Audit Report

Armin Chanchian

Audited on March 21, 2024

Reported on March 21, 2024

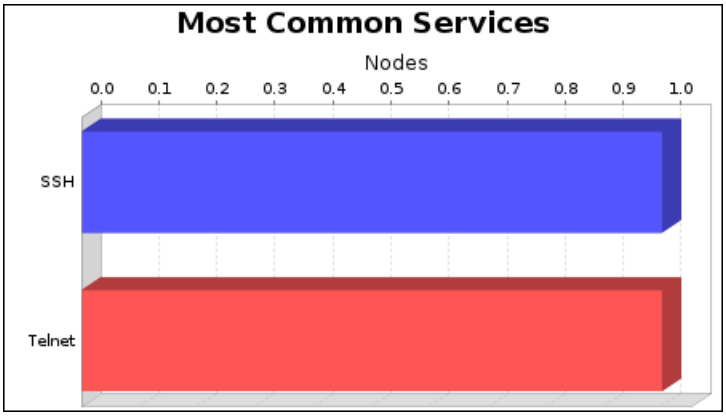
1. Executive Summary

This report represents a security audit performed by Nexpose 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
Metasploitable	March 21, 2024 13:35, EET	March 21, 2024 13:37, EET	2 minutes	Success

There is not enough historical data to display overall asset trend.

The audit was performed on one system which was found to be active and was scanned. No vulnerabilities were found during this scan.
One operating system was identified during this scan.
There were 2 services found to be running during this scan.



The SSH and Telnet services were found on 1 systems, making them the most common services.

2. Discovered Systems

Node	Operating System	Risk	Aliases
10.224.2.196	Ubuntu Linux 8.04	0.0	•metasploitable

3. Discovered and Potential Vulnerabilities

4. Discovered Services

4.1. SSH

SSH, or Secure SHell, is designed to be a replacement for the aging Telnet protocol. It primarily adds encryption and data integrity to Telnet, but can also provide superior authentication mechanisms such as public key authentication.

4.1.1. Discovered Instances of this Service

Device	Protocol	Port	Vulnerabilities	Additional Information
10.224.2.196	tcp	22	0	•OpenBSD OpenSSH 4.7p1 •ssh.algorithms.compression: none,zlib@openssh.com •ssh.algorithms.encryption: aes128-cbc,3des-cbc,blowfish-cbc,cast128-cbc,arcfour128,arcfour256,arcfour,aes192-cbc,aes256-cbc,rijndael-cbc@lysator.liu.se,aes128-ctr,aes192-ctr,aes256-ctr •ssh.algorithms.hostkey: ssh-rsa,ssh-dss •ssh.algorithms.kex: diffie-hellman-group-exchange-sha256,diffie-hellman-group-exchange-sha1,diffie-hellman-group14-sha1,diffie-hellman-group1-sha1 •ssh.algorithms.mac: hmac-md5,hmac-sha1,umac-64@openssh.com,hmac-ripemd160,hmac-ripemd160@openssh.com,hmac-sha1-96,hmac-md5-96 •ssh.banner: SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1 •ssh.hostkey.dsa.bits: 1024 •ssh.hostkey.dsa.fingerprint: 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd •ssh.hostkey.rsa.bits: 2048 •ssh.hostkey.rsa.fingerprint: 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3

Device	Protocol	Port	Vulnerabilities	Additional Information
				•ssh.hostkey.type: DSA,RSA •ssh.protocol.version: 2.0

4.2. 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.

4.2.1. 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.

4.2.2. Discovered Instances of this Service

Device	Protocol	Port	Vulnerabilities	Additional Information
10.224.2.196	tcp	23	0	•telnet.banner: _ _ _ _ _ _ _ _____ _ _ __ ____ ____| |_ __ _ ____ _ __ | | ___ (_) |_ __ _| |__ | | ____|____ \ | '_ ` _ \ / _ \ __/ _` / __| '_ \ |/ _ \ | | __/ _` | '_ \ |/ _ \ __) | | | | | __/ || (_| __ \ |_) | | (_) | | || (_| | |_) | | __// __/ |_| |_| |_|____|__|__,_|____/ .__/|_|____/|_|__|__,_|_.__/|_|____|____ __| |_| Warning: Never expose this VM to an untrusted network! Contact: msfdev[at]metasploit.com Login with msfadmin/msfadmin to get started metasploitable login:

