Introduction to Ethical Hacking

Module 1

Engineered by Hackers. Presented by Professionals.
China’s `Patriotic Hackers’ Attack U.S. Sites Including Google, NYT Says

“Patriotic hackers” backed by Chinese authorities conducted extensive computer hacking on U.S. government agencies and companies, including computer networks of Google Inc., according to a report published by the New York Times.

An examination of 250,000 diplomatic cables made public by WikiLeaks.org by the U.S. newspaper showed that high-level Chinese civilian and military officials assisted successful hacking attacks aimed at retrieving a wide range of U.S. government and military information.

At least one previously unreported attack conducted by Chinese hackers linked to the People’s Liberation Army in 2008 yielded more than 50 megabytes of e-mails, user names, and passwords from a U.S. government agency, the Times said.
3 more companies hacked! How secure is your online information?

In a sign that cyber security needs rapid quality improvements, two more U.S. companies, McDonald’s Corp and Walgreen Co, said they had been hacked in the past week, along with U.S. media company, Gawker.

After reports of Mastercard and Visa being hacked last week by a pro-Wikileaks group, which called itself 'Anonymous,' McDonald’s said its system had been breached and customers' "email and other contact information, birthdates and other specifics" had been compromised on Monday.

Much of this information was supposedly provided by a customer when they were signing up for online promotions or subscriptions. The fast food company did not specify how many accounts had been compromised.

On Friday, Walgreens said hackers had gained access to its customers' email database and spammed these accounts with instructions to enter personal information on other websites. Though the recent bouts of hacking are unrelated to the Mastercard, Visa and PayPal breaches, these new hackings seem to be forming a chain reaction through information gained from a previous breach.

Twitter said hackers broke into an unspecified number of users’ accounts and sent spam promoting acai berry drink, according to an AP report.

http://hken.ibtimes.com
Security News

December 20, 2010

Playing defense on the Net

On Nov. 30, only days before Internet activists shut down the websites of credit card companies Visa and MasterCard, five major online retailers faced a similar attack, timed to coincide with the start of the holiday shopping season.

The attacks against Visa and MasterCard paralyzed their company websites for hours. But even though the assault on the retail sites used similar methods, they didn’t have the same effect. The floods of illicit data were intercepted by a global network run by Akamai Technologies Inc.

Akamai is a Cambridge Internet infrastructure company, delivering massive amounts of online data for major businesses and government agencies. It is also one of many companies that defend the Internet from distributed denial of service, or DDOS, attacks, old but potent digital weapons wielded by criminals, protestors, and vandals around the world.

What was unusual about the recent attacks was that the public heard about them. Similar online data blitzes happen constantly, but they hardly ever do real damage, and even when they do, the effects are usually fleeting.

“The capabilities to stop them have significantly evolved over the last decade,” said Craig Labovitz, chief scientist at Arbor Networks Inc., a Chelmsford company that specializes in quashing DDOS attacks.

http://www.boston.com
Website for Tour company CitySights NY hit by hackers

Hackers have broken into the website of the New York tour company CitySights NY and stolen about 110,000 bank card numbers.

They broke in using a SQL Injection attack on the company's Web server, CitySights NY said in a Dec. 9 breach notification letter published by New Hampshire's attorney general. The company learned of the problem in late October, when, "a web programmer discovered [an] unauthorized script that appears to have been uploaded to the company's web server, which is believed to have compromised the security of the database on that server," the letter said.

CitySights NY believes that the SQL injection compromise occurred about a month earlier, on Sept. 26. In a SQL injection attack, hackers find ways to sneak real database commands into the server using the Web. They do this by adding specially crafted text into Web-based forms or search boxes that are used to query the back-end database.

This was one of the techniques used by Albert Gonzalez, who in March received the longest-ever U.S. federal sentence related to hacking the systems of Heartland Payment Systems, TJX and other companies.

