JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

CYBER SECURITY AND ETHICAL HACKING

Dr.P.Kannan[1],Mr.S.Akash[2] , Mr.T.Sibi Arasu[3] , Mr.S.Aswin[4]

1.Associate Professor, Department Of Computer Science, Dr.N.G.P Arts and Science College, Coimbatore
2.Student, Department Of Commerce With Information Technology, Dr.N.G.P Arts and Science College, Coimbatore
3. Student, Department Of Commerce With Information Technology, Dr.N.G.P Arts and Science College, Coimbatore
4. Student, Department Of Commerce With Information Technology, Dr.N.G.P Arts and Science College, Coimbatore

ABSTRACT

In an increasingly interconnected digital landscape, the importance of cyber security and ethical hacking cannot be overstated. This paper explores the fundamental concepts of cyber security, including threat landscape analysis, vulnerability assessment, and risk management strategies. Additionally, it delves into the ethical considerations and methodologies behind ethical hacking, emphasizing the role of ethical hackers in identifying and mitigating security vulnerabilities to protect individuals, organizations, and society as a whole. By examining real-world case studies and best practices, this paper aims to provide a comprehensive understanding of the symbiotic relationship between cyber security and ethical hacking in safeguarding information assets and promoting a secure digital ecosystem. Ethical hacking is the way to find out the weaknesses and vulnerabilities in the system or computer network. It is a way to describe the procedure of hacking in an ethical way for any network. The ethical hacker has the good purpose to do it. Basically, some of the hacker has even done very badly with some organizations like they have stolen very important information of their customers. In the government organizations they have damaged very confidential information like social security numbers and other sensitive information. A study shows that almost 90% attacks happen on the inside which shows that easy it is to invade into the system or network for insiders. We are tried to explore the ethics behind the ethical hacking and the problems lie with this particular field of information technology where security is concerned. Though ethical hacking has become a very upcoming technological subject from the last few years, now the doubt remains the true intentions of the hacker. Hackers in this context have had a very measurable impact of society.

KEYWORDS: *Cybersecurity, Ethical hacking, Network security, Information security, Encryption, Cyber Threat Intelligence*

I.INTRODUCTION

Cybersecurity is the practice of protecting computer systems, networks, and data from digital attacks. It encompasses various technologies, processes, and practices designed to defend against unauthorized access, exploitation, or damage.

Ethical hacking, also known as penetration testing or white-hat hacking, is the authorized and legal practice of attempting to infiltrate computer systems, networks, or applications to
identify vulnerabilities and weaknesses. Ethical hackers use the same techniques as malicious hackers but do so with permission and for the purpose of improving security posture.

Ethical Hacking : To crack passwords or to steal data? No, it is much more than that. Ethical hacking is to scan vulnerabilities and to find potential threats on a computer or network. An ethical hacker finds the weak points or loopholes in a computer, web application or network and reports them to the organization. So, let's explore more about Ethical Hacking step-by- step.

2.Mechanisms of an attack

How to identify that an attack is happening Ways different types of attacks might affect the business Tion-oriented advice about how to defend against attacks Many forms of cyber-attacks are common today, including zero-day exploits, malware, phishing, man-in-the- middle attacks, and denial of service attacks. Different ways of attacking computer systems and networks constantly evolve as cybercriminals find new vulnerabilities to exploit. Cyber Threat Intelligence (CTI) helps organizations stay informed about new threats so that they can protect themselves. Cyber security experts organize, analyze, and refine the information they gather about attacks to learn from and use it to protect businesses better.

Threat intelligence (or security intelligence) also helps stop or mitigate an attack that is in -progress. The more an IT team understands about an attack, the better they will be able to make an informed decision about how to combat it.

There are different types of threat intelligence, from high-level, and non-technical information to technical details about specific attacks. Here are a few different kinds of threat intelligence:

Strategic: Strategic threat intelligence is high-level information that puts the threat in context. It is non-technical information that an organization could present to a board of directors. An example of strategic threat intelligence is the risk analysis of how a business decision might make the organization vulnerable to cyber attacks.

