Global Information Assurance Certification Paper

SANS GIAC Advanced Incident Handling and Hacker Exploits

Practical Assignment for SANS Parliament Hill

Option 1 – Illustrate an Incident

The following information documents a recent incident handled by the incident response organization under my direction. While not an intrusion, it is illustrative of issues associated with the handling of common classes of incidents that introduce awareness of new exploits, expose vulnerabilities in activity access policies/processes/procedures, or otherwise lead to significant improvements on the defensive posture of the organizations affected.

Details have been heavily sanitized as our policy is that incident details are for official use only, not for public dissemination.

1. Executive Summary

Multiple telnet connection attempts were detected involving a single external anomalous source and multiple internal system addresses. These events were identified as a single incident and classified as a scan. Authoritative Internet information sources were consulted in an attempt to determine the possible motive and intent of the perpetrator. A determination was made that the most likely ultimate intent had been to execute a newly released exploit against SGI Irix systems. Firewall rules and intrusion detection system policies were modified to detect and contain future access attempts from the source. Firewall and intrusion detection system logs were examined to determine the full scope of the incident and whether any of the systems may have been compromised. Also, security officers were asked to poll system administrators to determine if any systems vulnerable to the exploit existed, and to provide logs relevant to the handling of this incident. Systems involved were determined not to be vulnerable to this exploit. Also system logs showed no evidence of attempts to use the exploit, and no actual logins appeared to have occurred during the period in question. The overall pattern of events detected supported a hypothesis that the scan was for reconnaissance rather than actual execution of an attack. Logs did however indicate a vulnerability in that firewall rules allowed telnet access to several internal systems, also investigation showed weaknesses in creation and maintenance of access logs on some systems.

2. Stages of Incident Handling

Incident handling consists in theory of a sequence of activities executed in sequence. (In practice, as described in detail below, the stages often occur in parallel, with aspects of identification continuing to occur while at least containment and possibly even eradication and recovery are on-going).

a. PREPARATION. Preparation involves advance planning for response to incidents,

and includes creation and dissemination of policy, establishment of organizational roles and responsibilities, and provision for the people, equipment, communications, etc. that will be required when an incident occurs.

b. IDENTIFICATION. Identification includes detection of anomalies, their assessment as to type and severity, and the notification of appropriate parties. Detection can occur through automated or manual review of network traffic or audit records, and can occur during the event or some time afterward. Assessment is a process of first determining whether an event is an incident or an artifact of normal activity. Then follows a process of creating, refining and testing of hypotheses concerning the motive and intent of the originator of the incident (who may be referred to as the perpetrator) and the effect of the incident, if any. Notification is a process of communicating relevant information to persons/organizations with a need to know.

c. CONTAINMENT. Containment consists of steps taken to limit the damage associated with an incident. Containment often involves isolation of affected systems or services.

d. ERADICATION. Eradication consists of steps taken to eliminate new vulnerabilities inserted as a result of an incident. The extent of eradication required depends on the level of access, if any, achieved.

e. RECOVERY. Recovery consists of steps taken to mitigate adverse effects of an incident, and restore operations to a correct state.

f. FOLLOW-UP. Follow-up consists of steps taken as a result of after-action analysis to determine lessons learned that can improve the process of preventing or handling incidents in the future.

3. Preparation

The enterprise had been prepared with some, necessarily incomplete policies, many of them however still in draft. A policy was in place requiring posting of warning banners with wording like the following:

