.153	X.X.84.99

1/8/00 1302:52PM	FTP_Syst	1093	21/FTP	202.159.51.153	X.X.84.99
1/8/00 1303:39PM	FTP_Syst	1094	21/FTP	202.159.51.153	X.X.84.99
1/8/00 1326:43PM	IPProtocolViolation	1106	2345	202.159.51.188	X.X.84.99
1/8/00 2136:56PM	IPProtocolViolation	1331	2345	202.159.51.185	X.X.84.99
1/8/00 2141:01PM	IPProtocolViolation	1332	2345	202.159.51.185	X.X.84.99
1/8/00 2149:13PM	IPProtocolViolation	1336	2345	202.159.51.185	X.X.84.99
1/9/00 0105:28AM	IPProtocolViolation	2195	2345	202.159.51.141	X.X.84.99
1/9/00 0927:36AM	IPProtocolViolation	2463	2345	202.159.51.140	X.X.84.99
1/9/00 2109:13PM	IPProtocolViolation	1026	2345	202.159.51.158	X.X.84.99
1/9/00 1011:01PM	IPProtocolViolation	1491	2345	202.159.51.158	X.X.84.99
1/10/00 1322:33PM	IPProtocolViolation	1031	2345	202.159.51.153	X.X.84.99
1/10/00 1330:15PM	IPProtocolViolation	1036	2345	202.159.51.153	X.X.84.99
1/10/00 1350:45PM	IPProtocolViolation	1883	2345	202.159.51.173	X.X.84.99
1/11/00 0353:58AM	IPProtocolViolation	1044	2345	202.159.51.136	X.X.84.99

Logon ID created 10 Jan 0503 AM and 2219 PM. Another Logon created 11 Jan 1221.

Vulnerability! "Port 2345: (TCP) HP OpenView Network Node Manager v6.1 for Windows NT 4.0 has a buffer overflow in its Alarm service which is installed on TCP port 2345 by default." Reference: http://www.netice.com/advice/Exploits/Ports/2345/default.htm

TCP/IP Protocol Violations
Type: Decode
Console Name: IPProtocolViolation
Technical description: Every network protocol has various rules, which must be followed for proper operation. As it collects packets and examines them, RealSecure checks whether certain rules are being followed. This is both to insure that RealSecure will not fail to interpret the packet properly, but also to insure that the packet is valid.
Why this is important: By deliberately injecting incorrect packets into the network, attackers can cause failures at the target host or cause a system like RealSecure to misinterpret traffic or fail.
False positives: Malfunctioning hardware or software can cause this report without necessarily representing a security risk.
What to do: Examine the reason given in the report. Check the source and destination addresses for other events signaled by RealSecure. Protocol violations are most significant in **conjunction with other attacks.**

Reference: ISS RealSecure console

Echo Vulnerability Check
Type: Denial of Service attack
Console Name: Echo_Denial_of_Service
Technical Description: This check watches for attempts at performing a denial of service attack against a machine on the network by attempting to engage a machine in an echo flood against itself.
Why this is important: This attack can effectively disable your UNIX server by causing it to spend all its time processing packets that it's echoed back to itself.
False positives: None

Systems affected: All UNIX systems
What to do: Kill and restart the inetd daemon.
How to remove this vulnerability: Edit the /etc/inetd.conf file and disable the echo service for inetd. This service is no longer necessary, but often active on UNIX hosts.

Reference: ISS RealSecure console

Associated vulnerabilities: http://cve.mitre.org/

Name CVE-1999-0103
Description: Echo and chargen, or other combinations of UDP services, can be used in tandem to flood the server, a.k.a. UDP bomb or UDP packet storm.

CERT® Advisory CA-1996-01 UDP Port Denial-of-Service Attack.
Original issue date: February 8, 1996
Last revised: September 24, 1997
Updated copyright statement

The CERT Coordination Center has received reports of programs that launch denial-of-service attacks by creating a "UDP packet storm" either on a system or between two systems. An attack on one host causes that host to perform poorly. An attack between two hnosts can cause extreme network congestion in addition to adversely affecting host performance. The CERT staff recommends disabling unneeded UDP services on each host, in particular the chargen and echo services, and filtering these services at the firewall or Internet gateway. Because the UDP port denial-of-service attacks typically involve IP spoofing, we encourage you to follow the recommendations in advisory CA-96.21.

