TEACHING SOFTWARE SECURTY TO NOVICES WITH USER FRIENDLY ARMITAGE

CHRISTOPHER MORALES-GONZALEZ
MATTHEW HARPER
XINWEN FU

INTRODUCTION

INTRODUCTION

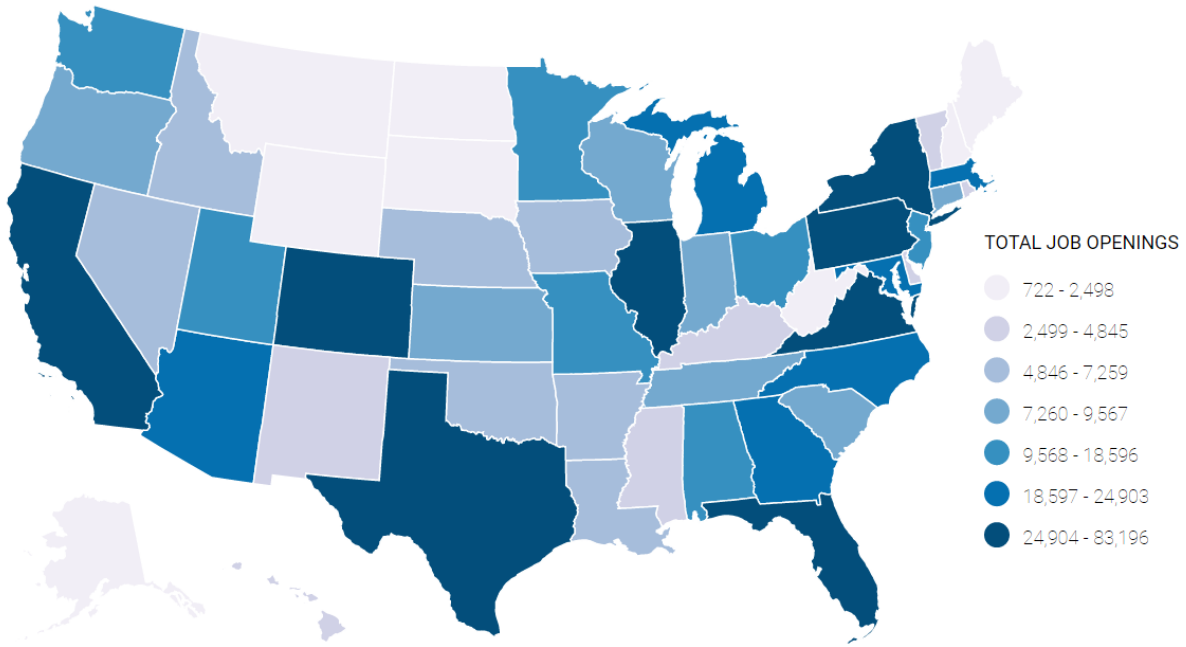
PREVALENCE OF CYBERCRIME

- Cybercrime becoming increasingly more common.
- Reported increase of 600% due to COVID-19
- Recent attacks
  - Ransomware attack on Costa Rica's government
  - Data breach against Saudi Aramco

INTRODUCTION

CYBERSECURITY JOB FULFILLMENT SHORTAGE

- Reported that there are over 700,000 cybersecurity job openings in the US alone in 2022.



INTRODUCTION

WHAT'S THE PROBLEM

- Lack of high-quality educational material for *novices*.
- The realm of cybersecurity is massive.
  - Too many options can often leave students flustered and discouraged.
- Software security typically requires C and assembly language to understand the advanced concepts such as the buffer overflow attack.
  - These are not novice-friendly.

INTRODUCTION

WHAT ARE WE TRYING TO DO?

- Creating educational material that will teach the *basics* of software security to *novices*.
- This material was created to be practical, realistic, modern, accurate and intuitive.

