



NYU

TANDON SCHOOL
OF ENGINEERING

NYU Cyber Fellows CS GY 6573 Penetration Testing

Final Project

©2020 NYU Tandon School of Engineering



- **Story and Mission**
- **Setup - Deploying VMs and Networking Test**
- **Deliverable and Grade**
- **Troubleshooting and Tips**



NYU

TANDON SCHOOL
OF ENGINEERING

Story



- **You have been approached by a company that just suffered a massive breach**

- Their company was accessed from their external facing servers
- Lost customer and employee data

- **They want to secure their systems but are not sure what needs to get done**





The largest media conglomerate in the world is NBN, which at various times in the company's history has stood for Network Broadcast News, Net Broadcast Network, and finally Near-Earth Broadcast Network. Now simply known as NBN, the corporation is headquartered right on Broadcast Square in Los Angeles after relocating from New Manhattan in the early 2020s. NBN also has offices and broadcast equipment along the entire length of the Los Angeles Space Elevator, particularly at Midway Station and the terminal space station known as the Castle.

The market dominance of NBN means that in most markets even non-subscribers must use NBN-owned infrastructure to access the network at all. As a result, a large percentage of data and media in all of human society passes through NBN. Privacy advocates worry that NBN has too much access and control over communications and media, and condemn NBN for its cooperation with repressive Mediterranean regimes. Some worry that NBN is using its wealth of data for purposes more nefarious than advertising, and that there is a reason why no antitrust laws were ever enforced against the corporation by U.S. or world governments.

A Letter from their CISO

Hello,

Thank you for helping following this security incident.

Attached are the server images we need to secure. Although we have stopped and closed out the existing compromise, we have reason to believe that our adversaries are still targeting our external-facing web server. Please review and report back with your methodology, findings, recommendations, priorities, and risk for our servers. Your discretion and attention to detail is appreciated but please also provide any critical data you find on these servers, such as flags or passwords.

I expect the report no later than the evening of Friday May 8th at 2355EST. Credits will be posted the following weekend.

Regards,
Bill Gibson, CISO

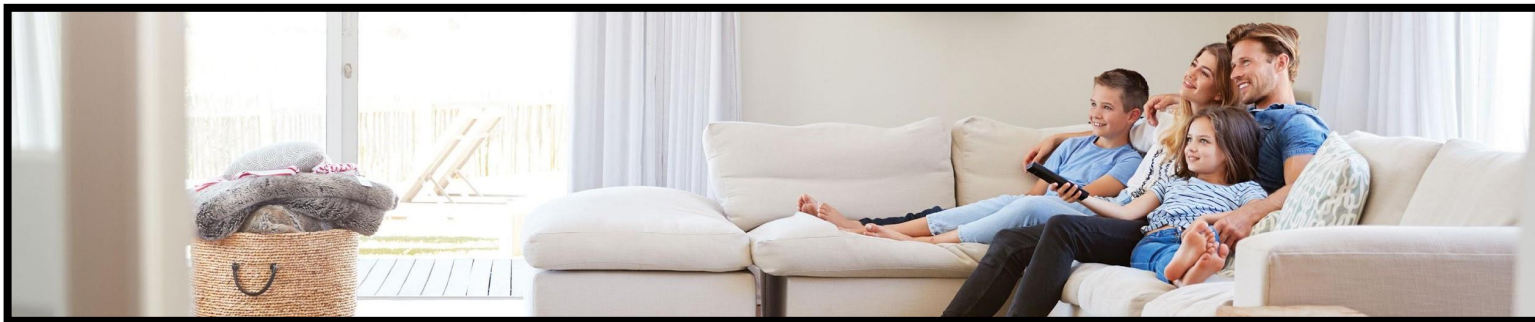
NBN Corp
1800 Archer Street
New York, NY
URL: 10.10.0.66

This email message is for the sole use of the intended recipient(s) and may contain confidential and privileged information. Any unauthorized review, use, disclosure or distribution is prohibited. If you are not the intended recipient, contact the sender by reply email and destroy all copies of the original message.



