ITDO6014
ETHICAL HACKING AND FORENSICS

Module 1: Cybercrime and Ethical Hacking

Course Objectives

- 1 To understand the concept of cybercrime and principles behind ethical hacking.
- 2 To explore the fundamentals of digital forensics, digital evidence and incident response.
- 3 To learn the tools and techniques required for computer forensics.
- 4 To understand the network attacks and tools and techniques required to perform network
- forensics.
- 5 To learn how to investigate attacks on mobile platforms.
- 6 To generate a forensics report after investigation.

Course Outcomes

- Define the concept of ethical hacking.
- Recognize the need of digital forensics and define the concept of digital evidence and incident response.
- Apply the knowledge of computer forensics using different tools and techniques.
- Detect the network attacks and analyze the evidence.
- Apply the knowledge of computer forensics using different tools and techniques.
- List the method to generate legal evidence and supporting investigation reports

Grading

Internal Assessment	20 Marks
Theory	80 Marks
Total	100 Marks

Text Book:

1. John Sammons, "The Basics of Digital Forensics: The Premier for Getting Started in Digital Forensics", 2nd Edition, Syngress, 2015.

2. Nilakshi Jain, Dhananjay Kalbande, "Digital Forensic: The fascinating world of Digital Evidences" Wiley India Pvt Ltd 2017.

3. Jason Luttgens, Matthew Pepe, Kevin Mandia, "Incident Response and computer forensics",3rd Edition Tata McGraw Hill, 2014.

What is cybercrime?

- Cybercrime is defined as any criminal misconduct carried out through a network, technical gadgets, or the internet. Although some cybercrimes are intended to cause harm to the victim, the vast majority are committed for financial gain.
- the 1834 hack to be the first cyberattack in history.
- Only two years after the invention of the telephone, adolescent guys stole into Alexander Graham Bell's telephone firm and wreaked havoc by misleading calls. Phone hacking, also known as phreaking, became popular in the 1960s and 1980s.

What is cybercrime?

- Rene Carmille, a French computer scientist, broke into the Nazi data registry in 1940 to disrupt their intentions to identify and monitor Jews.
- The introduction of email in the 1980s brought with it phishing schemes and viruses sent via attachments. Web browsers, like computer viruses, had grown prevalent by the 1990s.

Types of cybercrimes

- Cyber crimes can be classified in to 4 major categories as the following:
- 1) Cyber crime against **Individual**
- (2) Cyber crime Against **Property**
- (3) Cyber crime Against **Organization**
- (4) Cyber crime Against **Society**

Types of cybercrimes

- **(1) Against Individuals**
- (i) Email spoofing : A spoofed email is one in which the e-mail header is forged so that the mail appears to originate from one source but actually has been sent from another source.
- (ii) Spamming : Spamming means sending multiple copies of unsolicited mails or mass e-mails such as chain letters.
- (iii) Harassment & Cyber stalking : Cyber Stalking Means following an individual's activity over internet. It can be done with the help of many protocols available such as e- mail, chat rooms, user net groups.

Types of cybercrimes

- **(2) Against Property**
- (i) Credit Card Fraud : As the name suggests, this is a fraud that happens by the use of a credit card. This generally happens if someone gets to know the card number or the card gets stolen.
- (ii) Intellectual Property crimes : These include Software piracy: Illegal copying of programs, distribution of copies of software. Copyright infringement: Using copyrighted material without proper permission. Trademarks violations: Using trademarks and associated rights without permission of the actual holder. Theft of computer source code: Stealing, destroying or misusing the source code of a computer.

Types of cybercrimes

- (iii) Internet time theft : This happens by the usage of the Internet hours by an unauthorized person which is actually paid by another person.

- **(3) Against Organisations** UCDVESLTD
- (i) Unauthorized Accessing of Computer: Accessing the computer/network without permission from the owner. It can be of 2 forms:
- a) Changing/deleting data: Unauthorized changing of data. b) Computer voyeur: The criminal reads or copies confidential or proprietary information, but the data is neither deleted nor changed.

Types of cybercrimes

- (ii) Denial Of Service : When Internet server is **flooded with continuous bogus requests** so as to denying legitimate users to use the server or to crash the server.

- (iii) Computer contamination / Virus attack : A computer virus is a computer program that can infect other computer programs by modifying them in such a way as to include a (possibly evolved) copy of it. Viruses can be file infecting or affecting boot sector of the computer. Worms, unlike viruses do not need the host to attach themselves to.

