ECE 9609b / 9069b

Introduction to Hacking:

Ethics, Cyberlaws and Vulnerability Disclosure

Aleksander Essex

Western Engineering

What is a Hacker?

From Wikipedia:
Hacker, is a term used in computing that can describe several types of persons

- Hacker (hobbyist), who makes innovative customizations or combinations of retail electronic and computer equipment

What is a Hacker?

From Wikipedia:
Hacker, is a term used in computing that can describe several types of persons

- Hacker (hobbyist), who makes innovative customizations or combinations of retail electronic and computer equipment
- Hacker (programmer subculture), who combines excellence, playfulness, cleverness and exploration in performed activities

What is a Hacker?

From Wikipedia:
Hacker, is a term used in computing that can describe several types of persons

- Hacker (hobbyist), who makes innovative customizations or combinations of retail electronic and computer equipment
- Hacker (programmer subculture), who combines excellence, playfulness, cleverness and exploration in performed activities
- Hacker (computer security) someone who **seeks and exploits** weaknesses in a computer system or computer network

Why Study Hacking?

Sun Tzu (The Art of War): *It is said that:*

- if you know your enemies and know yourself, you will not be imperiled in a hundred battles;
- if you do not know your enemies but do know yourself, you will win one and lose one;
- if you do not know your enemies nor yourself, you will be imperiled in every single battle.

The Ethics of Hacking

Vulnerability Assessment

- Decide on a threat model

Vulnerability Assessment

- Decide on a threat model
- Identify potential vulnerabilities

Vulnerability Assessment

- Decide on a threat model
- Identify potential vulnerabilities
- Develop solution

Vulnerability Assessment

- Decide on a threat model
- Identify potential vulnerabilities
- Develop solution

Different approaches for different threats and technologies.
Uncovers foundational issues. Not really hacking.

Penetration Testing: Ethical Hacking

- Objective: actually test vulnerabilities identified in the vulnerability assessment

Penetration Testing: Ethical Hacking

- Objective: actually test vulnerabilities identified in the vulnerability assessment
- Method: break into system and take control of (i.e., “pwn”) as many components as possible

Penetration Testing: Ethical Hacking

- Objective: actually test vulnerabilities identified in the vulnerability assessment
- Method: break into system and take control of (i.e., “pwn”) as many components as possible
- Goal: achieve root/administrative privileges, pick up “trophies”

Penetration Testing: Ethical Hacking

- Objective: actually test vulnerabilities identified in the vulnerability assessment
- Method: break into system and take control of (i.e., “pwn”) as many components as possible
- Goal: achieve root/administrative privileges, pick up “trophies”
- Utility: demonstrating vulnerabilities makes them more “real” to clients than an assessment alone

Penetration Testing: Process

- Establish scope: what to attack, what not to touch, NDAs, legal issues, approvals

Penetration Testing: Process

- Establish scope: what to attack, what not to touch, NDAs, legal issues, approvals
- Assign teams:d Red team (attackers), white team (network admin/victim), blue team (management overseeing test)

Penetration Testing: Phases

- Passive scanning (no-contact)
  - Target's website
  - Source code
  - Social networking
  - Public databases (whois, Google, etc)

Penetration Testing: Phases

- Passive scanning (no-contact)
  - Target's website
  - Source code
  - Social networking
  - Public databases (whois, Google, etc)
- Active scanning (probe public exposure)
  - Scanning tools (Backtrack/Kali)
  - Social engineering
  - Sniffing traffic
  - Wireless "war driving"

Penetration Testing: Phases

- Passive scanning (no-contact)
  - Target's website
  - Source code
  - Social networking
  - Public databases (whois, Google, etc)
- Active scanning (probe public exposure)
  - Scanning tools (Backtrack/Kali)
  - Social engineering
  - Sniffing traffic
  - Wireless "war driving"
- Finding "Attack Surfaces" (locate exposed devices)
  - Network mapping
  - Firewalls
  - Locating routers

