Vol-07 Issue 03, March-2023

ISSN: 2456-9348
Impact Factor: 6.736

IJETRM
International Journal of Engineering Technology Research & Management

SECURITY SOLUTIONS FOR IT OPERATIONS

Sriharan M S[1]
Jeyaselvamurugan M[2]
Ram Karthick S[3]
[1]Mechanical Engineering, Bannari Amman Institute of technology, Sathamangalam
[2,3]Mechatronics Engineering, Bannari Amman Institute of technology, Sathamangalam

ABSTRACT:

We selected the domain cyber security, which is the one of the most expensive domains in IT operations. Most small-scale companies couldn't maintain security due to the need of skilled security people or they'll need to rely on third party security services. So, we begin to create a tool that collects less data from the company and provide end-to-end security analysis which helps them identify threats. Also, this tool gives full control to the company where the tool is customized in accordance with the company's needs. We took the market research on the existing tools. Most security tools identify the threats on provides solutions for those threats. Also hiring a security expert is too expensive. It is not just expensive it also creates a gap between the software developer and the security part. So, we thought of solving the problem by creating a tool that identifies the threat and provides solutions for those threats. Also, software developer can easily identify the threat and debug the threat without prior knowledge in Security. The cyber security project aims to protect internet-connected systems, including hardware, software, and data, from theft or damage. This involves implementing security measures, identifying vulnerabilities, and monitoring the system to ensure its effectiveness. The main objective is to minimize the risk of cyber-attacks and protect the organization's critical information and IT systems. The project requires a team of IT professionals, security experts, and other stakeholders to work together to design, implement, and monitor security measures. Cyber security is a critical aspect of an organization's IT strategy due to the increasing reliance on technology and the growing threat of cyber-attacks.

KEYWORDS:
Security, threat, debug, company, vulnarability

INTRODUCTION

Cyber security refers to the practice of protecting computer systems, networks, and electronic devices from theft, damage, unauthorized access, or any other malicious activity. It involves a range of technologies, processes, and practices designed to secure information, systems, and infrastructure from cyber-attacks. Cyber-attacks can take many forms, such as hacking, phishing, ransomware, malware, and social engineering. Cyber criminals often target organizations to steal sensitive data, disrupt operations, or extort money. Therefore, cyber security is crucial for businesses, governments, and individuals to ensure that their digital assets and operations are secure.

Some of the key areas of cyber security include:

Network security: This involves securing computer networks from unauthorized access, attacks, and intrusions.

Application security: This refers to the measures taken to secure software applications from threats and vulnerabilities.

Information security: This involves protecting sensitive information, such as personal data, financial information, and intellectual property, from unauthorized access or disclosure.

Endpoint security: This involves securing individual devices, such as laptops, smartphones, and tablets, from cyber-attacks.

Cloud security: This refers to the measures taken to secure data and applications stored in the cloud.

Cyber security professionals use a range of tools and techniques to protect digital assets, such as firewalls, antivirus software, intrusion detection systems, and encryption. They also conduct regular security assessments, monitor networks and systems for suspicious activity, and educate users on safe online practices.

iJETRM
International Journal of Engineering Technology Research & Management

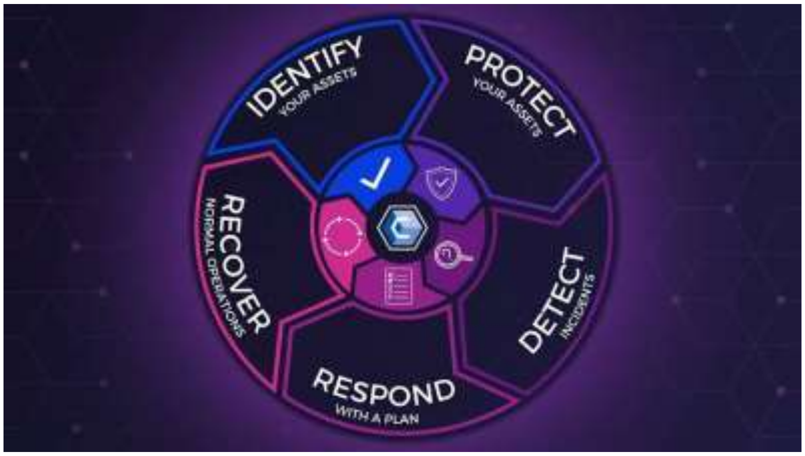

Fig.1 Key areas of cyber-Security

ETHICAL HACKING

Ethical hacking, also known as "penetration testing," is a process of identifying vulnerabilities and weaknesses in computer systems, networks, and applications, and then testing those vulnerabilities to determine the potential impact of an attack. The following are the different phases of ethical hacking:

Reconnaissance: The first phase of ethical hacking is reconnaissance, which involves gathering information about the target system or network. This information can include IP addresses, domain names, network topology, and operating systems. Ethical hackers use a variety of tools and techniques to collect this information, such as scanning tools and social engineering.

Scanning: In the second phase, ethical hackers use scanning tools to discover open ports, services, and vulnerabilities on the target system or network. This phase is critical as it helps to identify potential weaknesses that can be exploited in later stages.

Enumeration: The third phase of ethical hacking involves collecting detailed information about the target system or network. This includes user accounts, passwords, and system configurations. This information helps ethical hackers to plan their attack and identify potential targets for exploitation.

Exploitation: In this phase, ethical hackers attempt to exploit the vulnerabilities identified in the previous phases. They use various tools and techniques to gain access to the target system or network, such as password cracking, SQL injection, and buffer overflow attacks.

