# Analyzing and Improving the NCL Ethical Hacking Lab Exercises

**George Shoemaker**[1], **Ahmed Gedi**[1], **Balal Rahim**[1], **Nick Tan**[1], **Jens Mache**[1] **and Richard Weiss**[2]
[1]Lewis & Clark College, Portland, Oregon, USA
[2]The Evergreen State College, Olympia, Washington, USA

**Abstract**— *The NCL provides a wide range of exercises for cybersecurity education that are accessible to beginning students. The problem is that by not assuming any previous knowledge, their exercises are limited in the depth at which they can teach the material. The contribution of this paper is to combine an NCL exercise on network reconnaissance with exercises that both teach prerequisite knowledge and include more creative challenges. These functionalities are supplied by existing exercises from Cyber Aces and EDURange respectively. The former provides tutorials with videos, reading and formative assessment. The latter provides more complex challenges.*

**Keywords:** Cybersecurity education, ethical hacking, penetration testing, nmap

## 1. Introduction

We are concerned with investigating and improving introductory cybersecurity education. We began our investigation with the spring 2017 version of ethical hacking labs published by the National Cyber League (NCL). The NCL provides hands-on experience through bi-annual competitions. The entry fee is $25 and includes access to a "Gymnasium" where students can follow the "Ethical Hacking Lab Series" [2]. The learning environment of the labs was created by the Network Development Group (NDG) [3] and allows students to interact with the GUI of remotely hosted machines in real time. These machines are also connected by a network, so students can practice attacking and defending remotely. The only inconveniences we experienced while using the NDG's environment were permitting Java to run on our computers and scheduling reservations in advance. We analyzed the 20 ethical hacking labs by working through them and reporting on their strengths and weaknesses.

We are concerned that beginner students may not be equipped with the conceptual knowledge to understand the tasks in the labs, while advanced students are not presented with a challenge. We propose to remedy these problems with prerequisite material and a separate exercise that challenges students to apply the tool in new situations.

In this paper we focus on the the NCL's first lab entitled "Reconnaisance with Nmap & Amap". We offer our suggested improvements to the lab and discuss the Cyber Aces tutorials as prerequisite material and EDURange's network scanning game entitled "Total Recon" as a more challenging exercise.

## 2. NCL labs on ethical hacking

The NCL Ethical Hacking Labs introduce many important hacking tools. There are a total of 20 labs for the spring of 2017 that include diverse topics such as password cracking, networking penetration testing and packet analysis. Often a lab will pair a task with a tool, see Table 1. For example, Lab 9 is entitled "Backdooring with Netcat" and lists "Port Scanning", "Establishing Connections", and "Transferring Files with Netcat" as its objectives. Each lab has a diagram of the virtual network's topology, as seen in Figure 1, and a table of IP addresses and account credentials for each machine on the network. The Kali Linux machine is used most often in the labs, because it has many tools installed in an integrated environment. Students are guided through each activity by explicit instructions. These steps are often accompanied with screenshots to make sure the reader can follow them. When the task is completed, the student is instructed to close the viewer rather than practice or explore.

### 2.1 Critique

The instructions of the NCL ethical hacking labs read much like a cookbook in the sense that students are told what to do with little explanation. This allows beginners to superficially "complete" the labs, but they may not fully understand what they are doing. In our experience, we became frustrated when the explanations were unclear or too brief. A rare exception to this was an annotated command, seen in Figure 3, that clearly describes each component. We would like to see more clear annotations like this. We also sometimes found it difficult to distinguish the important information in the output of tools.

These issues are present in the NCL's first lab entitled "Reconnaissance with Nmap & Amap". After logging into the Kali Linux machine, students are instructed to view the man page, as seen in Figure 2. This page is hundreds of lines long. It is unclear what is important to students for the lab. Students are then instructed to open Wireshark, which is not listed in the objectives. Upon reflection we realized that Wireshark is included to demonstrate to students what `nmap` is doing under the hood. We would prefer that the lab focus first on the basic functions of `nmap` and introduce Wireshark later. Step 14 of Part 1 says to "[s]croll through the Wireshark output and notice how `nmap` uses [SYN] flags against all the ports to see if they are open or closed." In

