
Hacker Techniques, Tools, and Incident Handling

Chapter 1 Hacking: The Next Generation

Learning Objective

- Explore the history and current state of hacking and penetration testing, including their ethical and legal implications.

Key Concepts

- Birth and evolution of hacking
 - 1960s: individuals of technology enthusiasts, motivated by intellectual curiosity
 - 1980s: started gaining negative connotations, altering image of a hacker to a computer criminal, theft of service
- Ethical hacking and penetration testing in relation to black- and white-hat activities
- Laws and ethical standards for penetration testers and ethical hackers

Types of Hackers

- **Script kiddies** are beginners and possess basic skills.
- **Black hats** break into computer systems or use them without authorization.
- **Gray hats** walk the line between legal and illegal actions.
- **White hats** are employed to break security to expose vulnerability.
- **Suicide hackers** do not care if they get caught; goals include political, terrorist, or other aims.

TAP Principle of Controls

Technical:

software/hardware such as IDS, IPS, authentication, permissions, auditing, etc.

Administrative:

policies and procedures such as password policy, legal requirements, etc.

Physical:

locks, cameras, fences, gates, etc.

Hacker Motives

Monetary

Financial gains

Status

Gaining recognition

Terrorism

Scare, intimidate, or
cause panic

Revenge

disgruntled
employee/customer

Hacktivism

Bring attention to a
cause or group

Fun

No specific goal,
indiscriminate

Common Attacks (1)

- **Theft of access:** stealing passwords, subverting access mechanisms to bypass normal authentication
- **Network intrusions:** accessing a system of computers without authorization
- **Emanation eavesdropping:** intercepting radio frequency signals
- **Social engineering:** telling lies to manipulate people into divulging information they otherwise would not provide
- **Posting and/or transmitting illegal material**
- **Fraud:** intentional deception to produce illegal financial gain or damage another party
- **Software piracy:** violation of a license agreement, removing copy protection

Common Attacks (2)

- Dumpster diving: gathering discarded materials
- Malicious coding: software written to cause damage, destruction, or disruption; viruses, worms, spyware, Trojan horses
- Denial of service (DoS) and distributed DoS attacks: overloading a system's resources not to provide required services
- IP address spoofing: substituting a forged IP address for a valid address in network traffic or a message to disguise the true location of the message or person
- Unauthorized destruction or alteration of information
- Embezzlement: a financial fraud (theft, redirection of funds)
- Data-diddling: unauthorized modification of data
- Logic bomb: a piece of code designed to cause harm, intentionally inserted into software system

History of Hacking

1990s

1980s

- Hacking as skillful modification of systems
- Early Viruses, Phone Phreaking
- First Hacker Groups, Bulletin Boards
- First Hacking Conference, Polymorphic Codes in Viruses
-

Pre 1970

Famous Hacks over Time

- 1988 Robert T. Morris: the first Internet worm
- 1999 David L. Smith: Melissa virus
- 2001 Jan de Wit: Ana Kournikova virus
- 2004 Adam Botbyl: steal credit card info
- 2005 Cameron Lacroix: hacking phone

Famous Hackers and Groups

- **Individual Hackers:**

- Kevin Poulsen, Frank Abagnale, Kevin Mitnick

- **Groups:**

- **Black Hats:**

- › The Cult of the Dead Cow (cDc), Legion of Doom

- **White Hats:**

- › The Internet Storm Center, InfraGard

Modern Hacking and Cybercriminals

- Transformation of hobbyist hacking to cybercrime
- Cybercriminals seeking profits by aiming at financial data, industry information, and other valuable targets
- Emergence of national laws to counter cyber attacks

