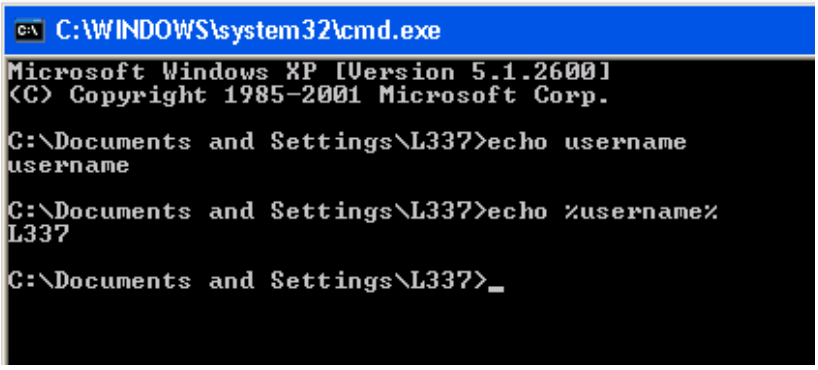
Turn In

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

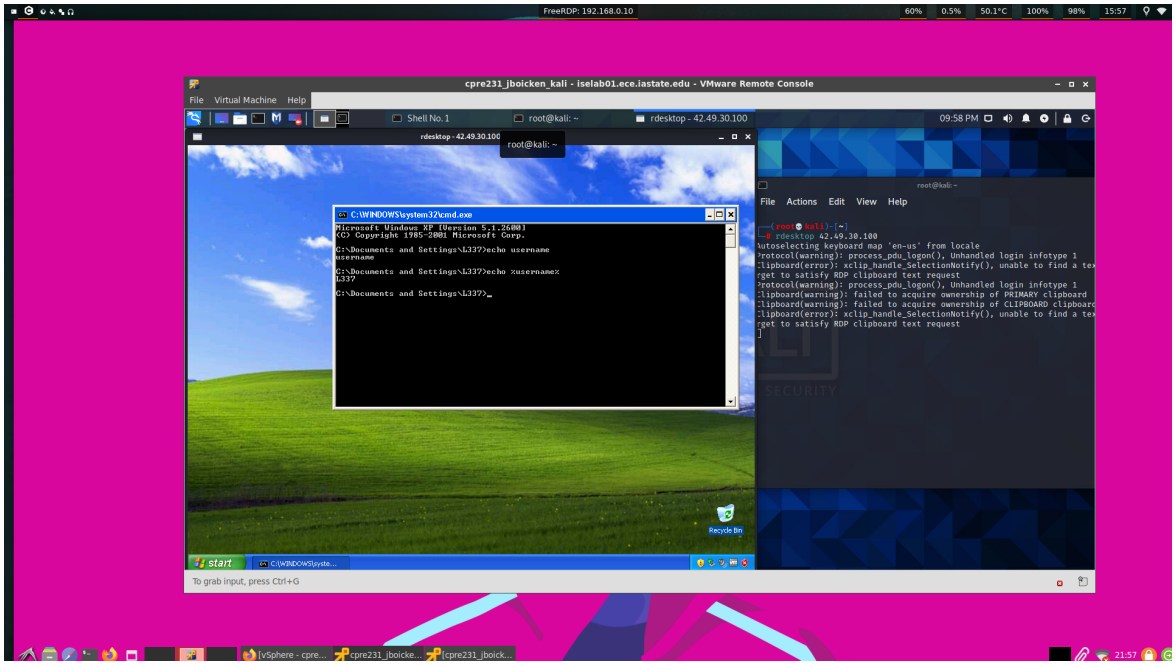
QUEUE	TOTAL	CLASS	ACTIVITY	LAST EVENT	SOURCE	AGE	COUNTRY	DESTINATION	AGE	COUNTRY
0	7			2021-02-23 15:49:05	73.19.46.2	7	UNITED STATES (.us)	15.218.53.108	6	UNITED STATES (.us)

ST	TIMESTAMP	EVENT ID	SOURCE	PORT	DESTINATION	PORT	SIGNATURE
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
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
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
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



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
```

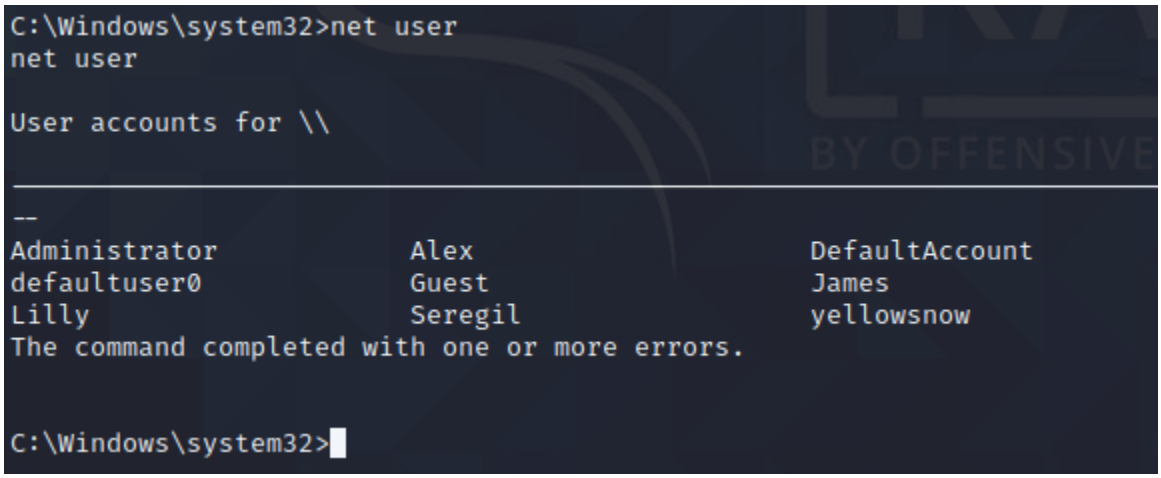
   I used vi to view the contents of the /etc/passwd.

   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 0xffffff00 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)



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