Table 1: NCL Preparatory Lab Exercises on Ethical Hacking (from spring 2017)

| Lab | Title | Tools |
|---|---|---|
| 1 | Reconnaissance with nmap & amap | nmap, amap, Wireshark |
| 2 | Social Engineering Attacks with Social Engineering Toolkit | SE tool kit |
| 3 | Metasploit Framework Fundamentals | Metasploit, netcat, wmap |
| 4 | Web Pentesting with Nikto & OWSP Zap | Nikto, OWASP Zap |
| 5 | Password Cracking with John the Ripper and Hashcat | John the Ripper, Hashcat, cewl, crunch |
| 6 | Creating and Installing SSL Certificates | SSL |
| 7 | Vulnerability Scanning with OpenVAS | OpenVAS |
| 8 | Enumerating SMB with enum4linux | enum4linux, smbclient, xHydra |
| 9 | Backdooring with Netcat | Netcat |
| 10 | Packet Crafting with Scapy | Scapy, Wireshark |
| 11 | Network Analysis | Sniffers, smbclient, tcpdump, Wireshark, Xplico |
| 12 | Client Side Exploitations | BeEF framework |
| 13 | Testing Firewall Rules with Firewalking | Firewalk, pfSense dashboard |
| 14 | Understanding SQL commands | Injections & SQL Injection |
| 15 | Understanding Buffer Overflows | Buffer Overflows |
| 16 | Evading IDS | SGUIL, Snorby, Squert |
| 17 | Packet Crafting with Hping | Hping |
| 18 | VNC as a Backdoor | TightVNC |
| 19 | Auditing Linux Systems | Lynis |
| 20 | Anti-Virus Evasion | Veil Framwork |

order to understand the significance of this output, a student would need to know about layer 4 of the OSI 7 layers of networking model. Students are instructed to enter a series of commands that use the -F, -A, and -Sc flags. The lab then switches to `amap`, but the difference between `nmap` and `nmap` is not made clear. Students are again instructed to look at the man page for `amap` and the -A and -B flags are tested on a specific port.

## 2.2 Improvements

With a few key changes, the NCL ethical hacking labs could be far more effective as a learning tool. We see the need for prerequisite material so that novice students can more easily fill the gaps in their understanding, and each lab can go deeper into its respective concepts and tools. For all 20 labs we suggest the Cyber Aces tutorials [1] to cover the OSI 7 layers of Networking and the Linux Core Commands. We particularly like these tutorials because they are free, information is presented in written and video form, and the material includes questions that test understanding.

Rather than introducing a tool by asking students to "[r]eview the man page...", we suggest a standard format to introduce each tool. There should be a basic description of what the tool does and how it works, a working example that is annotated (like in Figure 3), and instructions on how to access the documentation for the tool. This basic information is more likely to prepare the student to apply the tool in new situations.

By applying our improvements, the NCL's "Reconnaissance with Nmap & Amap" lab should begin with a conceptual description what `nmap` does and how it works: "`nmap` is a powerful network security scanner commonly used to discover IP addresses with open ports. It sends packets and automatically interprets the responses to determine information about a network." Then comes a working example of `nmap`. This could be as simple as `nmap <IP address>`, or a command with multiple flags that are annotated. Instead of the man page, students should first see the abbreviated help page by simply entering `nmap`. In this case, the `PORT SPECIFICATION AND SCAN ORDER` section of the help page is particularly relevant to the lab. The same should be done for `amap`: description, working example, help page.

The lab should emphasize that the open ports discovered with `nmap` can be more deeply investigated with `amap`. These sorts of "Aha!" moments make the exercises more engaging. Learning Wireshark along with `nmap` may be overwhelming. If it remains in the lab, Wireshark should appear at the end of the lab as a way for students to experiment further with `nmap`, and should also be introduced in three parts. The [SYN] [ACK] output of Step 14 part 1 could be contextualized within the concept of the TCP 3-way handshake, which is included in the Cyber Aces' discussion of Layer 4.

