NYU TANDON SCHOOL OF ENGINEERING

NYU Cyber Fellows
CS GY 6573
Penetration Testing

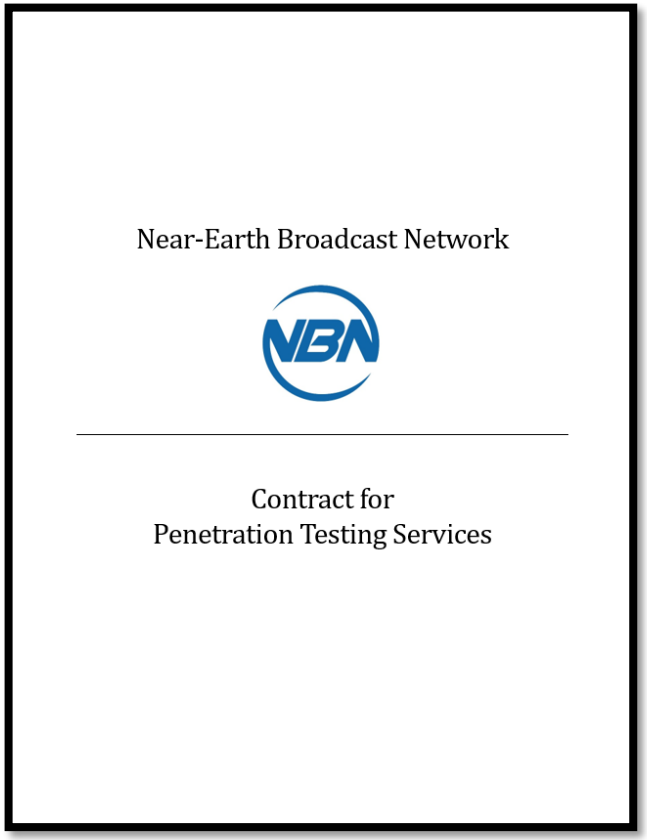
Final Project

Agenda

- **Setup**
- **Troubleshooting and Tips**

Pen Test Contract

- **Before moving forward, review the PenTest-Contract.pdf**
  - Separate attachment
  - Talks about test scope, deliverables, and how it will be graded


Near-Earth Broadcast Network

NBN

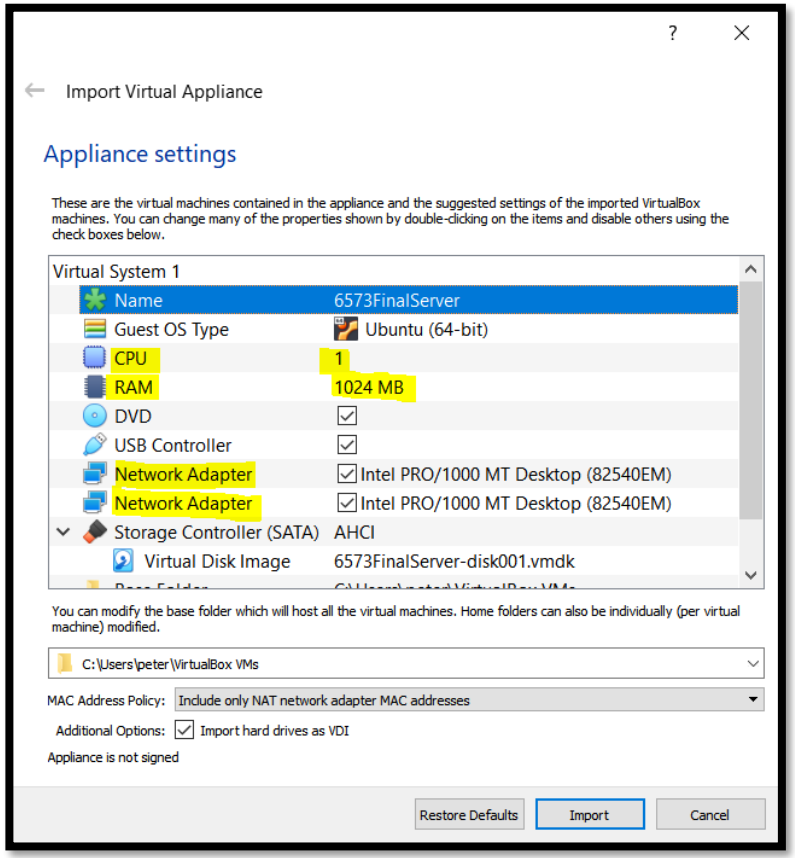
Contract for
Penetration Testing Services