Types of cybercrimes

- (iv) Email Bombing : **Sending large numbers of mails** to the individual or company or mail servers thereby ultimately resulting into crashing.
- (v) Salami Attack : When negligible amounts are removed & accumulated in to something larger. These attacks are used for the **commission of financial crimes**.
- (vi) Logic Bomb : It is an event dependent program. As soon as the designated event occurs, it crashes the computer, release a virus or any other harmful possibilities.

Types of cybercrimes

- (vii) Trojan Horse : This is an unauthorized program which functions from inside what seems to be an authorized program, thereby concealing what it is actually doing.

- (viii) Data diddling :
- Data diddling is a form of computer-based fraud where an individual **manipulates or alters data** with the intent of deceiving others or gaining some form of unauthorized advantage. This type of manipulation is often done discreetly, and the alterations might be subtle to avoid detection. The term "data diddling" is derived from the act of tweaking or diddling with data.

Types of cybercrimes

- (4) **Against Society**
- (i) Forgery : Currency notes, **revenue stamps, mark sheets etc. can be forged** using computers and high quality scanners and printers.
- (ii) Cyber Terrorism : Use of computer resources to intimidate or coerce people and carry out the activities of terrorism.
- (iii) Web Jacking : Hackers **gain access and control over the website of another**, even they change the content of website for fulfilling political objective or for money.

Types of cybercrimes

- **Cyberbullying**: Bullying an individual online is referred to as cyberbullying. Cyberbullying includes any threat to a person's safety, coercion of a person to say or do anything, and expressions of hatred or subjectivity against someone. While children are more likely to be victims of cyberbullying, adults are not exempt. According to a survey, 40% of polled teens said they had encountered online harassment, while 24% of adults aged 26–35 said they had experienced cyberbullying.

Types of cybercrimes

- **Malware**: Malware is a term that refers to any software program that is meant to infiltrate or harm a device. Viruses are a type of software that falls under the malware category. Viruses may cause a range of problems once they enter a device. They may **delete files, record your keystrokes, erase your disk drive**, or otherwise corrupt your data.
- **Phishing:** Phishing happens when **fraudsters act as an organisation** in order to dupe victims into disclosing important information. Scare techniques, such as notifying the victim that their bank account or personal device is under assault, are frequently used by cybercriminals to effectively fulfil their phishing aims.

Types of cybercrimes

- **Cyber spying:** Cyber spying occurs when hackers target a public or private entity's network in order to gain access to classified data, private information, or intellectual property. Cybercriminals may utilise the sensitive information they discover for a variety of purposes, including blackmail, extortion, public humiliation, and monetary gain.
- **Spyware:** Spyware is a software that cybercriminals employ to monitor and record their victims' actions and personal information. Often, a victim unintentionally downloads spyware onto their device, giving a cybercriminal unwitting access to their data. Cybercriminals can access a victim's credit card data, passwords, web cam, and microphone depending on the type of spyware employed.

Types of cybercrimes

- **Adware:** Adware is software that you may unintentionally download and install when installing another program. Every time someone views or clicks on an advertisement window, the developers of adware programs profit financially from their actions on people's computers. Although some adware software is lawful and innocuous, others are invasive due to the type and number of ads they display. Many nations consider some adware applications to be unlawful because they contain spyware, malware, and other dangerous software.

Types of cybercrimes

- **Hacking:** Any illegal access to a computer system is generally referred to as hacking. When a hacker gains unauthorised access to a company's or an individual's computers and networks, they can obtain access to important corporate information as well as personal and private data. Despite this, not all hackers are crooks. Some "white hat" hackers are employed by software businesses to identify faults and gaps in their surveillance systems. These hackers get into a company's network in order to uncover existing holes in their clients' systems and provide fixes to such issues.

Protection against cybercrime

- In order to protect ourselves from the perils of cybercrime, the following preventative actions can be taken:

- It is required to install an antivirus program. An antivirus program is designed to safeguard users against cybercrime. Modern programs monitor the machine's data for harmful content and give real-time security against dangers like phishing.
- Making use of a Virtual Private Network. A VPN connection will protect your online privacy. It's an important tool for privacy, which protects people from identity theft.

