CryptoKait's Coaching Guide

An Introduction to the National Cyber League

By: Kaitlyn Bestenheider

PACE UNIVERSITY

Seidenberg
School of Computer Science and Information Systems

CYBER SKYLINE

Version 1.0 of this document was originally written and published for use with the workshop:
"**N00bSec to Cyber-Champion: Hacking the National Cyber League for Success**"
Debuted at the 2018 Women in Cyber Security Conference in Chicago, IL.

Contents

Purpose

For me, there were a few different goals when writing this guide.

First and foremost, I wanted to share the benefits of competing in cybersecurity competitions such as the National Cyber League. It has truly shaped my education and my career to have had these experiences. I have never been to an interview where it did not come up and I know that it makes me a stronger candidate for the jobs I apply to.

Additionally, I wanted people to know that you don't have to be an "Elite H@x0r" to compete in your first competition. In my opinion, the National Cyber League is the hands-down single best competition to start with if you have never competed in a cybersecurity competition. You can read more about this under "Benefits."

It is also my belief that taking a plunge into something new can be difficult. I wanted to create a guide for first time students and coaches to help them feel sure in their decision to attempt this competition. I promise that you have the ability and skill to do well in this competition. This guide will help you to see that as well.

Lastly, I wanted to share my personal experience with some of the students who are apprehensive. I promise that you can't know less than I did during my first competition and I have risen through the ranks as the single worst competitor on my team to a team captain, to a coach, and now as the Chief Player Ambassador of the National Cyber League.

My success is not uncommon. My success is the result of a love for what I do and a curiosity to grow in my field. If you have those two characteristics, then you will do well in the National Cyber League.

Besides, the National Cyber League Games are fun! We all deserve to have a little fun in our education.

Acknowledgements

Firstly, I would like to thank the **Women in Cyber Security Conference** (WiCyS). I attended WiCyS for the first time in 2017 and I met many of the people who still influence me today. I wrote my original CFP without much hope that it would actually get accepted, but I'm about two weeks away from hosting my very first technical workshop.

I would like to thank the **National Cyber League** for giving me, not only the green light on this project, but their support in helping to create and host the original workshop designed for the 2018 WiCyS Conference.

My experience has been made possible (in part) by support from the **Pace University CyberCorps Program** and the **Pace University Women in Technology** grant from **General Electric.** I'd especially like to thank my team from **Pace University** who helped to run this workshop at the 2018 WiCyS Conference. Without them, I would not have been able to test-run this workshop or help as many people as I would like to.

Our team included: **Elizabeth Molloy**, **Vicente Gomez**, **Jeana Cosenza**, and **Andreea Cotoranu,** and **Dr. Li-Chiou Chen**.

Another important member of the team was our industry consultant, **Michael Lavacca**, a senior software engineer at Bloomberg, and my fiancé. His contributions and support have made every part of my education possible.

Special thanks to **Dan Mason**, NCL Commissioner, and **Franz Payer**, Cyber Skyline Founder, who have been exceedingly patient with my overly ambitious goals and procrastination that caused major rewrites and additional work for everyone at two in the morning the night before the workshop.

And not to be forgotten, I would like to thank Professor **John Watkins** from **Westchester Community College**. His passion for cybersecurity and his students helped me find this subject that I love so much. I am excited to go to work every day because he believed in me when I didn't believe in myself and enabled me to discover my own talents. I was in the wrong major until he introduced me to NCL.

Lastly, thanks to all the faculty who have taken the time to read this guide. It shows a love for your students and your craft that often goes underappreciated. It shows that you are seeking new paths for your students' success. I hope this guide will help you to influence your students the way my teachers have influenced me.

Benefits of the National Cyber League

For me, there are four main benefits of the National Cyber League.

Curriculum. NCL uses learning objectives based on industry-recognized certifications: **CompTIA Security+** and **EC-Council Certified Ethical Hacker (CEH).** It measures skills in industry-specific tasks such as Open Source Intelligence, Password Cracking, Log Analysis, and more.

Availability. With the only eligibility requirement being that the player is enrolled in a high school or collegiate institution, the NCL has so many **eligible** competitors. It's relatively **affordable** costing only $25 per player for the individual competition (preseason and regular season) and $10 for the postseason team competition. Even better, you can **compete from the comfort of your own home** through their online portal, **Cyber Skyline**. (Pro tip: You can totally compete in pajamas!)

Accessibility. With **clearly labelled** challenge **categories** and **difficulty levels** (Easy, Medium, and Hard), a **first-time player** can easily navigate the competition environment and test their hand at a variety of skills. Additionally, the **easy challenges are designed for students who are new to InfoSec**! Additionally, you are given multiple attempts for each question and immediate feedback on your accuracy. If I can capture a few flags as a fresh transfer from a theatre undergrad, you can definitely capture a few, too!