Penetration Testing: Phases

- Passive scanning (no-contact)
  - Target's website
  - Source code
  - Social networking
  - Public databases (whois, Google, etc)
- Active scanning (probe public exposure)
  - Scanning tools (Backtrack/Kali)
  - Social engineering
  - Sniffing traffic
  - Wireless "war driving"
- Finding "Attack Surfaces" (locate exposed devices)
  - Network mapping
  - Firewalls
  - Locating routers

Penetration Testing: Phases

- Fingerprinting (profile exposed devices)
  - O/S and patch level
  - Apps and patch level
  - Open ports
  - User accounts

Penetration Testing: Phases

- Fingerprinting (profile exposed devices)
  - O/S and patch level
  - Apps and patch level
  - Open ports
  - User accounts
- Prioritize targets (pick what to attack)

Penetration Testing: Phases

- Fingerprinting (profile exposed devices)
  - O/S and patch level
  - Apps and patch level
  - Open ports
  - User accounts
- Prioritize targets (pick what to attack)
- Exploit Vulnerabilities
  - Use appropriate attack tools
  - Find a way 'in'

Penetration Testing: Phases

- Fingerprinting (profile exposed devices)
  - O/S and patch level
  - Apps and patch level
  - Open ports
  - User accounts
- Prioritize targets (pick what to attack)
- Exploit Vulnerabilities
  - Use appropriate attack tools
  - Find a way 'in'
- Escalate Privilege
  - Gain root/admin access
  - Access accounts with cracked passwords
- Document and report findings

What Unethical hackers do different

- Target selection: different motivation (malicious, criminal). No ground rules

What Unethical hackers do different

- Target selection: different motivation (malicious, criminal). No ground rules
- Intermediaries: launches attack from intermediary systems to prevent tracking (additional victims)

What Unethical hackers do different

- Target selection: different motivation (malicious, criminal). No ground rules
- Intermediaries: launches attack from intermediary systems to prevent tracking (additional victims)
- Maintaining long-term access: rootkits, backdoors, trojans

What Unethical hackers do different

- Target selection: different motivation (malicious, criminal). No ground rules
- Intermediaries: launches attack from intermediary systems to prevent tracking (additional victims)
- Maintaining long-term access: rootkits, backdoors, trojans
- Covers tracks: wipes audit logs, hides malicious files

What Unethical hackers do different

- Target selection: different motivation (malicious, criminal). No ground rules
- Intermediaries: launches attack from intermediary systems to prevent tracking (additional victims)
- Maintaining long-term access: rootkits, backdoors, trojans
- Covers tracks: wipes audit logs, hides malicious files
- Hardens system: fixes vulnerabilities

What Unethical hackers do different

- Target selection: different motivation (malicious, criminal). No ground rules
- Intermediaries: launches attack from intermediary systems to prevent tracking (additional victims)
- Maintaining long-term access: rootkits, backdoors, trojans
- Covers tracks: wipes audit logs, hides malicious files
- Hardens system: fixes vulnerabilities
  Most important: **does not have consent** of account/resource owner.

Hacker Examples: Ethical or Unethical?

- Criminal organizations: monetary theft
- Script kiddie: amateur hacker who breaks into systems by using automated tools written by others motivations: thrills/mayhem/revenge

Hacker Examples: Ethical or Unethical?

- Criminal organizations: monetary theft
- Script kiddie: amateur hacker who breaks into systems by using automated tools written by others motivations: thrills/mayhem/revenge
- Hacktivist: typically causes website defacement, denial of service. Motivation: ideological/political.

Hacker Examples: Ethical or Unethical?

- Criminal organizations: monetary theft
- Script kiddie: amateur hacker who breaks into systems by using automated tools written by others motivations: thrills/mayhem/revenge
- Hacktivist: typically causes website defacement, denial of service. Motivation: ideological/political.
  What about Edward Snowden?

Hacker Examples: Ethical or Unethical?

- Criminal organizations: monetary theft
- Script kiddie: amateur hacker who breaks into systems by using automated tools written by others motivations: thrills/mayhem/revenge
- Hacktivist: typically causes website defacement, denial of service. Motivation: ideological/political.
  What about Edward Snowden?
- Nation state (e.g., NSA). Motivation: intelligence, counter-terrorism.