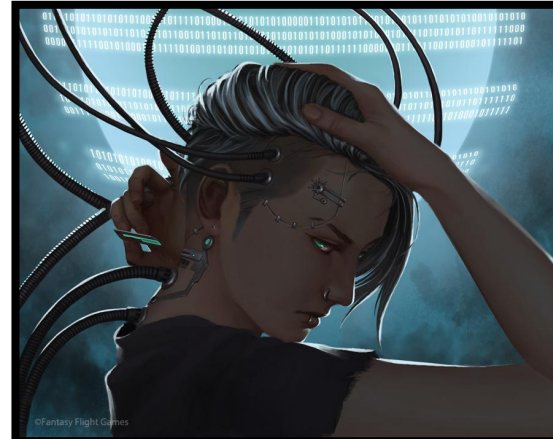


- **They have provided you with two images of systems from their network**
- **These images are development systems that they plan on deploying for their site**
 - The Webserver is under construction but will soon be used for
 - Customer online account access
 - Employee customer service
 - The client machine is an example of a system used by employees
 - Used for managing customer accounts with a custom application
- **Like many companies, they are concerned about their security**
 - There recently was security breach and they lost some important data
 - Although that attack vector has been mitigated, they are still concerned of residual risk





- **Your client wants a red team style test, and want to know**
 - What a threat source on the outside can achieve
 - What are the major vulnerabilities
 - How you exploited them
 - How they can fix them
 - The risk scores for the major vulnerabilities and the overall system





- **NBN knows their web server has some issues**

- You will be challenged to use previous knowledge and penetration testing methodologies to attack the server and the client

- **Goal: Get shell and eventually root on each machine**

- Scan and find vulnerabilities
- Guess and crack passwords
- Look for misconfigurations
- Everything we learned about

- **Try to access hidden data, "flags"**

- Represent critical data of NBN
- 8 flags total
- Flags are EXTRA CREDIT, optional





- **They will not be providing you with any system access or credentials**
 - These virtual machines, if configured and deployed correctly, should work
 - You should be able to test connectivity using ping
- **You are to attack their machines as an outsider would: over the network only**
 - You will not attack the internal client directly - must pivot through the web server
 - But if you discover an exploitable flaw or configuration that will allow a direct attack, you may use it (this is unlikely and unintended)
- **You shall not change any system passwords, configurations, or install software**
 - Don't install nmap, or any other applications
 - You are allowed to upload and execute files, such as scripts, payloads, or exploits
- **Performing a denial of service attack is outside the scope**
 - You shouldn't intentionally try to break anything, or reporting risk against it
 - If you break something, just delete the image and reload it

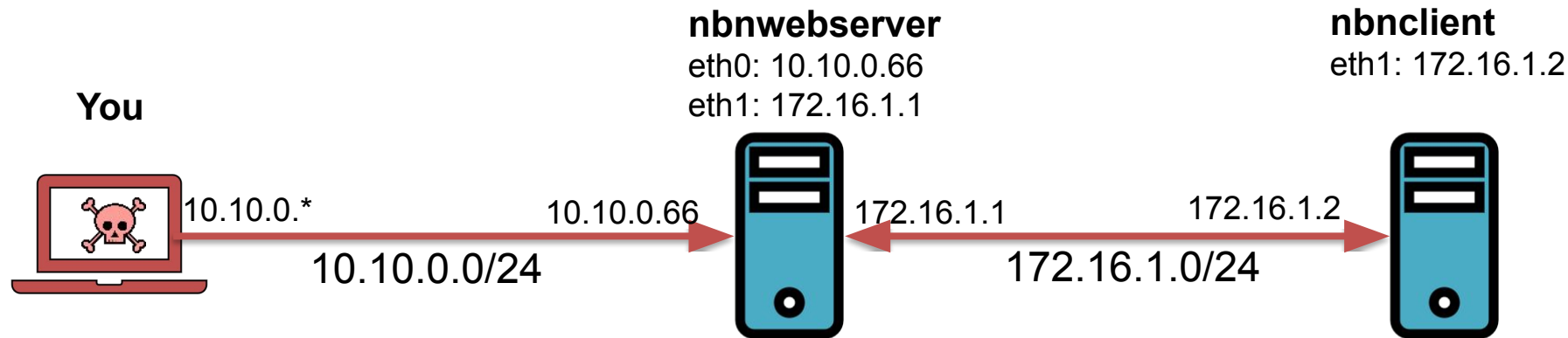
No attacks or using the system that would require physical access, such as editing the GRUB or logging in, even if you know passwords (CHEATING)