Tactical: Tactical threat intelligence includes the details of how threats are being carried out and defended against, including attack vectors, tools, and infrastructures attackers are using, types of businesses or technologies that are targeted, and avoidance strategies. It also helps an organization understand how likely they are to be a target for different types of attacks.

Cybersecurity experts use tactical information to make informed decisions about security controls and managing defenses**.**

Operational: Operational threat intelligence is information that an IT department can use as part of active threat management to take action against a specific attack. It is information about the intent behind the attack, as well as the nature and timing of the attack. Ideally, this information is gathered directly from the attackers, which makes it difficult to obtain.

Technical: Technical threat intelligence is specific evidence that an attack is happening or indicators of compromise (IOCs). Some threat intelligence tools use artificial intelligence to scan for these indicators, which might include email content from phishing campaigns, IP addresses of C2 infrastructures, or artifacts from known malware samples.

3. DATA PROTECTION

Data protection is a critical aspect of cybersecurity aimed at safeguarding sensitive information from unauthorized access, disclosure, alteration, or destruction. Here are some key elements of data protection in cybersecurity:

Encryption: Encrypting data ensures that even if unauthorized parties gain access to it, they cannot decipher its contents without the encryption key

Access Control: Implementing access controls ensures that only authorized users can access certain data or systems. This involves the use of authentication mechanisms like passwords, biometrics, or multi-factor authentication.

Data Loss Prevention (DLP): DLP solutions help prevent sensitive data from being leaked, either intentionally or unintentionally, by monitoring, detecting, and blocking unauthorized data transfers

Data Masking and Anonymization: Data masking techniques obscure sensitive information by replacing real data with fictitious data while maintaining its format. Anonymization goes a step further by removing personally identifiable information (PII) from data sets to protect individual identities.

Backup and Recovery: Regularly backing up data and having robust recovery mechanisms in place ensure that data can be restored in case of loss or corruption due to cyber attacks or other incidents.

Data Classification: Classifying data based on its sensitivity and importance helps prioritize protection measures and allocate resources effectively

Security Awareness Training: Educating employees and users about best practices for handling sensitive data, recognizing phishing attempts, and understanding their role in maintaining data security is essential for a comprehensive data protection strategy.

FEATURES OF CYBER SECURITY AND ETHICAL HACKING

Cybersecurity:

Protection: Cybersecurity focuses on safeguarding digital systems, networks, and data from unauthorized access, breaches, and attacks.

` **Risk Management**: It involves assessing risks, identifying vulnerabilities, and implementing measures to mitigate them.

Compliance: Cybersecurity professionals ensure that organizations adhere to regulatory requirements and industry standards to protect sensitive information.

Incident Response: Cybersecurity teams are responsible for detecting, responding to, and recovering from security incidents and breaches.

Continuous Monitoring: Monitoring systems for potential threats and anomalies is crucial in cybersecurity to detect and respond to threats promptly.

Encryption: Implementing encryption techniques to secure data both in transit and at rest is a fundamental aspect of cybersecurity.

Authentication and Access Control: Establishing robust authentication mechanisms and access controls to limit unauthorized access to sensitive information.

Ethical Hacking:

Authorized Testing: Ethical hackers are authorized professionals who simulate cyberattacks to identify vulnerabilities in systems, networks, and applications.

Penetration Testing: Ethical hackers conduct penetration tests to assess the security posture of an organization by attempting to exploit vulnerabilities.

Reporting and Remediation: After identifying vulnerabilities, ethical hackers provide detailed reports to organizations, along with recommendations for remediation.

White-Hat Approach: Ethical hackers adhere to ethical guidelines and legal frameworks while performing their assessments, ensuring they don't cause harm or breach privacy.

Knowledge Sharing: Ethical hacking involves sharing insights and knowledge gained from security assessments to improve overall cybersecurity practices.

