Paradigm Academic Press
Innovation in Science and Technology
ISSN 2788-7030
JUN. 2026 VOL.5, NO.2

Hacking Is an Unauthorized Access in Electronic Devices: Skills Technologies Are Necessary to Enhance Defense Strategies

Haradhan Kumar Mohajan[1]

[1] Chairman and Associate Professor, Department of Mathematics, Premier University, Chittagong, Bangladesh

Correspondence: Haradhan Kumar Mohajan, Chairman and Associate Professor, Department of Mathematics, Premier University, Chittagong, Bangladesh.

doi:10.63593/IST.2788-7030.2026.06.001

Abstract

Hacking is the technique of finding the weaknesses in the network system that exploits to gain unauthorized access to personal or business data that are in the networks, and the hacker is responsible for the legal consequences of his/her actions. The hacker has basic knowledge, desire, motivation, deep patience, planning workability, and financial supports. Usually an unethical hacker (black hat hacker) is a malicious guy who tries to steal, leak, and destroy confidential and valuable data and other sensitive information of the computer systems without permission of the user. S/he can usually be organized into two types of attacks: mass attacks and targeted attacks. On the other hand, an ethical hacker (white hat hacker) tries to strengthen the security mechanisms of the organization by exploring the weaknesses of it. This study tries to discuss the aspects of unethical hacking, types of hackers, and their behaviors.

Keywords: hacking, hacking techniques, hacker, cybercrime, cyber security

1. Introduction

After the advent of internet anybody can communicate with any person in any part of the world and makes any deal with just a click with any electronic device connected to network. Consequently, the physical distance barrier has been removed and transaction time has been highly reduced, but the cheating and frauds become very high that increase global concern (Begum et al., 2016). Information security is the protection of information system from unauthorized access, use, disclosure, disruption, modification, and destruction. In the digital world in our daily lives, we have observed that security attacks are growing in an exponential manner (Pal, 2016). Nowadays most of the currently available websites, networks, and applications are poorly and hastily configured, and malicious hackers can exploit these vulnerabilities and security gaps (Yaacoub et al., 2021).

Hacking is the act of identifying and exploiting weaknesses in digital devices, such as computers, smartphones, tablets, and networks by an unauthorized source through the installment of dangerous malware (Oakley, 2019). It is not a basic or regular activity that consists of two paths. The first path is towards the legal and permissioned work while the other path is towards the illegal and unapproved work (Memon et al., 2020). It is the most common form of cybercrime that can be used from monetary gain to political interest. It may be in different forms, such as web-spoofing, email bombing, Trojan attacks, phishing, fake websites, spyware, electronic bulletin boards, information brokers, virus attacks, wormhole attack, password cracking, etc. (Fuchs, 2014; Mohajan, 2025b).

Hackers are a type of programmers and software engineers, who usually steal the secret data, such as phone numbers, credit card details, addresses, online banking passwords, etc. (Kumar & Agarwal, 2018). They are mostly nerd, wild, and teenager types, and spend an average time of 57 hours a week on their system. They are experienced in C, C++, and Perl programming languages, and familiar with the UNIX (Chirillo, 2002; Mohajan,

2025c).

2. Literature Review

A literature review is a comprehensive summary and critical evaluation of existing scholarly work on a specific topic that is a section of a larger work of an article, a conference paper, a book, a book chapter, or a thesis (Creswell, 2013). It is an overview of previously published works on a particular topic. It involves finding scholarly literature on the topic, reading and taking notes, analyzing or evaluating the literature, writing the literature review, etc. (Torraco, 2016). It highlights how knowledge has evolved within the field, what has already been done, what is generally accepted, what is emerging, and what is the current state of thinking on the topic (Galvan, 2015). It provides the current state of knowledge, identify gaps in the research, and establish a foundation for new research. A good literature review has a proper research question, a proper theoretical framework, and a chosen research methodology (Baglione, 2012).

S. K. Ashwini and K. Thippeswamy have provided the brief information on ethical hacking, ethical hacking types, how ethical hacking works, methodology and hacking tools, and some needs and limitations of the ethical hacking (Ashwini & Thippeswamy, 2018). Rajinedr Singh and Shakti Kumar have shown that in Information and Communications Technology (ICT) no one is isolated, and are connected to each other through internet and new networking technology. They have observed that the network and windows security can be simple or complex depending upon the requirements. They have analyzed the security threats and internet protocol to determine the necessary security technology through the understanding of its importance, history, and various technologies that can be used to provide security measures (Singh & Kumar, 2014).

Imran Memon and his coauthors have shown that hacking is the most genius field of computer science that is getting bigger with the passage of time. They have used the methods and techniques of hacking, types of hacking, types of hackers, types of hacking attacks, common tools of hacking, the geography of hackers, phases of hacking, protection processes, past reports, instruments of hacking, and at last the future discussion on this field (Memon et al., 2020). Priyank Dinesh Gada has wanted to show how credit card hacking works, how smartphones can be hacked, how SIM swapping works, and other techniques with a practical approach. He also shows how to change International Mobile Equipment Identity (IMEI) number and other black hat hacking techniques used by hackers (Gada, 2024).

Md. Shaiful Islam and his coworkers have wanted to examine the challenges of cyber security to service delivery in the public administration. They have identified the cyber security issues, cyber threats, vulnerabilities, awareness among employees, and steps taken to ensure cyber security in the offices of public administration in Bangladesh (Islam et al., 2023). Minakshi Bhardwaj and G.P. Singh have discussed three types of attacks against computer systems: physical, syntactic and semantic attacks. A physical attack uses conventional weapons, such as bombs or fire. A syntactic attack uses virus-type software to disrupt or damage a computer system or network. A semantic attack is a more subtle approach. Its goal is to attack users' confidence by causing a computer system to produce errors and unpredictable results (Bhardwaj & Singh, 2011).

3. Research Methodology of the Study

Research is a creative and systematic work undertaken to increase the stock of knowledge that involves the collection, organization, and analysis of evidence to increase understanding of a topic; characterized by a particular attentiveness to control sources of bias and error (Kara, 2012). It searches for knowledge and truth that must be controlled, rigorous, systematic, valid and verifiable, empirical, and critical (Grover, 2015). Methodology is the analysis of the principles of methods, rules, and postulates employed by a discipline (John, 2017; Mohajan, 2018b). Research methodology is the systematic plan for conducting a study, detailing the specific procedures and techniques used to collect, analyze, and interpret data to answer research questions (Groh, 2018). It includes the overall research design, data collection methods, and data analysis techniques, explaining why these choices are made to ensure the results are valid, reliable, and replicable. It is a science of studying how research is to be carried out in a systematic way to solve a problem (Creswell, 2013). In this study we have dependent on the secondary data sources that are collected from research articles, hand books, books, thesis, and project reports (Mohajan, 2020). We have also stressed on the reliability and validity for the acceptance of ethical values (Mohajan, 2017). At the starting we have highlighted on the overview of hacking, and then we have discussed on hacker and its types. At the third step we have briefly discussed the tools of hacking, types of hacking, and finally we have highlighted on steps of hacking.

4. Objective of the Study

Hacking is the process of attempting to gain unauthorized access to computer resources. It has been a part of computing for last 50 years (Pal, 2016). There are many types of hacking in networking system, such as website hacking, network hacking, ethical hacking, unethical hacking, email hacking, password hacking, computer hacking, bank account hacking, etc. (Cekerevac et al., 2018). In the 21st century, hacking becomes one of the

most important skills in the networking system that is getting bigger with the passage of time (Mohajan, 2025c). Regular auditing, vigilant intrusion detection, good system administration practice, and computer security awareness are all essential parts of security efforts of an organization (Oakley, 2019). The hacker is a person who has a basic knowledge, desire, motivation, and some money. S/he must have a large dose of patience and planning workability. However, neither all hackers are all the same, nor all hackers have the same goals (Gada, 2024). Main objective of this study is to discuss the background and overview of hacking with identification and classification of hackers (Mohajan, 2025a). Some other minor objectives of the study are as follows (Mohajan, 2018a):

1) to highlight on hacker and its types,
2) to focus on tools and types of hacking, and
3) to emphasize on steps of hacking.