Analyst Action: Log the event, run queries and attempt to contact network site. Call other trusted sites and determine if they are seeing the same alarms.

Whois

209.221.200.255

Quantum Networking Solutions, Inc. (NETBLK-QNET-0)
1529 E Palmdale Blvd Ste 200 Palmdale, CA 93550
Netname: QNET-0 Netblock: 209.221.192.0 - 209.221.223.255

208.236.130.255

Plant Telephone Co. (NETBLK-UU-208-236-128)
PO Box 187
Tifton, GA 31793
US
Netname: UU-208-236-128
Netblock: 208.236.128.0 - 208.236.131.255

202.8.226.255
inetnum 202.8.226.192 - 202.8.226.255
netname SGI-DOC
descr Solid Group Inc. country PH

24.48.36.255
Adelphia Cable Communications (NETBLK-ADELPHIA-CABLE)
Main at Water Street Coudersport, PA 16915 US Netname: ADELPHIA-CABLE Netblock: 24.48.0.0 - 24.51.255.255 Maintainer: ADEL

210.79.254.255
inetnum 210.79.224.0 - 210.79.255.255
netname CETIN
descr China Engineering Technology Informations Networks country CN

Conclusion: This incident was reported expeditiously by the watch team at the time of the DNS zone transfers (within 1 hour). The incident was reported to the site system point of contact for the intrusion detection system (this person is the site admin) and the Information System Security Manager (ISSM) via e-mail as neither could be reached by pager. The start of the incident occurred over a weekend (very early Sunday morning) and the administrator was not available (he was paged as per policy). Alarms continued through the early morning hours. Later inspection by the system manager would indicate that at 0704 AM, approximately 6 hours after the zone transfers, an unauthorized logon ID was created by an unknown intruder. This account was determined to have root level access. From examination of the logs, the reconnaissance from 0222:17AM - 0245:43 AM must have provided interesting and lethal information to the attackers. At 0245:33 AM the attackers narrowed the activity to the compromised box (X.X.84.99). How did the intruder gain access? This information was never provided to the monitoring station. However, probes were observed to three rootable services against this network (Telnet, Portmap, and FTP). Initial access could have been gained through any of these services. After 0938:03 AM probes to common rootable services cease and activity is only seen to port 2345. This port has a buffer overflow vulnerability that, if successful, allows the execution of arbitrary code. Another matter of great concern was the outbound activity, echo denial of service alarms, observed from the source IP address to destination IP addresses outside our organization and sites not monitored by our IDS. This indicates that the source IP address is most likely spoofed, or it would not have been detected by the IDS. This further supports that the system was compromised and enforces the need for immediate action. The intruders were now using the network to conduct activity against other destinations. During more reasonable waking hours on 02 Jan 00, the network point of contact answered the page from the watch. He stated that the box in question belonged to a sub-contractor located away from his site and this matter would be looked into Monday 03 Jan 00. The compromise was not caught by the organization until 07 Jan 00. The compromise was reported to a computer emergency response team (CERT), but not the Computer Incident Response Team (CIRT-our organization) until 13 Jan 00. Between 02 Jan and 11 Jan 2000 the watch team continued to report activity to the network point of contact as well as the proper chain of command and law enforcement authorities. At some point between 07 Jan and 11 Jan a sniffer was placed on the network. Upon discovery of the attacker, the compromised box was removed from the network, replaced by another, and turned over to law enforcement as evidence. Log files from the monitoring station and the site were also confiscated and taken into evidence. The incident was

labeled "law enforcement sensitive." The only post information follow-up provided by the law enforcement investigators was that the attackers were caught while on the network. Kudos were given to the watch team for their exemplary performance and incident handling prowess. The watch team followed all recommended steps for incident handling. The watch team remained calm and followed organizational communications procedures. Watch logs (legal documents) were generated with all of the details of the observed attack. The integrity of these logs was maintained in a secure facility on a secure network. Evidence on exploits and vulnerabilities, associated with the alarms, was gathered from outside reputable sites and added into evidence. The questions of who, what, where and time frames of the attack (just the facts) were documented. The why and how as of yet is still unknown to the monitoring station analyst. Documentation of conversations between the remote site and the monitoring station was also performed. Conversations between personnel involved were conducted over secure telephone communications when details of the incident were discussed. The chain of command was kept informed of any changes and new developments.

