Journey to Becoming a Hacker: From Zero to Cybersecurity Ninja

Author: Yoshuam A. Alicea Casillas
Advisor: Dr. Jeffrey Duffani
Electric & Computer Engineering and Computer Science

Abstract

Time to time technology changes and the need for cyber security experts increases. While is true that lots of universities prepare students on this career, somehow students face trouble understanding how to acquire the necessary knowledge to perform well, once they land a job in cyber security field. Also, it seems that they need to separate the theory from practice to not only understand why things happens in this field but to know how they happened and the causes that made them. Is for this that we will walk you through the journey of how to start a training that will take you from zero knowledge in the topic to skillful hacker in a short period of time using knowing tools to find the knowledge and exposing yourself to competitive environments that will put in practice what you learned in your degree and what was self-taught.

Introduction

When people think to start a cyber security career, they often expect that pursuing a degree will get them ready to the professional world by having the necessary skills that a cyber security expert needs to overcome any challenge that will present in their jobs. But the problem these newcomers face is that hackers out there have been doing their bad deeds for long time, and even worse they have been doing it in real world scenarios. Some of them are trained by illegal hacktivist organizations and they have all the time in the world to achieve their objectives and to gather the day to day knowledge to become even better. In summary, these bad guys have more experience than any newcomer in the cyber security field. While your degree and university program will help you grasp all the cyber security concepts and theories behind it, we need to go further and find the experiences that will simulate the cyber war battlefield that you will be exposed once you start in your cyber security career. Knowing how a system can be exploited helps on how you can safe guard it. Is for this that we will take you to a journey of how we became skillful in the cyber security field while going through our cyber security degree and participating in Capture The Flag (CTF) competitions.

CTFs are puzzle-style problems that challenge the participants with different cybersecurity scenarios that mimic real world allowing the participant to acquire experience by understanding and exploiting a vulnerability that not only teaches the participant how to perform the attack but creates conscience on how to defend against it as well.

Background

With the current advance of technology cybersecurity threats increase everyday in a fast paced manner. No university is able to keep up with this rate of increase in technology since technology changes everyday. Cybersecurity students are at disadvantages against cybercriminals due to difference in experience.

Currently, there are websites that allow students gain the experience by getting expose to CTF competitions that allows them to understand how to identify a threat, what vulnerability it exploits, how to exploit that vulnerability and how to defend against it.

Problem

How can we train cybersecurity students to prepare them for they cybersecurity battlefield that exist in the cyberspace? Here we share how we became competitive cybersecurity professionals in a short period of time by exposing ourselves to a handful CTF competitions that put us under pressure to solve security challenges by placing us in the side of the hacker. Understanding how a hacker thinks and thinking like a hacker to learn how to detect vulnerabilities, exploiting them and protecting from them.

Methodology

We exposed the ourselves to basic computer skills that a cybersecurity expert should have in order to understand the computer environment that he moves in. We started with basic system administration on Linux operating system. Once the we felt comfortable moving around Linux we exposed ourselves to the different tools that Linux OS offer out of the box to then master the operating system. Then we got to different cyber security fields like:

- Web Application Security
- Reverse Engineering
- Cryptography
- Network Analysis

After we grasped the concept of the previous mentioned fields we put our acquired knowledge into practice by participating in the National Cyber League (NCL) and CTFTime.org platforms. NCL and CTFTime.org contains extra fields like password cracking, steganography, computer forensics, Log analysis, open source intelligence, and wireless network exploitation. After, our first exposition to this new fields. We studied them and tools relevant to each field to become skilled on them.

Results and Discussion

After competing in NCL and CTFTime.org we were able to keep up with experienced cybersecurity professionals by demonstrating knowledge and accuracy in our solves for the challenges. We were able to get on top 20 in gold bracket division on NCL individually and as a team. On CTFTime.org we were able to position ourselves number 1 in our country and top 600 globally from around 13K teams. We demonstrated to be very skilled in all the fields presented in each competition. (See Figures 1- 3 for an example of the type of challenges we were exposed)

User	Password Hash
Justen	c6ffca47b477506eb331930cc6ae6292
Tom	9594e0f07b4e6e280c6131ce48dbf80d
Rachel	8609c7cc715dea6500e08db180b16f51
Eve	315d1cc9faafa74129769751fdd92ea3
Elliot	247e8adf7ede165ad0bd6032e4c0dfc6

Figure 1 Password Cracking exercise presented on NCL Hint: Episodes of the series Law & Order SVU.

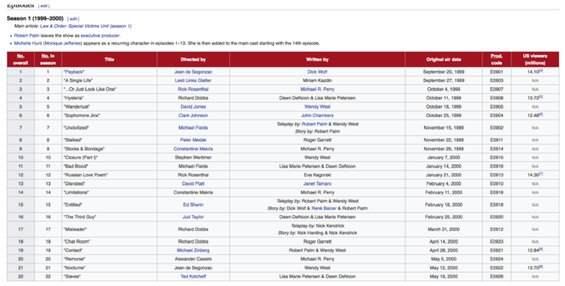

Figure 2 Performing reconnaissance to find the Episodes of the series Law & Order SVU. Wikipedia had a list of all the episodes

episodes.py - /Users/Yoshuam/Desktop/MSProject/categories/passcrack/episodes.py (3.6.0)

```
import wikipedia
from bs4 import BeautifulSoup
import re

# set language to english
wiki =  wikipedia

# Extract the page
law_and_order_sv_page = wiki.page('List of Law & Order: Special Victims Unit episodes')

# Convert to html format
html = law_and_order_sv_page.html()

# soup to parse html
soup = BeautifulSoup(html)

# classes to parse from html
table_classes = { "class": ["summary"]}

# extract tables from html that contains 'summary' class
wikitables = soup.findAll('td', table_classes)

# Initialize list that will have all the episode names
episodes = []

# extract the episodes name from the tables and store them in episode list
for table in wikitables:
    if table.text:
        episodes.append(table.text)

# sanitize input and eliminate references and symbols
for i in range(0, len(episodes)):
    episodes[i] = re.sub('[0-9\[\]\'\" ]', '', episodes[i]).lower()

# add rule of two numbers at the end of episode name and store them in a new list
episodes_two_numbers = []
for episode in episodes:
    for i in range(10):
        for j in range(10):
            episodes_two_numbers.append(episode + str(i) + str(j))

# write episodes name into 'episode.txt' file
with open('episodes.txt', 'w') as fp:
    fp.write('\n'.join(episode + '\n' for episode in episodes_two_numbers))
```

