CIS4204.01 **Brandon Thompson**
Dr. Ashokkumar Patel

Notes: Ethical Hacking

1 Chapter 1

1.1 Terms and Evolution of Hacking

Hackers / Crackers

- Access to computer system or network without authorization.
  - Breaks the law; can go to prison.

Ethical Hacker

- Performs most of the same activities as a hacker with the owners / company's permission.

Hackers became more prolific and dangerous after the availability of the Internet expanded to include the general public. Originally hacking was the skillful modification of systems. As the Internet began to include more people and technology, there was more of a following for hacking. First for fun or curiosity, then for maliciousness and financial reasons.

1.2 What is Hacking

- Stealing passwords and usernames - "Theft of access"
- Network intrusions - Form of digital trespassing
- Social Engineering - Humans are the weakest point of a computer system.
- Posting / transmitting illegal material - Illegal material can spread very quickly with the use of social media.
- Financial Fraud - Deception of one party to elicit information or system access typically for financial gain to to cause damage.
- Software / data piracy - the possession, duplication / distribution of software in violation of license agreement / act of removing copy protection.

- Dumpster Diving - gathering of material that has been discarded or left in unsecured or unguarded receptacles.
- Creating and Planting Malicious Code - refers to items such as viruses, worms, spyware, adware, rootkits, and other types of malware. (any type of software written to wreak havoc, destruction or disruption.)
- Unauthorized Destruction or Alteration - Modifying, destroying, or tampering of information without permission.
- Data diddling - Unauthorized modification of information to cover up other malicious activity.
- Denial of Service (DoS/DDoS) - Overload a systems resources so it cannot provide the required services to its users.
- Ransomware - encryption of key files on a system for the purpose of extracting payment from the victim.

1.3 Types of Hackers

- Black-Hat Hackers: Bad guys, may or may not have an agenda (Criminal)
- White-Hat Hackers: Good guys, have a code of ethics.
- Gray-Hat Hackers: Could be good or bad (do not trust)
- Suicide Hackers: Trying to prove a point, are not stealthy because they do not care about repercussions.
- Script Kiddies: No or limited training, use prebuilt tools, mainly curious.

1.4 Motives of Hackers

- Monetary - financial gain
- Status - Increased reputation within their communities
- Terrorism - To scare, intimidate, or cause panic to the target group or the victims
- Revenge / Hatred - Disgruntled employees
- Hacktivism - Bring attention to a cause, group, or political ideology.
- Fun - Attacks with no specific goal

1.5 Tasks of Ethical Hackers

- **Penetration Test**
  Perform attacks / exploits on system and network

  1. Attempt to break into a company's network or system or application to find the weakest link.
  2. Report on the attack to company
  3. Company decides how to use the information given by the attack.

- **Vulnerability Assessment / Research**

  1. Tester enumerates all vulnerabilities found in an application or system.
  2. Passively uncovering vulnerabilities or weaknesses.
  3. Correct found vulnerabilities.

- **Security Test**

  1. Analyze company's security policy and procedures.
  2. Security tester must examine best practices, legal issues, and industry regulations.

1.6 Goals of Penetration Tester

Every security minded organization enforces the CIA triad (confidentiality, integrity and availability). Penetration testers work to find the weaknesses in the client's environment that would disrupt the CIA triad. The anti-CIA triad is the DDA (Disclosure, Disruption, Alteration). Blue teams try to maintain CIA and red teams try to do DDA.

1.7 Penetration-Testing Methodologies

- White box model
  "Full information"
  - Tester is told about network topology.
  - Floor plan / network plan
  - Interviews with IT personnel and employees.
  - Information for routers, switches, firewalls, and IDS's.
  - List of OS running on systems.

- Black box model
  "No information"
  - Given to details about technologies used.
  - Tester has to find details themselves.
  - Tests security personnel's ability to detect an attack.
  - Staff does not know about the test.
- Gray box model
  "Some information"
  - Hybrid of white and black box model.