SIX Primary Phases of Incident Handling Addressed

1. **Preparation**: While the target networks do not fall under the administrative control of the monitoring station, measures and policies have been established in terms of intrusion detection, reporting procedures, and intervention. A Computer Incident Response Team (CIRT) was established and security policies were in place. Warning banners were posted, to identify the type of organization being accessed, as well as the repercussions for misuse and abuse. Additionally, by accessing the sight, the user consents to monitoring. Clearly defined roles and responsibilities have been set forth in writing as per organizational policy. All Computer Network Defense (CND) personnel have read current policies and have completed training requirements for their position.

Intrusion Detection Watch. A 24-hour monitoring watch was established at the monitoring site and intrusion detection analysts were assigned to each intrusion detection system (IDS). A watch supervisor was assigned per watch section to provide guidance and enforce established policies. Reporting procedures were clearly defined by organizational policy. A chain of command was established with respect to the reporting of incidents by severity. Procedures for reporting and notification are different for probes, attempted intrusions, intrusions, and root compromises. The watch personnel are educated on the reporting procedures for each type of incident. Points of contacts have been established for the monitored sites and posted on the watch for quick recall. However, a persistent problem is that while the monitoring station is available 24-hours a day, the sites are not. In the event that an incident is found, which warrants notification of the site, the point of contact may not be available until normal working hours. Without administrative rights, access to the remote sites network, and established policy for intrusion intervention (memorandum of agreement -very political) the watch is responsible for the proper reporting of the incidents and notifying cognizant authorities (i.e. chain of command and law enforcement). Additionally, the watch monitors news sites (CNN) and hacker sites for current events, new vulnerabilities, and exploits. These events are compiled and presented via operational brief. If the information requires more immediate routing, it is presented to the chain of command and incident handlers upon discovery.

Incident Handlers. An incident handling team is clearly defined. Incident handlers are identified and assigned an incident from its inception to conclusion. The incident handlers conduct research and contact individuals outside our organization. They gather evidence from the watch and coordinate with law enforcement agencies. Policies on reporting procedures and formats are provided to each site. Reports are received, reviewed, and entered into a database. Incident handlers provide and disseminate a "hot IP list" of active source IP addresses that are suspected of malicious behavior against networks within our organization.

Training. An organizational training coordinator has been assigned in writing. This person is responsible for the timely training of all personnel assigned to computer incident response, operational network administration, and security positions. A sequence of training qualifications and timeline for completion has been established. The training coordinator is responsible for the professional development and progress tracking of all assigned personnel.

Communication. All computer incident response personnel are provided a recall bill or call tree. A clearly defined procedure for contacting personnel is defined (pagers, cell phones, home phones). The order in which personnel are contacted is provided and in the custody of the watch supervisor. Secure communications are available through secure telephone lines, faxes, and encryption.

Checklists. Incident response and emergency response (contingency planning) checklists are located on the watch supervisor's desk. All CIRT personnel have access to and are trained to utilize these checklists.

Law Enforcement. Our organization has an on board law enforcement team which works hand in hand with the incident handlers and watch teams. These individuals are available 24-hours and are listed on the recall bill.

System Administrators. System administrators are assigned to the CIRT. These administrators are available 24-hours per day to assist to provide maintenance technical assistance. Administration of the remote site is the responsibility of the site administrators. The site administrator and the ISSM are normally listed as the point of contact for incidents. All site points of contact are informed of any changes in configuration, system downtime, and any conditions that may adversely affect network security.

Much preparation has been made at the monitoring station to effectively handle both incidents reported by other organizations and incidents observed real-time. The preparations made by the monitoring station directly impact the security of the remote site. However, without the ability to have access to the systems, it is imperative that the site administrators be contacted in a timely manner. Completing checklists prior to contact and ensuring that the data contained therein is accurate is imperative.

