Audit Report

brotherPrinter

Audited on January 22, 2024

Reported on January 22, 2024

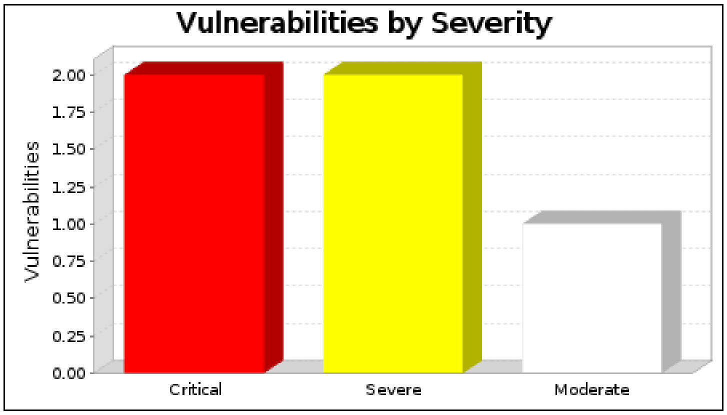
1. Executive Summary

This report represents a security audit performed by InsightVM from Rapid7 LLC. It contains confidential information about the state of your network. Access to this information by unauthorized personnel may allow them to compromise your network.

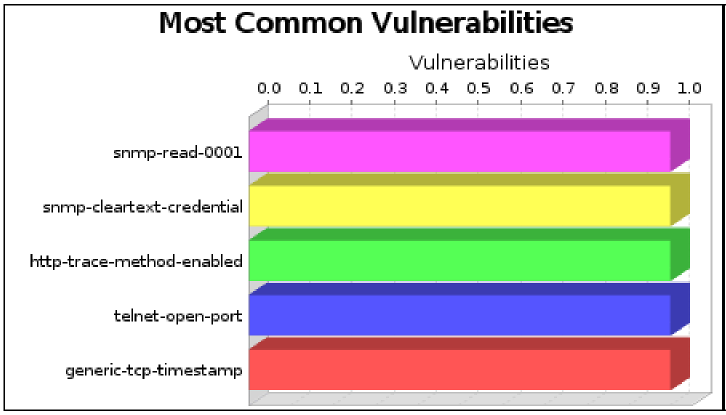
Site Name	Start Time	End Time	Total Time	Status
brotherPrinter	January 22, 2024 16:30, EST	January 22, 2024 16:44, EST	13 minutes	Success

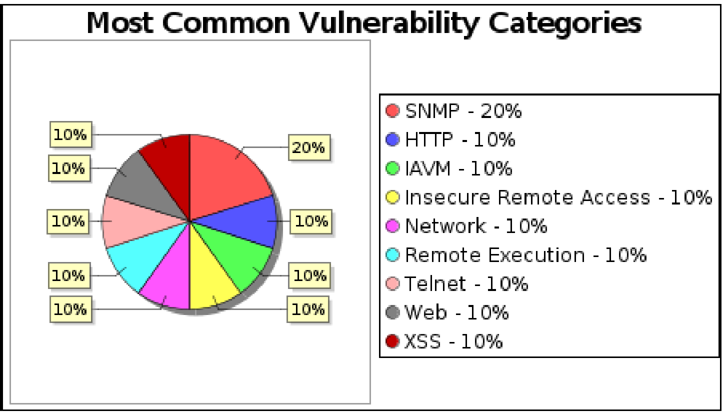
There is not enough historical data to display risk trend.

The audit was performed on one system which was found to be active and was scanned.

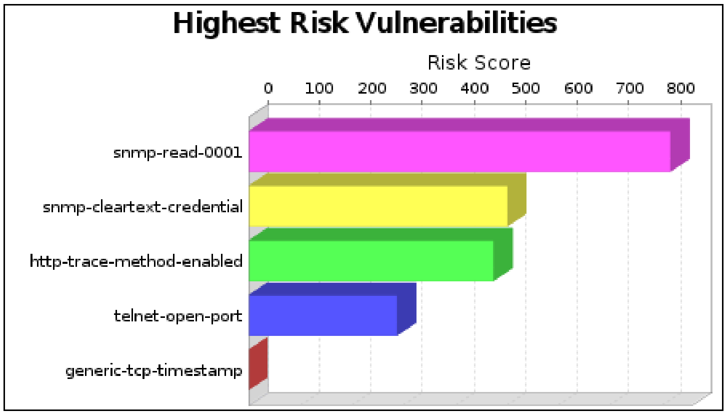


There were 5 vulnerabilities found during this scan. Of these, 2 were critical vulnerabilities. Critical vulnerabilities require immediate attention. They are relatively easy for attackers to exploit and may provide them with full control of the affected systems. 2 vulnerabilities were severe. Severe vulnerabilities are often harder to exploit and may not provide the same access to affected systems. There was one moderate vulnerability discovered. These often provide information to attackers that may assist them in mounting subsequent attacks on your network. These should also be fixed in a timely manner, but are not as urgent as the other vulnerabilities.