Cyberlaws

Access Device Statute

18 USC Section 1029: The Access Device Statute

- Protects against unauthorized access to accounts (money, products, services)

Access Device Statute

18 USC Section 1029: The Access Device Statute

- Protects against unauthorized access to accounts (money, products, services)
- Outlaws possessing, trafficking, or using devices and equipment to facilitate or engage in unauthorized access

Access Device Statute

18 USC Section 1029: The Access Device Statute

- Protects against unauthorized access to accounts (money, products, services)
- Outlaws possessing, trafficking, or using devices and equipment to facilitate or engage in unauthorized access
- Includes devices for generating credentials (passwords, PINs, credit card numbers)

Access Device Statute

Examples

- Phreakers (telephone system hackers)

Access Device Statute

Examples

- Phreakers (telephone system hackers)
- Crackers (password crackers, credit card number generators)

Access Device Statute

Examples

- Phreakers (telephone system hackers)
- Crackers (password crackers, credit card number generators)
- Skimmers (stealing debit/credit PINs)

Access Device Statute

Examples

- Phreakers (telephone system hackers)
- Crackers (password crackers, credit card number generators)
- Skimmers (stealing debit/credit PINs)

Examples (p.27)

Computer Fraud and Abuse Act

18 USC Section 1030 of the Computer Fraud and Abuse Act Protects computer *network* security (esp. of government and banks). Outlaws:

Computer Fraud and Abuse Act

18 USC Section 1030 of the Computer Fraud and Abuse Act Protects computer *network* security (esp. of government and banks). Outlaws:

- Unauthorized network access and threats thereof

Computer Fraud and Abuse Act

18 USC Section 1030 of the Computer Fraud and Abuse Act Protects computer *network* security (esp. of government and banks). Outlaws:

- Unauthorized network access and threats thereof
- Transmitting code/programs to cause damage (viruses, worms, etc)

Computer Fraud and Abuse Act

18 USC Section 1030 of the Computer Fraud and Abuse Act Protects computer *network* security (esp. of government and banks). Outlaws:

- Unauthorized network access and threats thereof
- Transmitting code/programs to cause damage (viruses, worms, etc)

Liable if you knowingly access a system without authorization and caused harm (even if you didn't know you would cause harm). Examples (p.30)

Electronic Communication Privacy Act

18 USC Sections 2510 of the Electronic Communication Privacy Act

Protects *communications* from unauthorized access.

- Wiretapping (interception)

Electronic Communication Privacy Act

18 USC Sections 2510 of the Electronic Communication Privacy Act

Protects *communications* from unauthorized access.

- Wiretapping (interception)
- Stored communications

Digital Millennium Copyright Act

Protects copyright holders from unauthorized access to their works

- Illegal to circumvent digital rights management (DRM) for profit

Digital Millennium Copyright Act

Protects copyright holders from unauthorized access to their works

- Illegal to circumvent digital rights management (DRM) for profit
- Can't sell anti-DRM technology. But where is the line drawn?

Digital Millennium Copyright Act

Protects copyright holders from unauthorized access to their works

- Illegal to circumvent digital rights management (DRM) for profit
- Can't sell anti-DRM technology. But where is the line drawn?
- "Encryption Research" and "security testing" ok
- Media backup tools often in gray area
- Only covers copyrighted works

Digital Millennium Copyright Act

Protects copyright holders from unauthorized access to their works

- Illegal to circumvent digital rights management (DRM) for profit
- Can't sell anti-DRM technology. But where is the line drawn?
- "Encryption Research" and "security testing" ok
- Media backup tools often in gray area
- Only covers copyrighted works

Examples (p.44)

Cyber Security Enhancement Act of 2002

- Stiffens penalties

Cyber Security Enhancement Act of 2002

- Stiffens penalties
- Up to life in prison for causing bodily harm or death

Cyber Security Enhancement Act of 2002

- Stiffens penalties
- Up to life in prison for causing bodily harm or death
- Examples: Hospital equipment, emergency response, traffic systems, air traffic control

Ethical Disclosure of Vulnerabilities

Hats: The Types of Hacker

- Black hat: uncovers vulnerability and illegally exploits it (or tells others how)

Hats: The Types of Hacker

- Black hat: uncovers vulnerability and illegally exploits it (or tells others how)
- White hat: uncovers vulnerability and exploits it with authorization