THIS IS A DEPARTMENT OF DEFENSE COMPUTER SYSTEM. THIS COMPUTER SYSTEM, INCLUDING ALL RELATED EQUIPMENT, NETWORKS AND NETWORK DEVICES (SPECIFICALLY INCLUDING INTERNET ACCESS), ARE PROVIDED ONLY FOR AUTHORIZED U.S. GOVERNMENT USE. DOD COMPUTER SYSTEMS MAY BE MONITORED FOR ALL LAWFUL PURPOSES, INCLUDING TO ENSURE THAT THEIR USE IS AUTHORIZED, FOR MANAGEMENT OF THE SYSTEM, TO FACILITATE PROTECTION AGAINST UNAUTHORIZED ACCESS, AND TO VERIFY SECURITY PROCEDURES, SURVIVABILITY AND OPERATIONAL SECURITY. MONITORING INCLUDES ACTIVE ATTACKS BY AUTHORIZED DOD ENTITIES TO TEST OR VERIFY THE SECURITY OF THIS SYSTEM. DURING MONITORING, INFORMATION MAY BE EXAMINED, RECORDED, COPIED AND USED FOR AUTHORIZED PURPOSES. ALL INFORMATION, INCLUDING PERSONAL INFORMATION, PLACED ON OR SENT OVER THIS SYSTEM MAY BE MONITORED.

USE OF THIS DOD COMPUTER SYSTEM, AUTHORIZED OR UNAUTHORIZED, CONSTITUTES CONSENT TO MONITORING OF THIS SYSTEM. UNAUTHORIZED USE MAY SUBJECT YOU TO CRIMINAL PROSECUTION. EVIDENCE OF UNAUTHORIZED USE COLLECTED DURING MONITORING MAY BE USED FOR ADMINISTRATIVE, CRIMINAL OR OTHER ADVERSE ACTION. USE OF THIS SYSTEM CONSTITUTES CONSENT TO MONITORING FOR THESE PURPOSES.

Other policies required firewalls and intrusion detection systems to be in place, established an agency incident handling team, called for reporting of incidents to the team, required local information systems security officers to have been appointed, required security training for system administrators, etc. The incident response team had procedures in place that called for routine monitoring of logs and other indicators, notification to the local site, law enforcement, network service provider(s), line manager(s), etc.

The incident response team was staffed with employees with backgrounds in a variety of disciplines, including both UNIX and Microsoft Windows products, as well as computer networking (specifically TCP/IP).

