Course Overview

CS 450/650

Objectives

- Overview of Course topics, assignments, relevance and logistics
- Discuss the relevant ethical issues associated with computer security
- Define computer security
- Discuss common threats and recent computer crimes that have been committed
- List and discuss recent trends in computer security
- Describe common avenues of attacks
- Describe approaches to computer security
- Get set up for future class meetings!

Cybersecurity Ethics

Ethics

- Commonly defined as a set of moral principles that guides an individual's or group's behavior
  - Information security efforts frequently involve trusting people to keep secrets that could cause harm if revealed
  - Trust is a foundational element in the people side of security
  - Trust is built upon a code of ethics, a norm that allows everyone to understand expectations and responsibilities

Why it's important

- The study of cybersecurity requires understanding of tools and techniques used in hacking, cybercrime and cyberwarfare
- This class will introduce several of these tools and techniques and allow you to experiment with them in a controlled, virtual machine environment
- Using these tools and techniques outside of a strictly controlled environment is unethical and potentially illegal
- Using these tools and techniques outside of a strictly controlled environment has the potential to cause serious harm to you and others

When to experiment with hacking tools

- When using these tools insure they are used in a strictly controlled environment
  - Virtual machines and or test networks
- If others are involved, they must be informed of the risks and provide explicit consent to participate
  - It's not okay to try to hack a neighbor or coffee shop WiFi network
  - It's not okay to scan public websites to look for vulnerabilities, without their knowledge and permission
  - It is okay to setup your own vulnerable machines and sites in a controlled environment and experiment with them.

General Cyber Ethics

- To be considered a professional in cybersecurity, one must perform ethically
- The ACM Code of Ethics and Professional Conduct provides an excellent example of the rules we should follow: https://ethics.acm.org/code-of-ethics/
- The following points from The ACM Code of Ethics and Professional Conduct are most important during our studies
  - 1.2 Avoid harm
  - 1.3 Be honest and trustworthy
  - 1.6 Respect privacy
  - 1.7 Honor confidentiality

Course Overview

Class Strategy

- Theory - forms the foundation for our work
- Practice – labs and assignments where we apply the theory
- Current examples of these topics in practice

Course Topics

To Mid-term	To Final Exam
Security Trends	Cloud Computing and IoT Security
Computer Security Concepts	Secure Software Development
The Role of People in Security	Web Application Security
Cryptographic Concepts	Security Tools and Techniques
Authentication and Remote Access	Incident Response
Types of Attacks and Malware	Penetration Testing
System Hardening and Baselines	Digital Forensics
Physical Security	

Syllabus and Textbook

- Find all course materials and most current syllabus in Canvas.
- Text is required
  - *Wm. Arthur Conklin, Greg White, Chuck Cothren, Roger L. Davis, Dwayne Williams. "Principles of Computer Security: CompTIA Security+ and Beyond, Sixth Edition (Exam SY0-601)*
  - Available online from UNR library
  - Excellent overview of most cybersecurity topics
- Chapters from 2 other books are linked in modules
- Quizzes will be from text readings

Software

- Virtual Machine Hypervisor
  - Oracle VirtualBox or equivalent
    - https://www.virtualbox.org/
- Labtainers VirtualBox VM Appliance
  - https://nps.edu/web/c3o/virtual-machine-images
- NCR or other virtual machines as required for in-class work

Assignments

- Generally one per week
  - Hands-on using Labtainer or other tools
  - Case studies

Quizzes

- 15 question quiz on each chapter
- Can be taken any time before the due date on Canvas
- ONE attempt 20 minute time limit

Projects

- Final Project
  - Task-based in a virtual environment
- Graduate (additional project for those enrolled in CS 650)
  - Research based project
- Requirement details in Canvas

Grading and Schedule

- Current schedule and grades always available in Canvas

Course Relevance and Context

- Fills in topics not covered in other CS classes
- Great preparation for Security+ certification
- Covering how attacks can happen and how to defend

Not a Cybersecurity Major?