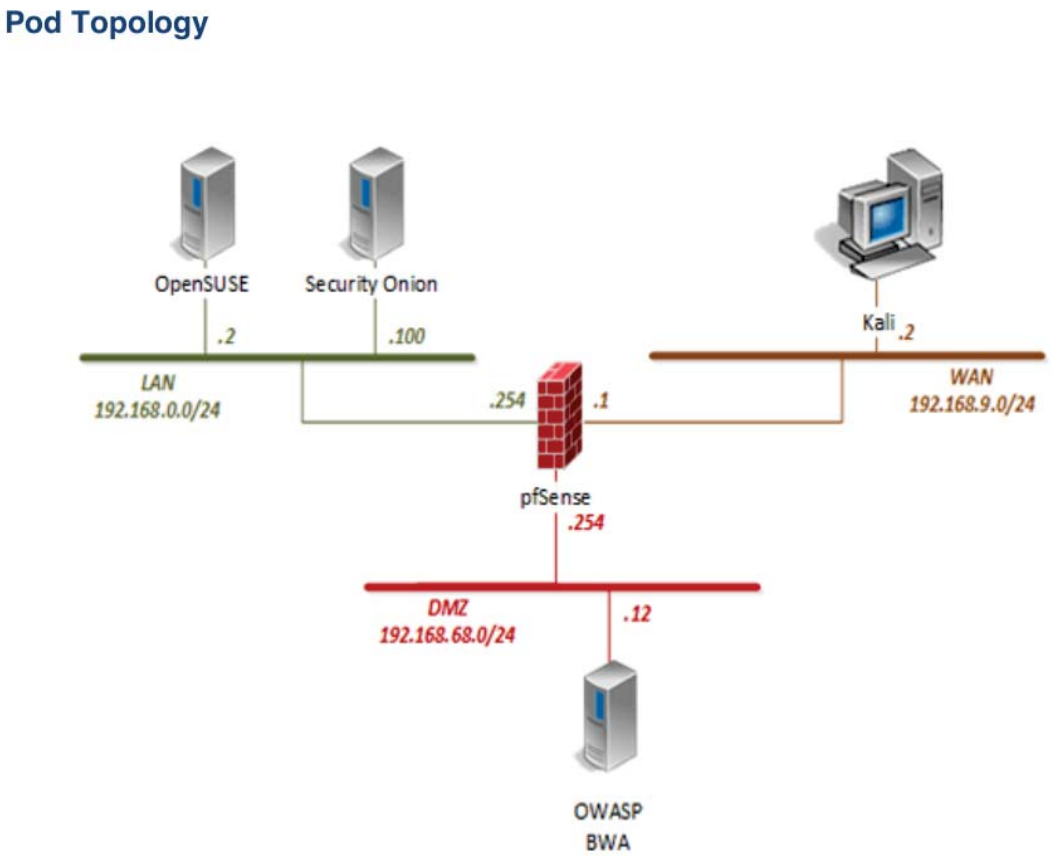


Fig. 1: Network topology

6. Open and review *Nmap's* manual by typing the command below followed by pressing **Enter**.

```
man nmap
```

Nmap has many options, including its own scripting engine. Review the man pages to get familiar with the switches and options. Press the **Spacebar** to go to the next page or press **Enter** to go to the next line.

Fig. 2: "Review the man pages..."

6. In the new *Terminal* window, type the command below to scan for which outward facing ports are open on the firewall. Press Enter.

```
nc -w 1 -zvn 192.168.9.1 1-100
```

This command instructs Netcat to do the following:

-w: wait one second
-z: port scanning mode
-v: verbose
-n: don't use DNS lookups
1-100: port range to scan

Fig. 3: Annotated command

## 3. Going further with EDURange

"Total Recon" is a hands-on security exercise implemented in the EDURange framework that is designed to be an engaging network reconnaissance exercise. Students use `nmap` and netcat (`nc`) to investigate hosts on a large network (the IP range has up to $2^{15}$ addresses). The multiple levels of the game provide scaffolding that allow students with a wide range of preparation to play the game.

We believe "Total Recon" would serve as an excellent next step for students after completing NCL's introductory `nmap` lab. To better engage students in the learning activity, levels are designed so that they are woven into the plot of the movie *Total Recall* (1990). As levels are solved, students progress through parts of the story. This balance of challenge and reward aims to provide students with an additional level of engagement and motivation that is not present in the NCL ethical hacking labs.

A major challenge of Total Recon is the size of the IP range that students must search. It is 16K addresses and can take more than 15 minutes with default `nmap` options. Students can hit any key to see a progress report and estimated time of completion.

The default options for nmap will first try ping. However, some hosts do not respond to ping, so nmap will not check for open ports without a response and will not report that it is live. Therefore the -Pn option must be used to skip this host discovery method.

Another major challenge is that without using options, nmap only scans 1000 common ports out of $2^{16}$ possible ports. One strategy is to first scan this subset to find interesting or unusual behavior, and then use the option -p- to scan all of the ports of a few IP addresses.

In level 4, a scan of the subnet requires more than 15 minutes to complete. With additional intelligence about the IP address search and an understanding of CIDR notation, students can reduce the scan time from 16 minutes to 2 seconds.

At another level, a firewall is introduced that can block traffic in and out of the network, restricting the information that nmap can obtain. However, there is one IP address that is not being filtered and the student must search through the data to find it.

At another level, the challenge is that nmap is not available and the student must use nc to get information. However, nc produces a significant amount of data which needs to be searched, for example using grep.