5. Overview of Hacking

Hacking is the act of compromising digital devices and networks through unauthorized access to an account or computer system, and a hacker is responsible for the legal consequences of his actions. It refers to the misuse of devices, such as computers, smartphones, tablets, and networks to cause damage to corrupt systems, gather information on users, steal data and documents, and disrupt data-related activity (Cekerevac et al., 2018). They also try to collect various data, such as business and private data, bank accounts, emails, websites, databases, etc. to damage and destruct them or for personal gaining (Sheikh, 2021). Hacking is not a regular activity that consists of two paths: The first path is towards the legal and permissioned work, and it is called ethical hacking while the other path is towards the illegal and unapproved work, and it is called unethical hacking (Memon et al., 2020; Mohajan, 2025d).

6. Hacker and Its Types

A hacker is a person skilled in information technology that solves problems by non-standard means, and achieves success. He is an expert computer programmer who has huge exceptional knowledge of computer programming and has enough information on the systems to hack (Gregg, 2006). The term “hacker” (skillful programmer) was coined in the 1960s by a couple of Massachusetts Institute of Technology (MIT) students of Tech Model Railroading Club (TMRC) to describe the students who creatively solved technical problems, especially those who found clever programming shortcuts (Sterling, 1992). It largely referred to persons capable of implementing elegant and technically advanced solutions to technologically complex problems. Initially it was a positive term for experts; and later it was adopted by mainstream media to describe computer criminals (Kartalopoulos, 2008).

The hacker has knowledge in both hardware and software operations. Consequently, s/he is the most dangerous threat to the information systems. There are mainly three types of hackers: white hat, black hat, and gray hat hackers (Moore, 2005). Other four types of hackers based on what they hack and how they perform the hack are green hat, red hat, blue hat hackers, and script kiddie (Levy, 1984). They are professional hackers and highly technical people who perform hacking for earning their personal incomes. For example, many white hat hackers are employed worldwide to test organizations’ computer security systems (Hoffman, 2013). Data security is a huge problem in the modern world. At present worldwide security spending reaches to $100 billion (Shital, 2023).

6.1 White Hat Hackers

White hat hackers are known as the good guys or ethical hackers or sneakers who hack with permission from the data owner, and who have non-malicious nature (Levy, 1984). They are certified hackers who work for the Government, non-government organizations (NGOs), and private firms under the rules and regulations provided by the Government through performing penetration testing and identifying loopholes in their cyber security (Banda et al., 2019). They work ethically aiming to improve security, and learn hacking from courses. They use their skills to find vulnerabilities and help organizations to improve their defenses (Cornwall, 1986). They are considered good hackers, and work for the benefit of the network system. They use their abilities for good, ethical, and legal purposes rather than bad, unethical, and criminal purposes (Shanmugapriya, 2013). The International Council of Commerce Consultants (ICC) is one of the organizations that has developed certifications, courseware, classes, and online training covering the diverse arena of white hacking (Pal, 2016).

White hat hackers are computer security specialists and try to find loopholes in the protected networks or the computer systems of an organization and improve the security. Usually, they are either hired or contracted by organizations to evaluate their security parameters (Shital, 2023). They have hacking skills for defensive purposes, and locate weaknesses and implement countermeasures. They provide detail security vulnerability reports to the organization and inform it of how they have gained access, and allow the organization to improve

its defenses (Hoffman, 2013).

6.2 Black Hat Hackers

The term “black hat hacker” was coined by American free software movement activist and programmer Richard Stallman. They are also known as “crackers” who hack the systems with malicious intent, and exploit vulnerabilities for personal gain, financial profit, and cause harm (Moore, 2005). They are considered as bad hackers and target to destroy the system, compromise the privacy, block communication, damage the computer system, and thieve the confidential information. They are familiar with computer networks, Linux, cryptography, and other skills (Hoffman, 2013). They are highly skilled and have knowledge in various hacking techniques (Sheikh, 2021). They are also computer hardware and software experts who break into the security of stealing or damaging the important or secret information, compromising the security of big organizations, shutting down or altering functions of websites and networks (Levy, 1984). They violate the computer security for their personal gain. They are engaged in various illegal activities, such as stealing data, spreading malware, and disrupting systems (Cornwall, 1986). They sabotage the systems to obtain information about their targets, such as bank information, personal details, phone numbers, etc. (Begum et al., 2016). They can sell the security vulnerability reports to criminal organizations on the black market or use it to compromise computer systems. They can make money by selling data and credit card information on the dark web. They can ruin reputation of anyone to take revenge (Hoffman, 2013).

American computer security consultant and author Kevin Mitnick is one of the most well-known black hat hackers and cybercriminals in the world, who hacked more than forty major corporations, and later he becomes a white hat hacker (Greenberg, 2022). American computer hacker, computer criminal and police informer, Albert Gonzalez is the largest credit card thief in history who has theft more than 170 million of credit card numbers (Stone, 2008). Some countries, such as China, Russia, and the USA hire black hat hacker to steal data related to militaries from other countries (Chng et al., 2022).

6.3 Grey Hat Hackers

The term “grey hat hacker” came into use in the late 1990s by the hacker group L0pht, and was derived from the concepts of the combination of white hat and black hat hackers (Hoffman, 2013). The grey hat hackers occupy a middle ground between the ethical intentions of white hats and the malicious activities of black hat hackers. They attack the device without seeking permission and considered to be illegal, but do not malachite like the black hat hackers (Harris et al., 2004). They neither illegally exploit the vulnerabilities and nor tell anybody how to do so. They sometimes act ethically but sometimes not, and sometimes they repair the vulnerability for a small fee (Regalado et al., 2015). They have skills and intent of the white hat but may break into any system or network without permission. They may disclose vulnerabilities they find without permission, which can be illegal. They work both defensively and aggressively (Nagarani, 2015). The LulzSec Group served as grey hat hacker, and exposed several vulnerabilities in high-profile companies and Government organizations. American well-known computer security researcher Charles Alfred Miller served as grey hat hacker at National Security Agency, iPhone, and Uber (Miller, 2009).

6.4 Green Hat Hackers

Green hat hackers are known as neophytes or newbies. They are the youngest and novice in hacking and cyber security. They have little or no knowledge and experience in hacking at all (Sheikh, 2021). They rely on the use of already written scripts, and ask lots of questions and are typically very curious. Their aim is to learn about cyber security and contribute positively to the field of cyber security (Levy, 1984). They can assist in identifying basic common vulnerabilities and bugs in applications, and have skills in input validation flaws or insecure data storage practices (Gregg, 2006). They can provide valuable feedback from a beginner perspective, and can offer insights into how a less experienced individual might attempt to exploit vulnerabilities that can be informative for developers in understanding potential attack vectors. They can create a controlled environment for learning and identifying security gaps (Hanusch, 2021).

6.5 Red Hat Hackers

Red hat hackers are the ultra-white hat hackers who use extreme and brute force techniques and tactics, and aggressively attacks and disables to combat against malicious black hat hackers through destroying data and systems to stop them (Moore, 2005). They are the greatest concern, danger, and threat for the black-hat community. They use aggressive methods, attack and technique to take down them down (Caldwell, 2011). They typically target Linux systems due to their open-source nature that provides easy access to both command-line interfaces and popular hacking tools. They upload viruses and destroy their devices and computers, or retrieve their information and kill off their devices (Levy, 1984). They are vigilantes in cyber security, and usually they hack Government agencies and top-secret headquarters in order to gain sensitive information (Chng et al., 2022).

6.6 Script Kiddie

A script kiddie is a new and unskilled hacker to the world of hacking, and exclusively relies on copying codes and scripts to perform malicious code injection and modification. S/he is an amateur hacker with limited technical knowledge, and relies on already-made programs in order to use them (Hanusch, 2021). S/he simply wants to buy all the tools s/he needs and uses them without doing anything themselves. S/he can use pre-made tools and scripts to launch attacks without understanding the underlying mechanisms. In some cases, script kiddies watch tutorial videos in order to apply them and use them for themselves (Levy, 1984). Sometimes s/he may rather pay money and performs a straightforward attack than come up with new, secret, or creative ways to carry out his/her plans (Banda et al., 2019).