In the CitySights NY incident, hackers were able to get names, addresses, e-mail addresses, credit card numbers and their expiration dates, and Card Verification Value 2 codes, used to validate online credit card purchases.

http://www.networkworld.com
Module Objectives

Elements of Information Security
- The Security, Functionality, and Usability Triangle
- Security Challenges
- Effects of Hacking
- Who is a Hacker?
- Hacker Classes
- Types of Hackers

Hacking Phases
- Types of Attacks on a System
- Why Ethical Hacking is Necessary?
- Scope and Limitations of Ethical Hacking
- What Do Ethical Hackers Do?
- Skills of an Ethical Hacker
- Vulnerability Research
Scenario: How Simple Things Can Get You into Trouble?

Gwen was working late. She could not complete her task so she spoke to her boss and took work home in a USB device. She worked the entire night and brought the work back to the office.

A few days later, someone else used the device who was not aware of the data Gwen had put on it. He misplaced the device and never found it again, but started using another USB device in the place of the old one.

Shortly after that, the company received a call from a client saying that details of their project were found online.

What went wrong? Who was responsible for this?
Internet Crime Current Report: IC3

Complaints received by IC3

Yearly Comparison of Complaints Received via the IC3 Website

http://www.ic3.gov

Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.
## Data Breach Investigations Report

<table>
<thead>
<tr>
<th>Type of Hacking</th>
<th>Percent of Breaches</th>
<th>Percent of Records</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use of stolen login credentials</td>
<td>38%</td>
<td>86%</td>
</tr>
<tr>
<td>Exploitation of backdoor or command/control channel</td>
<td>29%</td>
<td>5%</td>
</tr>
<tr>
<td>SQL Injection</td>
<td>25%</td>
<td>89%</td>
</tr>
<tr>
<td>Brute force and dictionary attacks</td>
<td>14%</td>
<td>&lt;1%</td>
</tr>
<tr>
<td>OS Commanding</td>
<td>14%</td>
<td>5%</td>
</tr>
<tr>
<td>Exploitation of default or guessable credentials</td>
<td>11%</td>
<td>&lt;1%</td>
</tr>
<tr>
<td>Footprinting and Fingerprinting</td>
<td>11%</td>
<td>&lt;1%</td>
</tr>
<tr>
<td>Cross-site Scripting</td>
<td>9%</td>
<td>2%</td>
</tr>
<tr>
<td>Exploitation of insufficient authentication</td>
<td>7%</td>
<td>2%</td>
</tr>
<tr>
<td>Exploitation of insufficient authorization</td>
<td>7%</td>
<td>&lt;1%</td>
</tr>
</tbody>
</table>

[http://www.verizonbusiness.com](http://www.verizonbusiness.com)
Types of Data Stolen From the Organizations

- Payment Card Information: 83%
- Non-Payment Card Information: 5%
- Intellectual Property: 3%
- Sensitive Company Data: 7%

Source of Breach
- External
- Internal
- Business Partner

**Essential Terminologies**

**Hack Value**
It is the notion among hackers that something is worth doing or is interesting.

**Target of Evaluation**
An IT system, product, or component that is identified/subjected to a required security evaluation.

**Attack**
An assault on the system security derived from an intelligent threat. An attack is any action violating security.
**Exploit**
A defined way to **breach the security** of an IT system through vulnerability

**A Zero-Day**
A computer threat that tries to **exploit computer application vulnerabilities** that are unknown to others or undisclosed to the software developer

**Security**
A state of well-being of information and infrastructure in which the possibility of **theft, tampering, and disruption of information and services** is kept low or tolerable
Essential Terminologies

**Threat**
An action or event that might compromise security
A threat is a potential violation of security

**Vulnerability**
Existence of a weakness, design, or implementation error that can lead to an unexpected and undesirable event compromising the security of the system

**Daisy Chaining**
Hackers who get away with database theft usually complete their task, then backtrack to cover their tracks by destroying logs, etc.
Elements of Information Security

C - Confidentiality
Assurance that the information is accessible only to those authorized to have access
Confidentiality breaches may occur due to improper data handling or a hacking attempt

I - Integrity
The trustworthiness of data or resources in terms of preventing improper and unauthorized changes
Assurance that information can be relied upon to be sufficiently accurate for its purpose

A - Availability
Assurance that the systems responsible for delivering, storing, and processing information are accessible when required by the authorized users
**Authenticity**

- Authenticity refers to the characteristic of a communication, document or any data that ensures the quality of being genuine or not corrupted from the original.
- Major roles of authentication include confirming that the user is who he or she claims to be and ensuring the message is authentic and not altered or forged.
- Biometrics, smart cards, or digital certificates are used to ensure authenticity of data, transactions, communications or documents.