Post-exploitation: After gaining access to the target system or network, ethical hackers move to the post-exploitation phase. This phase involves maintaining access to the system or network and establishing a foothold for future attacks.

Reporting: The final phase of ethical hacking is reporting. Ethical hackers document their findings and provide a detailed report to the organization that commissioned the ethical hacking exercise. The report includes information about the vulnerabilities found, the impact of those vulnerabilities, and recommendations for remediation. The organization can then use this report to improve its security posture and protect against future attacks.

SCANNING

The scanning phase is the second step in the process of identifying vulnerabilities and weaknesses in a computer system or network. During the scanning phase, the ethical hacker uses various tools and techniques to gather information about the target system or network. This information can include:

- IP addresses and network ranges.
- Open ports and services running on those ports.
- Operating system and application versions.
- Network topology and device configurations.
- Security policies and procedures.

The scanning phase can be divided into two types of scanning:

Network scanning: This involves using tools such as Nmap, Nessus, or OpenVAS to scan the target network for open ports, services, and vulnerabilities.

Host scanning: This involves using tools such as Ping, Traceroute, or Netcat to scan individual hosts on the network for open ports, running services, and vulnerabilities.

Once the ethical hacker has gathered information about the target system or network, they can use this information to plan their attack and identify potential vulnerabilities that can be exploited. It's important to note that the scanning phase should always be conducted with the owner's permission and with a clear understanding of the legal and ethical boundaries of the engagement.

The scanning phase in cyber security is an important stage in which security professionals scan the network or system for vulnerabilities, weaknesses, and potential security threats. Some of the problems that can be encountered during the scanning phase include:

False positives: Scanning tools can sometimes generate false positive results, which can lead to wasted time and resources as security professionals investigate non-existent vulnerabilities.

False negatives: Similarly, scanning tools can also generate false negative results, which means that real vulnerabilities may go undetected, leaving the system or network open to attack.

Network congestion: Scanning large networks can cause congestion on the network, which can slow down or even crash some systems.

Network segmentation: When a network is segmented, it can be difficult to scan all segments and identify all vulnerabilities. This can leave some parts of the network vulnerable to attack.

Limited scanning capabilities: Some scanning tools may be limited in their ability to detect certain types of vulnerabilities, leaving the network or system open to attack.

Legal and ethical concerns: Scanning can potentially violate laws and ethical considerations, especially when scanning systems or networks without proper authorization.

Resource consumption: Scanning tools can consume a significant amount of system resources, which can impact the performance of the system or network being scanned.

False alarms: Scanning tools can also generate false alarms, which can lead to security professionals investigating non-existent security threats, causing unnecessary stress and wasting time.

To minimize these problems, it is important to use reputable scanning tools, have proper authorization to scan the system or network, and have a clear plan and strategy for scanning. It is also important to regularly review and update scanning procedures to ensure they remain effective and minimize potential issues.

TOOLS USED

Ethical hacking tools are software applications designed to help security professionals identify vulnerabilities and weaknesses in computer systems and networks. These tools are commonly used in penetration testing, which is the process of assessing the security of a system by attempting to exploit its vulnerabilities in a controlled manner.

Some common ethical hacking tools include:

- **Nmap** - A network mapping tool used to discover hosts and services on a network.
- **Metasploit** - A powerful framework for exploiting known vulnerabilities in computer systems and applications.
- **Wireshark** - A network protocol analyzer that allows security professionals to capture and analyze network traffic.
- **Aircrack-ng** - A suite of wireless network hacking tools used to crack WEP and WPA-PSK keys.
- **John the Ripper** - A password cracking tool used to test the strength of passwords.
- **Nessus** - A vulnerability scanner that scans computer systems and networks for known vulnerabilities.

It is important to note that ethical hacking tools should only be used for legitimate purposes with the consent of the owner of the system or network being tested. Unauthorized use of these tools is illegal and unethical.

IJETRM
International Journal of Engineering Technology Research & Management

Fig.2 Some network scanning tools.

CONCLUSION

Based on the tool we made we found that the overall cost of making a software and managing it security could be drastically. Also, the developers of the software need not to be relied on some of the third-party software. I n which they must flex their software and their services in dependence with the third-party software and also, they might need to provide tons of their sensitive information to manage their security. On the other hand, if they choose to hire security experts to manage their security aspects the company might need to allot a separate team to manage such aspects this could increase their expense of the overall security management. So, we took a step to make a tool that could be customizable by the company to be able to customize according to their companies' requirements, also only some basic data is collected to manage the security aspects of the company. It will also reduce the overall expenses in managing their security.

REFERENCES

[1] Joel Snyder, he provides practical advice for IT operations teams to improve security and reduce the risk of cyber attacks "It Operations and security: Build a strong foundation".
[2] Richard A. Stallman, he advocates for the use of free software in IT operations to increase security and reduce the risk of data breaches and cyber-attacks. He argues that proprietary software is inherently less secure because the source code is not available for public scrutiny and because it can contain hidden vulnerabilities and backdoors. In his article "Free software for IT Operations".
[3] D.K Kim, he told the effectiveness of security solutions in IT operations by surveying IT professionals of various organizations. In the article he published "Investigating security solutions in IT Employees".
[4] Y.K Kim, the study found that firewalls, intrusion detection/ prevention systems and encryption were the most widely used security solutions and that regular monitoring and testing, security policies and procedures and staff training were important factors in the effectiveness of security solutions "Identifying the effectiveness of security solutions in IT Operations".