6.7 Blue Hat Hackers

Blue hat hackers are external cyber security professionals hired by an organization to find vulnerabilities in a system before its public launch, who violate laws or ethical standards for nefarious purposes, such as cybercrime, cyber warfare, and malice (Cornwall, 1986). They are as like script kiddies but want to take revenge against someone using hacking as a tool (Banda et al., 2019). But they are unlike green hat hackers and have no desire to learn new techniques and rely on the knowledge that they have already gained to perform their tricks. They are classified as invited security professionals to find any vulnerability in Microsoft Windows (Levy, 1984).

There are many skillful hackers that are present in the different countries but some countries are in the leading position in the field of hacking, such as China, the USA, Turkey, Russia, Taiwan, Brazil, Romania, India, Italy, Hungary, etc. (Cyware News, 2020).

7. Tools of Hacking

Kali Linux offers more than 600 preinstalled tools for ethical hacking. Some of the best use tools are Nmap, Metasploit, Nessus, Hydra, and Wireshark, and these are used by security professionals to find and fix vulnerabilities (Mohajan, 2025b).

7.1 Nmap

Network mapper (Nmap) is a free and open-source network vulnerabilities scanner that is used by penetration testers. It is an integral part of academic activities that provides more advanced service detection, vulnerability detection, and other features. It is a tool that can be used to discover services running on internet connected systems. It is also used by ethical hackers to assess their own networks for vulnerabilities (Haines et al., 2003).

The Nmap is created by American network security expert Gordon Lyon. It detects the vulnerabilities of the network and presents the report to the user (Lyon, 2008). It is an open source Linux command line tool that is used to scan Internet Protocol (IP) addresses and ports in a network and to identify hosts, services, operating systems, and firewall (Joshi, 2021). It is developed to scan big networks, and beneficial for network inventory, controlling service updates schedules, and monitoring host or service uptime. It is compatible with all major operating systems, such as Windows, Mac OS X, and Linux (Elhai & Hall, 2016). It helps the device to quickly map out a network without sophisticated commands, and supports simple commands and complex scripting through the Nmap scripting engine. It performs a basic port scan for fast result that identifies hosts on a network, and interrogates network services on remote devices to determine application name and version number (Medeiros et al., 2009).

7.2 Wireshark

Wireshark is a free and open source network scanner, which is one of the best packet analyzers available today that detects the vulnerabilities of the network. It was developed by Gerald Combs, Director of Open Source Projects at Riverbed Technology, USA; under the name Ethereal in 1997, and later it was renamed Wireshark in May 2006 due to trademark issues (Sanders, 2007). It is available for UNIX and Windows that capture live packet data from a network interface. It is a network packet analyzer that presents captured packet data in as much detail as possible (Lamping, 2004).

The Wireshark scanner can capture traffic from many different network media types, such as Ethernet, Wireless LAN, Bluetooth, Universal Serial Bus (USB), etc. It provides deep visibility into network communications, allowing users to analyze data at the packet level that seeks to simplify and enhance the process of network traffic analysis (Cheok, 2014). It is the world's leading network protocol analyzer that is used by network administrators, security professionals, and developers to capture, inspect, and troubleshoot network traffic in real time (Jain, 2022). It is widely used for network troubleshooting, open source network analysis, software and communications protocol development, and education that can capture and display real-time details of network traffic (Orebaugh et al., 2007).

7.3 Metasploit

The Metasploit tool is a computer security project that provides information about security vulnerabilities and

aids in penetration testing and intrusion detection system (IDS) signature development for creating security tools and exploits (Kennedy et al., 2011). It consists of tools, libraries, modules, and user interfaces, and the basic function of it is a module launcher that allows the user to configure an exploit module and launch it at a target system (Ajero, 2022). It allows the operator to easily build attack vectors to augment its exploits, payloads, encoders, and more in order to create and execute more advanced attacks. It is not just a tool but an entire framework that provides the infrastructure needed to automate mundane, routine, and complex tasks (Muñoz et al., 2018). It is available in two versions: commercial and free that are used with either a command prompt or a web interface (Foster & Liu, 2006).

The Metasploit is created by American network security expert, open source programmer and hacker H. D. Moore in 2003 as a portable network tool using Perl. With the help of Spoonm, he has released a total rewrite of the project, Metasploit 2.0, in April 2004 that includes 19 exploits with 27 payloads. In 2009, it is owned by a US-based cyber security company Rapid7, a leader in the vulnerability-scanning field. It operates as an open-source project and accepts contributions from the community through GitHub.com pull requests (Foster & Price, 2005). At present it has more than 2,074 exploits, organized under the platforms on AIX, Android, iPhone, BSD, BSDi, Cisco, Firefox, FreeBSD, HP-UX, Irix, Java, JavaScript, Linux, mainframe, NetBSD, NetWare, NodeJS, OpenBSD, macOS, Maemo, PHP, Python, R, Ruby, Solaris, Unix, and Windows (Rahalkar & Jaswal, 2017). It is widely used worldwide in network security professionals, system administrators, product vendors, and security researchers to perform penetration tests, verify patch installations, and perform regression testing (Teixeia et al., 2021).

7.4 Nessus

Nessus is a platform developed by Tenable Holdings, Inc., a cyber-security company based in Columbia, Maryland that scans for security vulnerabilities in devices, applications, operating systems, cloud services, and other network resources (Medhora & Finkle, 2016). In 1998, Renaud Deraison, the father of the Nessus vulnerability scanner, has created *The Nessus Project* as a free remote security scanner. It features high-speed asset discovery, configuration auditing, target profiling, malware detection, sensitive data discovery, etc. (LeMay, 2005).

It identifies software flaws, missing patches, malware, and misconfiguration errors across a wide range of operating systems, devices, and applications used in organizations (Mohajan, 2025e). It supports more technologies than competitive solutions, scanning operating systems, network devices, next generation firewalls, hypervisors, databases, web servers, and critical infrastructure, such as Common Vulnerability Scoring System (CVSS) v4, Exploit Prediction Scoring System (EPSS), and Tenable's Vulnerability Priority Rating (VPR) feature; for vulnerabilities, threats, and compliance violations (Awati, 2025). It is now available in two enterprise versions: Nessus Professional and Nessus Expert that support unlimited IT vulnerability assessments and multiple systems for vulnerability scoring. It provides more than 450 preconfigured templates to help users understand where vulnerabilities are present (Tenable, 2025).

7.5 The Hydra

Hydra (THC-hydra) is a powerful and versatile password cracking tool for testing the security of authentication systems in social media, such as Facebook, Instagram, twitter, etc. (Kumar & Agarwal, 2018). It is very fast, stable, and flexible network login hacking tool. It is an open-source tool designed to perform cyber-attacks through brute-force on various protocols and services to test the authentication mechanisms (Groza, 2009). It is easily available online at GitHub where all its newest releases are frequently updated. It is developed by German IT security expert and ethical hacker Van Hauser (Marc Heuse) (Yiannis, 2013). Some top uses of Hydra are password cracking, brute force attacks, dictionary attacks, secure shell (SSH) login testing, file transfer protocol (FTP) login testing, simple mail transfer protocol (SMTP) authentication testing, database login testing, web application login testing, voice over IP (VoIP) authentication testing, network device testing, etc. (Mamber, 1996).

The Hydra is a parallelized network login cracker built into various operating systems, such as Kali Linux, Parrot and other major penetration testing environments. It is capable of rapidly guessing and applying numerous password combinations to uncover authentication credentials across a variety of protocols (Dhanjani & Clarke, 2005). It is commonly used by penetration testers with a set of programs, such as crunch, cup, etc. Although it is widely used by cyber security professionals, its use must always be governed by legal authorizations to prevent abuse. It remains an essential tool in the arsenal of security testing (McNab, 2011). It supports more than fifty common login protocols on websites, such as FTP, SMB, POP3, IMAP, MySQL, VNC, SSH, HTTP(S), Cisco AAA, Cisco auth, Cisco enable, CVS, HTTP-Proxy, ICQ, IRC, LDAP, MS-SQL, NNTP, Oracle Listener, Oracle SID, PC-Anywhere, PC-NFS, PostgreSQL, RDP, Rexec, Rlogin, Rsh, SIP, SMTP, SMTP Enum, SNMP v1+v2+v3, SOCKS5, Subversion, Telnet, VMware-Auth, and XMPP (Kakarla et al., 2018).