Hats: The Types of Hacker

- Black hat: uncovers vulnerability and illegally exploits it (or tells others how)
- White hat: uncovers vulnerability and exploits it with authorization
- Gray hat: uncovers vulnerability, doesn't exploit it (or tell others how) and works with vendor to fix it

Hats: The Types of Hacker

- Black hat: uncovers vulnerability and illegally exploits it (or tells others how)
- White hat: uncovers vulnerability and exploits it with authorization
- Gray hat: uncovers vulnerability, doesn't exploit it (or tell others how) and works with vendor to fix it

N.B.: A fine line exists between Grey vs. Black. As a rule of thumb when conducting security research: **stay well away from personal private information and networked resources** without explicit written authorization from the owner. (Caveats and Examples)

Ethical Disclosure: An Ideal Scenario

How do you ethically disclose a vulnerability? Your first stop should be to notify the vendor.

1. Reporter discovers vulnerability and attempts to verify it

Ethical Disclosure: An Ideal Scenario

How do you ethically disclose a vulnerability? Your first stop should be to notify the vendor.

1. Reporter discovers vulnerability and attempts to verify it
2. Reporter sends notification to Vendor giving details

Ethical Disclosure: An Ideal Scenario

How do you ethically disclose a vulnerability? Your first stop should be to notify the vendor.

1. Reporter discovers vulnerability and attempts to verify it
2. Reporter sends notification to Vendor giving details
3. Vendor verifies vulnerability and develops and tests a solution (e.g., patch)

Ethical Disclosure: An Ideal Scenario

How do you ethically disclose a vulnerability? Your first stop should be to notify the vendor.

1. Reporter discovers vulnerability and attempts to verify it
2. Reporter sends notification to Vendor giving details
3. Vendor verifies vulnerability and develops and tests a solution (e.g., patch)
4. Vendor provides reporter with solution

Ethical Disclosure: An Ideal Scenario

How do you ethically disclose a vulnerability? Your first stop should be to notify the vendor.

1. Reporter discovers vulnerability and attempts to verify it
2. Reporter sends notification to Vendor giving details
3. Vendor verifies vulnerability and develops and tests a solution (e.g., patch)
4. Vendor provides reporter with solution
5. Vendor releases a disclosure statement

Ethical Disclosure: An Ideal Scenario

How do you ethically disclose a vulnerability? Your first stop should be to notify the vendor.

1. Reporter discovers vulnerability and attempts to verify it
2. Reporter sends notification to Vendor giving details
3. Vendor verifies vulnerability and develops and tests a solution (e.g., patch)
4. Vendor provides reporter with solution
5. Vendor releases a disclosure statement
6. User community provides feedback on vulnerability and solution

Ethical Disclosure: An Ideal Scenario

How do you ethically disclose a vulnerability? Your first stop should be to notify the vendor.

1. Reporter discovers vulnerability and attempts to verify it
2. Reporter sends notification to Vendor giving details
3. Vendor verifies vulnerability and develops and tests a solution (e.g., patch)
4. Vendor provides reporter with solution
5. Vendor releases a disclosure statement
6. User community provides feedback on vulnerability and solution

Where might this process break down in the real-world?

Cyber Emergency Reponse Team

If the vendor is unable or unwilling to process the disclosure, a *cyber emergency response team* might be able to help.

The Cyber Emergency Response Team (CERT) has a vulnerability reporting form with instructions. There are many different CERTs around the world, including in Canada. There are also government-run CERTs, such as US-CERT and the Canadian Cyber Incident Response Centre (CCIRC).

Kali Linux Exploitation Framework

A Brief Preview of Kali Linux

Kali Linux (`http://www.kali.org/`) is a free/open-source penetration testing framework and comes pre-loaded with a variety of tools for testing the security of networks, passwords, wifi, etc. It also has a variety of tools for performing digital forensics.
We will be using Kali in the assignments, and part of Assignment 1 will be to obtain and run a copy. You have several options for using Kali in a way that does not install anything on your computer:

- Burn a live-CD
- Write a live-USB
- Use a virtual machine, such as Virtual Box (free)