Tool Proficiency: Ethical hackers are proficient in using a variety of tools and techniques, including vulnerability scanners, network analyzers, and exploitation frameworks.

Continuous Learning: Given the evolving nature of cybersecurity threats, ethical hackers continuously update their skills and knowledge to stay ahead of potential attackers.

In summary, cybersecurity focuses on defending against and mitigating threats, while ethical hacking involves proactively testing systems for vulnerabilities to enhance overall security posture. Both are critical components of modern cybersecurity strategies.

5.TECHNOLOGY OF CYBER SECURITYAND ETHICAL HACKING

Cybersecurity technology encompasses various tools and practices aimed at protecting computer systems, networks, and data from unauthorized access, attacks, and breaches. Some key technologies and practices in cybersecurity and ethical hacking include:

Firewalls: Firewalls are network security devices that monitor and control incoming and outgoing network traffic based on predetermined security rules. They act as a barrier between trusted internal networks and untrusted external networks, such as the internet.

Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS): IDS and IPS are security appliances or software solutions that monitor network traffic for suspicious activity or policy violations. IDS detect potential threats, while IPS can take proactive measures to block or prevent those threats from reaching their targets.

Encryption: Encryption technology protects sensitive data by converting it into unreadable code that can only be accessed with the correct decryption key. It is widely used to secure communications, data storage, and authentication processes.

Vulnerability Assessment and Penetration Testing (VAPT): VAPT involves assessing and identifying security vulnerabilities in systems, networks, and applications. Penetration testing, a subset of VAPT, involves simulating cyberattacks to evaluate the security posture of an organization and identify weaknesses that malicious actors could exploit.

Security Information and Event Management (SIEM): SIEM systems collect, analyze, and correlate security event data from various sources across an organization's IT infrastructure. They provide real-time monitoring, threat detection, incident response, and compliance reporting capabilities.

Endpoint Security: Endpoint security solutions protect individual devices, such as computers, smartphones, and tablets, from malware, unauthorized access, and other security threats. They often include antivirus software, host-based intrusion detection/prevention systems, and device encryption capabilities.

S**ecure Software Development Lifecycle (SSDLC)**: SSDLC is an approach to integrating security into every phase of the software development process, from design and coding to testing and deployment. It aims to identify and mitigate security vulnerabilities early in the development lifecycle.

Ethical hacking, also known as penetration testing or white-hat hacking, involves authorized attempts to exploit vulnerabilities in systems, networks, or applications to identify and address security weaknesses before malicious hackers can exploit them. Ethical hackers use many of the same techniques and tools as malicious hackers but do so with permission and for the purpose of improving security. They play a crucial role in helping organizations proactively defend against cyber threats and protect their assets and data.

Secure Software Development Lifecycle (SSDLC): SSDLC is an approach to integrating security into every phase of the software development process, from design and coding to testing and deployment. It aims to identify and mitigate security vulnerabilities early in the development lifecycle.

Ethical hacking, also known as penetration testing or white-hat hacking, involves authorized attempts to exploit vulnerabilities in systems, networks, or applications to identify and address security weaknesses before malicious hackers can exploit them. Ethical hackers use many of the same techniques and tools as malicious hackers but do so with permission and for the purpose of improving security. They play a crucial role in helping organizations proactively defend against cyber threats and protect their assets and data.

6.STEPS ETHICAL HACKING

Reconnaissance

Before performing any penetration tests, hacker's footprint the system and gather as much information as possible. Reconnaissance is a preparatory phase where the hacker documents the organization's request, finds the system's valuable configuration and login information and probes the networks. This information is crucial to performing the attacks and includes:

Scanning

In this stage, the ethical hacker begins testing the networks and machines to identify potential attack surfaces. This involves gathering information on all machines, users, and services within the network using automated scanning tools.

Gaining Access

Once ethical hackers expose vulnerabilities through the process's first and second hacking phases, they now attempt to exploit them for administrative access. The third phase involves attempting to send a malicious payload to the application through the network, an adjacent subnetwork, or physically using a connected computer.