Figure 3 Script that perform web scrapping to retrieve the content of Wikipedia to obtain all the episodes of Law & Order SVU and creates a dictionary for password cracking

CTFTime.org platform was more challenging than NCL since challenges weren't as descriptive as in NCL but they had a write-up section after the end of competition where every team could share their solves and that way you could see the different approaches to solve the same problem creating awareness on competitors and at the same time increasing the mindset of each player to think out of the box in those challenges that were hard to solve. (see Figure 5 – 6 for an example of CTFTime.org challenge)

```
p=0xa6055ec186de51800ddd6fcbf01923384ff42d707a55f57af4fcfb0d1dc7bd97055e8275cd4b78ec63c5d592f567c66393a061324aa2e6a8d8fc2a910cbee1ed9

q=0xfa0f9463ea0a93b929c099320d31c277e0b0dbc65b189ed76124f5a1218f5d91fd0102a4c8de11f28be5e4d0ae91ab319f4537e97ed74bc663e972a4a9119307

e=0x6d1fdab4ce3217b3fc32c9ed480a31d067fd57d93a9eb52b472dc393ab7852fbcb11abbebfd6aaae8032db1316dc22d3f7c3d631e24df13ef23d3b381a1c3e04abcc745d402ee3a031ac2718fae63b240837b4f657f29ca4702da9af22a3a019d68904a969ddb01bcf941df70af0424f4ae5cbeb9c2151b324f387e525094c41

c=0x7fe1a4f743675d1987d25d38111fae0f78bbeaf6852cba5beda47db76d119a3efe24cb04b9449f53becd43b0b46e269826a983f832abb53b7a7e24a43ad15378344ed5c20f51e268186d24c76050c1e73647523bd5f91d9b6ad3e86bbf9126588b1dee21e6997372e36c3e7428473474889182966506 6e0dc523ed23c386bb520
```

Figure 5 RSA encryption challenge. You had to find the vulnerability and exploit it to decrypt the message

rsa.py - /Users/Yoshuam/Desktop/rsa.py (3.6.0)

```
import gmpy

# Convert each number from hex to integers
p = int(0xa6055ec186de51800ddd6fcbf01923384ff42d707a55f57af4fcfb0d1dc7bd97055e8
q = int(0xfa0f9463ea0a93b929c099320d31c277e0b0dbc65b189ed76124f5a1218f5d91fd0
e = int(0x6d1fdab4ce3217b3fc32c9ed480a31d067fd57d93a9ab52b472dc393ab7852fbcb1
c = int(0x7fe1a4f743675d1987d25d38111fae0f78bbeaf6852cba5beda47db76d119a3efe24

# Calculate modulus N
N = p * q

# Calculate phi(N)
phi_N = (p - 1) * (q - 1)

# Using gmpy find the modulus inverse of e
d = gmpy.invert(e, phi_N)

# Calculate the message and encode it into hex
message = hex(pow(c, d, N))[2:]

# Decode message from hex into text (ascii)
flag = message.decode('hex')

# print the secret message
print flag
```

Figure 6 Script we wrote in Python to exploit the low N vulnerability performing modulus inverse calculus to find the exponent of the private key

Conclusions

In a short period of time by treating learning as a competition, where increasing the knowledge in cybersecurity is what gives us the advantage, we managed to acquired skills and techniques in a fast paced manner with very high effectiveness. We learned how to use tools that already exist and how to make custom ones. How to detect, understand, exploit and protect from a vulnerability in different cybersecurity areas. We were able to compete head to head against current cybersecurity professionals with years of experience. Putting together what is taught on the cybersecurity degree with Capture The Flag competitions allowed us to obtain the require knowledge to be considered competitive in the cybersecurity field. We were easily able to map the teachings in our security courses to the problems in the scenarios given by NCL and CTFTime.org. Finally, by encouraging the students to take an extra step and participate in this kind of events and mixing it with the degree, will allow the program to produce highly skilled professionals ready to protect and defend the cyberspace of any entity, or company they aim to work for.

Acknowledgements

This material is based upon work supported by, or in part by the National Science Foundation Scholarship for Service (NSF-SFS) award under contract/award #1563978.

References

Y. Alicea (April 25, 2017) "Cybersecurity Competitions as Effective Cybersecurity Teaching Tools" [Online] Available: http://029e2c6.netsolhost.com/II-Proceedings/2017/IIVC2017_ALICEA.pdf.

M. Hess (2018, July 30). How to prepare for capture the flag https://www.ctbnuggets.com/blog/2018/07/how-to-prepare-for-a-capture-the-flag-hacking-comeptition/

NCL. (2018). NCL | National Cyber League | Ethical Hacking and Cyber Security. [Online] Available at: https://www.nationalcyberleague.org/

Team, C. *(2018). CTFtime.org / All about CTF (Capture The Flag). [Online] Ctftime.org. Available at: https://ctftime.org/.*