



A COMPREHENSIVE INVESTIGATION OF RECONNAISSANCE THREATS AND ITS REMEDIATION

Mahmudul Hasan¹, Mohammad Arifin Rahman Khan², Mohammed Ibrahim Hussain³, Mohd Abdullah Al Mamun⁴, Md. Moazzam Hossain⁵, Syed Mominul Islam⁶, K M Nurazzaman⁷

Project student, Computer Science and Engineering, Bangladesh University, Dhaka, Bangladesh¹

Assistant Professor, Computer Science and Engineering, Bangladesh University, Dhaka, Bangladesh²

Assistant Professor, Computer Science and Engineering, Bangladesh University, Dhaka, Bangladesh³

Mohd Abdullah Al Mamun, MBA in Information Technology, Westcliff University, USA⁴

Data Analyst, Revenco, Dhaka, Bangladesh⁵

Software Developer, Revenco, Dhaka, Bangladesh⁶

Service Associate, Midland Bank PLC., Dhaka, Bangladesh⁷

Corresponding Author: Mohammad Arifin Rahman Khan, E-mail: arifin.khan@bu.edu.bd

ABSTRACT: *The cyber world of today extends beyond the internet. Critical infrastructures, embedded systems, and telecommunication networks are all part of this interconnected network. Attacks by malicious actors targeting vital infrastructure pose a serious risk to government and commercial activities. Successful businesses rely on quick and simple network access, which also increases the vulnerability of important data to cybercriminals. Attackers and hackers of today are proficient and well-prepared with a variety of hacking tools to quickly take advantage of a little weakness. The initial stage of a cyberattack is known as reconnaissance, and this study will examine this stage to provide practical defenses. The methodology of this paper's complete approach to cybersecurity is Penetration Testing of Systems, Defending Against Foot printing and Reconnaissance, and foot printing and Reconnaissance. Understanding the techniques and resources employed to get data on possible targets is the first step. The second portion is dedicated to tactics and equipment for countering this kind of collection of information. The last stage uses simulated attacks to assess the security of the systems. The systematic approach seeks to improve the entire*



cybersecurity posture by the systematic identification, assessment, and mitigation of possible risks.

Keywords: *Reconnaissance, Penetration Testing, Cyber Security, Ethical Hacking, OSINT.*

1. INTRODUCTION

Today's world is dominated by information, data and technology, and all of the Information is now digitally stored and accessible online worldwide. The last three decades have seen exponential growth in the popularity of the Internet. There are networks in this communication system that the government, businesses, academic institutions, and private individuals hold. Our most vital infrastructures, such as finance and banking, science and technology, and aerospace communication, should be accessible worldwide. Every action we take clicking, buying, or posting on social media leaves a digital trace that bad actors may use to steal our identities, exploit our financial situations, or disrupt vital infrastructure. In these circumstances, Information posted online is more vulnerable and can be easily hacked by hackers. Hacking is one of the largest concerns digital businesses, governments, and people face worldwide. These Cybercriminals can breach systems and networks and have access to a special collection of extremely advanced tools. Cyber-attacks are not only a technical problem but also a larger (or more significant) social and economic problem that causes damage at various levels. They can cause a variety of damages, affecting personal, economic, and social sectors. The ninth annual report on the financial impact of cybercrime by Ponemon Institute and Accenture from 2019 indicates an alarming spike in cyberattacks, with phishing attacks growing by 8%, malware attacks by 11%, and ransomware attacks by 21%.[1][2] In addition, the study showed that the average all-around financial cost of cybercrime for organizations turned to 13.0 million dollars in 2018, an increase of 72% compared to five years earlier. [3]. Cybercrime is predicted to cost the universal economy almost \$9.8 trillion by the year of 2024. The price of cybercrime damage is predicted to increase by near about 15.2% annually over the next coming 2 years. The \$10.5 trillion in losses from cybercrime are expected to have accumulated more cost by 2025.[4][5]. Its world price is projected to be worth \$8.44 trillion in 2022 and it could line up \$23.84 billion by kicking off 2027 of course! Account warnings on the rise have implications for both global cybersecurity policy and regulation that seeks to prevent cyber-attacks whilst promoting



trust in digital constructs [6]. It is important to take some necessary measures to protect ourselves from the damage caused by cyber-attacks. Therefore, our investigation has followed by the following:

- Exploring Footprinting and reconnaissance techniques.
- Identify target vulnerabilities through reconnaissance techniques.
- Develop defense mechanisms against Footprinting and reconnaissance.
- Simulate a penetration testing attack and evaluate effectiveness of the counter measures.
- Enhance cybersecurity awareness
- Propose future security measures.

2. LITERATURE SURVEY

The research conducted by Kashyap and Selvarajah in 2021, highlight the focus is on one of the important phases known as “reconnaissance”, which is the first step in the methods of any kind of cyber-attack. A comparative review of several reconnaissance techniques is presented, emphasizing the possible harm and efficacy of each technique. They utilize several types of open-source Intelligence (OSINT) tools to gather information about the target website. This paper compares security postures between vulnerable and secure website. Their research divides reconnaissance techniques into two main categories such as passive and active reconnaissance. They also discussed about the pros and cons of each reconnaissance techniques. This study shows reconnaissance can help to identify potential vulnerabilities in a target system. They conclude that although active reconnaissance has a larger chance of being discovered, it offers more detailed information about the target system while passive reconnaissance is more covert [7].

In 2013, Sanghvi & Dahiya performed comprehensive research based on Reconnaissance. This paper discusses Cyber Reconnaissance focuses on Port Scanning and Fingerprinting of operating system (OS) attacks and proposes some easy-to-use solutions. They provide insights into reconnaissance as an early warning mechanism for any kind of hacking activity. There is notable investigate effort done to detect cyberattacks at the stage of research. The article also demonstrates the significance of timely detection and response to reconnaissance activities, which can efficiently prevent subsequent attacks. Their study



doesn't cover all possible reconnaissance techniques but covers techniques that help security professionals take the necessary steps [8].

Research is performed on the utilization of NMAP for footprinting and Reconnaissance by Singh et al. in 2022. They used a Cloudflare server for their study. The information provided can be useful to understand the concept of footprinting, the things that attackers look for in a footprint, and how to fend against it. This paper aims to explain the concept of Footprinting through the use of the Nmap ethical hacking tool. Their article also demonstrated how Nmap can be used to execute both basic and deep scans, giving a flexible tool for attackers to map out target networks and their vulnerabilities. The research also examined the countermeasures that might be performed to recognize and combat Nmap searches. The outcomes of the observation will be cooperative to avoid the footprinting [9].

Arabia-Obedoza et al. in the year 2020 researched about social Engineering attacking methodology. The paper's researchers looked into the social engineering attacks that are now in use as well as defenses against them, phishing attacks, human hacking, and online crime. Researchers investigate the relationship between reconnaissance and social engineering, offering an overview of the methods used to get intelligence through social engineering techniques. They emphasis on social engineering attacks. Which is a popular kind of reconnaissance techniques that takes advantage of vulnerabilities in persons. Establishing user awareness programs to reduce such dangers might be made easier with an understanding of these types of strategies. The study also draws attention to the psychological tricks used in social engineering, which may be a useful addition to technical reconnaissance techniques. According to their study, both technological as well as human aspects should be taken seriously in a complete defensive plan [10].

