J. A. “Drew” Hamilton, Jr., Ph.D.

Director, Center for Cyber Innovation

Professor, Computer Science & Engineering

CCI
Post Office Box 9627
Mississippi State, MS 39762

Voice: (662) 325-2294
Fax: (662) 325-7692
hamilton@cci.msstate.edu

Intro to Ethical Hacking

Reference:

Drew Hamilton Lecture Notes

Ethical Hacker Exam Guide, 9th ed.

Ervin, Kelly and Lee, William

Examples of Cybercrime

- Stealing usernames and passwords
- Network intrusion
- Social Engineering
- Posting or Transmitting Legal Material
- Fraud
- Identity Theft
- Software Piracy
- Dumpster Diving
- Malicious Code
- Unauthorized destruction or alteration of information
- Embezzlement
- Data-diddling
- Denial of Service (DoS)
- Ransomware

Famous Cases

- **1988 – Robert T. Morris**
- **1994 – Kevin Lee Poulsen**
- **1999 – David L. Smith**
- **2001 – Jan De Wit**
- **2002 – Gary McKinnon**
- **2004 – Adam Botbyl**
- **2005 – Cameron Lacroix**
- **2009 – Kristina Vladimirovna Svechinskaya**
- **2000's – Stuxnet**
- **2003 - Anonymous**

History

- Phone phreaking
- Woz’s club at MIT
- Train building
- Defcon

What is an Ethical Hacker?

- Types of Hackers
  - White Hat – ethical security professional
  - Gray Hat – chaotic neutral
  - Black Hat – unethical criminal
  - Script Kiddie – dumb n00b
  - Suicide hacker – just plain crazy
  - Hacktivist – Politically motivated

- An ethical hacker is usually a White Hat or Gray Hat hacker that follows a code of ethics, and has the responsibility of securing corporations and governments from Black Hat attacks.

What are your responsibilities?

- An ethical hacker always has permission to pentest a system.
- Protect personally identifiable information
- Understand contracts
- Black Hats – do not have permission or authorization

Code of Conduct and Ethics

- Protect private information such as name, addr, SSN, username
- Protect intellectual property
- Disclose potential dangers to the authorities
- Provide service in your area of competence
- Never use illegal software
- Never engage in deceptive financial practices
- Never use property of your clients or employers in an unintended way
- Disclose conflicts of interest

- Ensure good management
- Add to the profession by constant study
- Have integrity during business dealings
- Ensure ethical conduct without prejudice
- Never associate with malicious hackers or activities
- Never purposefully compromise a system
- Ensure all penetration tests are authorized
- Never join underground hacking communities for the purpose of spreading Black Hat philosophies
- Never be misleading with certifications
- Never be in violation of any law of the land

Ethical Hacking and Penetration Testing

- Penetration Testing – sanctioned hacking, hacking with permission
- IT Audit – evaluation of a system to confirm its wellbeing
- Black box testing – pentester has no knowledge of the system
- Gray box testing – pentester has some knowledge of the system
- White box testing – pentester has full knowledge of the system
- Keep these in mind during testing
  - Confidentiality – safeguard private information
  - Integrity – safeguard that the information is true and correct
  - Availability – safeguard that resources are available for use

Ethical Hacking and Penetration Testing

- **Hack Value – how attractive is the target?**
- **Target of Evaluation – something scanned for vulnerabilities**
- **Attack – actively engaging a TOE**
- **Exploit – clearly defined way to breach a system**
- **Zero Day – unknown vulnerability, freshly discovered**
- **Security – state of well-being or a system**
- **Threat – potential violation of security**
- **Vulnerability – weakness in a system, entry point**
- **Daisy Chaining – a sequence of attacks**

Hacking Methodology

- Footprinting
- Scanning
- Enumeration
- System Hacking
- Escalation of privilege
- Covering tracks
- Planting backdoors

Vulnerability Research and Tools

- **Searching for and uncovering vulnerabilities in a system**
- **classifying their severity as high, medium or low**
- **More passive than Ethical Hacking**

Incident Response

- Evidence collection
- Incidence Response Policies and Plans
- Response – what exactly happened here?
- Triage – what kind of damage was done?
- Investigation – impartial collection of evidence
- Containment – control the crime scene
- Analysis and tracking – examine the evidence, chain of custody
- Recovery – restore and rebuild operating system
- Repair – repairing the damaged system
- Debriefing – obtain feedback from all involved

Business Continuity Plan

- If services are not available, money is lost
- Disasters of all types can cause services to fail
  - Disaster Recovery Plan
- Fault Tolerance
- Back up the system
  - Alternate sites – Cold Site, Warm Site, Hot site
- Service Level Agreement (SLA)

System Recovery

- Regularly review Business Continuity Plan
- Conduct Disaster Recovery Plan drills
- Ensure service providers you use take adequate precautions
- Evaluate proper redundancy measures
- Keep emergency hardware on-hand
- Review the SLA to understand what is acceptable downtime
- Establish a communications resource
- Ensure the hot site can be deployed immediately
- Identify and document all points of failure
- Ensure that the company’s redundant storage is secure

Types of Evidence

- Best
- Secondary
- Direct
- Conclusive
- Opinion
- Corroborative
- Circumstantial

Chain of Custody

- What evidence has been collected?
- How was the evidence obtained?
- When was the evidence collected?
- Who has handled the evidence?
- What reason did each person have for handling the evidence?
- Where has the evidence traveled?
- Where will it be stored?

The Five Rules of Evidence

- **Reliable – consistent and leads to a common conclusion**
- **Preserved – chain of custody**
- **Relevant – evidence directly relates to the case**
- **Properly identified – proof of preservation (hash)**
- **Legally permissible – Judge says it fits the rules of evidence**

Reporting a Security Incident

- Adhere to known best practices and guidelines
- Refer to your employer's Incident Response Plan
- Consider if it should be reported to local law enforcement
- Should it be reported to a regulatory body?
- Include a timeline of events
- Before and after states of the system
- List everyone who was involved in the incident
- Document the motivations behind actions
- Recommend how to prevent the incident in the future
- Include a detailed report and have a short summary

Ethics and the Law

- As a hacker, be aware of computer crime laws in your area
- Always obey the Code of Ethics
- Clients are placing trust in you as a penetration tester
- If you go out of the scope of the pentest, the client can take legal action
- Familiarize yourself with common computer related laws
  - CFAA
  - US Privacy Act
  - FISMA

Summary

- Know the purpose of an ethical hacker
  - Having permission to test a system’s security
- Know the different between types of penetration tests
  - Black, white, gray box tests – know the client’s expectations
- Understand your targets
  - Client has to give guidance on what should be tested
- Understand your Code of Ethics
  - Acceptable behavior
- Know your opponents
  - Know the motivations behinds the types of hackers you will defend against
- Know your tools and terms
  - CEH has many tool names and definitions for terms, familiarize yourself