SOFTWARE SECURITY MODULE

1) CYBER ATTACK CYCLE
2) INTRODUCTION TO METASPLOIT AND ARMITAGE
3) DEMONSTRATION OF CYBER ATTACK CYCLE

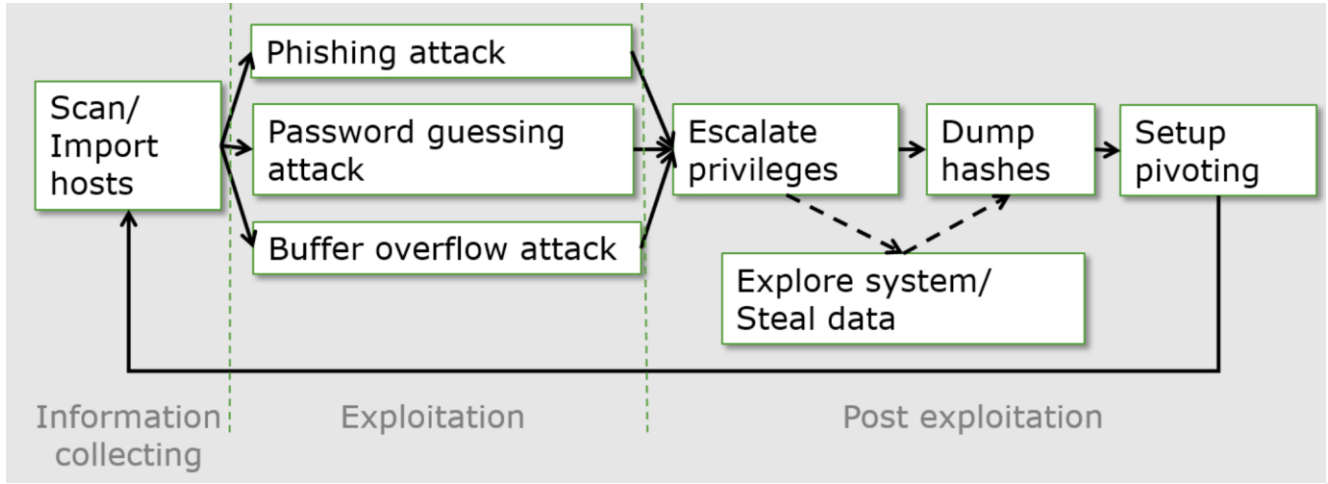
SOFTWARE SECURITY MODULE

CYBER ATTACK CYCLE

SOFTWARE SECURITY MODULE

CYBER ATTACK CYCLE

- To mitigate and defend against attacks, we must be able to think like an attacker.
- Different phases of a cyber attack:
  - Information Collecting
  - Exploitation
  - Post Exploitation



SOFTWARE SECURITY MODULE

CYBER ATTACK CYCLE – INFORMATION COLLECTING

- An attacker needs to gather information to attack their target effectively.
- Common method: Port Scanning
  - Can discover services running on the target and craft an attack.
  - If run on a *range* of addresses, they can also discover additional targets.

SOFTWARE SECURITY MODULE

CYBER ATTACK CYCLE – EXPLOITATION

- With this information gathered, the attacker can now begin to run exploits.
- Typically done via a remote attack.
- Some examples:
  - Brute force attack: Attacker continuously try to *guess* credentials.
  - Buffer overflow: Attacker injects malicious code into a target server remotely.
  - Social Engineering: Attacker sends an email containing a piece of malware that an unsuspecting party downloads and runs.
- *Goal:* The attacker wants to gain *some* access to the target machine.