Skills Assessment. NCL uses **real world scenarios** to test your skills at **industry-relevant challenges**. Not only does NCL **test your skill**, but it provides a **comprehensive scouting report** to each competitor at the end of each season**. Top tech companies** sponsor NCL at varies amounts to see a top performing scouting reports. Additionally, you can incorporate your experience and scouting report into your **resume** and cover **letter**. (I can honestly say I have never been to an interview where I was not asked about my NCL experience!)

Selected Challenges for Practice

Introduction

The following challenges were all taken from previous National Cyber League competitions starting in fall 2015. All credit for these challenges are due to NCL and Cyber Skyline.

Because these challenges are the intellectual property of NCL and Cyber Skyline, I cannot release the answers to these challenges.

The following keywords are important to understand.

> **Category** – A learning objective based on industry-relevant skills.
>
> **Challenge** – "A group of questions with a shared theme or artifact. E.g. A group of questions regarding a single log file" (NCL Word of the Week). Note: It is possible to capture multiple flags within a challenge without capturing all of them. You do not have to complete a challenge to gain points.
>
> **Question** – An individual question that, when answered correctly, awards a captured flag.
>
> **Attempts** – "The number of submissions that are allotted for a challenge. A challenge may have several questions, so the pool of submissions is shared with all the questions in a given challenge. Both a correct and an incorrect submission will count as a single attempt" (NCL Word of the Week).

Challenges will have a heading that appears at the following:

Challenge 01 – Open Source

It describes a Challenge # (not used by NCL or Cyber Skyline, meant only to help coordinate to the matching Coaching Guide Challenges), then the NCL Category.

Directions and needed files will immediately follow. Files will be named and a short link will be provided.

Lastly, challenge questions will be listed with the point values for each correct answer in parenthesis at the beginning.

If an asterisk (*) is found after the challenge category, this challenge is based on previous NCL challenges, but have been created for use in this guide.

Challenge 01 – Open Source

Answer the following questions about security issues.

1. (25 points) What is the CVE of the original POODLE attack?

2. (25 points) What version of VSFTPD contained the smiley face backdoor?

3. (25 points) What was the first 1.0.1 version of OpenSSL that was NOT vulnerable to Heartbleed?

4. (25 points) What was the original RFC number that described Telnet?

5. (25 points) How large (in bytes) was the SQL Slammer worm?

6. (25 points) Samy is my…

Challenge 02 – Open Source

We have intercepted an email sent between hackers. See what you can find out.

(use file: NCL-OpenSource-EmailHeader.txt or goo.gl/8Z4rPc)

1. (15 points) What is the recipient's email address?

2. (15 points) What is the sender's email address?

3. (15 points) What IP address retrieves the email?

4. (15 points) What is the content type of the message?

5. (15 points) What version of MIME is being used?

6. (15 points) What day of the week was the message received?

Challenge 03 – Cryptography *

Our officers have obtained password dumps storing hacker passwords. After obtaining a few plaintext passwords, it appears that they are all encoded using different number bases.

1. (15 points) 01000100 00110001 01110110 00110001 01101110 00110001 01110100 01111001

2. (15 points) 102 060 162 144 063 162 154 100 156 144 163

3. (15 points) 83 107 121 114 105 109

4. (15 points) 0x426174746c334672306e744949

5. (15 points) UGF0aCAwZiBFeGlsZQ==

Challenge 04 – Cryptography *

Our officers have obtained password dumps storing hacker passwords. After obtaining a few plaintext passwords, it appears that some sort of shift cipher was used.

1. (20 points) APY-FUVSG-4237

2. (20 points) UJS-ZOPMA-8931

Challenge 05 – Cryptography *

Our officers have obtained password dumps storing hacker passwords. See if you can crack them.

1. (25 points) .-.. .. ..-. . / .. ... / .-- .... .- - / .... .- .--. .--. . -. ... / .-- .... . -. / -.-- --- ..- .----. .-. . / -... ..- ... -.-- / -- .- -.- .. -. -- . / --- - .... . .-. / .--. .-.. .- -. ... .-.-.- / -. -.-. .-.. -....- -.- - -... -....- ....- --... ..--- ...-- .-.-..

Challenge 06 – Cryptography *

We have intercepted encrypted messages between hackers. Decipher them and find out what they are doing.

1. (15 points) Forot tolwCytKi nTitrl paowe

2. (20 points) Tyachrphs rect nad ninbeceeoek

3. (20 points) MsinCmrmsdiso opoie

Challenge 07 – Cryptography *

Our officers have obtained an encrypted message. The forensics team was able to find a file that contains the string, "private" which was used to encrypt the message. Take it from here and obtain the plaintext message.