NYU TANDON SCHOOL OF ENGINEERING

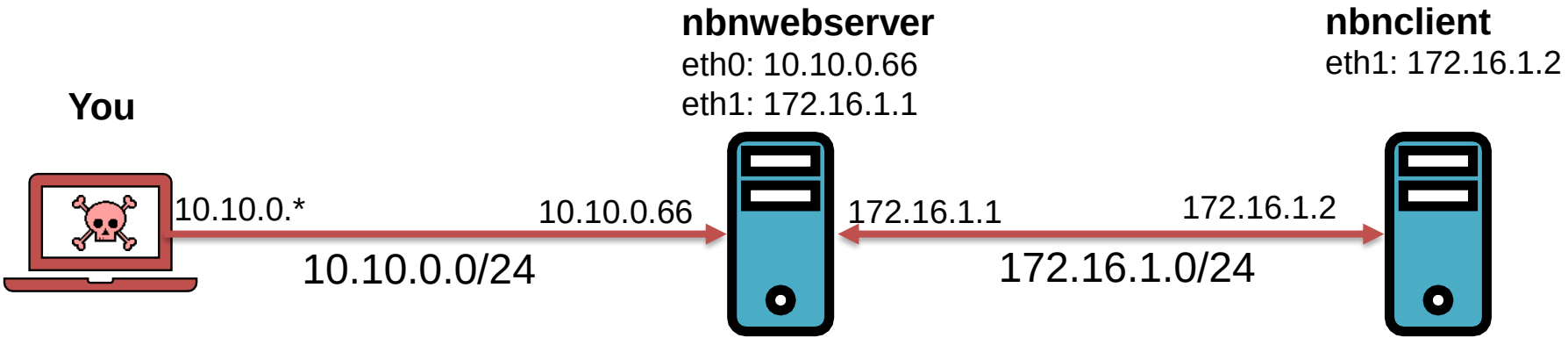
Setup

Deploy OVA

- **Download and add OVAs**
  - VMs networks are set to auto configure
    - /etc/rc.local and /var/networking.sh takes care of this
- **VM Setup**
  - Most settings should be automatic
  - Review highlighted areas on right --->
    - 1 GB ram, 1 processor per VM
    - 2 network cards on the server, only 1 on the client
- **Networking Setup, suggestion**
  - Set all interfaces to 'Host only' or 'Internal'
    - Same as Kali
- **After setup**
  - Make sure you can ping Webserver AND Client
    - From either your host or Kali VM
    - If not, double check your Host-Only Network settings
    - Make sure your routing table is correct



Network



- **You will need to create a static route to the 172.16.1.0/24 network**
  - Create the route and ping the other interface to test
    - `$ sudo ip route add 172.16.1.0/24 via 10.10.0.66`
    - On OS X - **sudo route add 172.16.1.0/24 10.10.0.66**
    - `$ ping 10.10.0.66`
    - `$ ping 172.16.1.1`
    - `$ ping 172.16.1.2`

- **You should be able to ping all interfaces of all machines**
  - eth0/eth1 may have different names after being deployed, such as enp0s3/enp0s8

Testing

- **This is what you should see**
  - Server Ping - Works
  - Server Ping – Works
  - Remote Client Pint – Works
  - Remote Client Connection - Fail

```
┌──(kali㉿kali)-[~/Desktop/share/nbn]
└─$ sudo ip route add 172.16.1.0/24 via 10.10.0.66

┌──(kali㉿kali)-[~/Desktop/share/nbn]
└─$ ping 10.10.0.66 -c 2
PING 10.10.0.66 (10.10.0.66) 56(84) bytes of data.
64 bytes from 10.10.0.66: icmp_seq=1 ttl=64 time=0.459 ms
64 bytes from 10.10.0.66: icmp_seq=2 ttl=64 time=2.13 ms

--- 10.10.0.66 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1026ms
rtt min/avg/max/mdev = 0.459/1.296/2.134/0.837 ms

┌──(kali㉿kali)-[~/Desktop/share/nbn]
└─$ ping 172.16.1.1 -c 2
PING 172.16.1.1 (172.16.1.1) 56(84) bytes of data.
64 bytes from 172.16.1.1: icmp_seq=1 ttl=64 time=0.409 ms
64 bytes from 172.16.1.1: icmp_seq=2 ttl=64 time=1.36 ms

--- 172.16.1.1 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1038ms
rtt min/avg/max/mdev = 0.409/0.883/1.358/0.474 ms

┌──(kali㉿kali)-[~/Desktop/share/nbn]
└─$ ping 172.16.1.2 -c 2
PING 172.16.1.2 (172.16.1.2) 56(84) bytes of data.
64 bytes from 172.16.1.2: icmp_seq=1 ttl=63 time=0.853 ms
64 bytes from 172.16.1.2: icmp_seq=2 ttl=63 time=2.58 ms

--- 172.16.1.2 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1041ms
rtt min/avg/max/mdev = 0.853/1.714/2.575/0.861 ms

┌──(kali㉿kali)-[~/Desktop/share/nbn]
└─$ ncat 172.16.1.2 22 -w 3 -v
Ncat: Version 7.91 ( https://nmap.org/ncat )
Ncat: TIMEOUT.
```