- Data Analyst is one of the hottest Cybersecurity careers.
- Developers can use this information to bake security into whatever you do.
  - Secure Development Life Cycle
- If you have trouble with the technology, work with a classmate
  - Just submit your own work

Take Notes!

- Hands-on demonstrations in class will make assignments easier, but you have to take notes

The Punchline

- Fundamentals, standards and recommended practices form the foundation to build defenses.

- **Class Intro Poll - https://www.questionpro.com/a/TakeSurvey?tt=37rdbb8Y%2BoPTFneCZs3WPG943ob4ZyMj**

Chapter 1

Computer Security Defined

- “ Measures and controls that ensure confidentiality, integrity, and availability of information system assets including hardware, software, firmware, and information being *processed, stored, and communicated**”
  - *also known as in use, at rest and in transit

Source: The NIST Internal/Interagency Report NISTIR 7298 (*Glossary of Key Information Security Terms* , May 2013)

Information Assurance as a part of security

- *Information assurance* is a term used to describe not just the protection of information, but a means of knowing the level of protection that has been accomplished

Computer Security Challenges

Attackers only need to find a single weakness, while the designer must find and eliminate all weaknesses to achieve perfect security

Security is still too often an afterthought to be incorporated into a system after the design is complete, rather than being an integral part of the design process

Security requires regular and constant monitoring

There is a natural tendency on the part of users and system managers to perceive little benefit from security investment until a security failure occurs

Many users and even security administrators view strong security as an impediment to efficient and user-friendly operation of an information system or use of information