**Non-Repudiation**

- It refers to the ability to ensure that a party to a contract or a communication cannot deny the authenticity of their signature on a document or the sending of a message that they originated.
- It is a way to guarantee that the sender of a message cannot later deny having sent the message and that the recipient cannot deny having received the message.
- Digital signatures and encryption are used to establish authenticity and non-repudiation of a document or message.
The Security, Functionality, and Usability Triangle

- Level of security in any system can be defined by the strength of three components:

  - Security (Restrictions)
  - Functionality (Features)
  - Usability (GUI)

Moving the ball towards security means less functionality and usability.
Security Challenges

- Compliance to government laws and regulations
- Evolution of technology focused on ease of use
- Direct impact of security breach on corporate asset base and goodwill
- Increased number of network-based applications
- It is difficult to centralize security in a distributed computing environment
- Increasing complexity of computer infrastructure administration and management
Security Challenges

Top Security Challenges
1. Increase in sophisticated cyber criminals
2. Data leakage, malicious insiders, and remote workers
3. Mobile security, adaptive authentication, and social media strategies
4. Cyber security workforce
5. Exploited vulnerabilities, operationalizing security
6. Critical infrastructure protection
7. Balancing sharing with privacy requirements
8. Identity access strategies and lifecycle

List of Security Risks
1. Trojans/Info Stealing Keyloggers/
2. Fast Flux Botnets
3. Data Loss/Breaches
4. Internal Threats
5. Organized Cyber Crime
6. Phishing/Social Engineering
7. New emerging viruses
8. Cyber Espionage
9. Zero-Day Exploits
10. Web 2.0 Threats
11. Vishing attacks
12. Identity black market
13. Cyber-extortion
14. Transportable data (USB, laptops, backup tapes)
15. “Zombie” networks
16. Exploits in new technology
17. Outsourcing projects
18. Social networking
20. Virtualization and cloud Computing

Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.
Module Flow

1. Info Security Overview
2. Hacking Concepts
3. Hacking Phases
4. Vulnerability Research
5. Ethical Hacking
6. Types of Attacks
Effects of Hacking

Damage to information and theft of information

Attackers may also use these PCs as “spam zombies” or “spam bots”

Attackers use backdoors such as Trojan horses, rootkits, viruses, and worms to compromise systems

Theft/damage of client or customer/business data, credit card details, and social security numbers, for identity fraud or theft

Theft of email addresses for spamming, passwords for access to online banking, ISP, or web services
Effects of Hacking on Business

1. According to the Symantec 2010 State of Enterprise Security Study, hacking attacks cost large businesses an average of about $2.2 million per year.

2. Theft of customers' personal information may risk the business's reputation and invite lawsuits.

3. Hacking can be used to steal, pilferage, and redistribute intellectual property, leading to business loss.

4. Attackers may steal corporate secrets and sell them to competitors, compromise critical financial information, and leak to the rivals.

5. Botnets can be used to launch various types of DoS and other web-based attacks which may lead to business down-time and significant loss of revenues.
Who is a Hacker?

Intelligent individuals with excellent computer skills, with the ability to create and explore into the computer’s software and hardware.

For some hackers, hacking is a hobby to see how many computers or networks they can compromise.

Their intention can either be to gain knowledge or to poke around to do illegal things.

Some do hacking with malicious intent behind their escapades, like stealing business data, credit card information, social security numbers, email passwords, etc.
**Black Hats**

Individuals with extraordinary computing skills, resorting to malicious or destructive activities and are also known as crackers.

**White Hats**

Individuals professing hacker skills and using them for defensive purposes and are also known as security analysts.