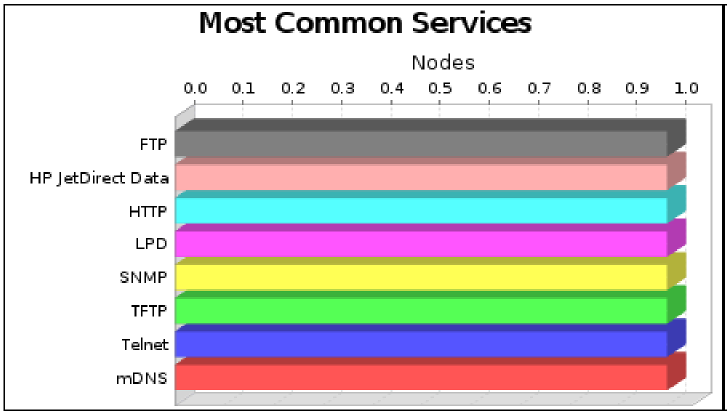
There were 1 occurrences of the snmp-read-0001, snmp-cleartext-credential, http-trace-method-enabled, telnet-open-port and generic-tcp-timestamp vulnerabilities, making them the most common vulnerabilities. There were 2 vulnerability instances in the SNMP category, making it the most common vulnerability category.

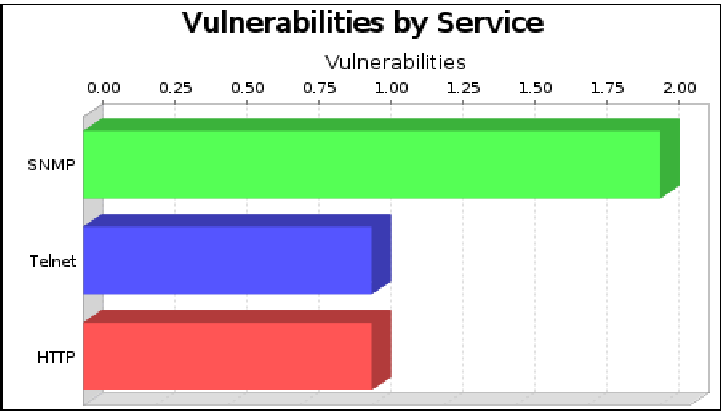


The snmp-read-0001 vulnerability poses the highest risk to the organization with a risk score of 818. Risk scores are based on the types and numbers of vulnerabilities on affected assets.

One operating system was identified during this scan.

There were 8 services found to be running during this scan.





The FTP, HP JetDirect Data, HTTP, LPD, SNMP, TFTP, Telnet and mDNS services were found on 1 systems, making them the most common services. The SNMP service was found to have the most vulnerabilities during this scan with 2 vulnerabilities.

2. Discovered Systems

Node	Operating System	Risk	Aliases
192.168.0.48	Brother HL-1210W series:84U-E07:Ver.1.05	2,083	•BRNC038961223DC •BRWC038961223DC

3. Discovered and Potential Vulnerabilities

3.1. Critical Vulnerabilities

3.1.1. Default or Guessable SNMP community names: public (snmp-read-0001)

Description:

The Simple Network Management Protocol (SNMP) is a commonly used network service. Its primary function is to provide network administrators with information about all kinds of network connected devices. SNMP can be used to get and change system settings on a wide variety of devices, from network servers, to routers and printers. The drawback to this service is the authentication is an unencrypted "community string". In addition many SNMP servers provide very simple default community strings. The community string "public" is a default on a number of SNMP servers.