8. Types of Hacking

Hacking is the activity of characterizing weaknesses in a knowledge processing system and a network to take advantage of the security to comprehend access to private knowledge through the exploitation of computers to commit fallacious acts like fraud, privacy invasion, stealing corporate/personal knowledge, etc. (Pal, 2016). Some devices that are at risk from hackers are smartphones, IoT gadgets, and older computers (Mohajan, 2015f). The computer and network hacks come in many forms and some of the most prevalent types are backdoors, denial of service (DoS), distributed DoS, phishing attacks, etc. (Gada, 2024).

8.1 Backdoors

When hackers can make an unapproved approach to any network by using a sound easy route without even being noticed by any security software, then it is known as backdoor hacking that contains the characteristics of all strikes (Li et al., 2022). A backdoor attack is a typically covert method of bypassing normal authentication or encryption in a computer, product, embedded device, or its embodiment, such as cryptosystem, algorithm, chipset, etc. (Eckersley & Portnoy, 2017). It represents a threat actor where the attackers can take over system resources, go through networks, and set up various malware programs. It is used for securing remote access to a computer, or obtaining access to plaintext in cryptosystems. A developer may create a backdoor so that an application, operating system or data can be accessed for troubleshooting (Ashok, 2017).

It may take the form of a hidden part of a program, a separate program, code in the firmware of the hardware, and parts of an operating system, such as Windows (Li et al., 2021). It may lead to data breaches, financial losses, reputational damage, and concerns about national security. Various types of malware are used in backdoor attacks, such as Cryptojacking, DoS attacks, Ransomware, Spyware, Trojan horse, federated learning, hardware, internet of things (IoT), Island hopping, Phishing, Steganography, etc. (Krieg et al., 2013).

8.2 Denial of Service

Denial of Service (DoS) attack is one of the major threats and is considered as one of the hardest problem in the internet today. It makes hacker capable of breaking any network without getting access in the network that targets the email or transmission control protocol (Elleithy et al., 2005). It is any type of attack on a networking structure to disable a server from servicing its clients that range from sending millions of requests to a server in an attempt to slow it down, flooding a server with large packets of invalid data, and to sending requests with an invalid (Fulp et al., 2001).

There are different types of DoS attacks, such as i) flood attack, that is flooding the target machine with external communications requests, so that it cannot respond to legitimate traffic, or responds so slowly as to be made unavailable; ii) logic and software attacks, that are internet packets are sent that should use bugs in the software (Nagesh & Sekaran, 2006); iii) Ping of Death, which is simulated against a Microsoft Windows 95 computer, iv) TCP SYN Flood, which is simulated against a Microsoft Windows 2000 IIS FTP Server, and v) distributed DoS (Mohajan, 2025e).

The DoS is an attack in which one or more machines target a victim that attempts to partially or completely prevent the victim from doing useful work, and to stop from viewing portions of the internet (Prakash et al., 2016). It clogs up so much memory on the target system that it cannot serve its users, or it causes the target system to crash, reboot, or otherwise deny services to legitimate users. As a result, a legitimate user or organization is deprived of certain services, such as web, email, or network connectivity that the user would normally expect to have. It poses significant threats to network security, disrupting critical services by overwhelming targeted systems with malicious traffic (Jain & Singh, 2012). It cannot be stopped or prevented, but some precautionary measures are taken into consideration to make the attacker very hard to attack. The network architecture should be built in a stronger way to secure the resources against various attacks. The host computers must be updated with the latest security patches and techniques (Bhardwaj et al., 2016).

8.3 Distributed DoS (DDoS)

The DDoS is demonstrated by simulating a distribution zombie program that will carry the Ping of Death attack. It makes the DoS strike efficient with number of sources and be controlled remotely. It has the characteristics of network foundation strike and operating system strike (Gresty et al., 2001). It is either flood attack or logic attack, but it uses many people, different computers, often from thousands of hosts infected with malware, and bots under the attacker's control, and usually attacks target sites, such as banks, credit card payment gateways, etc. (Dzaferovic et al., 2020). It occurs when multiple systems flood the bandwidth or resources of a targeted system, usually one or more web servers. It is analogous to a group of people crowding the entry door of a shop, making it hard for legitimate customers to enter, thus disrupting trade and losing the business money (Prince, 2016).

The first DDoS attack shutdown the entire internet access on the city for a couple of hours happened in 1997

during a hacker's conference event in Las Vegas by the well-known spammer and hacker Khan C. Smith. Revenge and blackmail as well as hacktivism can motivate these attacks (Lohachab & Karambir, 2018). Some common examples of DDoS attacks are UDP flooding, SYN flooding, and DNS amplification. The most obvious symptom of a DDoS attack is a site or service suddenly becoming slow or unavailable (Bhattacharyya & Kalita, 2016). If the attacks are from multiple sources, it can be difficult for the host to identify and stop those. One solution available to virtually all network admins is to create a blackhole route and funnel traffic into that route (Zuckerman et al., 2011).

8.4 Phishing Attacks

The most talked about topic in the world of social engineering is phishing that is the most common type of cybercrime. Phishing is a luring type cyber-attack that thieves use to "fish for" unsuspecting internet users' personal identifying information through emails and mirror-websites that the messages appear to come from well-known and trustworthy websites, and pressure has to act quickly, without thinking (Wright, 2016). It is a type of cybercrime where malicious actors trick victims into revealing sensitive information, such as usernames, passwords, credit card details, and personal data, by posing as a trustworthy entity (Ramzan, 2010). Attackers use deceptive emails, text messages, and fake websites to lure people into clicking malicious links or downloading malware, such as viruses, worms, adware, or ransomware (Jansson & von Solms, 2011).

The term "phishing" was coined by well-known spammer and hacker Khan C. Smith using the hacking tool AOHell that was released in 1994. Phishing may be various types, such as email phishing, spear phishing, whaling phishing, page hijacking, voice phishing, QR code phishing, SMS phishing, man-in-the-middle phishing, etc. Spear phishing is an email-spoofing attack that targets a specific organization or an individual, seeking unauthorized access to sensitive information. On the other hand, the whaling phishing is a type of fraud that targets high-profile end users, such as C-level corporate executives, politicians, and celebrities (Lin et al., 2019). The victims are asked to disclose name, parents name, place of birth, credit card numbers, social security numbers, account numbers, passwords, and other private information (Jansson & von Solms, 2011). Sometimes fake emails come from a reputable and recognize company that offers business proposal. The provided link appears to be the official website of the company, although it is fraudulent (Olivo et al., 2011). Anarchist hacking is performed by script kiddie that is not a professional type of hacking, because it cannot deal with any unapproved access. It makes strike only on any web content, such as Facebook, Instagram, and twitter (Son & Kim, 2008).

8.5 Password Cracking

Passwords are a system designed to provide authentication (Yan et al., 2004; Mohajan, 2025g). Human-memorable passwords remain a common form of access control to data and computational resources (Narayanan & Shmatikov, 2005). Password cracking is an attack vector that involves hackers attempting to determine a password for unauthorized authentication (Hellman, 1980). This can be done in several ways: i) brute-force attacks, which involves trying all possible combinations of characters until the correct password is found, it is time-consuming and requires significant computational power (Bahadursingh, 2020); ii) dictionary attacks, which involves the use of a dictionary of common passwords, and the hacker systematically tries each entry in the hope that the user has used a common password (Lundin, 2013); and iii) rainbow tables, which involves pre-computing the hashes for possible passwords and storing them in a 'rainbow table' (Burr et al., 2006). Password cracking can also do through other tactics, such as by memory-scraping malware, shoulder surfing, third party breaches, and tools like Redline password stealer (Oechslin, 2003).

8.6 Keyloggers

A keylogger is a type of spyware that records keystrokes of a user on the keyboard, and saves them to a log file; and the hackers use them to steal sensitive information, such as usernames, passwords, credit card numbers, messages, and other personal confidential information (Nyang et al., 2014). It is a smart malicious binary that takes an action to record keys that the user presses when the system is active at sensitive times. It can be used to study keystroke dynamics or human-computer interaction, and extremely useful for keeping track on ongoing criminal activity. It can be installed through malicious downloads, such as email attachments or by physically connecting a hardware device to a computer (Leyden, 2000).

