2023-2024 GSMST CS Club Cybersecurity Department Syllabus

Anish Goyal (Chief of Competitions)
Bibek Bhattari (CyberDragons Head)
Andrew Zeng (CyberDragons Assistant Head)

Table of Contents

1 Overview

1.1 About Us

Welcome to the 2023-2024 syllabus for GSMST CS Club's cybersecurity department! Our mission is to nurture the next generation of cybersecurity professionals at GSMST. We strive to provide a comprehensive learning experience that covers various aspects of cybersecurity, equipping our members with the knowledge and skills needed to defend against digital attacks and identify and address potential threat vectors.

1.2 Home of the CyberDragons

Our success in various cybersecurity competitions has earned GSMST CS Club cybersecurity the well-deserved nickname "CyberDragons," as it is the alias we use to compete in these competitions. Our dedication and relentless pursuit of knowledge in this ever-evolving field have set us apart from our competition, making us a force to be reckoned with. We take pride in building our members from the ground up, training them to excel at what they do.

1.3 What We Do

1. **Learning and Knowledge Sharing**: CyberDragons hosts weekly workshops and interactive sessions to delve into the world of cybersecurity. We cover a wide range of topics to broaden our members' understanding in both offensive and defensive hacking.
2. **Hands-On Practical Experience**: Theory alone isn't enough in cybersecurity. That's why we organize practical exercises during our weekly meetings that simulate *real-world scenarios* in the hacking industry. This element of interactivity helps develop critical thinking and problem-solving skills for aspiring hackers and cybersecurity professionals.
3. **Our Competitive Edge**: CyberDragons competes in multiple regional and national cybersecurity competitions. With a formidible team of skilled members, we put our expertise to the test. And we are consistently successful, every single time.

1.4 Competitive Opportunities

- CyberPatriot
- picoCTF
- Lockheed Martin's CyberQuest
- US Cyber Challenge: Cyber Quests
- TSA Cybersecurity Event
- NCL Cyber Skyline
- …and many more

2 Weekly Meeting Dates

2.1 Semester I

2.1.1 Welcome to CyberDragons (09/01/2023)

2.1.1.1 Meeting Summary

Our first meeting will start with a brief overview of what GSMST CyberDragons does and a rundown on each major competition we will focus on for the school year. After, we will tell students to install *VMWare Player* on their personal laptops (we will tell them they need their personal laptops days in advance). Next, we will go over CyberDragons applications. To conclude the meeting, we will walk through about *ten* easy vulnerabilities on the Windows 10 qualifying image to show new members how practice images work and how they are scored in real time. We will also emphasize throughout the entire meeting that new members should join the CyberDragons Discord server if they have any questions or need support.

2.1.1.2 CyberDragons Application Requirements

The application deadline is **September 18** at 11:59 PM. This means that members have two and a half weeks to complete the CyberDragons application, starting **September 1**. The requirements are as follows:

- Spend at least six hours on a qualifying image of your choice, and do the best you can. There is no need to email your image results like last year, as the images will be graded live by a remote scoring server (assuming you have an Internet connection). This also means that each applicant's progress can be monitored in real time.
- Complete the short answer questions Google Form.
- Pay $30 or get a fee waiver from Ms. Rachkovsk
- Complete the Team Phi Google Form for free membership (if you are a member of *Girls Who Code*)

As a side note, the point of the qualifying images is to gauge which operating system you enjoy working with, and as a result, all applicants are strongly encouraged to work with more than one of the qualifying images. While it is true that image scores will not be considered in th application, the top *six* scorers will join team Zeta, and the top scorer will receive a prize.

2.1.1.3 Meeting At-A-Glance

- Overview of what CyberDragons does
- Go over how competitions work/which ones we are competing in
- Announce applications and qualifying images
- Demo the Windows 10 qualifying image

2.1.2 CyberPatriot 101 (09/08/2023)

2.1.2.1 Meeting Summary

Our second meeting of the year will show members how to work on CyberPatriot practice images by dividing them into two groups. One group will be focused on solving a GNU/Linux practice image led by Bibek, with the other focused on Windows and led by Andrew. After twenty minutes, members will switch groups to learn more about the other operating system. Essentially, this meeting will expose a lot of new members to using an operating system for more than just casual browsing and work, but since that may be boring for a few of our returning members, we will also be reviewing some command-line basics.