SOFTWARE SECURITY MODULE

CYBER ATTACK CYCLE – POST-EXPLOITATION

- Once access is gained, there are a myriad of ways an attacker can cause more damage.
- Common example (Password cracking):
  - Privilege Escalation: Attacker will try to become the *root* user to have full control of the machine
  - Hash dump: Once *root*, the attacker can get the password hashes file (*shadow*).
  - Password cracking: The attacker can then use a tool like "John the Ripper" to get the passwords.
- Another common example:
  - Persistent access via a backdoor

SOFTWARE SECURITY MODULE

INTRODUCTION TO METASPLOIT AND ARMITAGE

SOFTWARE SECURITY MODULE

INTRODUCTION TO METASPLOIT AND ARMITAGE - METASPLOIT

- Commonly used penetration testing tool by cybersecurity professionals.
- Can perform entire exploits or specific portions of one.
- **No prior knowledge of how the attacks work required.**
- Pure Metasploit is command-line only.
  - This is error-prone and non-intuitive; would prove to be detrimental to a student's learning experience.
- Therefore, we need a solution.

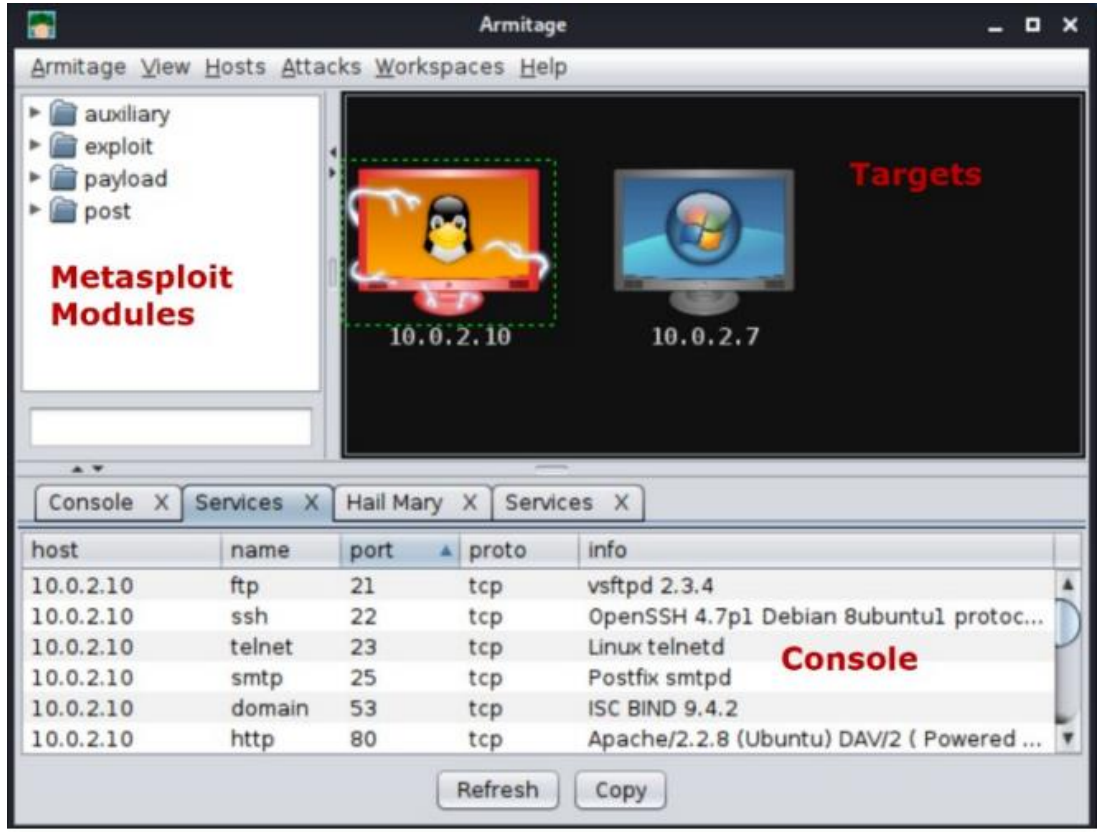
SOFTWARE SECURITY MODULE

INTRODUCTION TO METASPLOIT AND ARMITAGE - ARMITAGE

- Provides an intuitive Graphical User Interface (GUI) for Metasploit.
- Items chosen in the GUI will be mapped to Metasploit commands.
  - Removes requirement to remember syntax, flags, parameters, etc.
- Ability to perform various port scans for *information gathering*.
- Has “find attacks” feature to find an exploit for a vulnerability.
- Contains a variety of *post-exploitation* modules.
- Using this will improve efficiency and learning experience to further inspire students to explore more.