Successful Pings and Routing

- You should be able to ping and have full network access to the webserver
- You should NOT be able to do anything directly to the client besides ping

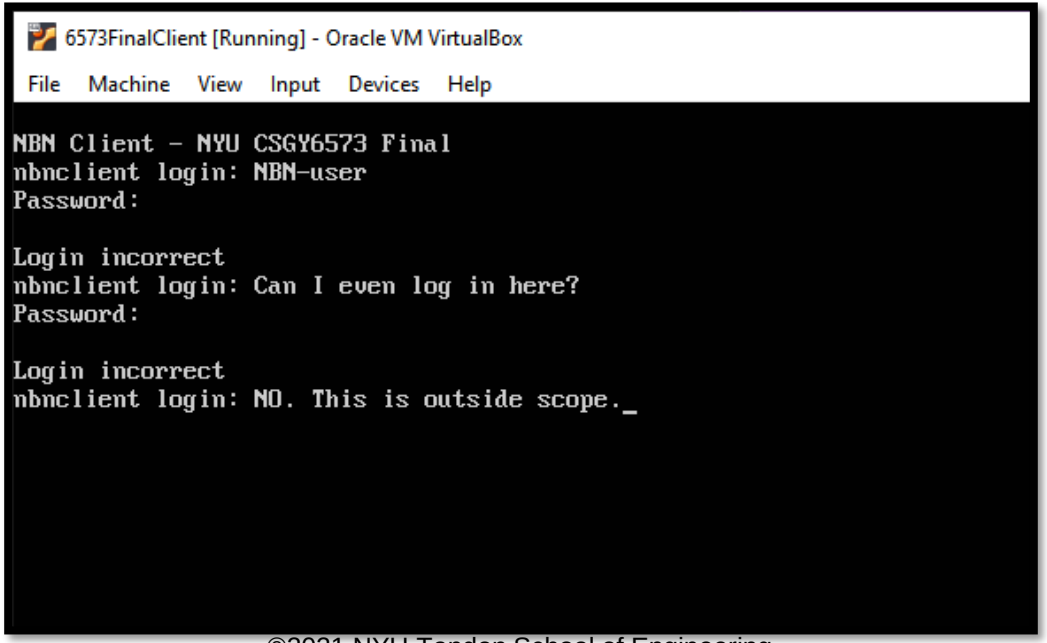
Routing Table

Manual entry

```
┌──(kali㉿kali)-[~/Desktop/share/nbn]
└─$ route
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
default         10.10.0.1       0.0.0.0         UG    100    0        0 eth0
10.10.0.0       0.0.0.0         255.255.255.0   U     100    0        0 eth0
10.10.0.0       0.0.0.0         255.255.255.0   U     100    0        0 eth0
172.16.1.0      10.10.0.66      255.255.255.0   UG    0      0        0 eth0
```

Remember - No Local Access

- Logging in over console (physical access) is disallowed as part of the rules of engagement, even if you have credentials
- Everything must be done over the network



NYU TANDON SCHOOL OF ENGINEERING

Troubleshooting and Tips

Methodology

- **Remember the pen testing methodologies from Lesson 1**
- **Basic**
  - Enumerate Enumerate Enumerate!
  - External-facing Vulnerabilities and Exposures
  - Privilege Escalation
  - Pivot and Repeat
- **Use everything we learned about this semester**

Post Exploit

- **Look for configuration errors, vulnerable services, weird ports, and poor security practices**
  - Same usernames may have same passwords
  - Passwords may be weak and can be cracked using the rockyou wordlist
    - **All passwords came from Rockyou, no mangling rules**
  - Research exploits on exploit-db.com or inside Metasploit
  - Create your own exploits for applications that you find
    - You may upload exploits and run them if you have access
    - Remember, you MAY NOT make changes to the system: configuration, services, iptables, networking, etc.
      - However, if this is possible and could introduce more vulns, it might be worth mentioning the potential impact!