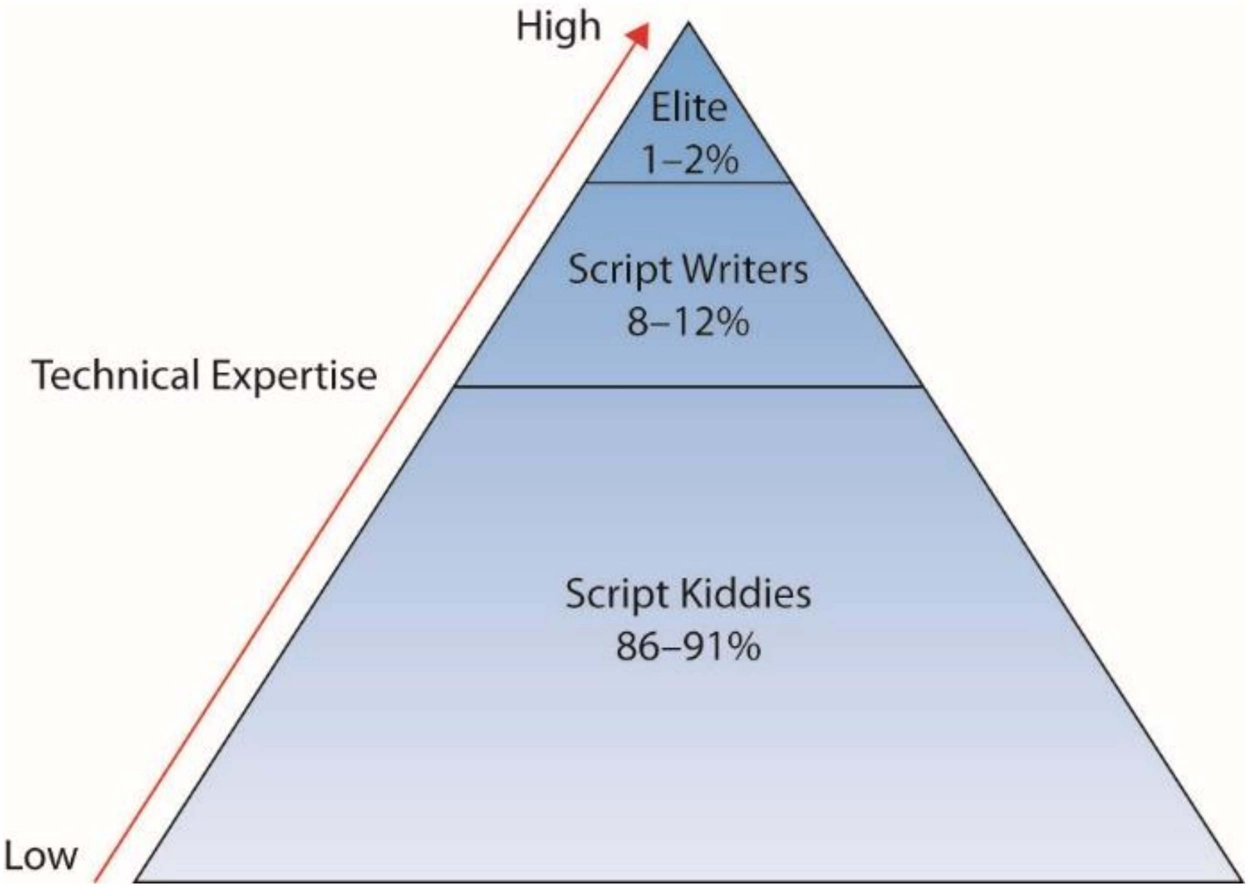
Common Terms

- **Adversary (threat agent) -** Individual, group, organization, or government that conducts or has the intent to conduct detrimental activities.
- **Attack -** Any kind of malicious activity that attempts to collect, disrupt, deny, degrade, or destroy information system resources or the information itself.
- **Countermeasure (mitigation) -** A device or techniques that has as its objective the impairment of the operational effectiveness of undesirable or adversarial activity, or the prevention of espionage, sabotage, theft, or unauthorized access to or use of sensitive information or information systems.
- **Risk -** A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of 1) the adverse impacts that would arise if the circumstance or event occurs; and 2) the likelihood of occurrence.
- **Security Policy -** A set of criteria for the provision of security services. It defines and constrains the activities of a data processing facility in order to maintain a condition of security for systems and data.
- **System Resource (Asset) -** A major application, general support system, high impact program, physical plant, mission critical system, personnel, equipment, or a logically related group of systems.
- **Threat -** Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.
- **Vulnerability -** Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.

Targets and Attacks

- Two general reasons a particular system is attacked
  - It is specifically targeted by the attacker
  - It is an opportunistic target

Threat Actors by Ability



Other Attributes of Actors

- Location (internal or external)
- Level of resources
- Intent

Threat Actors

http://e-mate2.s3-website-us-east-1.amazonaws.com/ThreatActors/ThreatActors.html

Advanced Persistent Threats (APTs)

- Well-resourced, persistent application of a wide variety of intrusion technologies and malware to selected targets (usually business or political)
- Typically attributed to state-sponsored organizations and criminal enterprises
- Differ from other types of attack by their careful target selection and stealthy intrusion efforts over extended periods
- High profile attacks include Aurora, RSA, APT1, and Stuxnet

APT Characteristics

Advanced

- Used by the attackers of a wide variety of intrusion technologies and malware including the development of custom malware if required
- The individual components may not necessarily be technically advanced but are carefully selected to suit the chosen target

Persistent

- Determined application of the attacks over an extended period against the chosen target in order to maximize the chance of success
- A variety of attacks may be progressively applied until the target is compromised

Threats

- Threats to the selected targets as a result of the organized, capable, and well-funded attackers intent to compromise the specifically chosen targets
- The active involvement of people in the process greatly raises the threat level from that due to automated attacks tools, and also the likelihood of successful attacks

Approaches to Defense (1 of 2)