Protection against cybercrime

- In order to protect ourselves from the perils of cybercrime, the following preventative actions can be taken:

- Unsolicited emails, text messages, and phone calls should be avoided, especially if they utilise the crisis to coerce people into circumventing standard security safeguards.
- Change the Wi-Fi network's default password to something more secure. Limit the number of devices that may connect to the Wi-Fi network and only allow trustworthy devices to connect.

Protection against cybercrime

- In order to protect ourselves from the perils of cybercrime, the following preventative actions can be taken:

- Use lengthy and complicated passwords that incorporate numbers, letters, and special characters.
- Make sure to update all the systems and programs, as well as to install and maintain an antivirus software up to date.
- Data backup should be a routine procedure since data may be quickly destroyed, infected, or manipulated.

Prevention against cybercrime

- **Use complex passwords:** Use various login details combinations for separate accounts and avoid writing them down.
- **Keeping online profiles secret:** Make sure to keep your social networking profiles (Facebook, Twitter, YouTube, and so on) private. Make sure to double-check your security settings. Take caution with the information you put on the internet. Once it's on the Internet, it's there for good.
- **Safeguarding data:** Encrypt sensitive files such as financial documents and tax returns, to protect your data.

Prevention against cybercrime

- **Safeguard mobile devices:** Many individuals are unaware that their mobile devices are exposed to dangerous software such as computer viruses. An individual should only download software from reputable sites. It is also critical that your operating system is kept up to date. Install anti-virus software and utilize a secure lock screen in addition. Otherwise, if you misplace your phone or lay it down for a few seconds, anyone may see all of your personal information on it. Someone may even install malicious software that uses GPS to follow your every step.

Prevention against cybercrime

- **Secure online identity:** When it comes to protecting one's identity online, an individual should be vigilant. When providing personal information such as your name, address, phone number, and/or financial information on the Internet, you must exercise extreme caution. While making an online purchase, etc., be sure to check whether the websites are safe. This includes turning on your privacy settings while using or visiting social networking sites.

Prevention against cybercrime

- **Safeguarding computers with security software:** For basic internet security, several types of security softwares are required. Firewall and antivirus software are key pieces of security software. A firewall is typically the first line of defence for your computer. It governs who can communicate, and access the computer via the internet. Assume a firewall to be a type of ‘policeman’ who monitors all data attempting to flow to and from the computer via the Internet, permitting transactions that it knows are secure while preventing ‘bad’ traffic such as cyberattacks.

Types of Cyber Criminals

- **1. Hackers:** The term hacker may refer to anyone with technical skills, however, it typically refers to an **individual who uses his or her skills to achieve unauthorized access to systems or networks so as to commit crimes.** The intent of the burglary determines the classification of those attackers as white, grey, or black hats.
- **(a). White Hat Hackers – These hackers utilize their programming aptitudes for a good and lawful reason**. These hackers may perform network penetration tests in an attempt to compromise networks to discover network vulnerabilities. Security vulnerabilities are then reported to developers to fix them.

Types of Cyber Criminals

- **(b). Gray Hat Hackers – These hackers carry out violations and do seemingly deceptive things however not for individual addition or to cause harm.** These hackers may **disclose** a vulnerability to the **affected organization** after having compromised their network.
- **(c). Black Hat Hackers** – These hackers are **unethical criminals** who violate network security for personal gain. They misuse vulnerabilities to bargain PC frameworks.

Types of Cyber Criminals

- **Internet stalkers:** Internet stalkers are people who maliciously monitor the web activity of their victims to acquire personal data. This type of cyber crime is conducted through the use of social networking platforms and malware, that are able to track an individual's PC activity with little or no detection.
- **Disgruntled Employees:** Disgruntled employees become hackers with a particular motive and also commit cyber crimes. It is hard to believe that dissatisfied employees can become such malicious hackers. In the previous time, they had the only option of going on strike against employers. But with the advancement of technology there is increased in work on computers and the automation of processes, it is simple for disgruntled employees to do more damage to their employers and organization by committing cyber crimes. The attacks by such employees brings the entire system down

Types of Cyber Criminals

- **Phreakers:** They are the ones who gain **illegal access to the telephone system**. They are considered to be the original computer hackers as they are the ones who break into telephone system illegally and make long distance calls. Phreaker word is a combination of, “Phone” + “Freak”. Many real hackers are phreakers since they deduct the cost of their telephone bills and continue skimming off networks in a more serene way. The emergence of the Internet and the significant fall in the costs of Telecommunications has remedied a great part to this problem. Nevertheless, there are phreakers who still take up the challenge to hack telephone networks.