Maintaining Access

The fourth phase of the ethical hacking process involves processes to ensure the hacker can access the application for future use. A white-hat hacker continuously exploits the system for further vulnerabilities and escalates privileges to understand how much control attackers can gain once they pass security clearance. Some attackers may also try to hide their identity by removing the evidence of an attack and installing a backdoor for future access.

Clearing Tracks

To avoid any evidence that leads back to their malicious activity, hackers perform tasks that erase all traces of their actions. These include:

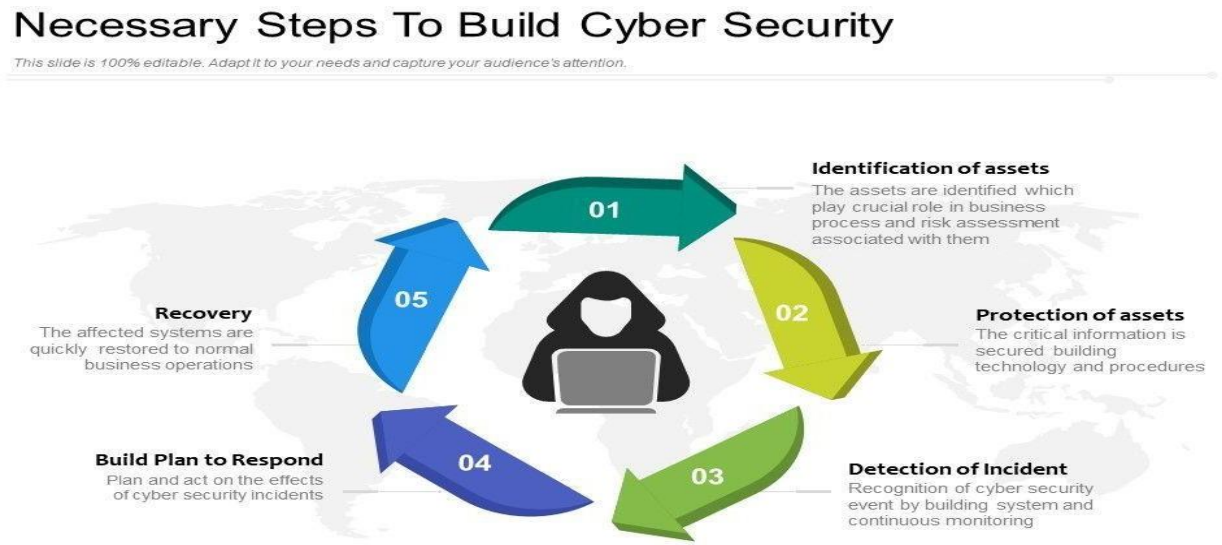
- Uninstalling scripts/applications used to carry out attacks

- Modifying registry values
- Clearing logs
- Deleting folders created during the attack

For those hackers looking to maintain undetected access, they tend to hide their identity using techniques such as:

- Tunneling
- Stenography

Having successfully performed all the 5 steps of ethical hacking, the ethical hacker then concludes the steps of ethical hacking by documenting a report on the vulnerabilities and suggesting remediation advice.



7.STEP OF CYBER SECURITY

PREPARATION: THE FIRST STEP TOWARDS A SECURE CYBER ENVIRONMENT

Preparation is about setting up the proper infrastructure and resources to safeguard your systems and data. This step involves the creation of cybersecurity policies, guidelines, and documentation to establish an environment that discourages cybercriminals. One key component of preparation is training employees on cybersecurity best practices to minimise the risk of a data breach.

- Creating and maintaining security policies
- Developing guidelines and procedures for employees
- Training employees on cybersecurity best practices
- Maintaining firewalls and other security systems

8.IDENTIFICATION: DETECTING AND ANALYZING THREATS

This step involves monitoring systems for suspected cyber-attacks. In this stage, cybersecurity professionals are looking for signs of suspicious activity, such as unusual login attempts or virus detection. The aim is to detect threats early so that they can be addressed before causing any significant harm.