NYU

TANDON SCHOOL
OF ENGINEERING

Setup



- **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

- `# 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`



• This is what you should see

- Server Ping - Works
- Server Ping – Works
- Remote Client Ping – Works
- Remote Client Connection - Fail

```
kali@kali: ~/Desktop/final 124x40
kali@kali:~/Desktop/final$ sudo ip route add 172.16.1.0/24 via 10.10.0.66
kali@kali:~/Desktop/final$ ping 10.10.0.66
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=0.306 ms
64 bytes from 10.10.0.66: icmp_seq=2 ttl=64 time=1.40 ms
^C
--- 10.10.0.66 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1025ms
rtt min/avg/max/mdev = 0.306/0.853/1.401/0.547 ms
kali@kali:~/Desktop/final$ ping 172.16.1.1
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=0.338 ms
64 bytes from 172.16.1.1: icmp_seq=2 ttl=64 time=1.08 ms
^C
--- 172.16.1.1 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1032ms
rtt min/avg/max/mdev = 0.338/0.707/1.077/0.369 ms
kali@kali:~/Desktop/final$ ping 172.16.1.2
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=0.636 ms
64 bytes from 172.16.1.2: icmp_seq=2 ttl=63 time=2.18 ms
^C
--- 172.16.1.2 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1024ms
rtt min/avg/max/mdev = 0.636/1.410/2.184/0.774 ms
kali@kali:~/Desktop/final$ ncat 172.16.1.2 22 -w 3 -v
Ncat: Version 7.80 ( https://nmap.org/ncat )
Ncat: TIMEOUT.
kali@kali:~/Desktop/final$
```

•Download and add OVAs

- VMs networks are set to auto configure
 - /etc/rc.local and /var/networking.sh takes care of this

•VM Setup

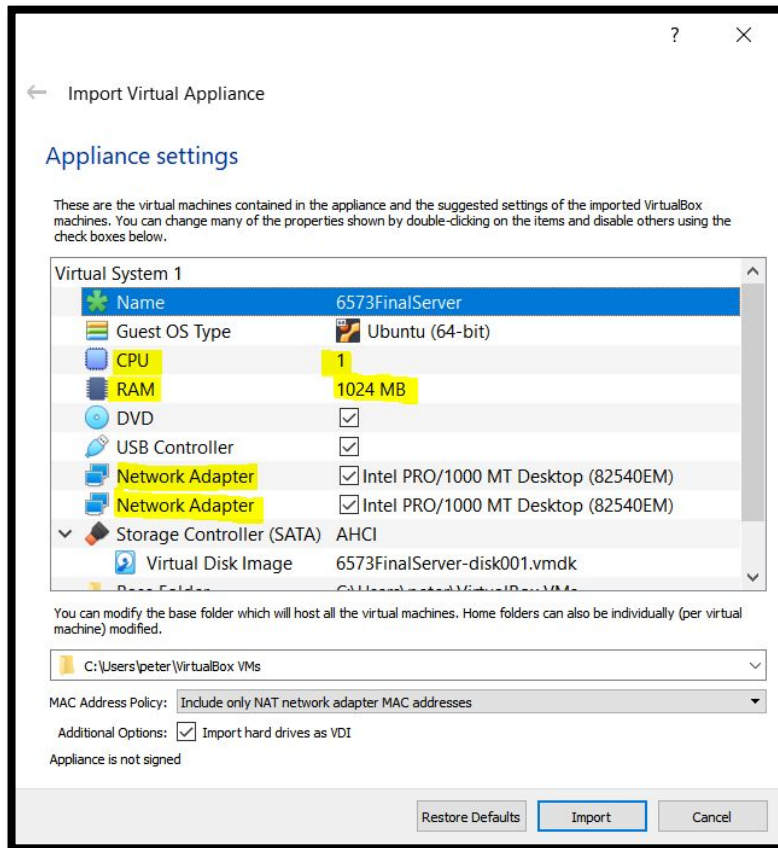
- Most settings should be automatic
- Review highlighted areas on right --->
 - 1 GB ram, 1 processor per VM
 - 2 network cards on the server, only 1 on the client

•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



- 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



```

root@kali:~# route
Kernel IP routing table
Destination      Gateway         Genmask         Flags Metric Ref    Use Iface
default          _gateway       0.0.0.0         UG    100    0      0 eth0
10.6.66.0        0.0.0.0        255.255.255.0   U     100    0      0 eth0
172.16.1.0       10.6.66.20     255.255.255.0   UG     0     0      0 eth0
    
```

Good, ping Webserver



```

root@kali:~# ping 172.16.1.1 -c 1
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=1.39 ms
    
```

Good, ping Client



```

root@kali:~# ping 172.16.1.2 -c 1
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=3.36 ms
    
```