Roy et al. Shows that the attackers collect information in different stages of the cyber kill chain, which is essential to determine how good or bad a particular attack will perform. This article also outlines and examines the approaches, strategies, and tools that hackers' custom to conduct investigation and footprinting actions throughout the attack process. After that, they go into great detail and provide a taxonomy of threatening reconnaissance methods. The taxonomy presents a system-based information collection approach for



reconnaissance tactics, based on the source being a third-party human. This observation shows a thorough explanation of competitive inspection, which have able to help in modeling and distinguishing this complex but essential aspect of cyberattacks. It also provides insights that can enhance self-protective tactics, for example cyber deception. Their study also has the potential to contribute to the development of countermeasures that hinder attackers' access to critical information necessary for successful attacks. Intrusion detection systems that are based on networks and hosts usually keep an eye out for known or evident hostile reconnaissance activities, such as scanning. To reduce reconnaissance, a variety of strategies have been put out in the literature. These include the usage of honeypots, honey authorizations, honey symbols, honey PINs, and parameters, and more. Understanding the wide range of reconnaissance operations and the corresponding countermeasures that may be used to protect against Reconnaissance and Footprinting is made easier with the help of this taxonomy [11].

Lianq and Selvarajah completed a research work which addresses the underlying notions behind reconnaissance and footprinting techniques while emphasizing the serious hazards that these practices pose for organizations and individuals. Their article also offers thorough research of how cyberattacks can be launched using confidential information that is obtained through reconnaissance. They point out how crucial it is to understand these strategies to create strong defenses [12].

Jafarian et al. published a research work in 2015. The article proposes an innovative strategy for tackling mutation-based reconnaissance attack mitigation. This research reveals how attackers' attempts at mapping network infrastructures might be evaded by dynamically changing IP addresses. This method raises the difficulty and expense of carrying out attacks in addition to impeding the attackers' capacity to obtain precise information [13].

The research work named "Social Engineering Incidents and Preventions" demonstrates several social engineering techniques that are used by attackers frequently. Their research also discussed the psychological principles to manipulate target behavior. Their research makes significant contributions to the human psychological insights, identifies human error as a key factor, and recommends effective prevention strategies [14].



The analysis of the literature emphasizes the importance it is to understanding reconnaissance methods to create effective cybersecurity protections. From the fundamentals of footprinting and reconnaissance to more sophisticated techniques like addressing mutation and social engineering, the studies offer insightful information on how cyber dangers are changing. The possibility of a successful attack increases with the amount of data and information the hacker can gather. In the always-evolving cyberspace, future research should keep looking into novel countermeasures and improving already-existing methods to keep one step ahead of attackers.

3. METHODOLOGY AND PROCESS

In conventional battle the opposing force would do everything to acquire as much intelligence as feasible prior to initiating an attack. They would make an organized effort to gather information on the available resources, their weaknesses and vulnerabilities, and identify the areas where they would be most vulnerable to damage. They might use many techniques to get this information, such as conducting surveillance, eavesdropping on and intercepting conversations, and deploying intelligence probes. Hackers use a similar method to obtain information about computer systems and resources via computer networks.

3.1 PHASE ONE

From this subsection point of view, our project tries to explain the Performing foot printing and Reconnaissance.

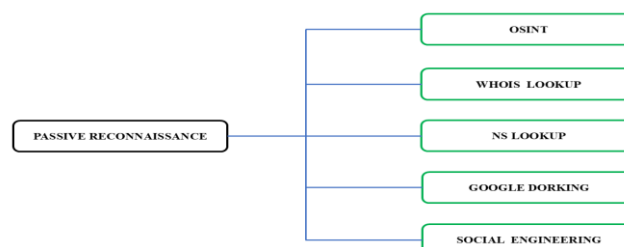


Figure 1 Passive Reconnaissance Techniques.

Passive reconnaissance also known as footprinting means minimizing interaction with the target which generates alerts in logs. It is gathering the information without alerting the target. The target of passive observation is to obtain as far as possible data and information



about the target system. Security instead of the attack is suggestively increased if the target host is up-to-date.

The concept of Open-Source Intelligence (OSINT) plays an important role in passive reconnaissance, enabling the gathering of publicly available information about a target without direct interaction. OSINT techniques consist of actions such as web scraping, data mining, and social media monitoring which allows the extraction of important information to increase situational awareness and help to make decisions for law enforcement organizations. Our research also collects data from another open sources such as social media, websites, public records, news articles, forums, the dark web, online directories, government documents, academic research, and technical footprints. OSINT facilitates in finding vulnerabilities in online applications and networks, allowing for proactive actions to protect vital information before exploitation by attackers. Ethical hackers also implement OSINT for targeting individuals and organizations, highlighting the requirement of data protection methods and security awareness training to prevent risks such as data breaches and identity theft. This non-intrusive OSINT technique gives complete, cost-effective knowledge which assists in identifying potential vulnerabilities. The attacker may execute OSINT via multiple tools including Spider foot, The Harvester, and Recon-ng. Spider Foot is an open-source intelligence (OSINT) automation tool built by Steve Micallef, designed to speed up the process of obtaining information on multiple targets such as IP addresses, domain names, and email addresses. By searching over 100 public information sources. It automates the gathering and analyzing of data, exposing relationships, patterns, and possible security concerns. It is used for reconnaissance, gathering information, and both active and passive reconnaissance approaches. Spider Foot is effective in network auditing, and vulnerability assessment, enabling customized modules and easy interface with other security tools.

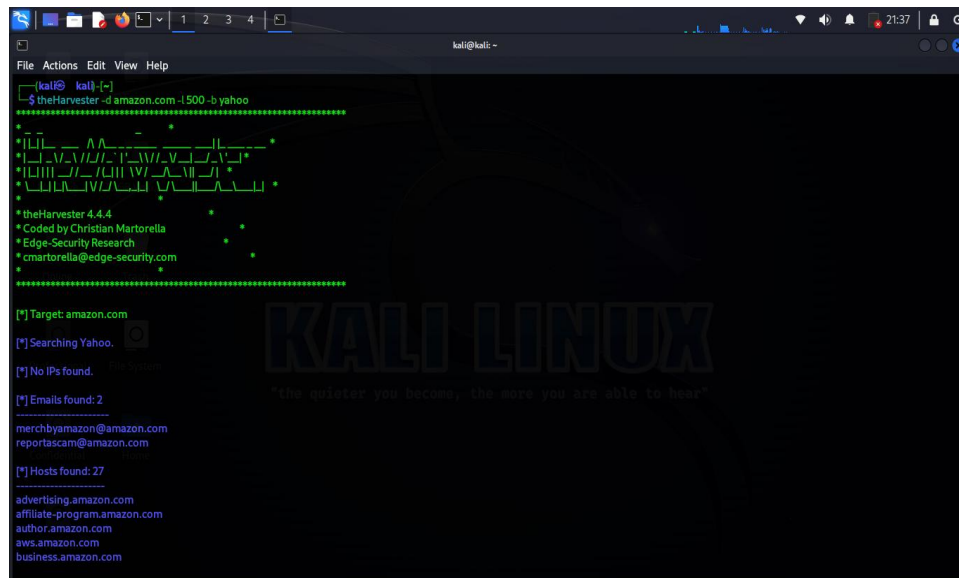


Figure 2: The Harvester Collect Target information.