4. Identification

Identification of this incident began when a pattern of telnet events was detected through review of firewall logs. An sanitized extract of the log follows.

```
Aug XX YY:32:36.957 FIREWALL gwcontrol: 201 telnet[2698969167]:
access denied for SOURCE-IP to DESTINATION-NET.1 [default rule] [no
rules found]
Aug XX YY:32:36.959 FIREWALL gwcontrol: 201 telnet[2698969169]:
access denied for SOURCE-IP to DESTINATION-NET.4 [default rule] [no
rules found]
Aug XX YY:32:36.958 FIREWALL telnetd[26842]: 121 Statistics:
duration=0.01 id=2YcKP rcvd=18 srcif=qfe0 src=SOURCE-IP/3117
dstif=hme0 dst=DESTINATION-NET.1/23 proto=telnet (Access denied)
Aug XX YY:32:36.959 FIREWALL telnetd[26842]: 121 Statistics:
duration=0.00 id=2YcKR rcvd=18 srcif=qfe0 src=SOURCE-IP/3120
dstif=hme0 dst=DESTINATION-NET.4/23 dstname=DESTINATION-NET.4
proto=telnet (Access denied)
Aug XX YY:32:36.960 FIREWALL telnetd[26842]: 121 Statistics:
interval=0.02 id=2YcKO srcif=qfe0 src=SOURCE-IP/3118 dstif=hme0
dst=DESTINATION-NET.2/23 dstname=DESTINATION-2.MIL proto=telnet
rule=123
Aug XX YY:32:36.965 FIREWALL gwcontrol: 201 telnet[2698969170]:
access denied for SOURCE-IP to DESTINATION-NET.5 [default rule] [no
rules found]
Aug XX YY:32:36.966 FIREWALL telnetd[26842]: 121 Statistics:
duration=0.00 id=2YcKS rcvd=18 srcif=qfe0 src=SOURCE-IP/3121
dstif=hme0 dst=DESTINATION-NET.5/23 dstname=DESTINATION-NET.5
proto=telnet (Access denied)
Aug XX YY:32:36.967 FIREWALL kernel: 226 IP  packet dropped (SOURCE-
IP->DESTINATION-NET.0: Protocol=TCP[SYN] Port 3115->23): dest is
subnet broadcast (received on interface INTERFACE-IP)
```

```
Aug XX YY:32:37.004 FIREWALL gwcontrol: 201 telnet[2698969168]:
access denied for SOURCE-IP to DESTINATION-3.mil [default rule] [no
rules found]
Aug XX YY:32:37.004 FIREWALL telnetd[26842]: 121 Statistics:
duration=0.05 id=2YcKQ rcvd=18 srcif=qfe0 src=SOURCE-IP/3119
dstif=hme0 dst=DESTINATION-NET.3/23 dstname=DESTINATION-3.mil
proto=telnet (Access denied)
Aug XX YY:32:37.008 FIREWALL telnetd[26842]: 121 Statistics:
duration=0.06 id=2YcKO rcvd=3 srcif=qfe0 src=SOURCE-IP/3118
dstif=hme0 dst=DESTINATION-NET.2/23 dstname=DESTINATION-2.mil
proto=telnet rule=123
Aug XX YY:32:37.842 FIREWALL kernel: 226 IP  packet dropped (SOURCE-
IP->DESTINATION-NET.255: Protocol=TCP[SYN] Port 3692->23): dest is
subnet broadcast (received on interface INTERFACE-IP)
Aug XX YY:32:39.804 FIREWALL kernel: 226 IP  packet dropped (SOURCE-
IP->DESTINATION-NET.0: Protocol=TCP[SYN] Port 3115->23): dest is
subnet broadcast (received on interface INTERFACE-IP)
Aug XX YY:32:40.793 FIREWALL kernel: 226 IP  packet dropped (SOURCE-
IP->DESTINATION-NET.255: Protocol=TCP[SYN] Port 3692->23): dest is
subnet broadcast (received on interface INTERFACE-IP)
Aug XX YY:32:42.369 FIREWALL telnetd[26842]: 121 Statistics:
duration=5.40 id=2YcKT rcvd=18 src=SOURCE-IP/3122 proto=telnet (Call
startup failure)
Aug XX YY:32:42.525 FIREWALL telnetd[27337]: 121 Statistics:
duration=5.25 id=2Yj7Y rcvd=18 src=SOURCE-IP/3169 proto=telnet (Call
startup failure)
Aug XX YY:32:42.647 FIREWALL telnetd[27338]: 121 Statistics:
duration=5.21 id=2Ylg5 rcvd=18 src=SOURCE-IP/3265 proto=telnet (Call
startup failure)
Aug XX YY:32:42.942 FIREWALL telnetd[27339]: 121 Statistics:
duration=5.27 id=2Ynoe rcvd=18 src=SOURCE-IP/3375 proto=telnet (Call
startup failure)
Aug XX YY:32:43.010 FIREWALL gwcontrol: 201 telnet[3719036929]:
access denied for SOURCE-IP to DESTINATION-119.mil [default rule] [no
rules found]
Aug XX YY:32:43.011 FIREWALL telnetd[27344]: 121 Statistics:
duration=0.18 id=2Yy2R rcvd=18 srcif=qfe0 src=SOURCE-IP/1801
dstif=hme0 dst=DESTINATION-NET.119/23 dstname=DESTINATION-119.mil
proto=telnet (Access denied)
Aug XX YY:32:43.038 FIREWALL telnetd[27340]: 121 Statistics:
duration=5.21 id=2Ypwl rcvd=18 src=SOURCE-IP/3480 proto=telnet (Call
startup failure)
Aug XX YY:32:43.118 FIREWALL telnetd[27341]: 121 Statistics:
duration=5.20 id=2YrEt rcvd=18 src=SOURCE-IP/3636 proto=telnet (Call
startup failure)

[586 lines deleted]
```

These log entries showed repeated attempts to connect to the telnet port (tcp/23) on all IP addresses on a particular class C network. The source, coming from IP address SOURCE-IP, was from a network not known to have any business relationship with the affected site or its users, in fact it was from another part of the world. The source address remained constant while the destination address changed each iteration. Destination addresses tried included .0 and .255 addresses, i.e. broadcast addresses.