2.1.2.2 Meeting At-A-Glance

- Separate into two halves (GNU/Linux and Windows 10)
- Explore command-line basics in Windows Powershell, Bash, and Command Prompt (CMD)
- Go over common vulnerabilities seen in practice images for both operating systems
  - This is basically expanding on the intuition they will gain from doing the qualifying images
  - But of course, since everyone procrastinates, there is a great chance that *nobody* would have started the qualifying images by this point. And therefore, this meeting will be helpful for newcomers who would still need a foundation of things to look out for while doing the qualifying images

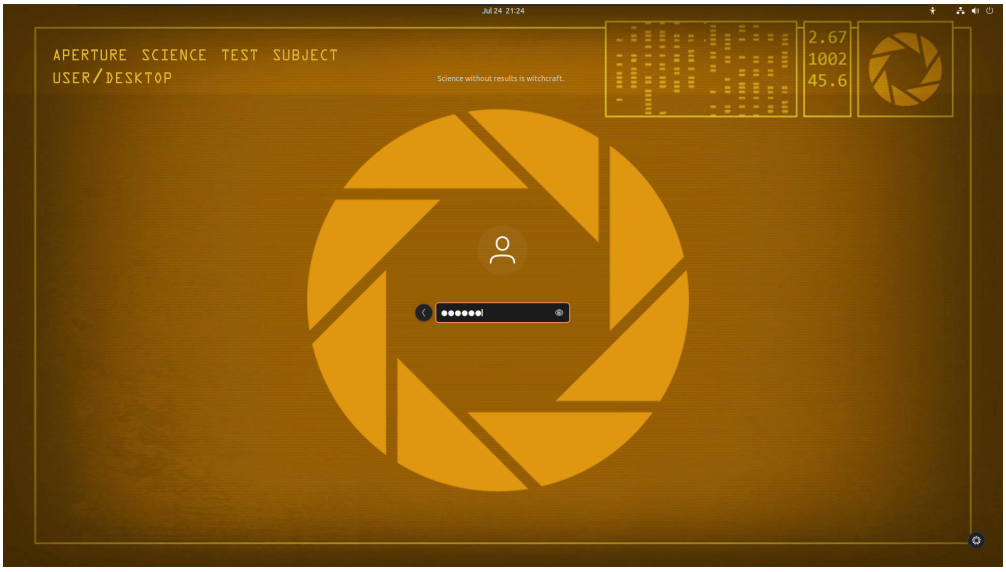

Figure 1: Login screen for the Ubuntu qualifying image

2.1.3 Over the Wire (09/15/2023)

2.1.3.1 Meeting Summary

In this meeting, students will be divided into teams with 2-4 people per team, with each team *randomly chosen*. Each team will compete to see who can reach the highest level on the online wargame Over The Wire. This meeting aims to polish new members' command-line skills and expose them to essential commands such as `SSH`, `find`, `grep`, and much more. Throughout the entire competition, CyberDragons officers will be available to help any members that are stuck without giving them the answers outright. Members may also use the Internet as an **educational tool** if they are stuck or have questions, but directly searching the answers is strictly forbidden. At the end, the team with the highest level gets free snacks.

2.1.3.2 Meeting At-A-Glance

- Mini CTF (Capture the Flag)-and-terminal-based competition
- Split up into random groups
- Winner incentive (snacks)

2.1.4 CyberDragons Inductions (09/22/2023)

2.1.4.1 Meeting Summary

As the official deadline for CyberDragons applications has passed, it is now time to induct new members into CyberDragons and announce the CyberPatriot team roster. Additionally, the highest-scoring individual on the qualifying images will receive a special award. For the rest of the meeting, CyberPatriot teams will get together and discuss the qualifying images and upcoming practice round with each other. Returning members are free to present personal anecdotes about their experiences in CyberPatriot. To end the meeting, everyone will reconvene to hear about the logistics of the CyberPatriot official practice round that will be held the week after.

2.1.4.2 Meeting At-A-Glance

- Celebrate the individual with the most discovered vulnerabilties
- Divide into groups for mostly asynchronous/networking time
- Meet as a collective to discuss logistics for the practice round to conclude.