There are two main types of keyloggers: hardware keyloggers and software keyloggers. A hardware keylogger is a physical device that is connected directly to the keyboard and the computer through manually using one of two approaches (Wajahat et al., 2019). It has a non-volatile memory device, such as flash memory that stores the recorded data, and retaining it even when power is lost; and a microcontroller that interprets the datastream between the keyboard and computer, processes it, and passes it to the non-volatile memory (Kuncoro & Kusuma, 2018). It may be different types, such as i) regular hardware keylogger, which is attached between the computer keyboard and the computer; ii) wireless keylogger sniffers, which collect packets of data being transferred from

a wireless keyboard and its receiver and then attempt to crack the encryption key being used to secure wireless communications between the two devices (Arghire, 2019); iii) firmware, which is responsible for handling keyboard events, and can be reprogrammed so that it records keystrokes as it processes them; iv) keyboard overlays, which is a fake keypad is placed over the real one so that any keys pressed are registered by both the eavesdropping device as well as the legitimate one that the customer is using (Wajahat et al., 2019); and v) key commands, which programs require keyloggers to know when the user is using a specific command. In the mid-1970s, the Soviet Union developed and deployed a hardware keylogger targeting US Embassy typewriters (Kirk, 2008).

A software-based keylogger is a computer program that can be installed without having direct access to the computer. It captures data when it travels across the keyboard and through the operating system that keeps track of keystrokes, saves them in a secure location, and subsequently sends them to the keylogger author (Aslam et al., 2004). Interrogation cycle, traps keylogger, rootkits keylogger, and keylogger kernel mood are the four primary categories of software keylogger. An early keylogger was written by Perry Kivolowitz and posted to the Usenet newsgroup net.unix-wizards, net.sources on November 17, 1983 (Le et al., 2008).

The main purpose of keyloggers is to tamper with the chain of events that occur when a key is pressed, and information is displayed on the screen as a result of the keystroke that can be used for both lawful and illegitimate objectives, depending on the user who is utilizing it (Berninger, 2012). Keylogger is common with many Trojans that is designed to mimic legitimate software and bypass anti-virus or anti-malware scanners (Javaheri et al., 2018). It is a sophisticated tool that can access not only the platform, but also the user's private information like their name, password, PIN, and card and bank statement. The aim of a keylogger is to act as a mediator between the system functions and user requests they come to know through discovering the pressed keys (Le et al., 2008).

8.7 Buffer Overflows

In programming and information security, buffer overflow is overloading a buffer within the memory of a system with more data than it is designed to handle. It is a software coding error that can be exploited by hackers to gain unauthorized access to corporate systems (Gerg, 2005). It occurs when data written to a buffer corrupts data values in memory addresses adjacent to the destination buffer due to insufficient bounds checking (Gupta, 2012). It also takes place when an attacker manipulates the coding error to carry out malicious actions and compromise the affected system (Lhee & Chapin, 2003). This can cause the system to crash or allow a hacker to execute arbitrary code. Various buffer overflow techniques have been discovered and numerous incidents of buffer overflow attacks have been happened. The techniques to exploit buffer overflow vulnerability vary by architecture, operating system, and memory region (Cowan et al., 1998). There are five main types of buffer overflows as,

i) Stack-based overflows: These are the most common and involve overloading the stack. These occur when an attacker sends data containing malicious code to an application, which store the data in a stack buffer (ALHusayn & Alsuwat, 2020).

ii) Heap-based overflows: These are more difficult to carry out than the stack-based approach. These target the heap, and attack flooding a program's memory space beyond the memory it uses for current runtime operations (Cowan et al., 2000).

iii) Format string attack: It takes place when an application processes input data as a command or does not validate input data effectively. It enables the attacker to execute code, read data in the stack, or cause segmentation faults in the application (Akritidis et al., 2005).

iv) Integer buffer overflow: It is the mathematical process of an integer overflow leads to an integer which is bigger for the integer that can hold. It is divided into three categories based on undersigned structural, symbolic and truncation issues underflow and overflow (Ren et al., 2019).

v) Unicode buffer overflow: It appears by adding Unicode characters into an entry expecting ASCII characters. When ASCII code just includes Western language characters, Unicode can initial a character for all languages (Shahab et al., 2020).

8.8 Privilege Escalation

Privilege escalation is a hacker gaining higher levels of access to a system than originally intended, often with the goal of gaining full control by exploiting vulnerabilities, misconfigurations, or weak controls (Kuzuno & Yamauchi, 2024). It occurs when the user is able to obtain a higher level of access than an administrator intended, possibly by performing kernel level operations (Yamauchi et al., 2021). There are two main types of privilege escalation: i) vertical privilege escalation, where a hacker starts with a low-level account and exploits a vulnerability to gain a higher-level account, such as an administrator account; and ii) horizontal privilege

escalation, where a hacker uses his existing account level to access resources that should be off-limits (Mehmood et al., 2023).

Vertical privilege escalation occurs when the user is able to obtain a higher level of access than an administrator intended, possibly by performing kernel level operations (Kim & Lee, 2023). Horizontal privilege escalation occurs when an application allows the attacker to gain access to resources which normally would have been protected from an application (Kuzuno & Yamauchi, 2024). It needs no upgrading the privilege of accounts, and often relies on the bugs in the system. The result is that the application performs actions with the same user but different security context (Diogenes, 2019).

9. Steps of Hacking

In information security, hacking refers to exploiting vulnerabilities in a system and compromising its security to gain unauthorized access and control. In ethical hacking the goal of this simulated attack is to uncover the weak points of the organizations and suggest ways to strengthen these (Makwana et al., 2025). It encompasses a range of activities, from simple password guessing to sophisticated attacks exploiting vulnerabilities in networking. There are mainly five phases in hacking and a hacker no need to follow these five steps in a sequential manner.

9.1 Reconnaissance

Reconnaissance is the preparation stage and is also called as Footprinting and information gathering phase, where the hackers try to gather as much information as possible on the targeted computer system and network (Bendjakhdel, 2019). This involved researching the target infrastructure, identifying potential vulnerabilities, and understanding the defenses of the system. The primary objective of it is to understand the target environment, infrastructure, and potential weak points, such as finding out the internet protocol (IP) address range, network, domain name system (DNS) records, etc. of the targets (Sanghvi & Dahiya, 2013).

Usually, the information is collected in three groups: network, host, and people involved. There are two types of Footprinting: i) active which directly interacts with the target to gather information about the target, ii) passive which tries to collect the information about the target without directly accessing the target, such as from social media, public websites, etc. (Shah et al., 2019).

9.2 Scanning

Scanning is the pre-attack stage that is done on the basis of information gathered during the reconnaissance phase to identify Internet Protocol (IP) addresses, open ports, live systems, running services, live hosts, and vulnerable services (Bou-Harb et al., 2014). It begins by inputting the root Uniform Resource Locator (URL), performing authentication if required, and then navigating from page to page to identify other URLs and elements, such as forms. But the system must provide a mechanism to identify already visited links to prevent the process from continuing indefinitely (Odion et al., 2023). It is a structured and deliberate process that aims to find the potential weaknesses in one organization's environment immersed in internet security. It works like a security health check for digital systems (Pandey & Chaudhary, 2022).

It helps ethical hackers to map the network, detect live machines, understand topology, identify weak points, and planning simulated attacks for testing defenses. It tries to increase the organization's defenses, reducing the likelihood of successful cyber-attacks and minimizing the impact of any potential security incidents (Bou-Harb et al., 2014). There are three types of scanning:

i) Port scanning: It involves scanning the target for the information, such as open ports, live systems, and various services running on the host. It is used to scan a network for open ports that can be potential entry points for attackers, such as Nmap (RSI Security, 2023).

ii) Network vulnerability scanning: It discovers open ports and identifies any unfamiliar services that are using them. It checks the target for known vulnerabilities and misconfigurations that can be exploited, for example, Nessus (RiskOptics, 2022).

iii) Web application scanner: It finds the topology of network, routers, firewalls servers if any, and host information and drawing a network diagram with the available information that serves as a valuable piece of information throughout the hacking process, such as SQL injection, cross-site scripting, etc. (Mohaidat & Al-Helali, 2024).

iv) Database scan: It assess the security of database systems by scrutinizing setup, access controls, and stored data for vulnerabilities, such as insecure permissions, injection issues, and unsafe configurations. It offers valuable insights to enhance database security and protect sensitive information (Pandey & Chaudhary, 2022).

v) Source code scan: It is crucial to proactively assess source code for security vulnerabilities to address issues before they become costly to correction that analyzes software applications' source code, detecting security flaws, coding errors, and vulnerabilities. It focuses on discover the potential issues like input validation errors,

improper coding practices, and the use of vulnerable libraries (Grance et al., 2003).

vi) Cloud vulnerability scan: It assesses the security of cloud environments, such as IaaS, PaaS, and SaaS installations, providing recommendations to enhance deployment security. It examines cloud configurations, access restrictions, and services to discover misconfigurations, inadequate security practices, and vulnerabilities specific to cloud platforms (Basan, 2023).