The whois service available at http://www.arin.net/whois/arinwhois.html was queried for

information regarding the source. (Had the source been from a network location assigned outside North America, alternative whois data sources would have been http://www.ripe.net/cgi-bin/whois for Europe and http://www.apnic.net/search for Asia/Pacific). Use of these whois services, unlike finger or similar attempts to connect to the source IP, was not considered likely to be visible to the perpetrator, also some indication as to the nature of the source is required for assessment purposes.

The whois lookup required several iterations as the first produced multiple hits, one that of a larger ISP who had resold or leased it to a smaller one. The input to the initial query was the SOURCE-ADDRESS
found in the firewall logs. The query produced multiple hits:

```
BIGISP (NETBLK-CIDR-BLK-BIG)     NETBLK-CIDR-BLK-BIG  XXX.YY.0.0 - XXX.YY.255.255
   LITTLEISP (NETBLK-LITTLEISP) LITTLEISP
                                XXX.YY.28.0 - XXX.YY.30.255
```

The input to the second whois query was "NETBLK-LITTLEISP". The final result of the query was:

```
LittleISP, Inc. (NETBLK-LITTLEISP)
      Street Address
      City, State ZIP
      US

      Netname: LITTLEISP
      Netblock: XXX.YY.28.0 - XXX.YY.30.255

      Coordinator:
        Name  (Handle) Email Address
        Phone Number

      Record last updated on 10-Jun-2000.
      Database last updated on 12-Sep-2000 07:35:02 EDT.
```

While it is not clear because of the sanitization of the data, LITTLEISP had no known relationship with the destination or its users; also it was not in the same geographic area.

Assessment – Round 1

Any organization that monitors networks connected to the Internet quickly becomes aware that scans of various types occur frequently. This scan however was particularly anomalous because scans of the telnet port are not common.

The telnet protocol is used to establish a remote terminal session between an authorized client (source) and a specific server (destination). Normal telnet events are characterized

by connections from a single source, usually on a known/authorized network, to a single destination. This event involved both an unknown/unauthorized source and multiple sequential destinations. Because of the nature of this event, it was immediately assessed to be an incident, rather than something associated with normal activity. Specifically, the incident was categorized as a telnet scan. The perpetrator was assumed to be trying to locate telnet servers on the network scanned, preliminary to attempting to exploit some vulnerability or other, as yet unidentified.

Notification

A primary incident handler was identified. (Unfortunately at this stage she was not assigned a specific measurable realistic achievable time-based reporting date). An initial incident report was generated. This report was forwarded to the organization's network service provider's incident response team. The site's information systems security officer, responsible for local incident handling, was notified. He was requested to contact the system administrator(s) to obtain the syslog data from machines to which telnet succeeded.

The enterprise network security officer/CERT manager was already aware, in this case directing the incident handling. The fact that telnet scanning was occurring was shared with other members of the enterprise incident handling team.

Communications with non-local persons and organizations were via encrypted electronic mail, or telephone calls.

5. Containment – Round 1

Intrusion detection systems (IDS) and perimeter defenses were adjusted to block access from the entire network containing SOURCEIP, as well as to log such attempts in greater detail.

Firewall and IDS logs were examined to determine whether additional records could be found involving SOURCEIP. Such logs were then used to determine the scope of the incident, which was determined to extend beyond the single class C network on which it had originally been detected. All indications however were than SOURCEIP had initiated only telnet scans, no other protocols being found in the logs.

Deployment of an onsite team was determined to be inappropriate at this point as no evidence of actual intrusion had yet been found. Similarly disconnection of the system from the network or disabling of the network service were not seriously considered. The risk of continuing operations was considered acceptable at this point. Backup procedures and schedules exist for production systems and no changes were made at this point pending further investigation.