- Correctness: ensuring the system is fully up to date
  - All patches installed and proper security controls in place
- Isolation: protecting a system from unauthorized use
  - Access control and physical security
- Obfuscation: making it difficult for an adversary to know when they have succeeded
  - Increasing the workload of an attacker makes it more difficult for them to succeed in their attack
  - Not a favored solution

Approaches to Defense (2 of 2)

- Cybersecurity kill chain
  - Step-by-step process to model how attacks target and achieve results on victim systems
- Threat intelligence
  - Set of actions taken to properly utilize resources to target the actual threats an enterprise is facing
  - Basis of understanding adversary tactics, techniques, and procedures (TTPs)
- Open-source intelligence
  - Processes used to collect threat intelligence information
  - Example OSINT: https://www.youtube.com/watch?v=F7pYHN9iC9I&t=146s

The Importance of Doing Things Right

- https://www.nytimes.com/2020/08/20/technology/joe-sullivan-uber-charged-hack.html

How Secure Are You?

QuestionPro Poll

The Current Threat Environment

- Verizon DBIR
  - Increase in ransomware
- Crowd Strike Global Threat Report

Real-time attack maps

https://threatbutt.com/map

https://threatmap.checkpoint.com/ThreatPortal/livemap.html

https://cybermap.kaspersky.com/

http://www.digitalattackmap.com

https://talosintelligence.com/fullpage_maps/pulse

Questions?

Assignments

- Read Chapter 1 and take quiz
- Read Chapter 2
- Login to Nevada Cyber Range
  - https://ncr.cse.unr.edu/
  - 2FA Authenticator apps:
    - Google Authenticator, Aegis, or Duo
  - **BRING AUTHENTICATOR DEVICE TO CLASS EVERY WEEK!**
- **Be ready to take notes next class**

NV CYBER

NEVADA CYBER CLUB

https://www.nevadacyberclub.com/discord

U.S. DEPARTMENT OF ENERGY'S CYBERFORCE® COMPETITION

DEFENDING U.S. ENERGY INFRASTRUCTURE

NATIONAL SECURITY AGENCY · UNITED STATES OF AMERICA

NSA Codebreaker Challenge

NCAE CYBER GAMES

PLAY | LEARN | PROTECT

CCDC NATIONAL COLLEGIATE CYBER DEFENSE COMPETITION

NCL THE NATIONAL CYBER LEAGUE

COLLEGIATE PENETRATION TESTING COMPETITION

Scholarship for Service Grant

- https://www.unr.edu/cybercorps-scholarship
- TLDR; Up to 2 years paid classes and cost of living and material stipends in exchange for up to 2 years of work in a government agency.
- Internships and job placement assistance
- Meeting Friday, August 30, 2024, 5:00 – 6:30 PM, WPEB130 – Pizza!
- RSVP here: https://unr.campuslabs.com/engage/event/10304015

Graduate Students Stick Around

Graduate Project

- Cybersecurity Conference Call for Posters/Demos
- Consider a topic related to a graduate thesis
- Actual analysis or experimentation.developement is preferred to literature review
- Small team projects may be considered if appropriate in scale
- Cyber competitions with grade based on results

Project Idea

- The goal of this prize challenge is to develop a mathematical model that uses as inputs:
  a) the system’s architecture,
  b) the functions and functional threads that the system must perform,
  c) the hardware and software within the system needed for each thread,
  d) the known cyber vulnerabilities present on each hardware and software component, and
  e) the adversary threat actors and tactics, techniques, and procedures they will use to exploit the open cyber vulnerabilities on the system to cause a cyber effect to impact functionality and execution.
  The mathematical model will be implemented within software algorithms to form core functionality for the desired cyber resiliency assessment capability. The challenge will include developing a cyber resiliency assessment prototype GUI that displays the assessment results. The GUI will be used during the challenge demonstration phase.

Project Idea

- Vulnerability Testing
- https://hackerone.com/opportunities/all
- Create and document testing plan and results
- Professional Pen Testing Report