**Suicide Hackers**

Individuals who aim to bring down critical infrastructure for a "cause" and are not worried about facing 30 years in jail for their actions.

**Gray Hats**

Individuals who work both offensively and defensively at various times.
Hacktivism is an act of promoting a political agenda by hacking, especially by defacing or disabling websites.

It thrives in the environment where information is easily accessible.

Aims at sending a message through their hacking activities and gaining visibility for their cause.

Common targets include government agencies, multinational corporations, or any other entity perceived as bad or wrong by these groups or individuals.

It remains a fact, however, that gaining unauthorized access is a crime, no matter what the intention is.
What Does a **Hacker** Do?

**Hacking Phases**

1. **Reconnaissance**
2. **Scanning**
3. **Gaining Access**
4. **Maintaining Access**
5. **Clearing Track**
Phase 1 - **Reconnaissance**

1. Reconnaissance refers to the preparatory phase where an attacker seeks to gather information about a target prior to launching an attack.

2. Could be the future point of return, noted for ease of entry for an attack when more about the target is known on a broad scale.

3. Reconnaissance target range may include the target organization’s clients, employees, operations, network, and systems.
Phase 1 - Reconnaissance

Reconnaissance Types

Passive Reconnaissance
- Passive reconnaissance involves acquiring information without directly interacting with the target
- For example, searching public records or news releases

Active Reconnaissance
- Active reconnaissance involves interacting with the target directly by any means
- For example, telephone calls to the help desk or technical department
Phase 2 - Scanning

Pre-Attack Phase
Scanning refers to the pre-attack phase when the attacker scans the network for specific information on the basis of information gathered during reconnaissance.

Port Scanner
Scanning can include use of dialers, port scanners, network mapping, sweeping, vulnerability scanners, etc.

Extract Information
Attackers extract information such as computer names, IP address, and user accounts to launch attack.
Phase 3 – Gaining Access

- Gaining access refers to the point where the attacker obtains access to the operating system or applications on the computer or network.

- The attacker can escalate privileges to obtain complete control of the system. In the process, intermediate systems that are connected to it are also compromised.

- The attacker can gain access at the operating system level, application level, or network level.

- Examples include password cracking, buffer overflows, denial of service, session hijacking, etc.
Phase 4 – Maintaining Access

- Maintaining access refers to the phase when the attacker tries to retain his or her ownership of the system.
- Attackers may prevent the system from being owned by other attackers by securing their exclusive access with Backdoors, RootKits, or Trojans.
- Attackers use the compromised system to launch further attacks.
- Attackers can upload, download, or manipulate data, applications, and configurations on the owned system.
Phase 5 – Covering Tracks

Covering tracks refers to the activities carried out by an attacker to hide malicious acts.

The attacker’s intentions include: Continuing access to the victim’s system, remaining unnoticed and uncaught, deleting evidence that might lead to his prosecution.

The attacker overwrites the server, system, and application logs to avoid suspicion.

Attackers always cover tracks to hide their identity.
Types of **Attacks** on a System

- There are several ways an attacker can **gain access to a system**.
- The attacker must be able to **exploit a weakness or vulnerability in a system**.

**Types of Attacks**

- Operating system attacks
- Configuration attacks
- Application level attacks
- Shrink wrap code attacks
Types of Attacks on a System

- Eavesdropping
- Identity Spoofing
- Snoopin Attacks
- Interception
- Replay Attacks

- Data Modification Attacks
- Repudiation Attacks
- DoS Attacks
- DDoS Attacks
- Password Guessing Attacks

- Man-in-the-Middle Attacks
- Back door Attacks
- Spoofing Attacks
- Compromised-Key Attacks
- Application-Layer Attacks
Operating System Attacks

Attackers search for **OS vulnerabilities** and exploit them to **gain access** to a network system.