5. Discovered Users and Groups

5.1. System

5.1.1. 10.224.2.196

Account Name	Type	Additional Information
adm	Group	•group-id: 4
admin	Group	•group-id: 112
audio	Group	•group-id: 29
backup	User	•gid: 34 •loginShell: /bin/sh •password: x •user-id: 34 •userDir: /var/backups
bin	User	•gid: 2 •loginShell: /bin/sh •password: x •user-id: 2 •userDir: /bin
bind	User	•gid: 113 •loginShell: /bin/false •password: x •user-id: 105 •userDir: /var/cache/bind
cdrom	Group	•group-id: 24
crontab	Group	•group-id: 108
daemon	Group	•group-id: 1
dhcp	User	•gid: 102 •loginShell: /bin/false •password: x •user-id: 101 •userDir: /nonexistent
dialout	Group	•group-id: 20
dip	Group	•group-id: 30

Account Name	Type	Additional Information
disk	Group	•group-id: 6
distccd	User	•gid: 65534 •loginShell: /bin/false •password: x •user-id: 111 •userDir: /
fax	Group	•group-id: 21
floppy	Group	•group-id: 25
ftp	User	•gid: 65534 •loginShell: /bin/false •password: x •user-id: 107 •userDir: /home/ftp
fuse	Group	•group-id: 107
games	Group	•group-id: 60
gnats	User	•full-name: Gnats Bug-Reporting System (admin) •gid: 41 •loginShell: /bin/sh •password: x •user-id: 41 •userDir: /var/lib/gnats
irc	User	•full-name: ircd •gid: 39 •loginShell: /bin/sh •password: x •user-id: 39 •userDir: /var/run/ircd
klog	User	•gid: 104 •loginShell: /bin/false •password: x •user-id: 103 •userDir: /home/klog
kmem	Group	•group-id: 15
libuuid	User	•gid: 101 •loginShell: /bin/sh •password: x

Account Name	Type	Additional Information
		•user-id: 100 •userDir: /var/lib/libuuid
list	Group	•group-id: 38
lp	User	•gid: 7 •loginShell: /bin/sh •password: x •user-id: 7 •userDir: /var/spool/lpd
lpadmin	Group	•group-id: 111
mail	Group	•group-id: 8
man	Group	•group-id: 12
mlocate	Group	•group-id: 109
msfadmin	Group	•group-id: 1000
mysql	User	•full-name: MySQL Server,,, •gid: 118 •loginShell: /bin/false •password: x •user-id: 109 •userDir: /var/lib/mysql
news	Group	•group-id: 9
nobody	User	•gid: 65534 •loginShell: /bin/sh •password: x •user-id: 65534 •userDir: /nonexistent
nogroup	Group	•group-id: 65534
nvram	Group	•group-id: 106
operator	Group	•group-id: 37
plugdev	Group	•group-id: 46
postdrop	Group	•group-id: 116
postfix	Group	•group-id: 115
postgres	User	•full-name: PostgreSQL administrator,,, •gid: 117

Account Name	Type	Additional Information
		•loginShell: /bin/bash •password: x •user-id: 108 •userDir: /var/lib/postgresql
proftpd	User	•gid: 65534 •loginShell: /bin/false •password: x •user-id: 113 •userDir: /var/run/proftpd
proxy	User	•gid: 13 •loginShell: /bin/sh •password: x •user-id: 13 •userDir: /bin
root	Group	
sambashare	Group	•group-id: 119
sasl	Group	•group-id: 45
scanner	Group	•group-id: 105
service	Group	•group-id: 1002
shadow	Group	•group-id: 42
src	Group	•group-id: 40
ssh	Group	•group-id: 110
sshd	User	•gid: 65534 •loginShell: /usr/sbin/nologin •password: x •user-id: 104 •userDir: /var/run/sshd
ssl-cert	Group	•group-id: 114
staff	Group	•group-id: 50
statd	User	•gid: 65534 •loginShell: /bin/false •password: x •user-id: 114 •userDir: /var/lib/nfs

Account Name	Type	Additional Information
sudo	Group	•group-id: 27
sync	User	•gid: 65534 •loginShell: /bin/sync •password: x •user-id: 4 •userDir: /bin
sys	User	•gid: 3 •loginShell: /bin/sh •password: x •user-id: 3 •userDir: /dev
syslog	Group	•group-id: 103
tape	Group	•group-id: 26
telnetd	User	•gid: 120 •loginShell: /bin/false •password: x •user-id: 112 •userDir: /nonexistent
tomcat55	User	•gid: 65534 •loginShell: /bin/false •password: x •user-id: 110 •userDir: /usr/share/tomcat5.5
tty	Group	•group-id: 5
user	User	•full-name: just a user,111,, •gid: 1001 •loginShell: /bin/bash •password: x •user-id: 1001 •userDir: /home/user
users	Group	•group-id: 100
utmp	Group	•group-id: 43
uucp	Group	•group-id: 10
video	Group	•group-id: 44
voice	Group	•group-id: 22

Account Name	Type	Additional Information
www-data	User	•gid: 33 •loginShell: /bin/sh •password: x •user-id: 33 •userDir: /var/www

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.