Another OSINT tool is The Harvester. It is designed to collect extensive information about a target, for example an open port, hostname, Autonomous System Numbers (ASN), the address of Internet Protocol, network subnet, email address, or the name of persons'. The Harvester can gather information from various search engines like Baidu, Bing, dns-dumpster, Duckduckgo, Google, Hunter, Qwant, Security Trails, Shodan, Trello, and many more. Our research used The Harvester tool to gather target's personal information such as home and workplace addresses, email address, telephone number, knowledge about computer, dark secrets, and routine assignments. It also includes several modules for efficient data collecting and analysis, aiding in developing an extensive overview of the target system.

Information regarding the domain owner, physical addresses, contact details (i.e. cell numbers and the addresses of email), and more can be found in a WHOIS record. Whois lookup is a method for querying a database to retrieve information about a registered domain name. Usually, WHOIS information and data both are stored in WHOIS databases and is taken care of by regional (i.e. country or local area etc.) Internet registries. The process of registering a domain typically requires a new domain owner to provide current contact data and information that are verifiable. We conducted WHOIS searches to gather administrative information, which consisted of domain name data, owner contact details,



name servers, and more. We conducted WHOIS searches to gather administrative information, which consisted of domain name data, owner contact details, name servers, and more. Our research found that, Attackers can use Internet Corporation for assigned names and numbers (ICANN) or whois. is the website to collect domain information.

NS lookup is used to collect information like domain registration information, organization contact details, domain registration date registrant's name, contact address, contact number i.e. cell number, and the address of email. etc. The servers that handle requests for the domain name and direct traffic to the website. It can also provide information about the date the domain registration expires and the date the Whois information was last updated. Domain Name Server (DNS) servers with most of the significant data can play an identical important role in building an attack against the goal. To collect DNS information such as DNS records, identify subdomains, and aid in uncovering additional points of interest within a target's network attackers use tools like Dnsenum and Dnsmap.

The Google Hacking Database (GHDB) is a powerful tool for both security professionals and cyber-criminals. They use specialized search engine queries, known as "Google dorks," to uncover sensitive information and vulnerabilities in Information Technology infrastructures. Our research identified that Attackers can detect vulnerable websites, discover private data such as credit card credentials, find out current software version information, and identify web application source code and vulnerabilities of IoT devices. Google hacking database (GHDB) queries reveal error messages, files containing passwords, sensitive directories, network data, and advisories, allowing attackers to launch exploits like buffer overflow and SQL injection attacks. Common query categories include footholds, files containing usernames, login portals, and vulnerable servers, enabling attackers to gather critical information for further exploitation.

Social engineering is the practice of playing on people's confidence in order to obtain information that is then used to launch a cyber attack. Social engineering is frequently used in marketing campaigns and people-reading studies. Social engineering has always been used to take advantage of kindness, fear, trust, and social obligation to manipulate the basic human tendency to trust. We look into the methods by which an attacker may try to launch a social engineering attack and document the information that could be gleaned from it,



including the victim's actions. The Social Engineering Attack Cycle was the methodology employed in this study. Social Media analysis tool Maltego is used to collect information and perform link analysis between various data points. It collects people, organizations, and website information and provides highly effective social media investigations. In this era of communication technology social media platforms is full of valuable information. Attackers can easily collect this information. SOSINT is the tool for gathering and analyzing social media intelligence data, including posts, interactions, and user connections. This can reveal valuable insights about the target's social media presence and activities. Social Engineering can be performed by using the Social Engineering Toolkit (SET), Phishing, Pretexting, Tailgating, and Reverse Social Engineering. We use various types of social Engineering attacking methodology in our research. The most prevalent kind of social engineering attack is phishing. In order to trick the target into acting quickly, the majority of phishing attacks use deceptive links that lead to malicious websites that host phishing landing pages, collect private data (for example names, addresses, Social Security numbers, etc.), and instill fear and a sense of urgency. According to our research, attackers can also employ evil-twin attacks, in which they fabricate a target user in order to have them connect to a fictitious wireless access point and authenticate with a fictitious server, thereby obtaining the user credentials. The Hackers can use various phishing tools and techniques like Phish Me, KnowBe4, Evilginx2 (man-in-the-middle attack, cookie stealing), SEToolkit, HiddenEye, King-Phisher, Gophish, and BlackEye(available 32 patterns of phishing attack). Social engineering is the practice of playing on people's confidence in order to obtain information that is then used to launch a cyber attack. Social engineering is frequently used in marketing campaigns and people-reading studies. Social engineering has always been used to take advantage of kindness, fear, trust, and social obligation to manipulate the basic human tendency to trust. We look into the methods by which an attacker may try to launch a social engineering attack and document the information that could be gleaned from it, including the victim's actions. The Social Engineering Attack Cycle was the methodology employed in this study. Social Media analysis tool Maltego is used to collect information and perform link analysis between various data points. It collects people, organizations, and website information and provides highly effective social media investigations. In this era of communication



technology social media platforms is full of valuable information. Attackers can easily collect this information. SOSINT is the tool for gathering and analyzing social media intelligence data, including posts, interactions, and user connections. This can reveal valuable insights about the target's social media presence and activities. Social Engineering can be performed by using the Social Engineering Toolkit (SET), Phishing, Pretexting, Tailgating, and Reverse Social Engineering.

We use various types of social Engineering attacking methodology in our research. Phishing is one of the most common category of social engineering attack. Most of the phishing attacks aim to obtain personal data and information (i.e. names, addresses, Social Security Numbers et cetera), use misleading associations that redirect target users to malicious websites that host phishing landing pages, and generate fear and a sense of emergency to manipulate the user into responding fast. Our investigation shows attackers can also utilize evil-twin attacks, where they have able to create a goal user to join to a fake wireless entree point and authenticate to a unfaithful/fake server and so happening the attacker can obtain the user identifications. The Hackers can use various phishing tools and techniques like PhishMe, KnowBe4, Evilginx2 (man-in-the-middle attack, cookie stealing), SEToolkit, HiddenEye, King-Phisher, Gophish, and BlackEye(available 32 patterns of phishing attack).

Pretexting is another method of social engineering. Attackers may concentrate on constructing a pretext, or an artificial situation, which they can exploit to steal or copy someone's personal data and information, and these types of corruptions, the scammer frequently impersonates a trustworthy person and claims they require particular data/information from the target to authenticate their identity.