Jump Bag. The CIRT has at it's disposal, laptop computer's with dual operating systems, approved forensic tool kits and sniffers(as well as a non-networked laboratory to test and evaluate tools and software prior to usage), windows resource kit, CD's with binaries for UNIX, incident reports forms for effective note taking of pertinent information, cellular phones and pagers, and a recall bill (phone list of all personnel). Disks, tapes, writable CD's, and burners are available for back-up and storage of information. Our organization has a toll free number that can be accessed worldwide, no need for calling cards or spare change

2. **Identification**: In the handling of this incident, the threat was identified at the time it was observed on the IDS. However, from inspection of the IDS logs, it seems that a significant amount of reconnaissance was conducted against the network prior to the compromise that may

have evaded detection. An incident ticket was generated which provided the following information:

Incident Report Form

1. Report Date:
2. Report Originator Information:
3. Target Information:
    a. Network Domain Name
    b. IP Address (e.g., xxx.xxx.xxx.xx)
    c. Computer Model (e.g., SUN SparcStation 10)
    d. Operating System/Version (e.g., SUN-OS 4.1.6)
    e. Security Mode (dedicated, system high, multilevel, etc)
    f. Security Classification (e.g., SBU, secret, etc.)
    g. Network/System Mission (e.g., administration, C2, communications, etc.)
    h. Network Structure/Type
    i. How was the Activity Detected
    j. Impact on Mission (if compromised)
4. Attack Session Information
    a. Date/dates of the session
    b. Time
    c. Attack Method (e.g., phf, telnet, etc)
    d. Success - successful Intrusion or Denial of Service attack (yes or no)
    e. Account (include host name if available)
    f. First Layer Point of Origin IP (source IP)
    g. Category of attack:
        Root Access
        User Access level
        Unauthorized attempted access
        Unauthorized probe/information gathering
        Denial of Service
        Malicious Logic
    h. For attempted intrusions, probes, denial of service attacks, and malicious logic infections: Estimated number of probes, attempts, or infections.
5. Brief Scenario (description of incident)
6. Countermeasure(s) installed (e.g., patches, tcp wrappers, shadow passwords, etc)
7. Impact Summary
    a. Number of systems attacked
    b. Number of systems affected
    c. Number of Users affected
    d. Total Work Hours Lost
    e. Other impact

The above is the actual form utilized by the watch team while working the incident. It provides pertinent information to be passed to the incident handlers and site system administrators. A specific incident handler is assigned to maintain continuity and establish a set point of contact. He/she is responsible for evaluating the incident, researching the vulnerability, and documenting all actions taken. A log of all incidents is maintained by the incident handling

team. Files are stored on secure directories with limited access. This data may also be passed to or accessed by, law enforcement officials. The watch team correctly handled the incident and attempted to inform the remote site at an early stage. The problem was that the remote site was unavailable to take action. Information was gathered and queries (correlations) were made to further define the scope of the attack. The information was passed on to the chain of command and, in the case of this incident, was passed to CIRT law enforcement personnel. The chain of custody for evidence is from the watch to the CIRT, with an e-mail going to the remote site administrators. Secure means of transmission are available (both phone and fax).

3. **Containment**: Containment is difficult in the case of this incident. The damage was well underway when the attempt to contact the site administrators was made. At first, the incident was seen as common probing. However, on Jan 7 2000, it was reported that a box on the target network was found to be compromised by the source IP address. If the attacker were registered to a U.S. ISP, the ISP would have been contacted. The problem with this incident is that the IP address was registered to an ISP in Indonesia. Caution should be taken not to disclose information about the target network personnel without a "need to know." Only information pertaining to the attacking network would be provided to the ISP. All forwarded logs would be sanitized. Though, the box was deemed to be compromised, the system was not immediately taken off the network. A sniffer was placed on the network to gather further evidence. All logs (from the remote site and the monitoring site) and the system itself were passed to law enforcement officials for forensic inspection. After evidence was gathered and the offenders identified, the system was taken off the network and was never reconnected. Therefor, there was no need to restore the system.
4. **Eradication**: Determining the cause of the incident is difficult from the perspective of the monitoring station security analyst. Theories were made as to the cause of the compromise, but no confirmations were provided by law enforcement. Information was deemed "law enforcement sensitive" and not disclosed. The source IP address was placed on a hot list and monitored for further activity. Activity from the target network was monitored closely for suspicious activity. Security practices and policies should be reviewed and recommendations should be made to improve network security. Administrators should be aware of the exploits that lead to the compromise and recommendations for eradication should be formulated.
5. Recovery: There was no need to restore the compromised system, it was taken offline and never returned. It was replaced by a new system. A vulnerability assessment was later performed against the network to take a snapshot of the security posture. Vulnerabilities and exploits were examined and applicable fixes were made. Due to the root level compromise, it is recommended that all passwords be changed. Account validation should be performed to ensure that no remaining unauthorized users are present on the network. It is the responsibility of the site administrator to ensure that all current patches are applied, ACL are updated, and firewall policies are current. Continued close monitoring of the network should be performed.
6. **Follow-up/Lessons Learned**: The incident was taken over by law enforcement for further forensic inspection. No final report was sent by the remote site or law enforcement. The site continues to be monitored and no further activity has been observed from the source IP address. Effective incident handling procedures were followed and the integrity of the evidence was preserved. The incident was reported in a timely manner, which could have prevented the intrusion. However, the site administrators were not available to take immediate action to prevent the compromise. This is a common problem when dealing with remote sites outside of