Some of the OS vulnerabilities:
1. Buffer overflow vulnerabilities
2. Bugs in operating system
3. Unpatched operating system
Application-Level Attacks

- Software applications come with tons of functionalities and features
- There is a dearth of time to perform complete testing before releasing products

Other application-level attacks include:
- Phishing
- Session hijacking
- Man-in-the-middle attack
- Parameter/Form Tampering
- Directory traversal attacks

Poor or non-existent error checking in applications leads to:
- Buffer overflow attacks
- Active content
- Cross-site scripting
- Denial of service and SYN attacks
- SQL injection attacks
- Malicious bots
Shrink Wrap Code Attacks

- Why reinvent the wheel when you can buy off-the-shelf "libraries" and code?
- When you install an OS/Application, it comes with tons of sample scripts to make the life of an administrator easy
- The problem is "not fine tuning" or customizing these scripts
- This will lead to default code or shrink wrap code attacks
Misconfiguration Attacks

If a system is misconfigured, such as a change is made in the file permission, it can no longer be considered as secure.

The administrators are expected to change the configuration of the devices before they are deployed in the network. Failure to do this allows the default settings to be used to attack the system.

In order to optimize the configuration of the machine, remove any redundant services or software.
Why Ethical Hacking is Necessary?

As hacking involves creative thinking, **vulnerability testing** and **security audits** cannot ensure that the network is secure.

To achieve this, organizations need to implement a "defense in depth" strategy by penetrating into their networks to estimate vulnerabilities and expose them.

Ethical hacking is necessary because it allows the countering of attacks from malicious hackers by **anticipating methods** they can use to **break into a system**.
Defense in depth is a security strategy in which several protection layers are placed throughout an information system. It helps to prevent direct attacks against an information system and data because a break in one layer only leads the attacker to the next layer.
Scope and Limitations of Ethical Hacking

Scope
Ethical hacking is a crucial component of risk assessment, auditing, counterfraud, best practices, and good governance.

Scope
It is used to identify risks and highlight the remedial actions, and also reduces information and communications technology (ICT) costs by resolving those vulnerabilities.

Limitations
However, unless the businesses first know what it is at that they are looking for and why they are hiring an outside vendor to hack systems in the first place, chances are there would not be much to gain from the experience.

Limitations
An ethical hacker thus can only help the organization to better understand their security system, but it is up to the organization to place the right guards on the network.
What Do Ethical Hackers Do?

Ethical hackers try to answer the following questions:

- What can the intruder see on the target system? (Reconnaissance and Scanning phases)
- What can an intruder do with that information? (Gaining Access and Maintaining Access phases)
- Does anyone at the target notice the intruders’ attempts or successes? (Reconnaissance and Covering Tracks phases)

- Ethical hackers are hired by organizations to attack their information systems and networks in order to **discover vulnerabilities** and **verify that security measures** are functioning correctly.

- Their duties may include **testing systems and networks for vulnerabilities** and attempting to access sensitive data by breaking security controls.
Skills of an Ethical Hacker

**Platform Knowledge**
Has in-depth knowledge of target platforms, such as Windows, Unix, and Linux.

**Network Knowledge**
Has exemplary knowledge of networking and related hardware and software.

**Computer Expert**
Should be a computer expert adept at technical domains.

**Security Knowledge**
Has knowledge of security areas and related issues.

**Technical Knowledge**
Has “high technical” knowledge to launch the sophisticated attacks.
Vulnerability Research

- The process of **discovering vulnerabilities and design flaws** that will open an operating system and its applications to attack or misuse.
- Vulnerabilities are classified based on **severity level** (low, medium, or high) and **exploit range** (local or remote).