1. (50 points) Wrkfs4Iyej zzqnihkmy smeila ppweiv nmof @peyi1. Io kiefvne. Brxkqvtx Tarv W.

Challenge 08 – PW Cracking *

Officers have obtained password dumps storing hacker passwords. After obtaining a few plaintext passwords, it appears that they overlap with the passwords from the **rockyou** breach.

1. (15 pts) 8549137cd494c22ae87eef3e18a46986
2. (15 pts) 0f96a320a8c0bf7e3f6d375b0d9d3a4c
3. (15 pts) 1a8cb8d148b513dfa1d285077fc4e3fb
4. (15 pts) 22a313110bf5b84c0a58eecc27deaa30
5. (15 pts) e4fd50109f0e40e8c1a895d8e5c71199

Challenge 09 – PW Cracking *

Our officers have obtained password dumps storing hacker passwords. It appears that they are all in the format: "SKY-KAIT-" followed by 4 digits. Can you crack them?

1. (15 points) c38d29e8899455c85ee03d11abbd262b
2. (15 points) ff8f9efad5c9f106ac39e5290d810c91
3. (15 points) 425206344bd204933a38236b715c498f
4. (15 points) ab37c335e51b2855cb5a11ca89041733
5. (15 points) 82dcf30f8c7c8d4f23961f7e0c1d3cee

Challenge 10 – PW Cracking *

Our officers have obtained password dumps storing hacker passwords. It appears that they are all based off of Pokémon. Can you crack them?

1. (15 points) 3546576a03c2c8229175eede8c02f891

2. (15 points) a19d7a52bff83b0e4012d2c766e2f731

3. (15 points) 5a31b6b31f92c8f797505ca26af4b9de

4. (15 points) 857875c031fce47b2d40be0ce3ffd0bf

5. (15 points) dc6054fbe36c8a2bd49b1d05b3b872ee

Challenge 11 – Network Traffic Analysis

Use the provided packet capture to answer these questions about FTP traffic.

(use file: NCL-NetworkTraffic-FTP.pcap or goo.gl/FJv6BS)

1. (20 points) What was the first username/password combination attempt made to log in to the server? ex. 'user/password'

2. (20 points) What software is the FTP server running? (Include name and version)

3. (20 points) What is the first username/password combination that allows for successful authentication? ex. 'user/password'

4. (20 points) What is the first command the user executes on the ftp server?

5. (20 points) What file is deleted from the ftp server?

6. (20 points) What file is uploaded to the ftp server?

7. (20 points) What is the MD5 sum of the uploaded file?

8. (20 points) What file does the anonymous user download?

Challenge 12 – Network Traffic Analysis

Use the provided packet capture to answer these questions about DNS traffic.

(use file: NCL-NetworkTraffic-DNS.pcap or goo.gl/nBSKWE)

1. (20 points) What is the type of the DNS query requested?

2. (20 points) What domain was requested?

3. (20 points) How many items were in the response?

4. (20 points) What is the TTL for all of the records?

5. (20 points) What is the IP address for the "welcome" subdomain?

Challenge 13 – Network Traffic Analysis

Use the provided capture to answer the following questions about a HTTP download.

(use file: NCL-HTTP.pcap or goo.gl/yF1WyN)

1. (20 points) What Linux tool was used to execute a file download?

2. (20 points) What is the name of the web server software that handled the request?

3. (20 points) What IP address initiated request?

4. (20 points) What is the IP address of the server?

5. (20 points) What is the md5sum of the file downloaded?

Challenge 14 – Scanning

Help new recruits understand how Nmap works. Specify your answers in the format -x or -xX or --xxxx.

1. (5 pts) What options would you use to get nmap to print the help summary?

2. (10 pts) What options would you use to set nmap to skip ping host discovery?

3. (10 pts) What options would you use to set nmap to the slowest predefined scan setting?

4. (10 pts) What options would you use to get nmap to use invalid checksums?

5. (10 pts) What options would you use to set nmap to fragment packets?

Coaching Guide

Introduction

This guide contains the following:

Information on how to build a team at your own school for both faculty members and students (because, yes! NCL can be run as a student organization).

A brief description of how I run practices at Pace University and why I run practice this way. Additionally, this section of the guide contains my most important coaching principals.

A list of extremely informal learning objectives that I try to introduce students to before their first competition.

Coaching tips for specific challenges. These tips will not give answers nor provide the steps to solve a problem command by command. They will, instead, show coaches my personal methods for guiding students through self-discovery.

Information you can share with your students on navigating the Cyber Skyline competition environment.

An extremely brief list of some my favorite tools and utilities.

A Few Matters of Business

The views and opinions expressed in this guide are strictly my own and do not reflect the views of the National Cyber League, Cyber Skyline, Pace University, or any of my employers.