System owners (as opposed to administrators) had not been notified yet. Passwords not

changed yet, no evidence existing that any had been compromised.

Assessment – Round 2

The next step in assessment consisted in attempting to understand the motive and intent of the telnet scan.

Vulnerabilities associated with telnet include some that are inherent in the protocol and some that are associated with faulty implementations. Vulnerabilities inherent in the protocol were fairly well-known e.g. (a) loss of confidentiality, because the cleartext session contents (including userid and password) are subject to sniffing, and (b) unauthorized access, because the authentication mechanism (passwords) is subject to guessing attacks.

Vulnerabilities associated with specific telnet implementations were assessed based on a search of several authoritative sources on the Internet for telnet vulnerabilities. The search was limited to recent vulnerabilities on the theory that these would provide the greatest return on time investment to a scanner. Results were as follows:

CERT Coordination Center (http://www.cert.org)

Most documented vulnerabilities were fairly old, however one recent note was available, CERT® Incident Note IN-2000-09, at http://www.cert.org/incident_notes/IN-2000-09.html. This incident note indicated that there had been "reports of intruder activity involving the telnet daemon on SGI machines running the IRIX operating system. Intruders are actively exploiting a vulnerability in telnetd that is resulting in a remote root compromise of victim machines." The CERT bulletin pointed to additional information available from the vendor, SGI, at ftp://sgigate.sgi.com/security/20000801-01-P

Later it was discovered that this particular vulnerability would have been discovered earlier without a search, by simply browsing the CERT current activity report, at the URL http://www.cert.org/current/current_activity.html.

SecurityFocus Bugtraq (http://www.securityfocus.com/**)**

The archive of the the Bugtraq mailing list was searched for recent telnet-related vulnerabilities. The most recent was the "IRIX telnetd Environment Variable Format String Vulnerability" documented at http://www.securityfocus.com/bid/1572, i.e. the same vulnerability reported in the CERT incident note cited above. This vulnerability was reported to the Bugtraq mailing list on August 14, 2000 by LSD contact@lsd-pl.net, in a message archived at http://www.securityfocus.com/archive/1/75864. LSD included a reference to exploit code, which was included in the SecurityFocus Bugtraq archive. Availability of this exploit allowed the analyst to experiment with its execution and

determine what if any evidence it would leave in logs (on a test system, of course, not one of the systems involved in the incident). The results of these tests indicated that, at least on the systems tested, the exploit would generate entries in TCP wrapper-generated logs (logs of the invocation of the telnetd) but would not generate entries in login logs or in other syslog entries.

The following is a summary of the exploit:

IRIX telnetd Environment Variable Format String Vulnerability

Name: IRIX telnetd Environment Variable Format String Vulnerability
Variants: This is itself a variant of the vulnerability reported in CERT Advisory CA-95.14, at http://www.cert.org/advisories/CA-95.14.Telnetd_Environment_Vulnerability.html
Operating System: Most or all versions of SGI Irix prior to 6.5.10
Protocols/Services: telnet (23/tcp)
Brief Description: telnet daemon can be used to gain administrator access.

Protocol Description

The telnet service is an interactive service. The protocol establishes a virtual terminal connection between a source computer and a destination computer to allow keyboard input and screen output to move between them as if they were physically the same system. The service establishes a TCP/IP session, which typically begins with connection to a login/authentication process followed by execution of an interactive command processor (shell). The service is typical of UNIX and similar multi-user systems, rather than single-user systems like Windows. One extension made to the protocol involves a capability to essentially pass environment information from the client UNIX command processor to the server command processor. It is an error in the implementation of this extension that is used by this exploit.

How the exploit works

The exploit uses an error in the handling of information passed by the telnet environment variable. Per the Bugtraq archive

> The telnet daemon, upon receiving a request via
> IAB-SB-TELOPT_ENVIRON request to set one of the _RLD
> environment variables, will log this attempt via syslog(). The data normally
> logged is the environment variable name, and the value of the environment
> variable. The call to syslog, however, uses the supplied variables as part of
> the format string. By carefully constructing the contents of these variables, it
> is possible to overwrite values on the stack such that supplied code may be
> executed as the root user.