This community string can allow attackers to gain a large amount of information about the SNMP server and the network it monitors. Attackers may even reconfigure or shut down devices remotely.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.48:161	Running SNMP serviceSuccessfully authenticated to the SNMP service with credentials: uid[] pw[public] realm[]

References:

Source	Reference
BID	2896
BID	3795
BID	3797
CVE	CVE-1999-0186
CVE	CVE-1999-0254
CVE	CVE-1999-0472
CVE	CVE-1999-0516
CVE	CVE-1999-0517
CVE	CVE-2001-0514
CVE	CVE-2002-0109
CVE	CVE-2010-1574
XF	6576

Source	Reference
XF	7827

Vulnerability Solution:

•Secure the SNMP installation

1. If you do not absolutely need SNMP, disable it. SNMP versions 1 and 2c are inherently insecure. SNMP version 3 provides more complex authentication and encryption.
2. If you must use SNMP be sure to use complex and difficult to guess community names. Use the same policy for community names as you use for passwords.
3. Try to make all your MIB's read only. This will limit the damage an attacker can do to your network.

•Secure the SNMP installation on Cisco IOS

1. For SNMP Servers running on Cisco IOS, a Cisco IOS Software upgrade should be performed as a permanent fix for this vulnerability.
2. Alternatively, create an Embedded Event Manager policy to remove the hard-coded SNMP community names using the following steps:
3. event manager applet cisco-sa-20100707-snmp
4. event timer countdown time 30
5. action 10 cli command "enable"
6. action 20 cli command "configure terminal"
7. action 30 cli command "no snmp-server community public RO"
8. action 40 cli command "no snmp-server community private RW"
9. action 50 cli command "end"
10. action 60 cli command "disable"
11. action 70 syslog msg "Hard-coded SNMP community names as per Cisco Security Advisory cisco-sa-20100707-snmp removed"

https://www.cisco.com/c/en/us/support/docs/csa/cisco-sa-20100707-snmp.html

3.1.2. SNMP credentials transmitted in cleartext (snmp-cleartext-credential)

Description:

The Simple Network Management Protocol (SNMP) is a commonly used network service. Its primary function is to provide network administrators with information about all kinds of network connected devices. SNMP can be used to get and change system settings on a wide variety of devices, from network servers, to routers and printers. The drawback to this service is the authentication is an unencrypted "community string". In addition many SNMP servers provide very simple default community strings.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.48:161	Successfully authenticated to the SNMP v1/v2c service.

References:

Source	Reference
CERT	CA-2002-03

Vulnerability Solution:

1. If you do not absolutely need SNMP, disable it. SNMP versions 1 and 2c are inherently insecure. SNMP version 3 provides more complex authentication and encryption.
2. If you must use SNMP be sure to use complex and difficult to guess community names. Use the same policy for community names as you use for passwords.
3. Try to make all your MIB's read only. This will limit the damage an attacker can do to your network.

3.2. Severe Vulnerabilities

3.2.1. HTTP TRACE Method Enabled (http-trace-method-enabled)

Description:

The HTTP TRACE method is normally used to return the full HTTP request back to the requesting client for proxy-debugging purposes. An attacker can create a webpage using XMLHTTP, ActiveX, or XMLDOM to cause a client to issue a TRACE request and capture the client's cookies. This effectively results in a Cross-Site Scripting attack.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.48:631	Running HTTP serviceHTTP TRACE request to http://192.168.0.48:631/ 1: Cookie: vulnerable=yes

References:

Source	Reference
APPLE	APPLE-SA-2009-11-09-1
BID	15222
BID	19915
BID	24456
BID	36956
BID	9506
CERT-VN	867593
CVE	CVE-2004-2320
CVE	CVE-2004-2763

Source	Reference
CVE	CVE-2005-3398
CVE	CVE-2006-4683
CVE	CVE-2007-3008
CVE	CVE-2008-7253
CVE	CVE-2009-2823
CVE	CVE-2010-0386
DISA_SEVERITY	Category II
DISA_VMSKEY	V0011706
IAVM	2005-T-0043
OSVDB	35511
OSVDB	3726
OVAL	1445
URL	http://www.apacheweek.com/issues/03-01-24#news
URL	http://www.kb.cert.org/vuls/id/867593
XF	14959
XF	34854

Vulnerability Solution:

•Apache HTTPD, Apache Tomcat

Disable HTTP TRACE Method for Apache

Newer versions of Apache (1.3.34 and 2.0.55 and later) provide a configuration directive called TraceEnable. To deny TRACE requests, add the following line to the server configuration:

TraceEnable off

For older versions of the Apache webserver, use the mod_rewrite module to deny the TRACE requests:

RewriteEngine On

RewriteCond %{REQUEST_METHOD} ^TRACE

RewriteRule .* - [F]