9.3 Gaining Access

Gaining access is the third stage where the attacker gets access to the computer system. He uses malware to enter the point-of-sale (POS) systems and harvests card details (Stallings & Brown, 2018). The techniques used during this stage can vary widely, depending on the specific vulnerability being exploited (Vest & Tubberville, 2019). Once a potential entry point has been identified, the hacker takes attempt to exploit the identified vulnerabilities to gain unauthorized access to the system (Islam et al., 2023).

9.4 Maintaining Access

Maintaining access is the process of sustaining accessibility to the computer system once access has been gained. In this case, malware is installed to continuously capture payment data (Griffiths, 2022). This can be done using Trojans, rootkits, backdoors or other malicious files until he finishes the tasks he planned to accomplish in that target even after system restarts, password changes, or other defensive measures (Martin, 2019). This stage is crucial for a hacker, as it allows him to continue exploiting the system even if his initial entry point is closed (Kaur et al., 2023).

9.5 Cleaning Tracks

Clearing tracks are hiding one's malicious acts to prevent being uncovered. An intelligent hacker always clears all evidence so that in the later point of time and no one will find any traces leading to him (Martin, 2019). This can be done through the deleting the log files that record intrusion events; altering modifying, and corrupting registry values; uninstalling all applications used during exploitation; deleting all folders created during the attack; and removing any trace of the attack (Ahn et al., 2010). If a hacker has successfully gained access to the networking system, exploited vulnerabilities, and exited without detection. For example, in 2019 in the Capital One breach, the hackers tried to hide their AWS activity logs but were eventually tracked through cloud service records (Clancy, 2022).

10. Conclusions

This paper deals with the basic ideas of unethically hacking that is used the skills to harm others. At present hacking is a big problem faced by Governments, companies, and private citizens around the world. Cybercriminal hackers are stealing billions of dollars, and cyber security has endangered worldwide. Hacking is an elite profession within the IT field that requires an extensive and detailed understanding of IT concepts and technologies. The internet allows the hackers to take files, programs, passwords, and other information from users, and sometimes users cannot understand it. To protect a networking system from hacker attacks, an organization needs to know the way of hacker's thinking and methodology, as well as about the tools, which s/he can use.

References

Ahn, G., et al. (2010). Representing and Reasoning about Web Access Control Policies. Proceedings of the 34th Annual IEEE International Computer Software and Applications Conference, COMPSAC 2010, Seoul, Korea, 19-23 July 2010.

Ajero, G. L. (2022). Differentiate Metasploit Framework Attacks from Others. M. Sc. Thesis, Stephen F. Austin State University.

Akritidis, P., et al. (2005). STRIDE: Polymorphic Sled Detection through Instruction Sequence Analysis. Proceedings of the 20th IFIP International Information Security Conference (IFIP/SEC 2005). IFIP International Information Security Conference.

ALHusayn, S. M. S., & Alsuwat, E. (2020). The Buffer Overflow Attack and How to Solve Buffer Overflow in Recent Research. *Academic Journal of Research and Scientific Publishing*, *2*(19), 1-13.

Arghire, I. (2019). Business Users Targeted by HawkEye Keylogger Malware. *Security Week*, 28 May 2019.

Ashok, I. (2017). Hackers using NSA malware DoublePulsar to infect Windows PCs with Monero mining Trojan. *International Business Times UK*.

Ashwini, S. K., & Thippeswamy, K. (2018). A Brief Information of Ethical Hacking. 3rd National Conference on Image Processing, Computing, Communication, Networking and Data Analytics.

Aslam, M., et al. (2004). Antihook Shield against the Software Keyloggers. In Proceedings of the National

Conference of Emerging Technologies.

Awati, R. (2025). What is the Nessus Vulnerability Scanning Platform? TechTarget and Search Networking.

Baglione, L. (2012). *Writing a Research Paper in Political Science*. Thousand Oaks, California: CQ Press.

Bahadursingh, R. (2020). A Distributed Algorithm for Brute Force Password Cracking on n Processors. doi:10.5281/zenodo.3612276

Banda, R., et al. (2019). Technological Paradox of Hackers Begetting Hackers: A Case of Ethical and Unethical Hackers and their Subtle Tools. *Zambia ICT Journal*, *3*(1), 40-51.

Basan, M. (2023). 12 Types of Vulnerability Scans & When to Run Each. eSecurityPlanet.

Begum, S., et al. (2016). A Comprehensive Study on Ethical Hacking. *International Journal of Engineering Sciences & Research Technology*, *5*(8), 214-219.

Bendjakhdel, S. E. (2019). Reconnaissance Study: Concept and Design. *El-Khaldounia Journal of Human and Social Sciences*, *11*(1), 10-17.

Berninger, V. W. (2012). *Past, Present, and Future Contributions of Cognitive Writing Research to Cognitive Psychology*. New York/Sussex: Taylor & Francis.

Bhardwaj, A., et al. (2016). *Three Tier Network Architecture to Mitigate DDOS Attacks on Hybrid Cloud Environments*. ACM Computing surveys.

Bhardwaj, M., & Singh, G. P. (2011). Types of Hacking Attack and their Counter Measure. *International Journal of Educational Planning & Administration*, *1*(1), 43-53.

Bhattacharyya, D. K., & Kalita, J. K. (2016). *DDoS Attacks: Evolution, Detection, Prevention, Reaction, and Tolerance*. Boca Raton, FL: CRC Press.

Bou-Harb, E., et al. (2014). Cyber Scanning: A Comprehensive Survey. *IEEE Communications Surveys & Tutorials*, *16*(3), 1496-1519.

Burr, W. E., et al. (2006). Electronic Authentication Guideline. Gaithersburg, MD: National Institute of Standards and Technology.

Caldwell, T. (2011). Ethical Hackers: Putting on the White Hat. *Network Security*, *2011*(7), 10-13.

Cekerevac, Z., et al. (2018). Hacking, Protection and the Consequences of Hacking. *Communications*, *20*(2), 68-72.

Cheok, R. (2014). *Wireshark: A Guide to Color My Packets*. SANS Institute.

Chirillo, J. (2002). *Hack Attacks Revealed: A Complete Reference with Custom Security Hacking Toolkit*. John Wiley & Sons.

Chng, S., et al. (2022). Hacker Types, Motivations and Strategies: A Comprehensive Framework. *Computers in Human Behavior Reports*, *5*(2022), 100167.

Clancy, R. (2022). What is Broken Access Control Vulnerability? EC-Council.

Cornwall, H. (1986). *Hacker's Handbook*. Publisher: E Arthur Brown.

Cowan, C., et al. (1998). StackGuard: Automatic Adaptive Detection and Prevention of Buffer-Overflow Attacks. Proceedings of the 7th USENIX Security Symposium USENIX: San Antonio, TX, January 1998, pp. 63-77.

Cowan, C., et al. (2000). Buffer Overflows: Attacks and Defenses for the Vulnerability of the Decade. Proceedings DARPA Information Survivability Conference and Exposition Hilton Head, SC, January 2000; 119-129.

Creswell, J. W. (2013). *Review of the Literature*. *Research Design. Qualitative, Quantitative, and Mixed Method Approaches* (4th Ed.). Thousand Oaks, California: SAGE Publications.

Cyware News. (2020). *Top 10 Countries with Most Hackers in the World*. Cyware Social.