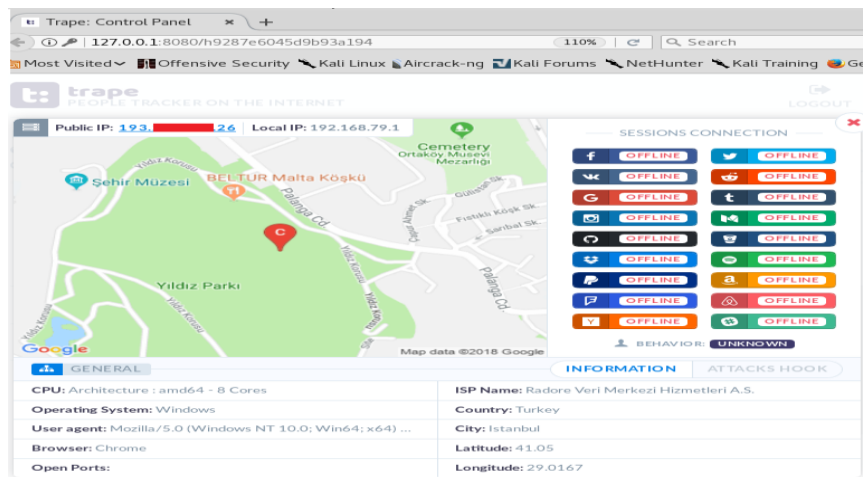


Figure 3: Collecting target information using TRAPE tool.

i.e., a hacker may call a bank and pose as a reliable individual in an attempt to persuade the representative to provide access or reveal usernames and passwords. To carry out this kind of assault effectively, attackers might need access to some private information. If the victim acquiesces, the perpetrators engage in identity theft or exploit the information for additional harmful actions. More sophisticated pretexting tactics involve deceiving victims into taking actions that bypass the organization's security protocols.

Tailgating is an effective community engineering attack used to gain physical access to access to an illegal site. Tailgating is performed by constantly following a lawful site user or a person into the zone without being identified by the official user. For example, an attacker could pretend to forget to carry his card and influence the victim to grant him entrance to a building or security zone. Radio frequency identification card attacks are especially widespread right now since many firms use these cards as access tokens because of their low cost and great user experience. An attacker could potentially exploit the RFID (radio frequency identification) network to gain entry into the designated secure area.

Reverse social engineering is a concept that could appear unusual and sophisticated to us, but it is a concept that tends to represent a risk to cyber security. Reverse social engineering is a strategy in which attackers pose themselves as authority or trustworthy persons, frequently providing support or services that convince their targets to share sensitive information or provide unethical access. Our research and investigation reflect that the attacker may appear as an IT specialist, a consultant or even a corporate representative.



They'll invest time and effort in creating a connection with the target, delivering technical guidance, addressing small challenges, or providing polite support. The risk of this strategy rests in the confidence that is effectively and gradually created over time. Once this trust is created, the attacker may influence the victim into exposing critical information or providing them access to protected systems. The target, ignorant of the fraud, provides credentials or permits remote access, thinking they are supporting a trustworthy person. The effects of these activities may be terrible. Once the attacker gets illegal access, they may compromise systems, steal sensitive data, or utilize the gained information for other malicious purposes.

Web archiving is a kind of passive reconnaissance technique. It is a service that archives web pages, allowing users to view previous versions of websites. This has able to provide insights into the past state and evolution of a target's web presence. The attacker can collect data and information by archiving the web using the Internet Archive (Wayback Machine).

Web scraping, often referred to as web harvesting and web data gathering, is the process of extracting data from websites. Web scraping is the automated extraction and analysis of online material. Due to the vast amount, diverse nature, and rapid pace of Big Web Data, manual collecting and categorization of this data is impractical for individual researchers or even big teams of researchers or commercial data professionals. As a result, researchers often rely on diverse technologies and tools to mechanize some or all components of Web data/information collecting and organizing. Web Scraping is the developing activity of automatically extracting and establishing material from the online/web in order to examine it further. Web Scraping consists of three phases such as website analysis, website crawling, and data organizing. To successfully do each of the three stages of Web Scraping, our researchers must possess knowledge of various Web technologies and proficiency in at least one widely-used programming language in the field of Data Science, such as R or Python. By using Web Scraping techniques attackers can collect a huge amount of data of an organization. Active Reconnaissance needs more preparation for the attackers. In this reconnaissance technique, the attackers directly connect with the target to gather information about the target system. At the time of using this technique leaving traces could lead the target to start an investigation or lead them to attackers.

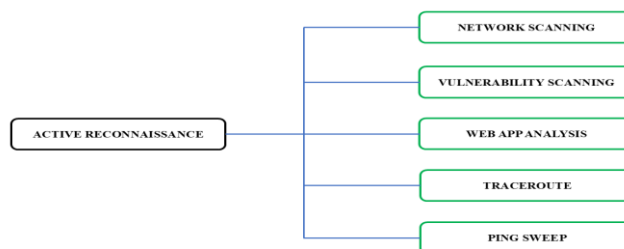


Figure 4: Active Reconnaissance Techniques.

To overcome these challenges our investigation, use a disposable operating system (Tails OS, Live Kali Linux), TOR network, and proxy chain. By using this technology our attacks can avoid tracking the digital trails. Active reconnaissance can be performed by using network scanning, vulnerability scanning, and Web application analysis.

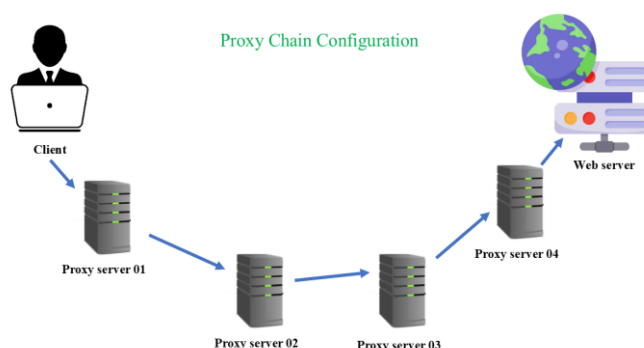


Figure 5: Configuration diagram of proxy chain.

Network scanning is a procedure used to discover active devices (hosts), services operating on them, and other facts about the system and network. Network scanning is the process of scanning a network, usually for system maintenance and security evaluation. Hackers use it for carrying out attacks. Our research use network scanning to check whether the network is vulnerable or not and try to find loopholes. By finding the issues, we can then perform appropriate cyber-attacks according to the vulnerability to get unauthorized access to the network. Our researchers can perform Network scanning using traceroute, ping sweeps, NMAP, and angry IP scanner tools and techniques. By using scanning our research team can gather Network information such as IP address, subnet mask, network topology, and domain name.



A traceroute scan offers a map of how information transmitted through the internet flows from its point of origin to its destinations. Traceroute is a network diagnostic tool used to monitor the way that data packets transit from one computer to another via a network, often from the user's device to a target server. It enables for the identification of pathways between source and destination devices, even when several network lines are involved in increasing network connectivity software utilities. It is a handy tool for identifying the feedback by delays and routing circles existing in a communication network transmit across packet switched nodes. It also helps identify any possible facts of failure met while on route to a given destination.

```
(kali@kali)-[~]
└─$ sudo nmap 192.168.0.1 -sS
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-07 10:18 UTC
Nmap scan report for 192.168.0.1
Host is up (0.0057s latency).
Not shown: 996 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
53/tcp    open  domain
80/tcp    open  http
1900/tcp   open  upnp
MAC Address: E4:C3:2A:62:7D:C8 (TP-Link Technologies)

Nmap done: 1 IP address (1 host up) scanned in 0.52 seconds

(kali@kali)-[~]
└─$ sudo nmap 192.168.0.1 -sT
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-07 10:19 UTC
Nmap scan report for 192.168.0.1
Host is up (0.012s latency).
Not shown: 996 closed tcp ports (conn-refused)
PORT      STATE SERVICE
22/tcp    open  ssh
53/tcp    open  domain
80/tcp    open  http
1900/tcp   open  upnp
MAC Address: E4:C3:2A:62:7D:C8 (TP-Link Technologies)

Nmap done: 1 IP address (1 host up) scanned in 0.40 seconds

(kali@kali)-[~]
└─$
```

Figure 6: Perform Nmap scanning of the target.