the administrative control of the monitoring station. A concrete communication plan should be established on the side of the remote site. A 24 hour point of contact with access to the system should be available in the event of an emergency. A memorandum of agreement or trust should be established between the remote site and the monitoring station that allows the IDS analysts to take evasive action on behalf of the targeted network.

Educating the site administrators on IDS would be of great benefit and expedite the handling of the incident. Understanding the importance and meaning of the alarms, prior to an incident, would assist the administrators in comprehending the full scope of the incident or "big picture." This practice would provide further assistance in identifying new exploits and vulnerabilities as well as changes to network baseline performance. Suspected out bound activity was observed from the targeted network. Out bound traffic and security practices for information leaving the network should be examined and monitored. Often, policies are strictly enforced against incoming activity but overlooked on the outgoing side.

Last Updated: July 25th, 2017

Upcoming Training

Security Awareness Summit & Training 2017	Nashville, TN	Jul 31, 2017 - Aug 09, 2017	Live Event
SANS San Antonio 2017	San Antonio, TX	Aug 06, 2017 - Aug 11, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
Community SANS Memphis SEC504	Memphis, TN	Aug 21, 2017 - Aug 26, 2017	Community SANS
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
Mentor Session AW - SEC504	Milwaukee, WI	Aug 23, 2017 - Sep 29, 2017	Mentor
Mentor Session AW - SEC504	New York, NY	Aug 24, 2017 - Sep 08, 2017	Mentor
Mentor Session - SEC504	Denver, CO	Aug 29, 2017 - Oct 10, 2017	Mentor
SANS San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS vLive - SEC504: Hacker Tools, Techniques, Exploits and Incident Handling	SEC504 - 201709,	Sep 05, 2017 - Oct 12, 2017	vLive
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
SANS Dublin 2017	Dublin, Ireland	Sep 11, 2017 - Sep 16, 2017	Live Event
Mentor AW - SEC504	Santa Clara, CA	Sep 11, 2017 - Sep 22, 2017	Mentor
Mentor Session - SEC504	Arlington, VA	Sep 20, 2017 - Nov 01, 2017	Mentor
Community SANS Columbia SEC504	Columbia, MD	Sep 25, 2017 - Sep 30, 2017	Community SANS
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS SEC504 at Cyber Security Week 2017	The Hague, Netherlands	Sep 25, 2017 - Sep 30, 2017	Live Event
Mentor Session - SEC504	Boston, MA	Sep 26, 2017 - Nov 07, 2017	Mentor
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Mentor Session AW - SEC504	Houston, TX	Oct 02, 2017 - Dec 11, 2017	Mentor
Mentor Session - SEC504	Columbia, SC	Oct 03, 2017 - Nov 14, 2017	Mentor
SANS October Singapore 2017	Singapore, Singapore	Oct 09, 2017 - Oct 28, 2017	Live Event
Community SANS Chicago SEC504	Chicago, IL	Oct 09, 2017 - Oct 14, 2017	Community SANS
SANS Phoenix-Mesa 2017	Mesa, AZ	Oct 09, 2017 - Oct 14, 2017	Live Event