Dhanjani, N., & Clarke, J. (2005). *Network Security Tools: Writing, Hacking and Modifying Security Tools*. Publisher: O'Reilly Media, Inc.

Diogenes, Y. (2019). *Cybersecurity: Attack and Defense Strategies.* Erdal Ozkaya, Safari Books Online (2nd Ed.), Packt.

Dzaferovic, E., et al. (2020). DoS and DDoS vulnerability of IoT: A review. *Journal of Sustainable Engineering and Innovation*, *1*(1), 43-48.

Eckersley, P., & Portnoy, E. (2017). Intel's Management Engine is a Security Hazard, and Users Need a Way to

Disable It. Electronic Forum Foundation.

Elhai, J. D., & Hall, B. J. (2016). Anxiety about Internet Hacking: Results from a Community Sample. *Computers in Human Behavior*, 54, 180-185.

Elleithy, K., et al. (2005). Denial of Service Attack Techniques: Analysis, Implementation and Comparison. *Journal of Systemics, Cybernetics and Informatics*, *3*(1), 66-71.

Foster, J. C., & Liu, V. (2006). *Writing Security Tools and Exploits*. Syngress Publishing, Inc., Canada.

Foster, J. C., & Price, M. (2005). *Sockets, Shellcode, Porting, and Coding: Reverse Engineering Exploits and Tool Coding for Security Professionals*. Syngress Publishing, Elsevier.

Fuchs, C. (2014). Anonymous: Hacktivism and Contemporary Politics. In: Idem (Ed.), *Social Media, Politics and the State*, pp. 88-106. New York: Routledge.

Fulp, E., et al. (2001). Preventing Denial of Service Attacks on Quality of Service. DARPA Information Survivability Conference and Exposition (DISCEX II'01), II(2), June 2001, pp. 159-172.

Gada, P. D. (2024). The Art of Hacking. *Journal of Emerging Trends and Novel Research*, *2*(12), a73-a84.

Galvan, J. L. (2015). *Writing Literature Reviews: A Guide for Students of the Social and Behavioral Sciences* (6th Ed.). Pyrczak Publishing.

Gerg, I. (2005). An Overview and Example of the Buffer-Overflow Exploit. IAnewsletter. *Information Assurance Technology Analysis Center*, *7*(4), 1-23.

Grance, T., et al. (2003). Guide to Selecting Information Technology Security Products. National Institute of Standards and Technology, NIST Special Publication 800-36.

Greenberg, A. (2022). Kevin Mitnick, Once the World's Most Wanted Hacker, is Now Selling Zero-Day Exploits. Wired.

Gregg, M. (2006). *Certified Ethical Hacker (CEH) Version 9 Cert Guide*. Pearson Publishing. Pearson Education, Inc.

Gresty, D. W., et al. (2001). Requirements for a General Framework for Response to Distributed Denial-ofService. 17th Annual Computer Security Applications Conference (ACSAC'01), December 2001, pp. 422.

Griffiths, C. (2022). The Latest 2022 Cyber Crime Statistics. AAG IT.

Groh, A. (2018). *Research Methods in Indigenous Contexts*. New York: Springer.

Grover, V. K. (2015). Research Approach: An Overview. *Golden Research Thoughts*, *4*(8), 1-7.

Groza, B. (2009). Analysis of a Password Strengthening Technique and Its Practical Use. Third International Conference on Emerging Security Information, Systems and Technologies, Athens, Glyfada, 2009.

Gupta, S. (2012). Buffer Overflow Attack. *IOSR Journal of Computer Engineering*, *1*(2012), 10-23.

Haines, J., et al. (2003). Validation of Sensor Alert Correlators. *IEEE Security & Privacy*, *99*(1), 46-56.

Hanusch, Y. F. (2021). Financial Institutions Should Decline Hackers' Requests for Voluntary Compensation. *South African Journal of Philosophy*, *40*(2), 162-170.

Harris, S., et al. (2004). *Gray Hat Hacking: The Ethical Hacker's Handbook*. McGraw-Hill Osborne Media.

Hellman, M. E. (1980). A Cryptanalytic Time-Memory Trade-Off. *IEEE Transactions on Information Theory*, *26*(4), 401-406.

Hoffman, C. (2013). Hacker Hat Colors Explained: Black Hats, White Hats, and Gray Hats. How-To Geek.

Islam, M. S., et al. (2023). *'Cyber Security'- A Concern for Improving Public Service Delivery: Challenges and Way Forward*. Cabinet Division, Government of the People's Republic of Bangladesh.

Jain, A., & Singh, A. K. (2012). Distributed Denial of Service (DDoS) Attacks: Classification and Implications. *Journal of Information and Operations Management*, *3*(1), 136-140.

Jain, V. (2022). *Wireshark Fundamentals: A Network Engineer's Handbook to Analyzing Network Traffic*. Springer Science and Business Media, New York.

Jansson, K., & von Solms, R. (2011). Phishing for Phishing Awareness. *Behaviour & Information Technology*, *32*(6), 584-593.

Javaheri, D., et al. (2018). Detection and Elimination of Spyware and Ransomware by Intercepting Kernel-level System Routines. *IEEE Access*, 6, 78321-78332.

John, S. (2017). *Scientific Method*. New York, NY: Routledge.

Joshi, S. (2021). What is Nmap and Why You Should Use It? The Hack Report.

Kakarla, T., et al. (2018). A Real-world Password Cracking Demonstration Using Open Source Tools for Instructional Use. *IEEE International Conference on Electro/Information Technology (EIT)*.

Kara, H. (2012). *Research and Evaluation for Busy Practitioners: A Time-Saving Guide*. Bristol: The Policy Press.

Kartalopoulos, S. V. (2008). Differentiating Data Security and Network Security. International Conference on *Communications*, ICC'08, IEEE, pp.1469-1473, 19-23 May 2008.

Kaur, P., et al. (2023). Access Control Application Prevention and Mitigation of Cyber Attacks. *International Journal of Research and Innovation in Applied Science*, *8*(10), 91-105.

Kennedy, D., et al. (2011). *Metasploit: The Penetration Tester's Guide*. San Francisco: No Starch Press.

Kim, Y. M., & Lee, B. (2023). Extending a Hand to Attackers: Browser Privilege Escalation Attacks via Extensions. Proceedings of the 32nd USENIX Conference on Security Symposium, Article No.: 395, pp.7055-7071.

Kirk, J. (2008). Tampered Credit Card Terminals. IDG News Service.

Krieg, C., et al. (2013). Hardware Malware. *Synthesis Lectures on Information Security Privacy and Trust*, *4*(2), 1-115.

Kumar, S., & Agarwal, D. (2018). Hacking Attacks, Methods, Techniques and Their Protection Measures. *International Journal of Advance Research in Computer Science and Management*, *4*(4), 2353-2358.

Kuncoro, P., & Kusuma, B. (2018). Keyloggers is a Hacking Technique That Allows Threatening Information on Mobile Banking User. Third IEEE International Conference on Information Technology, Information System and Electrical Engineering (ICITISEE), Yogyakarta, Indonesia.

Kuzuno, H., & Yamauchi, T. (2024). Mitigation of Privilege Escalation Attack Using Kernel Data Relocation Mechanism. *International Journal of Information Security*, *23*(5), 3351-3367.

Lamping, U. (2004). *Wireshark User's Guide*. For Wireshark 2.1.

Le, D., et al. (2008). Detecting Kernel Level Keyloggers through Dynamic Taint Analysis. College of William & Mary, Department of Computer Science, Williamsburg, VA, Tech.

LeMay, R. (2005). Nessus Security Tool Closes Its Source. CNET.

Levy, S. (1984). *Hackers: Heroes of the Computer Revolution*. Anchor Press/Doubleday Garden City, NY.

Leyden, J. (2000). Mafia Trial to Test FBI Spying Tactics: Keystroke Logging Used to Spy on Mob Suspect Using PGP. The Register.

Lhee, K.-S., & Chapin, S. J. (2003). Buffer Overflow and Format String Overflow Vulnerabilities. *Software: Practice and Experience*, *33*(5), 423-460.

Li, Y., et al. (2021). Backdoor Attack in the Physical World. arXiv:2104.02361v2 [cs.CR] 24 Apr 2021.