Because these challenges are captured from previous National Cyber League competitions, they are under the sole ownership of NCL and Cyber Skyline. It is unethical to share and distribute public answer keys to these challenges. As such, this guide will NOT provide a list of correct answers, but merely the methods to find some of them.

If you need further guidance on any of the challenges found in this guide, please contact me via Twitter, @CryptoKait, or email, cryptokait@gmail.com. I would be more than happy to coach you through a challenge!

How to Build Your Own Team for Students

Your first step should be to reach out to a faculty member you believe will support your endeavor. You're initial goal should be to gain their support and advice. If possible, ask them to act as your coach. Ideally, if they can train you and your soon-to-be-developed team, then you don't have to worry about much more. Connect them with this guide, the NCL Coaches Calls, and NCL's resource materials via their webpage.

Unfortunately, this may not be the case. If your contact can not act as a coach and advisor, you can absolutely make a team all by yourself. It's going to require more work, but it's an achievable goal.

When I first started my graduate degree, I heard a lot about the CCDC team (another collegiate cyber competition), but didn't really hear about NCL. So I went to my advisor and proposed leading an NCL team as well. While my advisor would have offered any resources I needed, I only requested some funding to help make it easier for students to join. From there, I built my dream team. In our very first season, we ranked 11th in our bracket missing the leaderboard by 1 flag.

Another step to build your team is to reach out to all faculty teaching a related course. Request that they offer their students extra credit for participating in the NCL Games. Explain to them the benefits of competing in NCL and how it could relate to their curriculum.

Lastly, if nothing else, you can always invite your friends over, order some pizza, and see what you can do.

The only way you can fail to build a team is to not sign up. A team of one in better than a team of none. Compete in the competition for the first time, learn more about it, and then go to your faculty again with more knowledge and offer your own experience as a guide for the importance of this competition.

If you need help or advice, feel free to reach out to me on Twitter @CryptoKait or via email: cryptokait@gmail.com. I wish you the best and I look forward to seeing your name on the leaderboard very soon!

How I Run Practice

At Pace University, I host an open lab practice. Anyone can come and go as they please. Students who attend more frequently statistically do better in the actual competition. Every week, I cover one new challenge category and one review challenge category. Attendees are welcome to work on challenges with me and the group or work on their own materials. Students most frequently chose to listen to a short 20-minute lecture to introduce new materials and then work by themselves for the remainder of the lab, asking questions when stumped.

One of my biggest rules is that I never answer a question or provide specific directions. I have worked hard to understand the challenges and the road blocks that a competitor might run in to. **I coach by asking the right questions.** This coaches guide will show you how I instruct the various challenges and give you examples of the questions I ask my students to help guide them.

Why Do I Do It This Way?

During the competition, as a coach, you cannot help your students directly. You must learn to give guidance without telling them what to do. You will also need to work with your students to teach them to accept this kind of guidance. I receive a lot of pushback from students the first time I try to help them this way, but I truly believe in this method.

Teaching students to work through their own roadblocks without help is much more useful than telling them what to do. Sure, if you help them that way, they will know what to do if they run into that specific problem, but what if they run into something different? How will they learn to troubleshoot this type of issue if you do not train them?

Learning Objectives

The following is my informal list of the topics I attempt to cover with my students before they begin the National Cyber League Games. These are the foundational skills they will need to navigate the competition without learning challenge by challenge. This is not a comprehensive list. This is only what I attempt to cover at a very introductory level before the first competition. The goal should be to create familiarity over mastery so the student can explore and develop their own mastery during the competition.

My List of Super Informal Learning Objectives

1. Building Virtual Machines
   1.1. Win7
   1.2. Kali-Linux

2. Open Source Intelligence
   2.1. Threat Intel
      2.1.1. Google It!
   2.2. Email Header
      2.2.1. Easy Random Skill You Probably Already Have!)
   2.3. Metadata
      2.3.1. Viewing and Extracting Metadata
   2.4. Certificate Request
      2.4.1. How to Handle an Unknown File Extension

3. Cryptography
   3.1. Numeric-based Crypto
      3.1.1. Binary
      3.1.2. Octal
      3.1.3. Decimal
      3.1.4. Hexadecimal
      3.1.5. Alphanumeric
      3.1.6. Base-64
   3.2. Historical Cryptography
      3.2.1. Substitution
         3.2.1.1. Cesarean Shift (Easiest)
         3.2.1.2. Atbash (Reverse Alphabet)
         3.2.1.3. Morse Code (dots and dashes)
         3.2.1.4. Vigenere (recognized by secret word, phrase, key, etc.)
         3.2.1.5. Symbolic Substitution
      3.2.2. Transposition
         3.2.2.1. Columnar
         3.2.2.2. Transposition

4. Log Analysis
   4.1. History
      4.1.1. Having the right tool
      4.1.2. How to Handle an Unknown File Extension
   4.2. NGNIX
      4.2.1. Use What You Know! (Format data using Excel if that's all you know!)