Ethical Hacking

- Ethical hacking involves an authorized attempt to gain unauthorized access to a computer system, application, or data. Carrying out an ethical hack involves duplicating strategies and actions of malicious attackers. This practice helps to identify security vulnerabilities which can then be resolved before a malicious attacker has the opportunity to exploit them.
- Also known as “white hats,” ethical hackers are security experts that perform these security assessments. The proactive work they do helps to improve an organization’s security posture. With prior approval from the organization or owner of the IT asset, the mission of ethical hacking is opposite from malicious hacking.
- Ethical Hacker hacks the target system before any harmful hacker can. This allows the security team of the organization to apply a security patch in the system and effectively eliminate an opening for the attacker to enter the system or execute a hack.

Phases of Ethical Hacking

Phases of Ethical Hacking

- There are multiple phases involved in any elaborate hacking process.

RSGMACRP

- **Reconnaissance:**
- **Objective:** Gather information about the target system or network.
- **Example:** A penetration tester may use publicly available information, such as domain names, IP addresses, and organizational details, to build a profile of the target.

Phases of Ethical Hacking

Scanning:

- **Objective:** Identify live hosts, open ports, and services running on the target.
- **Example:** Using network scanning tools like Nmap or Nessus to discover active devices, open ports, and potential vulnerabilities on the target network.

Gaining Access (or Gaining a Foothold):

- **Objective:** Exploit vulnerabilities to gain initial access to the system.
- **Example:** Attempting to exploit known vulnerabilities in software or misconfigurations to gain unauthorized access. This could involve using techniques like SQL injection, cross-site scripting (XSS), or exploiting weak passwords.

Phases of Ethical Hacking

- **Maintaining Access:**
  - **Objective:** Establish a persistent presence on the system to simulate a real-world threat.
  - **Example:** Creating backdoors or planting malware to maintain access even if the initial vulnerability is patched. This phase helps assess an organization's ability to detect and respond to ongoing attacks.
- **Analysis:**
  - **Objective:** Collect and analyze data from the compromised system for further exploitation or to identify additional vulnerabilities.
  - **Example:** Extracting sensitive information, such as user credentials or critical data, to demonstrate the potential impact of a successful cyberattack.

Phases of Ethical Hacking

- **Covering Tracks:**
  - **Objective:** Erase or conceal evidence of the ethical hacking activities to simulate an attacker covering their tracks.
  - **Example:** Deleting logs, modifying timestamps, or taking other measures to make it harder for defenders to trace the ethical hacker's activities.
- **Reporting:**
  - **Objective:** Document and communicate findings, including vulnerabilities discovered, the extent of potential damage, and recommendations for remediation.
  - **Example:** Providing a detailed report that outlines the security weaknesses identified during the ethical hacking process, along with prioritized recommendations for mitigating those vulnerabilities.

Phases of Ethical Hacking

- **Post-Testing Actions:**
  - **Objective:** Assist the organization in implementing security measures to address identified vulnerabilities.
  - **Example:** Collaborating with the organization's IT and security teams to implement patches, configuration changes, or other measures to enhance the security posture based on the ethical hacker's recommendations.
- Throughout these phases, ethical hackers follow a strict code of ethics and adhere to legal guidelines to ensure that their activities are authorized, transparent, and conducted in a responsible manner. The goal is to help organizations improve their security by proactively identifying and addressing vulnerabilities before malicious actors can exploit them.

Rules of Ethical Hacking

- Here are the most important rules of Ethical Hacking:
- An ethical hacker must seek authorization from the organization that owns the system. Hackers should obtain complete approval before performing any security assessment on the system or network.
- Determine the scope of their assessment and make known their plan to the organization.
- Report any security breaches and vulnerabilities found in the system or network.

Rules of Ethical Hacking

- Keep their discoveries confidential. As their purpose is to secure the system or network, ethical hackers should agree to and respect their non-disclosure agreement.
- Erase all traces of the hack after checking the system for any vulnerability. It prevents malicious hackers from entering the system through the identified loopholes.

Goals of Ethical Hacking

- Hack your systems in a non destructive fashion
- Enumerate vulnerabilities and if, necessary, prove to upper management that vulnerabilities exists.
- Apply results to remove vulnerabilities & better
- secure your systems.