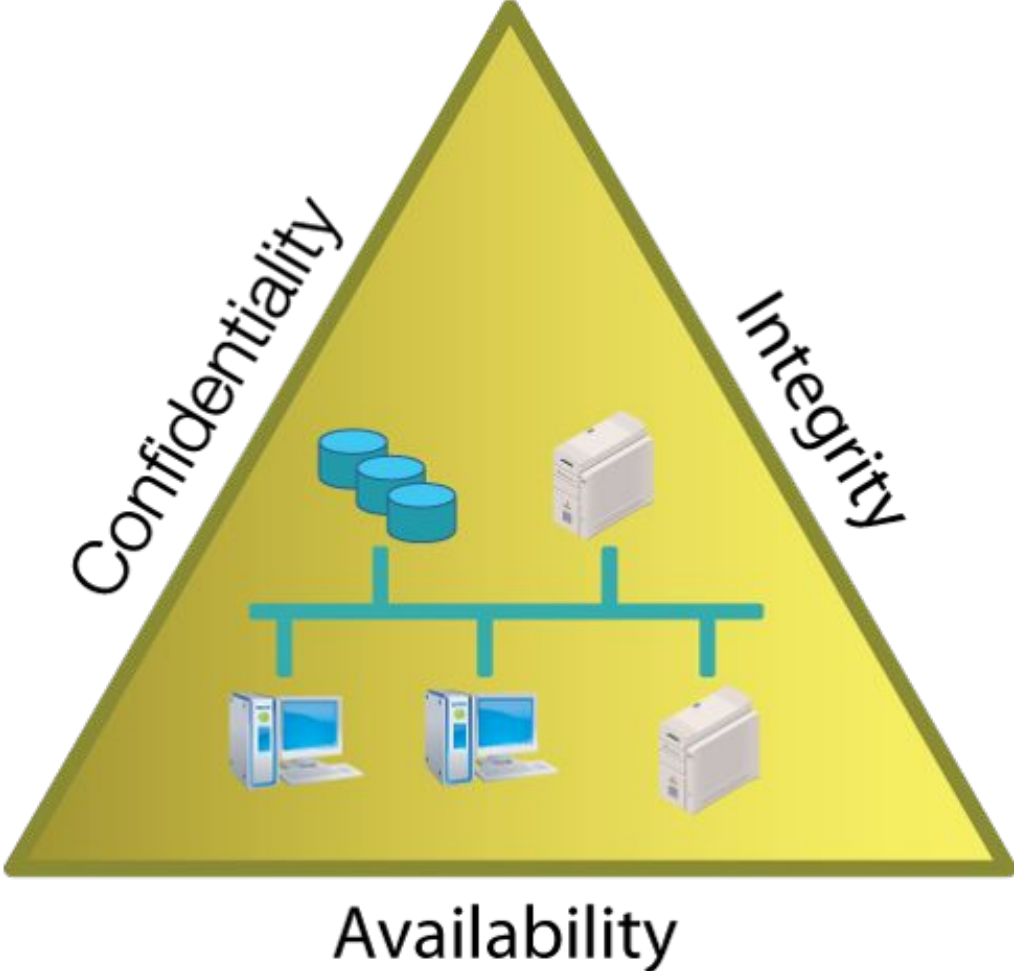
Ethical Hacking and Penetration Testing

- **Ethical hackers** require permission to engage in penetration testing
- **Penetration testing** is the structured and methodical means of investigating, uncovering, attacking, and reporting on a target system's strengths and vulnerabilities
- Penetration tests are commonly part of **IT audits**

Key Points about Ethical Hacking

- It requires explicit permission of “victim”
- Participants use the same tactics and strategies as regular hackers
- It can harm a system if you do not exercise proper care
- It requires detailed advance knowledge of actual techniques a regular hacker will use.
- It requires that rules of engagement or guidelines be established prior to any testing

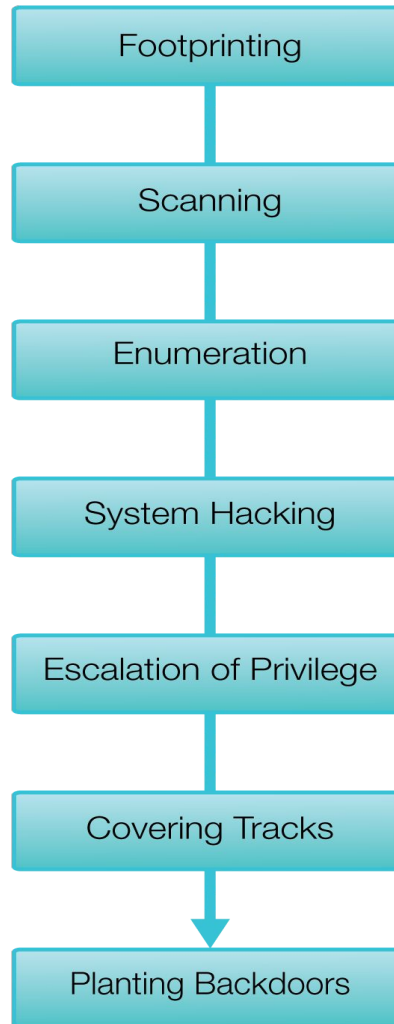
C-I-A Triad



C-I-A Triad

- **Confidentiality:** safeguarding information or services against disclosure to unauthorized parties
- **Integrity:** ensuring that information is in its intended format or state, i.e., ensuring that data is not altered
- **Availability:** ensuring that information or a service can be accessed or used whenever requested
- **Anti-triad**
 - **Disclosure:** Information is accessed by an unauthorized party
 - **Alteration:** Information is maliciously or accidentally modified
 - **Disruption:** Information and/or services are not accessible or usable when called upon