Ping sweeps are a typical method in reconnaissance, which involves sending ICMP echo requests to several IP addresses to discover which hosts are active on a network. Ping sweep is also known as an ICMP sweep or ping scan. Ping sweep is an approach to efficiently verify whether devices within a network range are switched on and responding to network requests.

NMAP may assist in mapping by visiting multiple checkpoints and capturing vital information while bypassing firewalls and intrusion detection systems. NMAP is an ideal network scanning tool for the attackers to perform traceroute analysis. Our research highlighted that Network Mapper (NMAP) is a robust network scanning tool used to discover hosts, open



and close ports, scan network interfaces, target specifications, services, and version detection, SCTTP/UDP/TCP scan, Script scan, timing and performance firewall/IDS evasion and spoofing, different types of file output and open ports on a network. NMAP is a flexible tool that may be applied efficiently in reconnaissance operations across several disciplines. The attacker uses NMAP to collect all of the Network data and find out network vulnerabilities.

A vulnerability in Cyber security mentions to a weakness or chance in a data or information and communication scheme that cybercriminals can exploit and gain unlawful access to a target computer system. Vulnerabilities weaken schemes and make a method to malicious attacks. Cybersecurity vulnerabilities can be the result of software bugs, poor access control system, human errors and system complexity. Vulnerabilities may be classified as six major categories such as hardware, software, network, personal, physical site and organizational vulnerabilities. Our research enlightens Vulnerabilities like weak or stolen credentials, misconfiguration, out of date software, lack of encryption, poor data sanitization, insider threats unauthorized access, vulnerable APIs and zero-day vulnerability can be exploited by malicious attackers. There are various types of tools and techniques such as Nessus and Open VAS. They can identify the potential vulnerability of a target system. Users can use Nessus to execute a vulnerability scan and store the database on a separate machine from the server using an administrative console. Attackers have the ability to adjust the levels of port scanning to account for firewalls and intrusion detection systems. To obtain more precise and comprehensive details about Windows-based hosts within a domain of Windows, it is advisable for attackers to establish a group of domains and create an account with registry of access by remotely.

Users can use Nessus to execute a vulnerability scan and store the database on a separate machine from the server using an administrative console. Attackers have the ability to adjust the levels of port scanning to account for firewalls and intrusion detection systems. To obtain more precise and comprehensive details about Windows-based hosts within a domain of Windows, it is advisable for attackers to establish a group of domains and create an account with registry of access by remotely. Nessus provides users with the capability to operate an administrative console that conducts vulnerability scans and stores the database



on a machine separate from the server. Additionally, attackers have the option to set various levels of port scanning to account for the systems of instruction detection and firewalls. To obtain more precise and comprehensive information regarding Windows-based hosts within a domain of Windows, moreover it is also advisable for attackers to establish a domain group and an account which has possible to access by the way of that. Attackers use identified vulnerabilities to perform successful attacks.

Our research collects information about web application security and vulnerability by using Burp suite and OWASP ZAP tools. By identifying potential vulnerabilities attackers can get access to the target system. There are various kinds of vulnerabilities like Broken Access Control (BAC), Cryptographic Failures, SQL injection, Insecure Design, Security Misconfiguration, Vulnerable & Outdated Components, Identification and Authentication Failures (IAF), and many more which can be recognized using burp suite.

Our research team gather all the information for further analysis to find out potential attacking methods. Combining data from multiple sources to create a comprehensive profile of the target, ensuring all gathered information is consistent and corroborates other findings. Guaranteeing the accurateness and reliability of the gathered data and information, eliminating false positives, and confirming the legitimacy of the data. Collected information like security policies and network and host information can help attackers map a successful attack.

3.2 PHASE TWO

Reconnaissance is the preliminary phase of a cyber-attack. There is a lot of research work done to prevent reconnaissance attacks. There's no way to keep any organization's digital presence 100% invisible to attackers. But there are various actions security advisors can execute to make their job harder. In order to prevent hackers from accessing a network or an organization safely we will have to know where can they collect data, create a set of segments and review the traffic on those segments regularly. To defend footprinting and reconnaissance we need to implement some strategies that protect against information gathering by malicious actors. To make a secure network environment some necessary Network security measures should be taken. Our researches also need to take steps simultaneously to perform some initial reconnaissance, configure firewall, imply network



segmentation, monitor traffic and logs, implement Intrusion detection and prevention system, deploy vulnerability scanning tools, conduct regular security awareness and educate employees about security risks. Steps that might be minimize the area of attack include web application isolation, close unused ports, eradicate unnecessary software functionality, eliminate vulnerable VPN, implement Zero Trust Network Access (ZTNA), virtual meeting isolation, implement least privilege access and Intrusion Prevention System etc.

A firewall is a system security tool. It is a barrier between the WAN network and external attackers. Firewalls provide a key function in eliminating reconnaissance attacks. Firewall filters may protect Supervisory Control and Data Acquisition (SCADA) networks from reconnaissance by identifying port scanning methods and preventing intrusion attempts, boosting network security against attackers.

Next-generation monitoring tactics become more sophisticated and covert. It requires advanced advanced firewall policies to detect and prevent such evasive methods. By using firewalls like pfSense(It is an Open-source distribution of firewall or router.), Cisco ASA (It is an enterprise grade firewall solution.), and Juniper SRX (It is a high performance security solution for network.)the network administrator can filter incoming and outgoing data congestion based on predefined security instructions. Integrating distributed firewall applications, security rules, and OpenFlow counters in Software Defined Networking (SDN) environments may successfully identify and neutralize reconnaissance attempts at an early stage. It also offers a proactive defensive mechanism against malicious actors.

Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) serve significant roles in battling reconnaissance crimes in network security. IDS and IPS continually monitor the network, recognizing anticipated incidents and collecting information about them, avoiding the events, and reporting them to security supervisors.

By using IDS and IPS network administrator can monitor network traffic for suspicious activities. Tools-like Snort, Suricata, and Cisco Firepower can provide alerts and block malicious traffic in real time. The integration of IDS/IPS with operating systems strengthens security measures against sophisticated attacks, enhancing the ability to detect and prevent cyber threats effectively.



Network reconnaissance entails searching for active hosts, enumerating services, and finding vulnerabilities. Implementing network access control techniques may assist prevent illegal access during reconnaissance attempts. The network access control (NAC) system ensures that only authorized and compliant devices to the network. Cisco ISE and Aruba ClearPass are some such as of network access control (NAC) schemes.

Security information and event management (SIEM) is a security solution that helps industries detect and handle possible security threats and vulnerabilities before they have a chance to cause damage their operations. SIEM technology is used to Real-time monitoring, log management, incident response, and compliance reporting. SIEM aids in reconnaissance by gathering and analyzing security data to detect risks or incidents. SIEM systems gather, analyze, and correlate security data from many sources to identify and react to attacks by utilizing Splunk, IBM QRadar, and ArcSight.