Failed, but expected.



```

--- 172.16.1.1 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 1.391/1.391/1.391/0.000 ms
root@kali:~# ping 172.16.1.2 -c 1
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=3.36 ms
--- 172.16.1.2 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 3.361/3.361/3.361/0.000 ms
root@kali:~# nc 172.16.1.2 22
Ncat: Connection timed out.
    
```



NYU

TANDON SCHOOL
OF ENGINEERING

Deliverable and Grade

- **You will be required to deliver a report covering penetration test**
- **Your report should have these sections**
 - **Reviewed in Lesson 1**
 - Executive Summary
 - Introduction
 - Methodology
 - Findings
 - Conclusion
 - Appendixes
- **This format is the guide and what the rubric will be looking for**
 - However, the real world – this is not the rule 100% of the time
 - The report should always be formatted to address the details, methods, results, and goals of the test

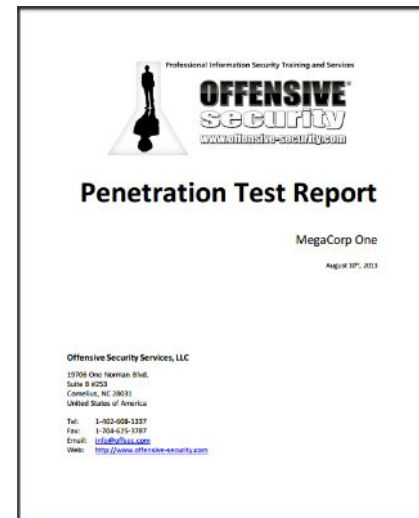
• Templates and Examples

- Offensive Security has a good template ☐
 - Their template combines Methodology & Findings section but then uses an Appendix to list all the Findings detail
 - This is a clean alternative when the report is written as a narrative

• More examples:

<https://github.com/juliocesartfort/public-pentesting-reports>

• If you use a template or outside sources, cite them



<https://www.offensive-security.com/reports/sample-penetration-testing-report.pdf>

- **For this report, please provide these sections**

- Keep each section short and on-point
- Entire report may vary in length.
 - Max page count should be less than 20 pages even if you have pictures, tables, attachments, title page, table of contents

- **Section Specific Details – What the rubric is looking for:**

- **Executive Summary**

- 2 paragraphs minimum
- Explain the purpose of the report, address the major flaws, list immediate actions/fixes, and provide overall security rating to the client

- **Introduction**

- 3 paragraphs minimum
- Review the goals and purpose of the test, and describe the type of test you performed
- Describe the rules of engagement, POCs, timelines/schedules, targets, scope
- Address the major flaws, list immediate actions/fixes, and provide overall security rating to the client

•Methodology

- Explain your high-level methodology or steps, and the tools you used
- Include how you scored risk or criticality
- Step by step details, either as a narrative or as instructions

•Findings

- Provide a run down of each vulnerability you discovered
- How you found it, and exploited it (if applicable)
 - Provide tools or methodology, reader must be able to recreate your finding
- Why that vulnerability should be important to a system owner
- Recommend a way they can fix it or mitigate it
- This section can be or utilize tables, bullets, paragraphs, or a combination
- There could be **hundreds** of findings if you scanned with an automated scanner. Please don't include information-only or very low risk findings. Focus on low and everything greater

•You may include figures, diagrams, or screencaps if it helps make your point but including these are not necessary

•Conclusion

- Restate and summarize the test goals, results, targets, risk, and immediate fixes

•Appendixes – Some ideas

- Tables
 - Open ports, protocols, services (and their versions),
 - usernames, passwords, variables, interesting info
- This could contain raw tool output too, such as nikto, Nessus, ZAP, Metasploit, **if it's meaningful**
 - Don't include nmap results. Make a table.
- Flags
- Source code of exploits you write
- **If you combined Methodology & Findings, should have one appendix as your findings section**
- Example, Appendix A - Topology, Ports, Protocols discovered, Appendix B - Flags found, Appendix C - Exploits written, etc

