TU – BCA

ENGLISH-II

FONT-FACE SHOULD BE “TIMES NEW ROMAN”

FONT-SIZE SHOULD BE 12

CONTENT MUST BE JUSTIFIED

DON’T JUST ONLY USE ABBREVIATION

FOLLOW KISS PRINCIPAL

Your Name

Department of English

CACS 103: English II

Date

Ethical Hacking

Hearing the term ‘Hack’ sculpts a stereotypical thought of anti-social and illegal act into our brain, which is at odds with the term ‘Ethical Hacking’. Ethical hacking is a way of assessing the Information Security Environment of an organization, put into effect by individuals or groups who are adept in computers and networking. Ethical hacking can also be defined as the service that provides the securities for the customer’s networks, information assets and identifies the vulnerabilities to maintain the reputation of the corporate sectors before it exploits the company. Thus, ethical hacking can help in testing the systems/ networks by finding out various vulnerabilities.

Hacking is of different types such as back door hacking, viruses and malwares, Trojan horses, Denial of Services, crackers, and ethical hacking. The main aspect in ethical hacking is that target permission is essential for performing hacking on the information. In ethical hacking, a user (ethical hacker) will get permission to access the crucial data. Ethical hacking can be used while performing security audits in the organization. An ethical hack is performed by an Ethical Hacker. An ethical hacker is also referred as a white hat and a disreputable hacker/ malicious person is referred as a black hat. White hat hackers have the same knowledge and mindset as that of a malicious hacker but they use this knowledge ethically to defend against the malicious hackers. The goal of an ethical hack is neither to damage nor to steal any valuable information, it’s more of a service for a client to test their information technology (IT) environment on how it would defy an actual hacker attack.

This type of the hacking system provides the high securities to the customer’s methodologies and techniques to yield high qualities of framework. Ethical Hacking comprehends penetration testing, which is a method of evaluating the security of a computer system or network by simulating an attack from malicious outsiders (who do not have an authorized access to the organization's systems) and malicious insiders (who have some level of authorized access). Penetration testers use a combination of manual testing and automated tools to evaluate an organization's security posture. These tools can range from basic network scanners to advanced exploitation frameworks, such as the Metasploit Framework. This process involves an active analysis of the system for any potential vulnerabilities that could result from poor or improper system configuration, due to hardware or software flaws or operational weaknesses. The final output from this assessment is a detailed report about the detected problems and vulnerabilities and a possible solution for each of them. Security issues uncovered through the penetration test are presented to the system's owner.

Back in 2019, Nepal Electronic Payment System (NEPS), a shared card switching system of 17 banks, was targeted by Chinese hackers. The hackers allegedly injected malware into Nepal Electronic Payment System to drain the cash from the automated teller machines (ATMs). Nepal Electronic Payment System had claimed that Nepali banks lost over Rs 35 million in this cyber heist. Such types of fraudulent hacking and cyber-attacks in online/ IoT (Internet of Things)/ networking world are as common as robbery and theft in real world.

It is important to note that ethical hacking is a highly specialized field that requires a deep understanding of computer systems, networks, and applications, as well as an in-depth knowledge of hacking techniques and tools. Ethical hackers must also be familiar with various regulations and standards, such as the Payment Card Industry Data Security Standard (PCI DSS), the Health Insurance Portability and Accountability Act (HIPAA), and the Federal Risk and Authorization Management Program (FedRAMP).

“Government agencies and business organizations today are in constant need of ethical hackers to combat the growing threat to IT security. A lot of government agencies, professionals and corporations now understand that if you want to protect a system, you cannot do it by just locking your doors.” says Jav Bavisi, CEO of EC-Council. The growing field of Information Technology presumes online transactions, exchange of information through e-mails, use of web applications, cloud services and many more which is the ultimate target of hackers and security breachers. Also, unethical hacking creates havoc on busy networks. Here is where Ethical Hacking has our back, to protect our data privacy, to secure us on interwebs and provide us with fret-free computing/networking experience.

In conclusion, ethical hacking is a critical component of modern cybersecurity. By using hacking techniques to identify and fix security vulnerabilities in computer systems, networks, and applications, organizations can prevent malicious attacks and protect their customers. Ethical hackers are highly specialized professionals who work closely with organizations to assess their security posture and provide recommendations for remediation. To ensure the highest level of security, organizations should engage the services of a professional ethical hacking firm.