Web applications may be protected using a web application firewall (WAF). WAFs may offer important security protection for websites, mobile applications, and APIs. WAF may monitor, filter, and block data packets sent and received by web applications, protecting them against attacks. WAFs protect web applications by filtering and monitoring HTTP traffic between a web application and the internet. It also gives protection against automated scanning and reconnaissance techniques. Provide security against SQL injection, cross-site scripting (XSS), and other web application attacks using various tools like ModSecurity, AWS WAF, Cloudflare WAF, etc.

Code review approaches in cybersecurity encompasses the systematic analysis of source code in order to identify and mitigate vulnerabilities. Code review helps to maintain software and bug fixing properly, which is very important for cyber security. SonarQube, Veracode, and Checkmarx tools automate Code Review and Static Analysis by analyzing source code for security vulnerabilities and coding errors. Code review tools help to integrate information from multiple sources. These data aids code review processes may be improved to enhance software quality, maintainability, and error resistance in various surveillance scenarios.

Web application security audits and penetration testing helps to identify and deal with vulnerabilities in web applications, strengthen website security against cyber-attacks.



Dynamic Application Security Testing (DAST) aids for online application security in cybersecurity, offering real-time vulnerability detection via simulated attacks, boosting overall security posture quickly. Web application security testing is performed by using OWASP ZAP, Burp Suite, and Acunetix. These tools are used to perform dynamic analysis of web applications to identify security vulnerabilities. It helps to reduce the risk of security and vulnerabilities.

The most effective way for an organization's cyber security is to increase cyber security awareness among the organization's employees. Employee Training and Awareness of an organization can mitigate the risk of cyber-attack. Simulated phishing campaigns using PhishMe, KnowBe4, and Cofense to educate employees about recognizing and responding to phishing attempts. It helps to eradicate cyber-attacks on an organization.

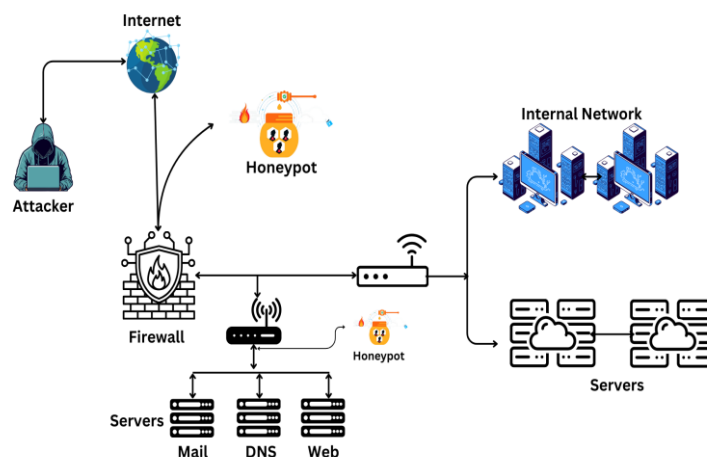


Figure 7: Integration of honeypots to provide security of the servers.

Regular security awareness training is essential for minimizing the danger of cyber attacks. As risks grow, staff members must keep updated on the most recent strategies utilized by hackers. Ongoing training helps to reinforce suggested procedures, such as spotting phishing attempts and knowing the necessity of secure passwords. By providing employees with training on a regular basis organization may decrease human error, which is a primary source of security breaches. Moreover, a knowledgeable workforce is better positioned to react to possible risks promptly, limiting the effect of an assault. Thus, ongoing security awareness initiatives are vital for maintaining a solid cyber security posture. Security Awareness Training programs that cover numerous features of cyber security, with social



engineering, password management, and data protection. SANS Securing the Human, Cybrary, and Infosec IQ tools are used in Interactive modules, quizzes, and tracking of employee progress.

Data masking is an approach to produce something that is not real but a realistic version of your organizational data. The purpose is to secure sensitive data, while offering an appropriate substitution when actual information is not needed such as, in user training, sales demonstrations, or software testing. Data Masking and Encryption techniques are used to secure sensitive information. Delphix, Informatica Data Masking, and IBM InfoSphere Optim tools are used for Static and dynamic data masking, tokenization, and role-based access control. VeraCrypt, BitLocker, and OpenSSL provide full disk encryption, file and folder encryption, and secure communication protocols (e.g. TLS/SSL). Encryption tools encrypt data when it is transferred from sender to destination. This technique can mitigate man-in-the-middle attacks.

The integration of honeypots in cybersecurity is now recognized as an essential strategy for increasing detection of threats and mitigation. Honeypots function as deception devices indicated to attract and analyze threatening activity, offering significant information into attacker behavior and tactics. Different types of honeypots (ie. honey net, email honeypot, database honeypot, malware honeypot, spider honeypot and honey bots) are used to mitigate emerging cyberattacks. Integrating honeypots enhances cybersecurity by offering proactive threat detection, reducing false positives, and integrating with existing security frameworks, contributing to organizational resilience against evolving cyber threats. Detecting reconnaissance techniques is difficult, but it doesn't have to be impossible. Tools like Acalvio ShadowPlex, Cynet 360 AutoXDR, Rapid7 Threat Command and Threat Connect can be used to detect and prevent reconnaissance attacks. These tools apply threat intelligence and deception technology like honeypots to mitigate cyberattacks. Implementing a robust defense strategy involves multiple layers of security measures, including network security, web application protection, employee training, and data security. By leveraging the right tools and techniques, organizations can effectively mitigate the risks associated with foot printing and reconnaissance, ensuring their systems and data remain secure.



4. RESULT AND DISCUSSION OF PENETRATION TESTING OF THE SYSTEM

Penetration testing is a methodology of identifying and exploiting security vulnerabilities to test the effectiveness of security measures. It involves test preparation, execution, and analysis phases using automated tools. A penetration tester, also acknowledged as a moral hacker, is accountable for identifying vulnerabilities and weaknesses in computer schemes, networks, and applications in order to help organizations progress their security posture. Ethical hackers and penetration testers assist organizations in finding possible attack routes in their digital infrastructure by pointing out vulnerabilities and flaws in that infrastructure. Ethical hacking, also known as penetration testing, involves simulating cyber-attacks to identify and define vulnerabilities in a computer system or Network. By using penetration testing methodology, our penetester and research team will assess the risks that are associated with potential security breaches. The penetration testing process consists of seven different phases.

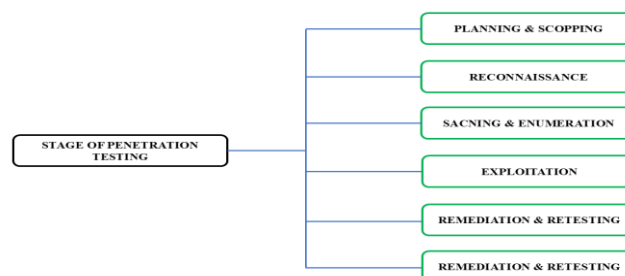


Figure 8: Stages of penetration testing.