SOFTWARE SECURITY MODULE

INTRODUCTION TO METASPLOIT AND ARMITAGE - ARMITAGE



SOFTWARE SECURITY MODULE

DEMONSTRATION OF CYBER ATTACK CYCLE

SOFTWARE SECURITY MODULE

DEMONSTRATION OF CYBER ATTACK CYCLE - SETUP

- Oracle's VirtualBox hypervisor with "NatNetwork" network type.
- Virtual Machines:
  - Metasploitable 2: Intentionally vulnerable machine made for *safe* practice.
  - Kali Linux: *Popular* cybersecurity learning platform for penetration testing.
  - Windows 10: We preconfigure this machine to disable:
    - *Windows Defender Firewall* settings
    - *Virus and Threat Protection* settings
    - *Real-Time Protection* security functionality

SOFTWARE SECURITY MODULE

DEMONSTRATION OF CYBER ATTACK CYCLE - SETUP

- *Vchat:*
  - We developed our own *novel* vulnerable chat server in C.
  - Contains specific vulnerabilities for penetration testing purposes.
  - Showcases that working services such as a chat server can be problematic - even on the *latest* Operating Systems.
  - Allows for future modules
- Metasploit Modules:
  - We've developed our own custom Metasploit modules to attack *vchat*
    - Buffer overflow module
    - DoS module
    - DDoS module

SOFTWARE SECURITY MODULE

DEMONSTRATION OF CYBER ATTACK CYCLE - DEMONSTRATION

- Understanding theory is important, but *intuitive* hands-on labs is crucial to the *reinforcement* of what they learned.
- Shows that the content can be *directly applied* into a *real-world* situation and the consequences of poor software security.
- All stages of the cyber attack cycle are performed.
  - First on the Metasploitable machine
  - Then, on vchat on the Windows 10 Machine

SOFTWARE SECURITY MODULE

DEMONSTRATION OF CYBER ATTACK CYCLE - DEMONSTRATION

- Armitage on Kali Linux will perform msf or nmap scans against Metasploitable (*Information collection*).
- Armitage will “find attacks” on Metasploitable.
- Attacker will run the “unreal_ircd_3281_backdoor”. (*Exploitation*)
- Attacker will use Armitage’s post-exploitation modules to “dump the hash” and use John the Ripper to obtain user credentials. (*Post-exploitation*)

SOFTWARE SECURITY MODULE

DEMONSTRATION OF CYBER ATTACK CYCLE - DEMONSTRATION

- An attack against *vchat* on the Windows 10 VM is very similar.
- Armitage will use a msf or nmap scan to indicate vchat's port, 9999, is open. (*Information collection*)
- Will use three modules for three separate attacks (*Exploitation*).
  - Double-click the modules on the Armitage GUI and follow intuitive prompts.
- The buffer overflow module will allow us to perform some *post-exploitation* techniques such as keystroke logging and camera streaming.

SOFTWARE SECURITY MODULE

HANDS-ON LABS

SOFTWARE SECURITY MODULE

HANDS-ON LABS

- *Hands-on 1:* Hack into Metasploitable through unreal_ircd_3281_backdoor.
- *Hands-on 2:* Hack into Windows 10 using buffer overflow using premade Metasploit module.
- *Hands-on 3:* Capture a screenshot through Metasploit meterpreter payload.
- *Hands-on 4:* Perform keystroke logging through Metasploit meterpreter payload.
- *Hands-on 5:* Deploy persistent backdoor
- *Hands-on 6:* Buffer overflow attack via Python code. Intentionally designed for students who are familiar with Python and want to investigate the buffer overflows, DoS and DDoS mechanisms.