5. Password Cracking
   5.1. Having the right tool
      5.1.1. Cain
      5.1.2. John the Ripper
      5.1.3. Many Many Many options
   5.2. Using a Pre-made Wordlist
   5.3. Creating an Enumerated Wordlist
      5.3.1. Use What You Know! (Format data using Excel if that's all you know!)
      5.3.2. Crunch Wordlist Generator
   5.4. Creating a Wordlist Using a Database.

6. Network Traffic Analysis
   6.1. Having the right tool
      6.1.1. Introduction to Wireshark
      6.1.2. Introduction to Network Miner

7. Wireless Access Exploitation
   7.1. Having the right tool.
      7.1.1. Introduction to Wireshark
      7.1.2. Introduction to Aircrack-ng

8. Scanning
   8.1. Having the right tool.
      8.1.1. Introduction to Nmap
      8.1.2. Introduction to WPScan

9. Linux Command Line

10. PowerShell

Challenge 01 – Open Source

Answer the following questions about security issues.

1. (25 points) What is the CVE of the original POODLE attack?
2. (25 points) What version of VSFTPD contained the smiley face backdoor?
3. (25 points) What was the first 1.0.1 version of OpenSSL that was NOT vulnerable to heartbleed?
4. (25 points) What was the original RFC number that described Telnet?
5. (25 points) How large (in bytes) was the SQL Slammer worm?
6. (25 points) Samy is my…

Kait's Coaching Tips:

The first thing you should have your students do is to have them define "Open Source Intelligence" (the category name) also known as OSINT. While answers will vary, the underlying message should be that it's data that can be collected from publicly available sources.

After they understand the information out there is publicly available, ask them how they would find out how many cups are in a gallon or how far it is to Mars? Hopefully they will answer that they just "Google it."

"Just Google It" is my publicly proposed alternative title for the OSINT section of NCL. This section is based entirely on security trivia or easily researched skills. Tell them this section should be low stress and is the BEST place to start for the person brand new to InfoSec.

Notes: Sometimes, they make some especially hard OSINT trivia challenges. Make sure your students know that not being able to find the specific answer NCL is looking for does not make them dumb or incapable. Sometimes, things are just meant to be difficult. If you get stuck for too long, just move on.

Challenge 02 – Open Source

We have intercepted an email sent between hackers. See what you can find out. (use file: NCL-OpenSource-EmailHeader.txt or goo.gl/8Z4rPc)

1. (15 points) What is the recipient's email address?
2. (15 points) What is the sender's email address?
3. (15 points) What IP address retrieves the email?
4. (15 points) What is the content type of the message?
5. (15 points) What version of MIME is being used?
6. (15 points) What day of the week was the message received?

Kait's Coaching Tips:

Students should be told to look to the category and challenge names for clues. In this instance, knowing what an "Email Header" is could prove helpful, although I did not know what it was when I first saw this challenge.

Most of these are relatively easy to find by skimming the image above. During the actual season, I copied and pasted this into a notepad file so I could use "Ctrl+F" to search the document for multiple instances of keywords.

This is a good section to talk about persistence, process of elimination, and navigating the Cyber Skyline competition portal. For example, an inexperienced student might notice the many different IP addresses and not be able to identify the correct one by sight. Let students know that it's ok to try multiple things to learn along the way.

Remember, Cyber Skyline will have a button on the left that will allow you to see all previous attempts. Use this to not waste tries on the same answers more than once.

Challenge 03 – Cryptography *

Our officers have obtained password dumps storing hacker passwords. After obtaining a few plaintext passwords, it appears that they are all encoded using different number bases.

1. (15 points) 01000100 00110001 01110110 00110001 01101110 00110001 01110100 01111001
2. (15 points) 102 060 162 144 063 162 154 100 156 144 163
3. (15 points) 83 107 121 114 105 109
4. (15 points) 0x426174746c334672306e744949
5. (15 points) UGF0aCAwZiBFeGlsZQ==

Kait's Coaching Tips:

This is one of the few times I teach a full lesson before having my students attempt a challenge. For this, introduce them to the concept of numerical cryptography starting with binary (which we all know and recognize). Describe this as base-2. Then discuss base-3 and ask what numbers would be included: 0, 1, and 2. Talk about why 3 is not included in base-3. Move to octal, or base-8, and discuss why it only goes to 7. Following this, discuss decimal, or base-10, which uses all numbers.

This is the tricky part, if something is base-11 or higher, what do we do? We start to use letters to count. Discuss hexadecimal and base64.

Distribute the chart on the following page. Have students learn to use the chart to identify different number bases.