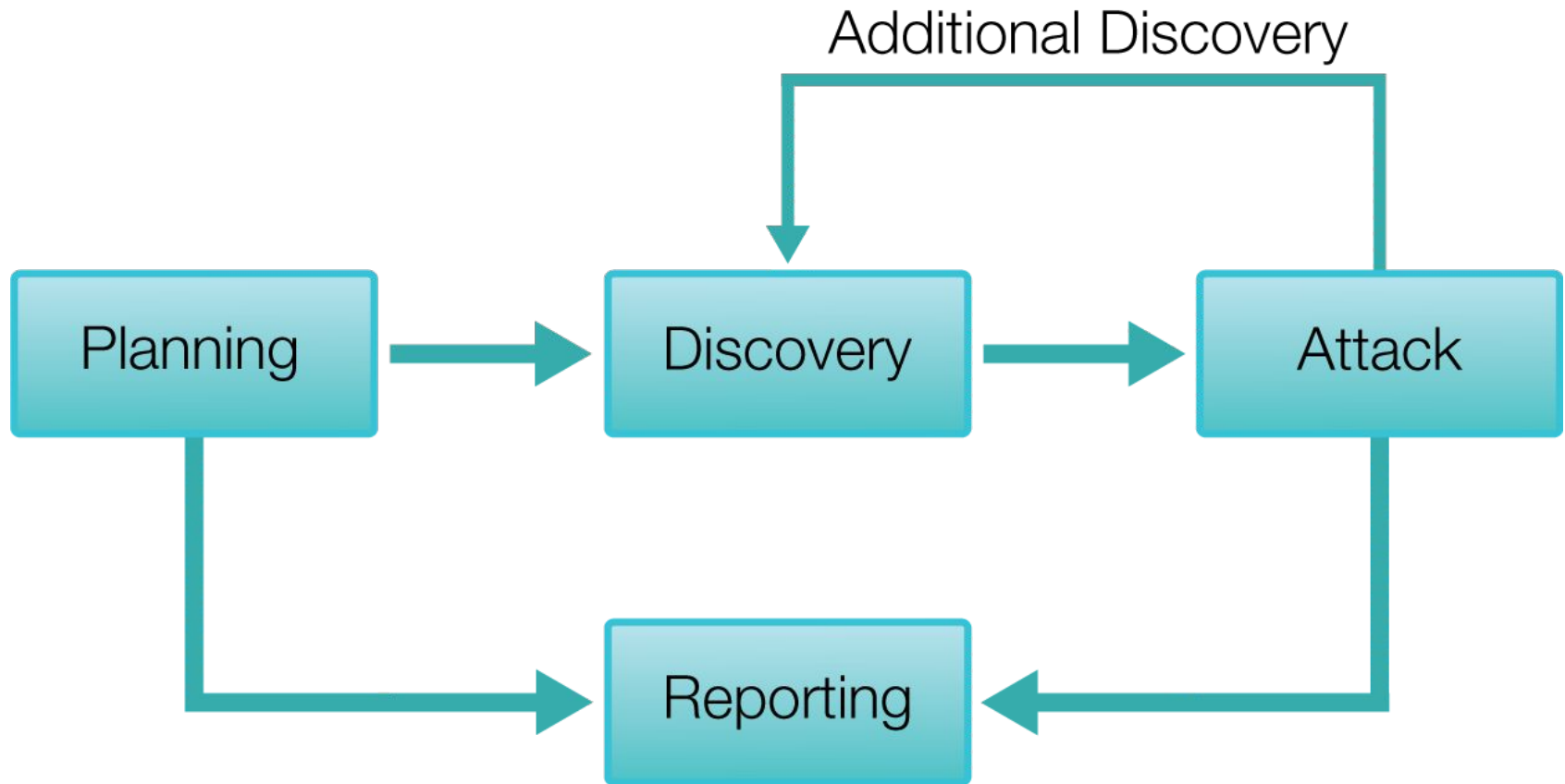
Common Hacking Methodologies



Hacking Methodologies

- **Footprinting:** An attacker passively acquires information about the intended victim's system
- **Scanning:** actively acquire more detailed information about a victim; a ping sweep of all victim's known IP addresses to see which machines respond
- **Enumeration:** extract more-detailed and useful information from a victim's system
- **System hacking:** actively attack a system
- **Escalation of privilege:** obtains privileges on a given system higher than should be permissible
- **Covering tracks:** purging information from the system to destroy evidence of a crime
- **Planting backdoors:** for later use

Penetration Testing Flow



Performing a Penetration Test

- Next logical step beyond ethical hacking
- Require rules to be agreed upon in advance
- NIST 800-42 Guideline on network security testing
- Technical attack
- Administrative attack
- Physical attack

Laws and Ethical Standards

- Ethical hackers should exercise proper care not to violate the rules of engagement
- When considering breaking guidelines
 - Trust: questioning of other details
 - Legal action against ethical hacker
- Regulations
 - Computer Fraud and Abuse Act
 - U.S. Communications Assistance for Law Enforcement Act
 - Sarbanes-Oxley Act (SOX)
 - Federal Information Security Management Act (FISMA)

Summary

- Birth and evolution of hacking
- Ethical hacking and penetration testing in relation to black- and white-hat activities
- Laws and ethical standards for penetration testers and ethical hackers