2.1.5 Official Practice Round (10/13/2023)

2.1.5.1 Meeting Summary

In preparation for our CyberPatriot competitions, members will collaborate with their teams to complete the official practice round and practice creating writeups in a Google Doc to familiarize themselves with the norms of CyberDragons. This meeting will allow members to experiment with an official CyberPatriot image (developing shell scripts and README parsers) or work around thier chosen system.

2.1.5.2 Meeting At-A-Glance

- Run through official CyberPatriot images
  - The practice round images will be *ten times easier* than the qualifying images. Therefore, we expect everyone to ace the images and this round should serve as a morale booster.
- Gain experience in working with a team and documenting progress

2.1.6 Review Writeups and Qualifier Images (10/20/2023)

2.1.6.1 Meeting Summary

With the first official round of CyberPatriot in a day, this meeting will allow students to reflect on any practice completed during their time in CyberPatriot. The answer keys for the practice images will be released during this meeting for members to look at with their teams. The officers and returning members will be present to assist any burning questions about the qualifying images and CyberPatriot in general that newer members may have. It is expected that CyberDragons members review the forensic questions and vulnerabilities within the qualifying and practice round images to strengthen their team. It is also *highly recommended* for CyberDragons members to review writeups for the practice round and rounds from previous years.

2.1.6.2 Meeting At-A-Glance

- Reflect on completed CyberPatriot practice
- Officers and returning members assist with questions
- Review qualifying images and improve team structure
- Utilize answer keys for the qualifying images

2.1.7 Terminal Teasers (10/27/2023)

2.1.7.1 Meeting Summary

This workshop will begin with a quick introduction to the Bash syntax; once the introduction ends, every student will be given a reference sheet to refer to if needed. Students will randomly break into groups of three and be given a virtual machine with multiple forensic questions. Each question will be only solvable through a Bash script. Students will be given a piece of a riddle for every question solved. The first team to solve all queries and determine the correct answer to the riddle will be awarded a prize.

2.1.7.2 Meeting At-A-Glance

- Students form groups of three and receive virtual machines with forensic questions with a focus on using Bash scripts
- Each solved question provides a riddle piece, and the first team to solve the riddle wins a prize

2.1.8 Last Meeting Before Round II (11/03/2023)

2.1.8.1 Meeting Summary

With the second round of CyberPatriot on the following day, this meeting will be utilized to reflect and review what we did in the first round, compiling results from both the writeups and reflections written from the conclusion of the first competition. This meeting will be more hands-off, prompting more self-reflection and improvements instead of an informative one.

2.1.8.2 Meeting At-A-Glance

- Members review and reflect what they plan to do differently in the second round that they did not do in the first round

As a side note, round II of CyberPatriot this year falls on the **November SAT** date. So, we'll tell everyone not to sign up for the November SAT ahead of time.

2.1.9 Powershell Sherlock Holmes-esque Crime (11/10/2023)

2.1.9.1 Meeting Summary

The interactive workshop begins with a brief introduction to PowerShell and its importance in cybersecurity. Following this, students will be immersed in a crime-solving scenario involving a virtual machine, enabling them to actively apply PowerShell and develop a deeper understanding of the tool while sparking their interest. The meeting aims to familiarize students with PowerShell's practical applications and promote engagement in the subject.

2.1.9.2 Meeting At-A-Glance

- Introduction to fundamentals of PowerShell:
  - Syntax
  - CMDLets
  - PowerShell objects and why everything is an object
  - Pros of Powershell, how it can be used to alter the system
- Reference Materials for people to review and use when working through a Powershell interactive challenge
- Model it similar to a Crime Solving Case (centered around Sherlock Holmes)

2.1.10 Encryption/Decryption Murder Mystery (11/17/23)

2.1.10.1 Meeting Summary

In this workshop, participants will receive a concise introduction to the tools available for decrypting hidden messages. Next, they will collaborate in randomized teams of 2-4, engaging in a scavenger hunt-style game that will take them through the main tower of GSMST. They will decipher clues to uncover the criminal's identity as they progress through the game. The activity may offer multiple pathways, allowing students to explore different routes (and not cheat off people further ahead) and enhance their problem-solving skills.