- Using anti-malware and intrusion detection systems
- Analyzing system logs for unusual activity
- Monitoring network traffic
- Identifying potential security weaknesses and vulnerabilities

9.CONTAINMENT: ISOLATING AND LIMITING HARMFUL ACTIVITIES

Containment involves containing the threat once it has been identified. This step is about isolating the issue and limiting its spread to minimize further damage. This may include isolating affected devices or servers and securing them from being accessed by unapproved users.

- Isolating affected devices/servers from the network
- Disabling the user account used to initiate the attack
- Limiting access controls
- Stopping the spread of malware

10.ERADICATION: REMOVING THE THREAT

Once the threat has been contained, the next step is to eradicate it from the network or device entirely. It can be done by identifying the source of the attack, removing the infected files, or patching the vulnerabilities in the system. By removing the root cause, you prevent future attacks that may exploit the same vulnerability.

- Identifying and removing the source of the attack
- Removing infected files
- Patching system vulnerabilities
- Updating systems and software to eliminate the risk of further attacks

11.RECOVERY: RESTORING NORMAL OPERATIONS

Once the threat is eradicated, the focus is on restoring the network or device to normal operations. This may involve implementing new security protocols, performing backups of data, and restoring any affected systems. This stage is crucial to prevent further disruptions and ensure business continuity.

- Restoring data from backups
- Implementing new security protocols and processes
- Performing system checks and confirming that it can resume normal operations
- Communicating with stakeholders any downtime incurred, if necessary

12.LESSONS LEARNED: EVALUATING AND IMPROVING CYBERSECURITY MEASURES

The final step in the cybersecurity process is to evaluate and learn from the experience. This involves reviewing what was done well and what could have been improved, then implementing changes to prevent future cyber-attacks. Cybersecurity is a continuous process, and evaluating and improving measures is essential to stay ahead of cybercriminals.

- Conducting post-incident analysis to identify lessons learned

- Implementing changes across the organization's cybersecurity infrastructure to prevent future cyber-attacks
- Benchmarking past performance against industry standards and making recommendations for improvement

13.CONCLUSION

In conclusion, the symbiotic relationship between cybersecurity and ethical hacking underscores the dynamic and evolving landscape of digital defense in today's interconnected world. Ethical hacking serves as a proactive mechanism for identifying vulnerabilities, bolstering resilience, and fortifying defenses against malicious cyber threats. By adhering to ethical principles and legal frameworks, ethical hackers play a pivotal role in promoting transparency, accountability, and trust in digital ecosystems.

Together, cybersecurity and ethical hacking form the cornerstone of a comprehensive defense strategy aimed at thwarting cyber adversaries, protecting sensitive data, and ensuring the uninterrupted operation of vital infrastructure. Collaboration, knowledge sharing, and a commitment to ethical conduct are essential tenets that underpin the effectiveness of both disciplines in mitigating emerging threats and staying ahead of evolving attack vectors.

In an era marked by unprecedented digital innovation and pervasive connectivity, the imperative for organizations and individuals to prioritize cybersecurity and embrace ethical hacking practices cannot be overstated. By fostering a culture of cybersecurity awareness, investing in cutting-edge technologies, and cultivating a community of skilled professionals, we can collectively navigate the complex challenges of cyberspace and build a more secure and resilient digital future for generations to come.

REFERENCES

1. https://www.ibm.com/topics/cybersecurity
2. https://securityintelligence.com/articles/what-is-data-protection/
3. https://www.cisco.com/c/en/us/products/security/what-is-cybersecurity.html
   https://www.coursera.org/articles/what-is-ethical-hacking
4. Beginners Guide to Ethical Hacking and Cyber Security - Abhinav Ojha - 9 Jul 2023 (218)
5. Hacking: Be a Hacker with Ethics - Harsh Bothra - 24 Jun 2017 – (216)