To perform the penetration testing process, the penetester should define the plan and scope of work. The organization and the pentester must discuss before the actual testing start to go over the procedures and objectives. By doing this discussion, all ambiguities are resolved and everyone agrees to the testing procedure. Pentester ought to inquire and remain concerned about the organization's expectations. Mutual Understanding of the network and the system can help to identify and resolve the vulnerability.

Reconnaissance is the preliminary phase of the penetration testing process. Pentester gathers information analyses by using two types of reconnaissance techniques (Active and passive reconnaissance). Active reconnaissance is performed to scan networks, web

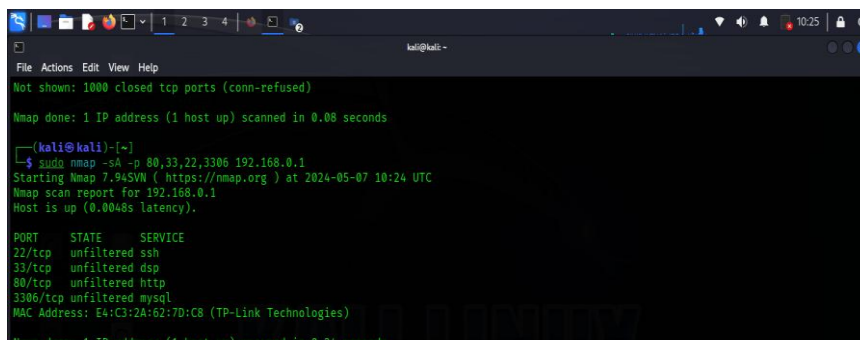


applications, etc, and identify vulnerabilities. NMAP is used to scan the target networks and NESSUS or Open VAS is used to identify potential vulnerability of the target system.

Passive reconnaissance is performed to retrieve information from open sources without interacting with the target system. OSINT tools like Spider Foot or The Harvester is used to gather publicly available information about the target system. Whois.is or ICANN whois is used to retrieve information about the domain names. Tools like Dsnenun, and Dnsmap help pentester obtain domain information or IP address mapping. Google Dorking is an advanced search operation technique which is also known as Google Hacking database (GHDB). It can help the pentester to gather publicly available personal or organizational information.

Scanning and enumeration step involves advanced network scanning and web application scanning. NMAP is used here for detailed scanning. It also performs traceroute and ping sweep techniques to track the pathway packets take to reach a destination and scan a range of IP addresses to determine which hosts are alive. Metasploit is used to test and execute exploits. Dnsenum is used for DNS enumeration, and to identify domain names and associated records. Shodan is an open-source search engine, that is used to collect information and credentials of IoT devices.

We perform exploits against the vulnerabilities have discovered during the "exploitation" phase. Certain vulnerabilities, such as using the default password to get into a system, can be easily exploited and executed. We use Metasploit to execute exploits and gain control over the target system. Burpsuite and OWASP ZAP follow the same working methodology and help the us to test



```
File Actions Edit View Help
Not shown: 1000 closed tcp ports (conn-refused)
Nmap done: 1 IP address (1 host up) scanned in 0.08 seconds

(kali@kali)~$ sudo nmap -sA -p 80,33,22,3306 192.168.0.1
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-07 10:24 UTC
Nmap scan report for 192.168.0.1
Host is up (0.0048s latency).

PORT      STATE      SERVICE
22/tcp    unfiltered ssh
33/tcp    unfiltered dsp
80/tcp    unfiltered http
3306/tcp  unfiltered mysql
MAC Address: E4:C3:2A:62:7D:C8 (TP-Link Technologies)
Nmap done: 1 IP address (1 host up) scanned in 0.24 seconds
```

Figure 9: Nmap ports scanning.

During this stage, our penetration tester attempts to go a bit deeper by acquiring the information, such as looking for relevant files and attempting to increase their privileges. The pentester can attempt to utilize the compromised workstation to leak password hashes to access further systems, or they can use the successfully attacked systems that weren't previously accessible by using an exploited computer.

Our security researcher's team can use Mimikatz to extract Passwords and other credentials from memory. Power sploit is used to exploit and manipulate the Windows system. Empire framework is used for the execution of PowerShell and Python agents.

The pentester reports to the organization after completing the investigation. It should be presented in a way that makes sense, including vulnerabilities that need to be resolved, how our pentester gained access to the system, what was found within the organization's system, how to resolution matters that were detected, and so on. A technical report and an "executive summary" should be included in the report.

Dradis and Faraday are the tools for organizing and reporting the outcomes of the penetration testing. These tools help pen testers to create a well-structured report.

At last of the penetration testing, we need to take some necessary steps to resolve the identified vulnerabilities. Remediation refers to actions taken to fix the identified potential vulnerabilities. It may include reconfiguring the system or network architecture, applying security patches, and changing the working process of the system. After completing the remediation process, the system should be retested to ensure that the vulnerabilities have been effectively addressed.



Table 2: Find Potential Vulnerabilities using Reconnaissance Techniques.

Potential Vulnerabilities	Active Reconnaissance	Passive Reconnaissance
Open Ports and Services	Port Scanning by using NMAP	Evaluating service flags using network surveillance.
Unpatched Software	Nessus, OpenVAS used to identify potential vulnerabilities.	Collect version information from Open sources.
Weak Passwords	By using Hydra perform Brute Force Attacks.	Credential leaks from data breaches
Outdated SSL/TLS Certificates	Nmap with NSE scripts can perform SSL Scanning.	Logs of public certificates' transparency.
DNS Misconfigurations	Using nslookup identify DNS Zone Transfers	DNS enumeration tools are used.
Cross-Site Scripting (XSS)	Automated Scanner OWASP ZAP can be used to identify vulnerability.	By analyzing website content and user inputs.
Weak Encryption	Aircrack-ng is used to identify weak encryption.	Weak encryption by checking public key databases and repository.
Misconfigured Services	Scan network using Nmap.	Reviewing configuration files if publicly available.
Publicly Accessible Databases	SQLmap is a tool commonly used to perform direct access attempts on SQL databases.	Conduct a Shodan search to identify databases that are publicly accessible.
SQL Injection	SQLmap is used for SQL Injection Testing.	Reviewing web application code and public reports.
Social Engineering Vulnerabilities	Phishing attacks using social engineering tools.	Gathering personal information from social media and open-source



		data.
Physical Security Weaknesses	Physical Penetration Testing	Monitoring and evaluating physical security settings.
Weak Access Controls	Access Control Testing using Metasploit.	Reviewing public documentation and access policies.

5. FUTURE WORK

In the meantime, as information technology keeps improving, the frequency of cyber-attacks is constantly increasing. To protect ourselves against such attacks, it is essential that we always engage in ongoing research on cyber security. Future enhancements of this study will concentrate on expanding multiple aspects of research and tools. Here are some possible areas that might be enhanced:

- i. Implementing real-time threat information in cybersecurity enables the proactive detection and mitigation of vulnerabilities. Threat intelligence assists in categorizing hazardous actions and circumstances enabling rapid detection and more efficient response tactics. This method aims to enhance the capacity to detect potential attack patterns and provide Quantum computers are expected to be used as mainstream computers within the next few years. As quantum computers can handle increasing amounts of data, they will be able to offer more computational power. Quantum-resistant encryption will play a vital role in the field of cybersecurity. Quantum-resistant encryption will help cyber security professionals to data against cyber threats.
- ii. Advanced threat detection and machine learning algorithm can examine huge volumes of data to identify the patterns of cyber threats. The integration of advanced machine learning (ML) algorithms and the techniques of artificial intelligence (AI) which will help security advisors to increase the capability of threat detection and remediation methodology.
- iii. AI-Driven Privacy solution
- iv. Integration of human aspects in cybersecurity will be the key factor against cyber-attacks. This involves investigating how human behavior, decision-making, and



awareness influence security procedures and establishing remedies to mitigate vulnerabilities emerging from these components.