EVALUATION

CLASS SETUP

LEARNING EFFECTIVENESS

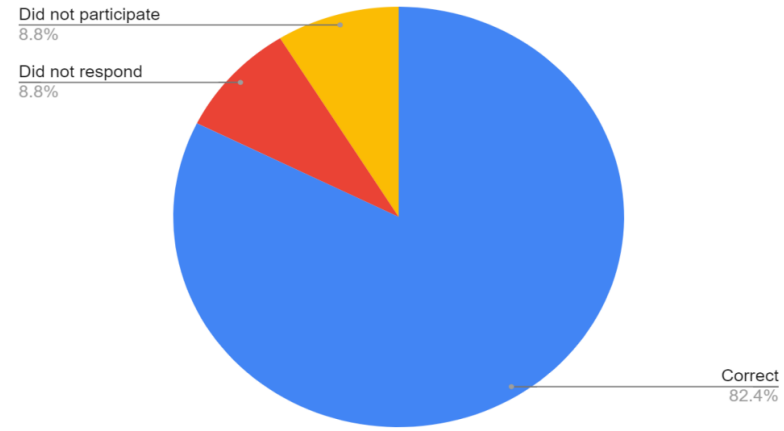
EVALUATION

CLASS SETUP

- We had run a GenCyber cybersecurity camp for 40 high school students from grades 9 – 12 in 2022 summer.
- During the camp, after running through our software security module, the Hands-on labs were given to the students.
- At the end of the camp, we ran a Capture-the-Flag (CTF) competition that contained a software security challenge.
- Students were encouraged to form teams of up to two to promote collaboration and develop crucial communication skills.
- Submissions done through Google Forms

EVALUATION

LEARNING EFFECTIVENESS



- TAs had helped students during the Hands-on Labs.
  - All camp students were able to finish Hands-on Labs 1-5.
  - Some were able to finish Hands-on Lab 6.
- On the day of the CTF
  - 34 students attended and did not have help from TAs.
  - The software security question (hacking Metasploitable then dumping and cracking password hashes) was one of the most successful flags in terms of correctness.

CONCLUSION

CONCLUSION

- Presented our methodology and module for teaching the basics of software security to *novice* cybersecurity students.
- First, explained the cyber attack cycle.
- Then, introduced Metasploit and Armitage
- Finally, we provided a live demonstration of how a cyber crime can be carried out.
- We prove the effectiveness by teaching high school students and analyze the results of a CTF and hands-on labs.

THANK YOU!

REFERENCES

- [1] “2022 cyber security statistics trends and data,” PurpleSec, 18- Jul-2022. [Online]. Available: https://purplesec.us/resources/cyber-securitystatistics/#Cybercrime.
- [2] Cybersecurity Supply/Demand Heat Map. [Online]. Available: https://www.cyberseek.org/heatmap.html.
- [3] K. C. Williams and C. C. Williams , “Five key Ingredients for Improving Student Motivation ,” Research in Higher Education Journal, Aug-2011. [Online]. Available: http://aabri.com/manuscripts/11834.pdf.
- [4] X. Fu, “GenCyber”, 25-May-2021. [Online]. Available: https://github.com/xinwenfu/GenCyber.

REFERENCES

- [5] X. Fu, “Vulnerable Chat Server (vchat),” Malware Analysis vchat, 31-May-2022. [Online]. Available: https://github.com/xinwenfu/Malware-Analysis/tree/main/vchat.
- [6] M. Harper and X. Fu, Making DoS and DDoS Metasploit modules. [Online]. Available: https://github.com/DaintyJet/Making-Dos-DDoS-Metasploit-Module-Vulnserver.