Pivoting

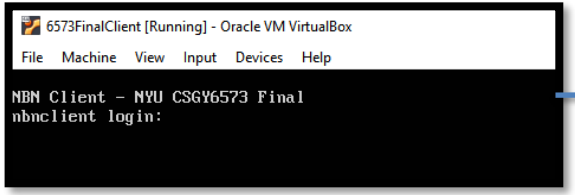
- **The internal client is protected but can communicate with the webserver**
- **Try routing with Proxychains and "ssh -D"**
  - Proxychains cannot send non-standard packets (nmap -sS or scapy)
  - Configure in /etc/proxychains.conf
  - Use with nmap -sT, since this is the full TCP connect
  - Don’t use proxychains4, use proxychains3 (comes with Kali 2021)
    - https://blog.techorganic.com/2012/10/10/introduction-to-pivoting-part-2-proxychains/
    - https://blog.elearnsecurity.com/nessus-and-metasploit-scan-networks-in-pivoting.html
- **You can also try routing with Metasploit**
- **Create Relays to get to addresses and ports that are blocked**

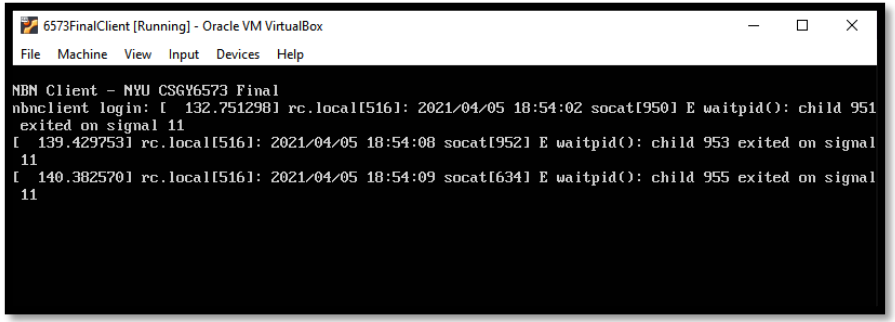
Other Tips

- **If you are fuzzing or exploiting, these can be dangerous!**
  - You can and probably will crash some applications.

- **Fuzzing things over the network may be more successful if you use python sockets instead of piping to netcat**

- **If you do crash something, you should see the error**
- **Not all errors means something is crashed. Ask on Slack if you're not sure**
  - If something did break, just restart the VM
  - Tip: Crashing socat does not mean you crashed the binary that socat is running





Client Buffer Overflow Exploit

- **It is possible to exploit the client from Kali, example using proxy chains:**
  - Top: Setting up listener
  - Bottom: Sending exploit
    - Note successful proxychains connection shows
      - ➢ **`|S-chain|-<>127.0.0.1.[port]…`**

```
kali@kali:~/Desktop/final$ ncat -nlvp 4444
Ncat: Version 7.80 ( https://nmap.org/ncat )
Ncat: Listening on :::4444
Ncat: Listening on 0.0.0.0:4444
Ncat: Connection from 172.16.1.2.
Ncat: Connection from 172.16.1.2:60008.
hostname
nbnclient
```

```
kali@kali:~/Desktop/final$ python exploit_remote.py | proxychains ncat 172.16.1.2
ProxyChains-3.1 (http://proxychains.sf.net)
|S-chain|-<>-127.0.0.1:9050-<><>-172.16.1.2:[redacted]
```

- **Shell keeps closing?**
  - Try using msf-venom option
    - ➢ **`PrependFork=TRUE`**

Have Fun

- **This is meant to be fun and a final chance to practice your skills**

- **Questions are welcome! Get on slack!**
  - Don't get stuck and waste hours on one detail or possible vulnerability
  - **Do** research and reference the topics we learned

- **This is NOT a group project, work alone on your report**
  - Teamwork = cheating

- **Not sure what to do next? Step back and enumerate!**

- **If you do enjoy the pen testing part, please participate in other CTFs, hacking events, or try some on vulnhub.com**

Questions / Comments

- **Root is achievable on all systems**

- **If you have any questions or discover any problems, please ask in slack or office hours**
  - Unless:
    - It is giving away your strategy
    - Sharing how you found a flag
    - Explaining a possible vulnerability
  - Email professor or TA other questions

- **You will must work alone. Any sharing of strategies or teamwork will be considered cheating and penalized with a project grade of 0.**

- **Good luck!**