Signature of the attack

Per the CERT Incident Note, generation of a syslog message similar to

> overly long syslog message detected, truncating
> telnetd[xxxxx]: ignored attempt to setenv (_RLD, ^?D^X^\
> ^?D^X^^ ^D^P^?^?$^B^Cs#^?^B^T#d~^H#e~^P/d~^P/`~^T#`~^O
> ^C ^?^?L/bin/sh

or

overly long syslog message, integrity compromised, aborting

Additional Information

See above links to additional information

At this point in the incident handling the working hypotheses was modified to be: the perpetrator was trying to locate vulnerable SGI Irix systems preparatory to or in conjunction with an attempt to use the recently publicized telnetd exploit to gain administrator access.

Questions remaining included:

Were there any vulnerable systems on the networks that were scanned?

Did any of the scans get through to vulnerable systems?

Was the scan merely reconnaissance or was it an actual intrusion attempt?

If an intrusion attempt, did any succeed?

Containment – Round 2

An advisory message was sent to all supported sites regarding the SGI Irix telnetd vulnerability. The message required identification/reporting of any vulnerable systems. Results were negative. (At least one site had used a SGI system in the past, however it was out of service).

Also at this time results began to come in regarding logs of systems involved in the original incident. Results again were negative; there were no indications of any anomalies.

Assessment – Round 3

Firewall log entries of all sites with connections from SOURCEIP were reviewed in greater detail. Particular attention was paid to duration of connections. A factor tending to make this incident appear less threatening included the fact that connection duration tended to be extremely brief implying that the perpetrator may not have been attempting to use the exploit, or the exploit may have been immediately failing. Further experimentation with the exploit code showed however that on some potential target systems the exploit code would hang, implying that had the scans included an exploit attempt we should have seen longer durations.

The conclusion reached, based on the information available, was that the incident had been a scan for reconnaissance purposes or preparatory to an attack, rather than an actual attack. Given that the source was blocked, and no vulnerable systems had been identified that might be subject to insider exploit, no additional action was considered to be required in connection with the incident per se.

6. Eradication

As there was no evidence of intrusion, there was nothing to eradicate.

7. Recovery

As there were no adverse effects associated with this incident, recovery was unnecessary. Technically, of course full recovery would have required complete restoration of the original state of perimeter defenses, which would have included removal of additional access controls put in place vis a vis the source, however these were left in place for some time as a precaution.

8. Follow Up or Lessons Learned

Major lessons learned were:

Better procedures and taskings may be needed with respect to incident handling.

Some system administrators need better instructions regarding handling of audit logs, to ensure their retention for potential use by incident handlers.

Some legacy applications continue to require virtual terminal access, however telnet should be replaced by less vulnerable services such as SSH.

Some sites need additional access controls and logging of access to potentially vulnerable services/servers, e.g. via TCP wrappers.

9. Assessment and Containment Process – UNIX (tools used)

The UNIX commands cat and more were used to view the syslog configuration file /etc/syslog.conf and the log files it specified.

The UNIX grep command was used to search log files for entries matching specified patters, such as a source or destination IP address.

Firewall and IDS logs were viewed and searched using proprietary vendor software.

10. Backup and Restoration Process – UNIX

Systems are routinely backed up/recovered using dump/restore facilities. Because no

compromises were identified, no additional backup/recovery was performed. Had an intrusion occurred, an early step would of course have been a disk to disk (dd) copy of appropriate files to tape. Also a vulnerability scan using a commercial assessment package would have been performed prior to recommending return to service of a compromised system.

11. Chain of Custody Procedures, Affirmations and Evidence Listing

Had it been necessary, backups, copies of notes and other evidence would have been signed off on/witnessed at critical points. Because no compromises were identified, no such steps were taken.

Jeffrey Roth
14 September 2000