Another challenge is that ssh uses port 22 by default, but can be running on any port. Version scan options may help to find the non-standard port more conveniently than manually trying all open ports.

In additional levels, students are introduced to the advantage of using stealthy scans which can result in extra information. The scenario culminates in a final challenge that requires additional Linux command line skills to "turn on the reactor" and win the game.

The beauty of the game as a teaching tool is that it requires students to try out options and flags to make progress. With knowledge of the nmap's help page (possibly introduced in the NCL nmap lab), students can learn through exploration and experimentation, and there isn't just one way to progress to the next level. Students are motivated to search for strategies and options can significantly change waiting time for scan completion and amount of information produced.

# 4. Related Work

Research shows that hands-on exercises increase student interest in cybersecurity [8]. The SEED Project [4] has a large number of advanced exercises, including buffer overflows and malware analysis but requires downloading VMs. DETERLab [6], [5] has a variety of exercises contributed by several schools, from code injection to DDoS. Security Injections [7] is more narrowly focused on secure coding. The NICE Challenge Project provides a set of goal-oriented, open-ended online exercises[1], while EDURange [11], [10], [9] aims to provide more scaffolding.

[1] https:www.nice-challenge.com

# 5. Conclusion

The development of ethical hacking exercises is still a work in progress. In our critique of the National Cyber League's Ethical Hacking labs, we highlighted the use of "cookbook" style instructions that don't require much analytical thinking. In order to ensure that the lab is accessible to beginners, we recommend the Cyber Aces tutorials as prerequisite material. We would like to see instructions that connect to conceptual information and recommend that more open ended challenges be introduced as a distinct exercise such as EDURange's "Total Recon". It is the combination of these elements (a conceptual foundation, an introductory lab, and a more challenging exercise) that will ensure that students can gain conceptual and practical knowledge in manageable pieces.

## Acknowledgments

This work is supported by NSF grants 1516100 and 1516730, and by the John S. Rogers program. We thank the EDURange team, especially Michael Locasto, Erik Nilsen, Franklyn Turbak and students Stefan Boesen, Mark Grossman, Kahea Hendrickson, Jeff Ladish, Yesha Maggi, Nick Stephens, and Noah Weiner.

# References

[1] Cyber Aces tutorials. https://tutorials.cyberaces.org/tutorials. Accessed: 2017-05-24.

[2] NCL labs. https://www.nationalcyberleague.org/lab-exercises. Accessed: 2017-05-24.

[3] NDG. https://www.netdevgroup.com/products/requirements. Accessed: 2017-05-24.

[4] DU, W., AND WANG, R. Seed: A suite of instructional laboratories for computer security education. *Journal on Educational Resources in Computing (JERIC) 8*, 1 (2008), 3.

[5] MIRKOVIC, J., BENZEL, T., FABER, T., BRADEN, R., WROCLAWSKI, J., AND SCHWAB, S. The deter project: Advancing the science of cyber security experimentation and test. In *Technologies for Homeland Security (HST), 2010 IEEE International Conference on* (2010), pp. 1–7.

[6] PETERSON, P. A., AND REIHER, P. L. Security exercises for the online classroom with deter. *Proc. of the 3rd USENIX CSET* (2010).

[7] TAYLOR, B., AND KAZA, S. Security injections: modules to help students remember, understand, and apply secure coding techniques. In *Proceedings of the 16th annual joint conference on Innovation and technology in computer science education* (2011), ACM, pp. 3–7.

[8] WEISS, R., MACHE, J., AND NILSEN, E. Top 10 hands-on cybersecurity exercises. *Journal of Computing Sciences in Colleges 29*, 1 (2013), 140–147.

[9] WEISS, R., TURBAK, F., MACHE, J., NILSEN, E., AND LOCASTO, M. E. Finding the balance between guidance and independence in cybersecurity exercises. In *2016 USENIX Workshop on Advances in Security Education (ASE 16)* (Austin, TX, 2016), USENIX Association.

[10] WEISS, R. S., BOESEN, S., SULLIVAN, J. F., LOCASTO, M. E., MACHE, J., AND NILSEN, E. Teaching cybersecurity analysis skills in the cloud. In *Proceedings of the 46th ACM Technical Symposium on Computer Science Education* (New York, NY, USA, 2015), SIGCSE '15, ACM, pp. 332–337.

[11] WEISS, R. S., TURBAK, F., MACHE, J., AND LOCASTO, M. E. Cybersecurity education and assessment in EDURange. *IEEE Security & Privacy 15*, 3 (2017).