In Apache Tomcat, the HTTP Trace can be disabled by adding security constraints into the Java Servlet specification within the web.xml configuration file and by setting the attribute allowTrace="False" to the HTTP connector in server.xml. For Spring Boot embedded Tomcat configuration, please refer here

•IIS, PWS, Microsoft-IIS, Internet Information Services, Internet Information Services, Microsoft-PWS

Disable HTTP TRACE Method for Microsoft IIS

For Microsoft Internet Information Services (IIS), you may use the URLScan tool, freely available at http://www.microsoft.com/technet/security/tools/urlscan.mspx

•Java System Web Server, SunONE WebServer, Sun-ONE-Web-Server, iPlanet

Disable HTTP TRACE Method for SunONE/iPlanet

- For Sun ONE/iPlanet Web Server v6.0 SP2 and later, add the following configuration to the top of the default object in the 'obj.conf' file:

```
<Client method="TRACE">
  AuthTrans fn="set-variable"
     remove-headers="transfer-encoding"
     set-headers="content-length: -1"
     error="501"
</Client>
```

  You must then restart the server for the changes to take effect.
- For Sun ONE/iPlanet Web Server prior to v6.0 SP2, follow the instructions provided the 'Relief/Workaround' section of Sun's official advisory: http://sunsolve.sun.com/pub-cgi/retrieve.pl?doc=fsalert%2F50603

- Lotus Domino

  Disable HTTP TRACE Method for Domino

  Follow IBM's instructions for disabling HTTP methods on the Domino server by adding the following line to the server's NOTES.INI file:
  HTTPDisableMethods=TRACE
  After saving NOTES.INI, restart the Notes web server by issuing the console command "tell http restart".

3.2.2. Unencrypted Telnet Service Available (telnet-open-port)

Description:

Telnet is an unencrypted protocol, as such it sends sensitive data (usernames, passwords) in clear text.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.48:23	Running Telnet service

References:

Source	Reference
URL	https://www.pcisecuritystandards.org/documents/PCI_DSS_v3.pdf

Vulnerability Solution:

Disable the telnet service. Replace it with technologies such as SSH, VPN, or TLS.

3.3. Moderate Vulnerabilities

3.3.1. TCP timestamp response (generic-tcp-timestamp)

Description:

The remote host responded with a TCP timestamp. The TCP timestamp response can be used to approximate the remote host's uptime, potentially aiding in further attacks. Additionally, some operating systems can be fingerprinted based on the behavior of their TCP timestamps.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.0.48	Able to determine system boot time.

References:

Source	Reference
URL	http://uptime.netcraft.com
URL	http://www.forensicswiki.org/wiki/TCP_timestamps
URL	http://www.ietf.org/rfc/rfc1323.txt

Vulnerability Solution:

•Cisco

Disable TCP timestamp responses on Cisco

Run the following command to disable TCP timestamps:

```
no ip tcp timestamp
```

•FreeBSD

Disable TCP timestamp responses on FreeBSD

Set the value of net.inet.tcp.rfc1323 to 0 by running the following command:

```
sysctl -w net.inet.tcp.rfc1323=0
```

Additionally, put the following value in the default sysctl configuration file, generally sysctl.conf:

```
net.inet.tcp.rfc1323=0
```

•Linux

Disable TCP timestamp responses on Linux

Set the value of net.ipv4.tcp_timestamps to 0 by running the following command:

```
sysctl -w net.ipv4.tcp_timestamps=0
```

Additionally, put the following value in the default sysctl configuration file, generally sysctl.conf:

```
net.ipv4.tcp_timestamps=0
```

- OpenBSD
  Disable TCP timestamp responses on OpenBSD
  Set the value of net.inet.tcp.rfc1323 to 0 by running the following command:

```
sysctl -w net.inet.tcp.rfc1323=0
```

Additionally, put the following value in the default sysctl configuration file, generally sysctl.conf:

```
net.inet.tcp.rfc1323=0
```