2.1.10.2 Meeting At-A-Glance

- A murder mystery where students physically walk around the building
- Students use encryption and decryption techniques to decipher clues and progress through the game

2.1.11 Computer Forensics (12/01/2023)

2.1.11.1 Meeting Summary

This meeting will focus on how to approach forensic questions for the upcoming state round. We will ask new members to share what has worked for them during previous rounds and then have our veteran members share their tactics. In addition, we will have our cybersecurity heads will share their tactics. Once everyone is done sharing, we will review some practice forensic questions and solve them in groups.

2.1.11.2 Meeting At-A-Glance

- Equip CyberDragons members to solve forensics questions in anticipation for the state round

2.2 Semester II

2.2.1 Welcome Back & Introduction to Offensive Security (01/12/2024)

2.2.1.1 Meeting Summary

In this meeting, students will be introduced to the two major competitions we will focus on this semester: Lockheed Martin CyberQuest and PicoCTF. With the focus of this semester being CTFs, We will also be going over a brief explanation of what offensive security is, the various techniques and types, and how it differs from what students learned last semester. We will also do a live demo of some CTF problems after encouraging members to try them first.

2.2.1.2 Meeting At-A-Glance

- Welcome back + here is information on competitions for this semester
- Introduction to offensive security types (Web exploitation, reverse engineering, *etc.*)

2.2.2 Final Review Before Semifinals

2.2.2.1 Meeting Summary

This meeting will be celebratory in nature of the various team accomplishments in CyberPatriot while reviewing and reminding them about the review materials to assist them for the (probably) final competition. This meeting may also reflect upon the entire 2023-2024 CyberDragons CyberPatriot experience.

2.2.2.2 Meeting At-A-Glance

- Celebrate CyberDragons' CyberPatriot accomplishments
- Review for the semifinals round

2.2.3 Web Exploitation (01/19/2024)

2.2.3.1 Meeting Summary

This meeting will be going over the basics of Web Hacking, Starting with OWASP 10 vulnerabilities which consist of commonly found web applications security vulnerabilities, to techniques such as SQL injections, Cross Site (XSS) Scripting, and Directory Traversal. In addition to common techniques, we will also be going over using BurpSuite, a commonly used tool for web exploitation. We will end this meeting by having students apply what they learn through interactive websites like HackTheBox and HackThisSite.

2.2.3.2 Meeting At-A-Glance

- Introduction to OWASP Top 10 vulnerabilities and common web application security issues
- Learn SQL injections, Cross-Site Scripting (XSS), and Directory Traversal.
- Familiarization with BurpSuite, a widely used web exploitation tool.
- Apply knowledge on interactive platforms like HackTheBox and HackThisSite to gain practical experience.

2.2.4 Command-line Network Penetration (02/09/2024)

2.2.4.1 Meeting Summary

In this meeting, members will use network tools such as `netcat` and `nmap` to exploit the vulnerabilities of a network or server through the shell. Additionally, members will learn how to use `aircrack-ng` and Wireshark to probe into Wi-Fi networks and listen and monitor network traffic in real time. First, we will review basic terminal commands that were touched on in previous meetings, as well as how to navigate filesystems through the terminal. Then, we will focus on network penetration through the use of these tools. Finally, we will focus on practical exercises in hacking servers on HackTheBox.

2.2.4.2 Meeting At-A-Glance

- Recap basic terminal commands and filesystem navigation to prepare for network penetration
- Use netcat and nmap to identify and exploit network/server vulnerabilities through the shell. Learn to probe and monitor Wi-Fi networks using `aircrack-ng` and Wireshark in real-time.

2.2.5 Hacking Tools (02/23/2024)

2.2.5.1 Meeting Summary

In this workshop, members will learn how to use common hacking tools such as Metasploit, a versatile penetration testing framework, GDB (GNU Debugger) for program analysis, SQLMap to uncover web application vulnerabilities, John The Ripper for advanced password cracking, Hydra to conduct password attacks, Hashcat for cracking hashed passwords, and Radare2, an open-source reverse engineering framework for CTF competitions. Members will be given a problem set where they have to use these tools, or combinations of them, to solve as many problems as they can. They can work individually or as a team.