It's at this point, I teach them how to crack these ciphers. My personal technique is to just type the name of the number base "to text" into Google. So, if something was in binary, I would type "binary to text." Sometimes, I also search "to ASCII" the more technical term for the language we can read.

With number-based encryption, I also like to use the following challenge to discuss multiple layers of encryption. For example, if you decrypt a base64 cipher and get a series of 1's and 0's, you should try to decrypt that from binary to text. Example:

MTAxMDEwMCAxMTAxMDAwIDExMDAwMDEgMTExMDEwMCAxMDAwMDAgMTExMDEx
MSAxMTAwMDAxIDExMTAwMTEgMTAwMDAwIDExMTAxMDAgMTEwMTExMSAxMTAxMT
ExIDEwMDAwMCAxMTAxMTAxIDExMTAxMDEgMTEwMDAxMSAxMTAxMDAwIDEwMDAw
MCAxMTEwMTExIDExMDExMTEgMTExMDAxMCAxMTAxMDExIDEwMDAwMQ==

Identifying Numeric Based Encryption

Base-n	Characters Found in Encryption Type
Base-2 (binary)	0,1
Base-3 (ternary)	0,1,2
Base-8 (octal)	0,1,2,3,4,5,6,7
Base-9 (nonary)	0,1,2,3,4,5,6,7,8
Base-10 (decimal)	0,1,2,3,4,5,6,7,8,9 (all numbers)
Base-16 (hexadecimal)	0,1,2,3,4,5,6,7,8,9,a,b,c,d,e,f
Base-36 (alphanumeric)	All numbers and lowercase letters
Base-62 (sexagesimal)	All numbers and all capital and lowercase letters
Base-64	All numbers, capital and lowercase letters, and + and /. (Often ends in "=" or "==" which is padding)

** For some (if not most) of these you will have to change an option to switch between **encryption** and **decryption**. Make sure you have the proper settings selected for your task! **

Challenge 04 – Cryptography *

Our officers have obtained password dumps storing hacker passwords. After obtaining a few plaintext passwords, it appears that some sort of **shift cipher** was used.

1. (20 points) APY-FUVSG-4237
2. (20 points) UJS-ZOPMA-8931

Challenge 05 – Cryptography *

Our officers have obtained password dumps storing hacker passwords. See if you can crack them.

1. (25 points) .. - .----. ... -. --- - - .... --.. . --- ..-. - .... . -.. --- --. .. -. - ....-. .. --. .... - --..-- .. - .----. ... - .... --.. . --- ..-. - ....-. .. --. .... - .. - . - .... . -.. --- --. -. -.-. .-.. -....- ..-. -.-- -... .-- -....- .---- -.... .---- ---..

Challenge 06 – Cryptography *

We have intercepted encrypted messages between hackers. Decipher them and find out what they are doing.

1. (15 points) Hiarmeakn loihsraycggt d
2. (20 points) Tria edemnlray
3. (20 points) I lei edbehiulghviadtrbdnas i

Challenge 07 – Cryptography *

Our officers have obtained an encrypted message. The forensics team was able to find a file that contains the string, "secret" which was used to encrypt the message. Take it from here and obtain the plaintext message.

1. (50 points) Zeu @ctas1 vggsklif sevc cgk? Ltnip'k lxsvf wvhe xjvq tdp frc.

Kait's Coaching Tips:

In reference to Challenges 04-07, I'm going to lump these all together. They all require two basic skills.

(see next page)

1. Reading directions thoroughly for tips and hints.
2. A basic understanding of introductory cryptography.

Why do I say this? Because Challenge 05 declares in the directions that it is a shift cipher. Likewise, Challenge 06 tells you it's a substitution cipher. In the coaches' guide directions above, I bolded these keywords for emphasis, but in the actual competition, they are purposefully not bolded.

This is another section I teach students before I have them start working on challenges.

Here, for sake of brevity, I'm going to pull a Gilderoy Lockhart and say, "For further details, see my published works." (Harry Potter reference, anyone?)

Anyway, I give students two options worth of reading homework. They can either read "The Code Book" by Simon Singh, or they can read my "Introduction to Cryptography" blog, which can be found at https://cryptokait.wordpress.com/2017/12/02/an-introduction-to-cryptography/ or the short link: https://goo.gl/RQye5w

After they have completed the reading of their choice, we will discuss methods of identifying various cryptographic ciphers. I recommend using online utilities while cracking these ciphers.

My personal favorite is a website called Rumkin. This can be found with a quick Google search. Make sure you click the "Cipher Tools" link.

Challenge 08 – PW Cracking *

Officers have obtained password dumps storing hacker passwords. After obtaining a few plaintext passwords, it appears that they overlap with the passwords from the **rockyou** breach.