- Microsoft Windows NT, Microsoft Windows NT Workstation, Microsoft Windows NT Server, Microsoft Windows NT Advanced Server, Microsoft Windows NT Server, Enterprise Edition, Microsoft Windows NT Server, Terminal Server Edition, Microsoft Windows 95, Microsoft Windows 98, Microsoft Windows 98SE, Microsoft Windows ME, Microsoft Windows 2000, Microsoft Windows 2000 Professional, Microsoft Windows 2000 Server, Microsoft Windows 2000 Advanced Server, Microsoft Windows 2000 Datacenter Server, Microsoft Windows XP, Microsoft Windows XP Home, Microsoft Windows XP Professional, Microsoft Windows XP Tablet PC Edition, Microsoft Windows CE, Microsoft Windows Server 2003, Microsoft Windows Server 2003, Standard Edition, Microsoft Windows Server 2003, Enterprise Edition, Microsoft Windows Server 2003, Datacenter Edition, Microsoft Windows Server 2003, Web Edition, Microsoft Windows Small Business Server 2003, Microsoft Windows Server 2003 R2, Microsoft Windows Server 2003 R2, Standard Edition, Microsoft Windows Server 2003 R2, Enterprise Edition, Microsoft Windows Server 2003 R2, Datacenter Edition, Microsoft Windows Server 2003 R2, Web Edition, Microsoft Windows Small Business Server 2003 R2, Microsoft Windows Server 2003 R2, Express Edition, Microsoft Windows Server 2003 R2, Workgroup Edition
  Disable TCP timestamp responses on Windows versions before Vista
  Set the Tcp1323Opts value in the following key to 1:

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters
```

- Microsoft Windows Server 2008, Microsoft Windows Server 2008 Standard Edition, Microsoft Windows Server 2008 Enterprise Edition, Microsoft Windows Server 2008 Datacenter Edition, Microsoft Windows Server 2008 HPC Edition, Microsoft Windows Server 2008 Web Edition, Microsoft Windows Server 2008 Storage Edition, Microsoft Windows Small Business Server 2008, Microsoft Windows Essential Business Server 2008, Microsoft Windows Server 2008 R2, Microsoft Windows Server 2008 R2, Standard Edition, Microsoft Windows Server 2008 R2, Enterprise Edition, Microsoft Windows Server 2008 R2, Datacenter Edition, Microsoft Windows Server 2008 R2, Web Edition, Microsoft Windows Server 2012, Microsoft Windows Server 2012 Standard Edition, Microsoft Windows Server 2012 Foundation Edition, Microsoft Windows Server 2012 Essentials Edition, Microsoft Windows Server 2012 Datacenter Edition, Microsoft

Windows Storage Server 2012, Microsoft Windows Vista, Microsoft Windows Vista Home, Basic Edition, Microsoft Windows Vista Home, Basic N Edition, Microsoft Windows Vista Home, Premium Edition, Microsoft Windows Vista Ultimate Edition, Microsoft Windows Vista Enterprise Edition, Microsoft Windows Vista Business Edition, Microsoft Windows Vista Business N Edition, Microsoft Windows Vista Starter Edition, Microsoft Windows 7, Microsoft Windows 7 Home, Basic Edition, Microsoft Windows 7 Home, Basic N Edition, Microsoft Windows 7 Home, Premium Edition, Microsoft Windows 7 Home, Premium N Edition, Microsoft Windows 7 Ultimate Edition, Microsoft Windows 7 Ultimate N Edition, Microsoft Windows 7 Enterprise Edition, Microsoft Windows 7 Enterprise N Edition, Microsoft Windows 7 Professional Edition, Microsoft Windows 7 Starter Edition, Microsoft Windows 7 Starter N Edition, Microsoft Windows 8, Microsoft Windows 8 Enterprise Edition, Microsoft Windows 8 Professional Edition, Microsoft Windows 8 RT, Microsoft Windows Longhorn Server Beta

Disable TCP timestamp responses on Windows versions since Vista

TCP timestamps cannot be reliably disabled on this OS. If TCP timestamps present enough of a risk, put a firewall capable of blocking TCP timestamp packets in front of the affected assets.

4. Discovered Services

4.1. FTP

FTP, the File Transfer Protocol, is used to transfer files between systems. On the Internet, it is often used on web pages to download files from a web site using a browser. FTP uses two connections, one for control connections used to authenticate, navigate the FTP server and initiate file transfers. The other connection is used to transfer data, such as files or directory listings.

4.1.1. General Security Issues

Cleartext authentication

The original FTP specification only provided means for authentication with cleartext user ids and passwords. Though FTP has added support for more secure mechanisms such as Kerberos, cleartext authentication is still the primary mechanism. If a malicious user is in a position to monitor FTP traffic, user ids and passwords can be stolen.

4.1.2. Discovered Instances of this Service

Device	Protocol	Port	Vulnerabilities	Additional Information
192.168.0.48	tcp	21	0	•ftp.banner: 220 FTP print service:V-1.13/Use the network password for the ID if updating. •ftp.plaintext.authentication: false

4.2. HP JetDirect Data

4.2.1. Discovered Instances of this Service

Device	Protocol	Port	Vulnerabilities	Additional Information
192.168.0.48	tcp	9100	0	•hp.pjl.id: Brother HL-1210W series:84U-E07:Ver.1.05

4.3. HTTP

HTTP, the HyperText Transfer Protocol, is used to exchange multimedia content on the World Wide Web. The multimedia files commonly used with HTTP include text, sound, images and video.

4.3.1. General Security Issues

Simple authentication scheme

Many HTTP servers use BASIC as their primary mechanism for user authentication. This is a very simple scheme that uses base 64 to encode the cleartext user id and password. If a malicious user is in a position to monitor HTTP traffic, user ids and passwords can be stolen by decoding the base 64 authentication data. To secure the authentication process, use HTTPS (HTTP over TLS/SSL) connections to transmit the authentication data.

4.3.2. Discovered Instances of this Service

Device	Protocol	Port	Vulnerabilities	Additional Information
192.168.0.48	tcp	80	0	•debut 1.20 •http.banner: debut/1.20 •http.banner.server: debut/1.20
192.168.0.48	tcp	631	1	•debut 1.20 •http.banner: debut/1.20 •http.banner.server: debut/1.20 •verbs-1: GET •verbs-2: HEAD •verbs-3: POST •verbs-4: TRACE •verbs-count: 4

4.4. LPD

The Line Printer Daemon Protocol (LPD), specifies a method by which clients can send documents to a printer or print daemon over TCP/IP.

4.4.1. Discovered Instances of this Service

Device	Protocol	Port	Vulnerabilities	Additional Information
192.168.0.48	tcp	515	0	

4.5. SNMP

Simple Network Management Protocol (SNMP), like the name implies, is a simple protocol used to manage networking appliances by remote clients. It is primarily UDP-based and uses trivial authentication by means of a secret community name.

4.5.1. Discovered Instances of this Service

Device	Protocol	Port	Vulnerabilities	Additional Information
192.168.0.48	udp	161	2	•assignedNumber: 2435 •snmp.banner: Brother NC-8400w, Firmware Ver.B ,MID 84U-E07 •snmp.name: BRWC038961223DC •snmp.sysObjectID: 1.3.6.1.4.1.2435.2.3.9.1 •snmp.uptime: 1 day, 23:54:54.70 •snmp.version: v1/v2c •sysDescr: Brother NC-8400w, Firmware Ver.B ,MID 84U-E07

4.6. TFTP

TFTP, or Trivial File Transfer Protocol, is a simplified version of FTP. It is designed to work over UDP, and supports only file reading and file writing, but not directory listing. No authentication mechanism exists.

4.6.1. Discovered Instances of this Service

Device	Protocol	Port	Vulnerabilities	Additional Information
192.168.0.48	udp	69	0	

4.7. Telnet

The telnet service provides console access to a machine remotely. All data, including usernames and passwords, is sent in cleartext over TCP. In recent times, most networks have phased out its use in favor for the SSH, or Secure SHell, protocol, which primarily provides strong encryption and superior authentication mechanisms.

4.7.1. General Security Issues

No Support For Encryption

The number one vulnerability that the telnet service faces is its inherent lack of support for encryption. This is an artifact from the time period in which it was invented, 1971. There existed little knowledge of cryptography outside of military environments, and computer technology was not yet advanced enough to handle its real-time use. SSH should be used instead of telnet.

System Architecture Information Leakage

Most telnet servers will broadcast a banner which details the exact system type (ie: hardware and operating system versions) to any connecting client, without requiring authentication. This information is crucial for carrying out serious attacks on the system.

4.7.2. Discovered Instances of this Service

Device	Protocol	Port	Vulnerabilities	Additional Information
192.168.0.48	tcp	23	1	

4.8. mDNS

4.8.1. Discovered Instances of this Service

Device	Protocol	Port	Vulnerabilities	Additional Information
192.168.0.48	udp	5353	0	•dns-sd-1: _printer._tcp.local. •dns-sd-2: _ipp._tcp.local. •dns-sd-3: _http._tcp.local. •dns-sd-4: _pdl-datastream._tcp.local. •dns-sd-count: 4

5. Discovered Users and Groups

No user or group information was discovered during the scan.

6. Discovered Databases

No database information was discovered during the scan.

7. Discovered Files and Directories

No file or directory information was discovered during the scan.

8. Policy Evaluations

No policy evaluations were performed.

9. Spidered Web Sites

No web sites were spidered during the scan.