2.2.5.2 Meeting At-A-Glance

- Learn how to use various hacking tools like Metasploit, GDB, SQLMap, John The Ripper, Hydra, Hashcat, and Radare2.
- Members will receive a problem set and use the tools to solve vulnerabilities and challenges
- Gain hands-on experience with tools used in penetration testing, password cracking, web app vulnerability discovery, and reverse engineering
- Engage in problem-solving similar to CTF competitions to apply acquired skills effectively

2.2.6 Steganographic Art Gallery (03/01/2024)

2.2.6.1 Meeting Summary

Students will be introduced to steganography as an art of concealing information through digital media files and byte/color channel manipulation. We will expose our members to various steganography techniques and have them create their own hidden messages through (school appropriate) images. Towards the end of the meeting, we will have a steganography "art gallery," where members rotate to a new device clockwise every minute to take a look at that at that laptop's steganographic images and the creator's instructions on how to decode them. And then they attempt to decode the images for each computer, hopefully successfully most of the time!

2.2.6.2 Meeting At-A-Glance

- Explore the art of concealing information within digital media files using steganography techniques.
- Members will create their own hidden messages within school-appropriate images with instructions on how to decode them
- Rotate through laptops, viewing and successfully decoding steganographic images created by fellow members
- Foster an enjoyable environment for learning steganography through practical application and peer interaction

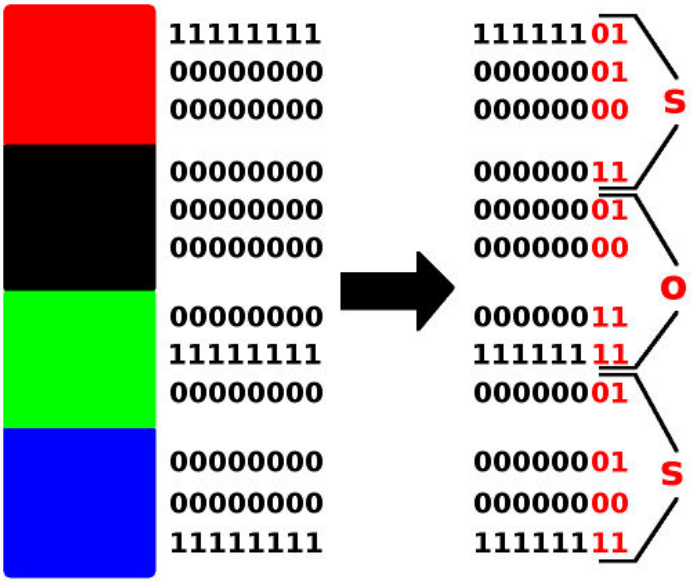

Figure 2: An example of Least Significant Bit steganography

2.2.7 Review Session for Lockheed Martin CyberQuest and picoCTF (03/08/2024)

2.2.7.1 Meeting Summary

This meeting will consist of a review of the last four meetings in preparation for next week's picoCTF competition. Once review is over, students will be given a Kahoot to test their knowledge and highlight any parts they lack. For the excess time, students will break themselves into groups and work on some practice problems on picoGym to prepare for actual CTF questions.

2.2.7.2 Meeting At-A-Glance

- Engage members with a Kahoot to test their knowledge and identify areas that need improvement
- Utilize excess time for hands-on learning on

2.2.8 picoCTF Competition Meeting (03/22/2024)

2.2.8.1 Meeting Summary

Students work on US Cyber Challenge: Cyber Quests or picoCTF asynchronously with their teams.

2.2.8.2 Meeting At-A-Glance

- Work on picoCTF or Cyber Quests

2.2.9 picoCTF Award Ceremony (03/29/2024)

2.2.9.1 Meeting Summary

This meeting will start with an award ceremony honoring our top three highest achieving teams (If there are less than six teams, we will reduce the ceremony to award to the top team only). After the award ceremony, there will be a group discussion about any pitfalls and traps that participating teams encountered and any helpful strategies that helped them succeed in this year's competition. Once the group discussion is over, the heads will review any CTF questions members have.

2.2.9.2 Meeting At-A-Glance

- Award top-performing team(s) in picoCTF
- Review strategies and pitfalls
- Go over questions

2.2.10 Chill

2.2.10.1 Meeting Summary

We are planning to organize an end-of-year party to celebrate our accomplishments during this school year. We will also discuss our future goals and aspirations for the upcoming years. Lastly, we will bid farewell to our senior club members and spend the remaining time unwinding.

2.2.10.2 Meeting At-A-Glance

- Celebrate accomplishments
- Talk about the future of CyberDragons
- Relax