- **Due date posted on the class website**
 - We will not have a final exam - this is the final
- **Report will be worth about 1/3rd of your grade**
 - Equal weight given to your report and your technical accomplishments
 - Even if you don't get root shells or exploit the client, you can still write a very meaningful report
 - Bonus extra credit points for flags
- **Having a report that is useful for our fictional client**
 - It should have the major sections of a good pen test report
 - Not having those sections will be a loss of points
- **Your ability to utilize the tools, techniques, and methods learned**
 - There may be more than one way to accomplish an exploit, and more than one vulnerability to achieve a goal or an effect
- **Demonstrate knowledge of the pen testing methodology**
- **Demonstrate excellent communication to explain vulnerabilities, their associated impact and risk to the target organization**
- **Demonstrate knowledge of identifying and exploiting vulnerabilities**
 - This will be graded based on how many vulnerabilities you identify and exploit
 - Being able to explain why that vulnerability is bad and how it can be fixed

- **There are 8 flags hidden on these hosts and are worth additional points**

- 1 point per flag
- They may be an image or text
- Flags may be encoded, hidden, obfuscated
- Flags may be in different places, different folders, different permissions

- **Syntax will always start with "flag" and have a message inside brackets**

```
❏ flag{this_is_what_a_flag_will_look_like}
```

- If what you found is not in this format, or says 'NOTAFLAG', it's not a flag

- **These flags will represent critical data if this were a real business**

- By finding flags, it would be a way to show the client that their data is exposed
- This would be a good point to make on your report!

- **You should put all flags you find into your report and explain how you found them**



NYU

TANDON SCHOOL
OF ENGINEERING

Troubleshooting and Tips

- **Remember the pen testing methodologies from Lesson 1**

- Recon - There is interesting company information provided at the start of this slide
 - There are no internet targets or organizations though

- **Basic**

- Enumerate Enumerate Enumerate!
- External-facing Vulnerabilities and Exposures
- Privilege Escalation
- Pivot and Repeat

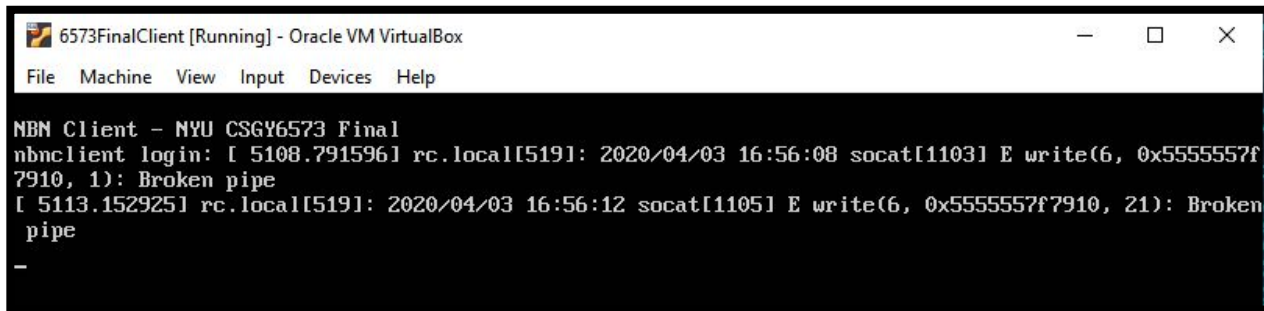
- **Use everything we learned about this semester**

• 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!

- **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 2020)
 - <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**

- **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



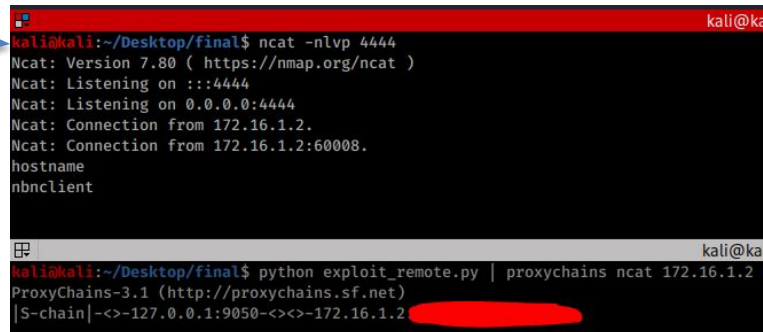
```

6573FinalClient [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

NBN Client - NYU CSGY6573 Final
nbnclient login: [ 5108.791596] rc.local[519]: 2020/04/03 16:56:08 socat[1103] E write(6, 0x5555557f7910, 1): Broken pipe
[ 5113.152925] rc.local[519]: 2020/04/03 16:56:12 socat[1105] E write(6, 0x5555557f7910, 21): Broken pipe
-
    
```

• 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
    
```

• Shell keeps closing?

- Try using msf-venom option
 - PrependFork=TRUE

- **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**



- 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!