- v. Extended research on Blockchain and Decentralized Networks Technology will diminish network & financial management system vulnerabilities.
- vi. Collaborative Research Initiative will help to increase cybersecurity.
- vii. the most appropriate countermeasures. Effective implementation of this method will detect vulnerabilities prior to their exploitation.

6. CONCLUSION

This research paper is to express the importance of reconnaissance and footprinting techniques in the field of cyber security. This study shows the methods and tools used in both performing and defending against reconnaissance and footprinting activities. This paper provides a robust framework for cybersecurity professionals. The first phase of the paper highlights various types of methodology of active and passive reconnaissance tools and techniques. It also shows the importance of information-gathering techniques in the sector of cyber security. Phase two demonstrated the necessity of defense methodology. It also discussed the implementation of firewalls, IDS/IPS, and SIEM systems to mitigate the risk of cyber-attacks. Phase three of this paper gives a structured approach to penetration testing. Finally, this study contributes valuable Insights and practical knowledge of enhancing cyber security and ensuring protection against potential vulnerabilities.

References

- [1] <https://newsroom.accenture.com/news/2019/cost-of-cybercrime-continues-to-rise-for-financial-services-firms-according-to-report-from-accenture-and-ponemon-institute>
- [2] <https://policycommons.net/artifacts/1606169/the-cost-of-cybercrime/2295943/>
- [3] <https://policycommons.net/artifacts/1606169/the-cost-of-cybercrime/2295943/>
- [4] https://www.business-standard.com/finance/personal-finance/cybercrime-costs-to-hit-10-5-trn-by-2025-how-insurance-may-save-your-biz-124072400476_1.html
- [5] <https://cybersecurityventures.com/cybercrime-to-cost-the-world-9-trillion-annually-in-2024/>



- [6] World Economic Forum. (2023). Notable cyberattacks in 2023. Retrieved from World Economic Forum.i
- [7] Kashyap, P., & Selvarajah, V. (2021, September). Analysis of Different Methods of Reconnaissance. In 3rd International Conference on Integrated Intelligent Computing Communication & Security (ICIIC 2021) (pp. 509-519). Atlantis Press.
- [8] Sanghvi, H. P., & Dahiya, M. S. (2013). Cyber reconnaissance: an alarm before cyber attack. *International Journal of Computer Applications*, 63(6).
- [9] Singh, Y., Singh, P., & Sinha, G. (2022). Footprinting Using Nmap. *Journal of Informatics Electrical and Electronics Engineering (JIEEE)*, 3(2), 1-15.
- [10] Arabia-Obedoza, M. R., Rodriguez, G., Johnston, A., Salahdine, F., & Kaabouch, N. (2020, October). Social engineering attacks a reconnaissance synthesis analysis. In 2020 11th IEEE Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON) (pp. 0843-0848). IEEE.
- [11] Roy, S., Sharmin, N., Acosta, J. C., Kiekintveld, C., & Laszka, A. (2022). Survey and taxonomy of adversarial reconnaissance techniques. *ACM Computing Surveys*, 55(6), 1-38.
- [12] Lianq, K. S., & Selvarajah, V. (2022, April). Footprinting and Reconnaissance: Impact and Risks. In 2022 IEEE International Conference on Distributed Computing and Electrical Circuits and Electronics (ICDCECE) (pp. 1-5). IEEE.
- [13] Jafarian, J. H., Al-Shaer, E., & Duan, Q. (2015). An effective address mutation approach for disrupting reconnaissance attacks. *IEEE Transactions on Information Forensics and Security*, 10(12), 2562-2577.
- [14] A. Kamruzzaman, K. Thakur, S. Ismat, M. L. Ali, K. Huang and H. N. Thakur, "Social Engineering Incidents and Preventions," *2023 IEEE 13th Annual Computing and Communication Workshop and Conference (CCWC)*, Las Vegas, NV, USA, 2023, pp. 0494-0498, doi: 10.1109/CCWC57344.2023.10099202.



BIOGRAPHY



At the moment **Mahmudul Hasan** is working with his project under the department of Computer science and engineering, Bangladesh University. In future he wants to work with a research team under the sector of cybersecurity and the latest technologies under the field of communication technologies.



Mohammad Arifin Rahman Khan has received one of his research degree from Edith Cowan University, Australia in 2019 and completed his M.Sc. degree from London Metropolitan University, London in 2010. He is working as a principal supervisor for this project. According to his professional career, Mohammad khan has teaching experienced from the national and foreign universities, moreover more than 5 years he has experienced from the position of research assistant. He is also working as a director of thesis and project for the département of CSE in Bangladesh University. His research interests include mobility management, multimedia transmission, and quality-of service (QoS) etc. provision issues in the next-generation of wireless/mobile networks.



Mohammed Ibrahim Hussain has completed the Masters in E-Commerce from London, UK. He had completed Bachelor Degree in Computer Science and Engineering from The National Technical University of Ukraine, Kiev, Ukraine. He has successfully completed Cisco Certified Network Associate (CCNA), Microsoft Certified Technology Specialist (MCTS) and Microsoft Certified T Professional (MCITP) on Server 2008 platform. He is also nominated Book Reviewer of The National Curriculum of Textbook Board. His research interest includes Operating Systems, Networking, and Microwave.



Mohd Abdullah Al Mamun is a dedicated professional currently pursuing a second MBA in Information Technology at Westcliff University, USA. With a strong academic foundation, he holds a Post Graduate Diploma in Human Resource Management from the Bangladesh Institute of Management, an MBA in Human Resource Management from BRAC University, Bangladesh, and a BBA in Human Resource Management from Stamford University Bangladesh. He has contributed his expertise to both the nonprofit sector and the financial industry, particularly in the human resources, where he played a pivotal role in organizational development and employee management. His passion for information technology and its crucial role in today's world, his commitment to extensive research aimed at advancing the field and honing his skills. Mr. Mamun's diverse educational background uniquely positions him to contribute valuable insights to the intersection of information technology and human resource management, making him an asset in various research and journal endeavors.



Md. Moazzam Hossain has completed his B.Sc. in computer science and engineering degree in 2023 from Bangladesh University. At the current moment he is working as a data analyst with REVENCO. In future he wants to involve himself like a research member for the field of wireless communication.



Syed Mominul Islam has completed his B.Sc. in computer science and engineering degree in 2023 from Bangladesh University. At the current moment he is working as a Software Developer with REVENCO. In future he wants to involve himself like a research member for the field of communication technology.



K M Nurazzaman has completed his B.Sc. in computer science and engineering degree in 2023 from Bangladesh University. At the current moment he is working as a Service Associate, with Midland Bank PLC. In future he wants to involve himself like a research member for the field of cybersecurity and wireless communications.