1. (15 pts) 8549137cd494c22ae87eef3e18a46986
2. (15 pts) 0f96a320a8c0bf7e3f6d375b0d9d3a4c
3. (15 pts) 1a8cb8d148b513dfa1d285077fc4e3fb
4. (15 pts) 22a313110bf5b84c0a58eecc27deaa30
5. (15 pts) e4fd50109f0e40e8c1a895d8e5c71199

Challenge 09 – PW Cracking *

Our officers have obtained password dumps storing hacker passwords. It appears that they are all in the format: "SKY-KAIT-" followed by 4 digits. Can you crack them?

1. (15 points) c38d29e8899455c85ee03d11abbd262b
2. (15 points) ff8f9efad5c9f106ac39e5290d810c91
3. (15 points) 425206344bd204933a38236b715c498f
4. (15 points) ab37c335e51b2855cb5a11ca89041733
5. (15 points) 82dcf30f8c7c8d4f23961f7e0c1d3cee

Challenge 10 – PW Cracking *

Our officers have obtained password dumps storing hacker passwords. It appears that they are all based off of Pokémon. Can you crack them?

1. (15 points) 3546576a03c2c8229175eede8c02f89
2. (15 points) a19d7a52bff83b0e4012d2c766e2f731
3. (15 points) 5a31b6b31f92c8f797505ca26af4b9de
4. (15 points) 857875c031fce47b2d40be0ce3ffd0bf
5. (15 points) dc6054fbe36c8a2bd49b1d05b3b872ee

Kait's Coaching Guide:

For this section, you are going to need to know a bit about password cracking utilities.

(see next page)

First, let's cover some important vocabulary you are going to be using.

> **Hash/Hashing –** in shortest terms, the password is stored on an encryption known as a hash. The process of one-way encryption that is performed to protect a password in storage is called hashing.
> **Dictionary attack** – attempting every entry on a pre-made list.
> **Hybrid attack** – combines dictionary with brute-force by attempting every possible variation of the entries on a pre-made list using common substitution principles or adding leading or trailing numbers, etc.
> **Rainbow-tables** – uses pre-computed hashes.
> **Brute-force** – attempting every possible combination of letters, numbers, and characters.

In NCL, you almost never really need to use **brute-force password attacks**. The most important skill is using the correct **wordlist**. Now usually, a **dictionary attack** is sufficient. Occasionally, you will need to use the same **wordlist** with additional attack parameters to run a **hybrid attack**.

In my experience, there are 3 different wordlist types you will need for the NCL and that's why these three challenges were selected. First, as in Challenge 12, you will need to know how to implement a pre-made wordlist, such as the rockyou wordlist.

Second, as in Challenge 13, you will need to know how to create your own enumerated wordlist. You know that all the passwords will begin with "SKY-PWDS-####". For the brand-new competitor with little kali experience, I recommend using Excel again. Simply put "SKY-PWDS-0000" into cell A1, and then use the autofill feature to increment by one as you continue down column A until you reached "SKY-PWDS-9999". This gives a short list of just 10,000 passwords to attempt which takes only a few minutes.

If you are comfortable attempting to use Kali CLI, then I highly recommend **Crunch Wordlist Generator**. It takes a few seconds and one command to generate the entire list. Much less work than Excel, but as I've stated before, you must do what works for you!

Lastly, as in Challenge 14, you need to be able to generate your own wordlist from a database. I chose this challenge because it was my favorite database to work with.

I started with the names of all Gen-1 Pokémon and ran a dictionary attack. This did not work. I changed gears and ran a hybrid attack. This resulted in the first answer: "Charizard6".

After some additional research, I found this to be his Poke-dex (an index ID) number. I then altered my wordlist to include all generations of Pokémon with their Poke-deck

number and ran a dictionary attack for success. But, how did I alter the database? I used what I knew: Excel. (Can you tell I do this a lot?) Trust your gut. You've got this.

As far as password cracking tools go, there are several choose from. In Kali, **John the Ripper** comes pre-installed. For Windows, I prefer to use **Cain**. It's got a nice GUI, but unfortunately won't always install on all OS without changing firewall permissions. It will work just fine on a Windows 7 virtual machine which is what I use during the competition.

Challenge 11 – Network Traffic Analysis

Use the provided packet capture to answer these questions about FTP traffic.
(use file: NCL-NetworkTraffic-FTP.pcap or goo.gl/FJv6BS)

1. (20 points) What was the first username/password combination attempt made to log in to the server? ex. 'user/password'
2. (20 points) What software is the FTP server running? (Include name and version)
3. (20 points) What is the first username/password combination that allows for successful authentication? ex. 'user/password'
4. (20 points) What is the first command the user executes on the ftp server?
5. (20 points) What file is deleted from the ftp server?
6. (20 points) What file is uploaded to the ftp server?
7. (20 points) What is the MD5 sum of the uploaded file?
8. (20 points) What file does the anonymous user download?