An administrator needs vulnerability research:

- To identify and correct the network vulnerabilities
- To protect the network from being attacked by intruders
- To get information that helps to prevent the security problems
- To gather information about viruses
- To find weaknesses and alert the network administrator before a network attack
- To know how to recover from a network attack
Vulnerability Research Websites

- US-CERT Vulnerability Notes Database: http://www.kb.cert.org
- National Vulnerability Database: http://nvd.nist.gov
- Secunia CSI: http://www.secunia.com
- SecuriTeam: http://www.securiteam.com
Vulnerability Research Websites

- **CodeRed Center**
  - [http://www.eccouncil.org](http://www.eccouncil.org)

- **SecurityTracker**
  - [http://www.securitytracker.com](http://www.securitytracker.com)

- **Symantec**
  - [http://www.symantec.com](http://www.symantec.com)

- **TechNet**
  - [http://blogs.technet.com](http://blogs.technet.com)

- **Hackerstorm Vulnerability Database Tool**
  - [http://www.hackerstorm.com](http://www.hackerstorm.com)

- **HackerWatch**
  - [http://www.hackerwatch.org](http://www.hackerwatch.org)

- **SecurityFocus**
  - [http://www.securityfocus.com](http://www.securityfocus.com)

- **Security Magazine**
  - [http://www.securitymagazine.com](http://www.securitymagazine.com)
Vulnerability Research Websites

- SC Magazine
  http://www.scmagazine.com

- Computerworld
  http://www.computerworld.com

- Techworld
  http://www.techworld.com

- Hacker Journals
  http://www.hackerjournals.com

- Help Net Security
  http://www.net-security.org/

- CNET Blogs
  http://news.cnet.com

- Security Watch
  http://securitywatch.eweek.com

- Windows Security Blogs
  http://blogs.windowsecurity.com
What is Penetration Testing?

Penetration testing is a method of actively evaluating the security of an information system or network by simulating an attack from a malicious source.

Security measures are actively analyzed for design weaknesses, technical flaws, and vulnerabilities.

Active Assessment

Attack Stimulation

Black box testing simulates an attack from someone who is unfamiliar with the system, and white box testing simulates an attacker that has knowledge about the system.

The results are delivered comprehensively in a report to executive, management, and technical audiences.
Why Penetration Testing?

- **Identify the threats** facing an organization's information assets
  - Reduce an organization's IT security costs and **provide a better return on security investment (ROSI)** by identifying and resolving vulnerabilities and weaknesses

- Provide an organization with assurance - a thorough and **comprehensive assessment** of organizational security covering policy, procedure, design, and implementation
  - Gain and maintain **certification to an industry regulation** (BS7799, HIPAA etc.)

- **Adopt best practices** by conforming to legal and industry regulations
  - Focus on high severity vulnerabilities and **emphasize application-level security issues** to development teams and management

- Provide a comprehensive approach of preparation steps that can be taken to prevent upcoming exploitation
  - Evaluate the efficiency of **network security devices** such as firewalls, routers, and web servers
Penetration Testing Methodology

1. Information Gathering
2. Vulnerability Analysis
3. External Penetration Testing
4. Internal Network Penetration Testing
5. Router and Switches Penetration Testing
6. Firewall Penetration Testing
7. IDS Penetration Testing
8. Password Cracking Penetration Testing
9. Wireless Network Penetration Testing
10. Application Penetration Testing
11. Social Engineering Penetration Testing
12. Denial of Service Penetration Testing
13. Stolen Laptop, PDAs, and Cell Phones Penetration Testing

Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.
Penetration Testing Methodology

- Physical Security Penetration Testing
- Database Penetration Testing
- VoIP Penetration Testing
- VPN Penetration Testing
- War Dialing
- Virus and Trojan Detection
- Log Management Penetration Testing
- File Integrity Checking
- Bluetooth and Handheld Device Penetration Testing
- Communication System Penetration Testing
- Email Security Penetration Testing
- Security Patches Penetration Testing
- Data Leakage Penetration Testing
Module Summary

- Ethical hacking enables organizations to counter attacks from malicious hackers by anticipating certain attacks by which they can break into the system.

- An ethical hacker helps in evaluating the security of a computer system or network by simulating an attack by a malicious user.

- Ethical hacking is a crucial component of risk assessment, auditing, counterfraud, best practices, and good governance.

- Ethical hackers can help organizations to better understand their security systems and identify the risks, highlight the remedial actions, and also reduce ICT costs by resolving those vulnerabilities.
The greatest enemy of knowledge is not ignorance, it is the illusion of knowledge.

- Stephen Hawking, Theoretical Physicist and Cosmologist