Kait's Coaching Guide:

This is another opportunity for students to work with what may be an unknown file extension. For others, this may be very familiar to classwork they have done. If you Google anything about "**pcap**," you're going to discover a tool called **Wireshark**.

While there is a pretty steep learning curve to Wireshark compared to some of the other utilities we will be using, the challenges selected here were designed to be accessible to someone with little to no exposure to the program.

Some helpful information can include, "What is a pcap or packet capture?" and "What can it capture?" The biggest thing that needs to be understood about Wireshark before attempting this challenge is that you can apply filters to the data. You can ask students to find out what kind of filters can be applied, but most commonly (in NCL), they will need to learn to filter by protocol.

With this file in particular, most of the answers can be found in plaintext under the "Info" column.

That being said, the information can be found even more simply by "Following the TCP stream." While I'm usually a little more cryptic while teaching, this is the one time I will tell students to right click a packet, go down to "Follow" and select "TCP." I do this because the information they find after will ensure that they remember the steps.

Knowing some basic FTP commands will also prove useful, but since the ones used in this pcap are pretty straightforward, a person could get by without them by making some educated guesses.

Challenge 12 – Network Traffic Analysis

Use the provided packet capture to answer these questions about DNS traffic.
(use file: NCL-NetworkTraffic-DNS.pcap or goo.gl/nBSKWE)

1. (20 points) What is the type of the DNS query requested?
2. (20 points) What domain was requested?
3. (20 points) How many items were in the response?
4. (20 points) What is the TTL for all of the records?
5. (20 points) What is the IP address for the "welcome" subdomain?

Kait's Coaching Guide:

Remembering the earlier advice to filer by protocol, if you simply type the challenge category, "DNS" into the filter bar and hit enter, you are going to reduce the amount of packets you are dealing with (down to just two!).

Because you only really need to work with two packets, this is a great time to teach your students about queries and responses as well as the parts of a packet.

Unlike the previous challenge, only the first two questions can be solved by searching the "Info" column. For this challenge, you will need to dig deeper. Notice that highlighting a packet will show various packet details in the middle box. If you click the arrows on the far left, you will see the information expand. Click around for a bit and learn what is available in these expanded views.

If you don't understand the question, try googling keywords to see what they mean. For example, question 4 asks for the TTL. The expanded views will not tell you what the "TTL" is, but you can find the "Time-to-Live" which is what TTL stands for. Little searches like this can go a long way so be sure to try to pick up the vocabulary terms along the way.

Challenge 13 – Network Traffic Analysis

Use the provided capture to answer the following questions about a HTTP download. (use file: NCL-HTTP.pcap or goo.gl/yF1WyN)

1. (20 points) What Linux tool was used to execute a file download?
2. (20 points) What is the name of the web server software that handled the request?
3. (20 points) What IP address initiated request?
4. (20 points) What is the IP address of the server?
5. (20 points) What is the md5sum of the file downloaded?

Kait's Coaching Guide:

Now that your students are getting a little more comfortable with Wireshark, see if they remember to apply the HTTP filter without reminding them. If they don't a gentle reminder will prove helpful by reducing the number of packets from 40 to 2.

Once again, they will need to examine the packet details in depth. At this point, they shouldn't have much trouble working through this challenge. If they are still struggling, loop back through the advice for Challenges 15 and 16.

My favorite resource for learning more about Wireshark is YouTube videos. Additionally, I found the following list of filters especially helpful when I was first starting out:

http://www.lovemytool.com/blog/2010/04/top-10-wireshark-filters-by-chris-greer.html

Challenge 14 – Scanning

Help new recruits understand how Nmap works. Specify your answers in the format -x or -xX or --xxxx.

1. (5 pts) What options would you use to get nmap to print the help summary?
2. (10 pts) What options would you use to set nmap to skip ping host discovery?
3. (10 pts) What options would you use to set nmap to the slowest predefined scan setting?
4. (10 pts) What options would you use to get nmap to use invalid checksums?
5. (10 pts) What options would you use to set nmap to fragment packets?

Kait's Coaching Guide:

This challenge could almost belong in Open Source. I won't spend a long time explaining it, but I did want to discuss nmap in general.

Nmap and Zenmap are almost exactly the same utilities. Nmap uses a CLI and Zenmap uses a GUI. When first starting to use Nmap, students can run templated scans using Zenmap. They can use the foundation commands of Zenmap and alter them to build some of their first Nmap commands.

The best way to learn Nmap is to find an "Nmap Cheat Sheet." There are several freely available online.

Contact

For more information, updated resources, or further questions, contact:

Kaitlyn Bestenheider

www.CryptoKait.wordpress.com

Twitter: @CryptoKait

CryptoKait@gmail.com