Li, Y., et al. (2022). Backdoor Learning: A Survey. arXiv:2007.08745v5 [cs.CR] 16 Feb 2022.

Lin, T., et al. (2019). Susceptibility to Spear-Phishing Emails: Effects of Internet User Demographics and Email Content. *ACM Transactions on Computer-Human Interaction*, *26*(5), 32.

Lohachab, A., & Karambir, B. (2018). Critical Analysis of DDoS: An Emerging Threat over IoT Networks. *Journal of Communication and Information Networks*, *3*(3), 57-78.

Lundin, L. (2013). *PINs and Passwords, Part 2*. SleuthSayers.org. Orlando.

Lyon, G. F. (2008). *Nmap Network Scanning: The Official Nmap Project Guide to Network Discovery and Security Scanning*. Insecure.Com LLC (US), California.

Makwana, D., et al. (2025). Ethical Hacking and Hacking Attacks. *Journal of Neonatal Surgery*, *14*(28s), 940-945.

Mamber, U. (1996). A Simple Scheme to Make Passwords Based on One-Way Functions Much Harder to Crack. *Computers & Security*, *15*(2), 171-176.

Martin, J. A. (2019). What is Access Control? A Key Component of Data Security. CSO Online.

McNab, C. (2011). Network Security Assessment: Know Your Network. O'Reilly Media, Inc.

Medeiros, J., et al. (2009). A Data Mining Based Analysis of Nmap Operating System Fingerprint Database.

Computational Intelligence in Security for Information Systems. *Advances in Intelligent and Soft Computing*, 63, 1-8.

Medhora, N., & Finkle, J. (2016). Cybersecurity Software Maker Tenable CEO Steps Down. Reuters.

Mehmood, M., et al. (2023). Privilege Escalation Attack Detection and Mitigation in Cloud Using Machine Learning. *IEEE Access*, 11, 46561-46576.

Memon, I., et al. (2020). The World of Hacking: A Survey. *University of Sindh Journal of Information and Communication Technology*, *4*(1), 31-37.

Miller, C. (2009). *The Mac Hacker's Handbook*. Dai Zovi, Dino. Indianapolis, IN: Wiley.

Mohaidat, A. I., & Al-Helali, A. (2024). Web Vulnerability Scanning Tools: A Comprehensive Overview, Selection Guidance, and Cyber Security Recommendations. *International Journal of Research Studies in Computer Science and Engineering*, *10*(1), 8-15.

Mohajan, H. K. (2017). Two Criteria for Good Measurements in Research: Validity and Reliability. *Annals of Spiru Haret University Economic Series*, *17*(3), 58-82.

Mohajan, H. K. (2018a). Aspects of Mathematical Economics, Social Choice and Game Theory. PhD Dissertation. University of Chittagong, Chittagong, Bangladesh.

Mohajan, H. K. (2018b). Qualitative Research Methodology in Social Sciences and Theoretical Economics. *Journal of Economic Development, Environment and People*, *7*(1), 23-48.

Mohajan, H. K. (2020). Quantitative Research: A Successful Investigation in Natural and Social Sciences. *Journal of Economic Development, Environment and People*, *9*(4), 50-79.

Mohajan, H. K. (2025a). Artificial Intelligence: Prospects and Challenges in Future Progression. *Art and Society*, *4*(7), 38-50.

Mohajan, H. K. (2025b). Machine Learning: A Brief Review for the Beginners. Unpublished Manuscript.

Mohajan, H. K. (2025c). Deep Learning: A Brief Study on Its Architectures and Applications. *Art and Society*, *4*(8), 41-49.

Mohajan, H. K. (2025d). Cybercrime: A Potential Threat to Global Community. Unpublished Manuscript.

Mohajan, H. K. (2025e). Vulnerability of Cyber Security is An Unexpected Threat to Global Internet System. Unpublished Manuscript.

Mohajan, H. K. (2025f). Addiction and Consumption of Cyber Pornography have Increased Risk Factors and Harmful Effects among Emerging Adults. Unpublished Manuscript.

Mohajan, H. K. (2025g). Cyber Child Pornography: An Unexpected Global Heinous Crime against Children. Unpublished Manuscript.

Moore, R. (2005). *Cybercrime: Investigating High Technology Computer Crime*. Matthew Bender & Company.

Muñoz, F. R., et al. (2018). Analyzing the Traffic of Penetration Testing Tools with an IDS. *Journal of Supercomputing*, *74*(11), 6454-646.

Nagarani, C. (2015). Ethical Hacking and Its Value to Security. *Global Journal for Research Analysis*, *4*(10), 163-164.

Nagesh, H. R, & Sekaran, K. C. (2007). Proactive Solutions for Mitigating Denial-of-Service Attacks. *International Journal of Computer Science and Network Security*, *7*(7), 167-175.

Narayanan, A., & Shmatikov, V. (2005). Fast Dictionary Attacks on Passwords Using Time-Space Tradeoff, CCS'05, November 7-11, 2005, Alexandria, Virginia.

Nyang, D., et al. (2014). Keylogging-Resistant Visual Authentication Protocols. *IEEE Transactions on Mobile Computing*, *13*(11), 2566-2579.

Oakley, J. G. (2019). Why Human Hackers? In *Professional Red Teaming*, pp. 15-28, Springer.

Odion, T. O., et al. (2023). VulScan: A Web-Based Vulnerability Multi-Scanner for Web Application. 2023 International Conference on Science, Engineering and Business for Sustainable Development Goals. IEEE Xplore.

Oechslin, P. (2003). Making a Faster Cryptanalytic Time-Memory Trade-Off. Proceedings of Advances in Cryptology (CRYPTO 2003), Lecture Notes in Computer Science, 2729, 617-630, Springer.

Orebaugh, A., et al. (2007). *Wireshark & Ethereal Network Protocol Analyzer Toolkit*. Syngress.

Pal, S. (2016). Overview of Hacking. *IOSR Journal of Computer Engineering*, *18*(4), 90-92.

Pandey, S., & Chaudhary, A. (2022). Vulnerability Scanning. TechRxiv.

Prakash, A., et al. (2016). Detection and Mitigation of Denial of Service Attacks Using Stratified Architecture. *Procedia Computer Science*, *87*(2016), 275-280.

Prince, M. (2016). Empty DDoS Threats: Meet the Armada Collective. CloudFlare.

Rahalkar, S., & Jaswal, N. A. (2017). *Metasploit Revealed: Secrets of the Expert Pentester*. Packt Publishing Ltd., Mumbai.

Ramzan, Z. (2010). Phishing Attacks and Countermeasures. In Stamp, Mark; Stavroulakis, Peter (Eds.). *Handbook of Information and Communication Security*. Springer.

Regalado, D., et al. (2015). *Grey Hat Hacking: The Ethical Hacker's Handbook* (4th Ed.). New York: McGraw-Hill Education.

Ren, J., et al. (2019). A Buffer Overflow Prediction Approach Based on Software Metrics and Machine Learning. *Security and Communication Networks*, *2019*(1), Article ID: 8391425.

RiskOptics. (2022). Vulnerability Scanners: Passive Scanning vs. Active Scanning. https://reciprocity.com/blog/vulnerability-scanners-passive-scanning-vs-active-scanning

RSI Security. (2023). 7 Types of Vulnerability Scanners. RSI Cybersecurity Blog.

Sanders, C. (2007). *Practical Packet Analysis: Using Wireshark to Solve Real-World Network Problems*. No Starch Press.

Sanghvi, P. H., & Dahiya, S. M. (2013). Cyber Reconnaissance: An Alarm before Cyber Attack. *International Journal of Computer Applications*, *63*(6), 36-38.

Shah, M., et al. (2019). Penetration Testing Active Reconnaissance Phase: Optimized Port Scanning with Nmap Tool. 2nd International Conference on Computing, Mathematics and Engineering Technologies (ICoMET), 1-6. IEEE.

Shahab, A., et al. (2020). An Automated Approach to Fix Buffer Overflows. *International Journal of Electrical and Computer Engineering*, *10*(4), 3777-3787.

Shanmugapriya, R. (2013). A Study of Network Security Using Penetration Testing. International Conference on Information Communication and Embedded Systems, pp. 371-374, IEEE, 2013.

Sheikh, A. (2021). Introduction to Ethical Hacking. Certified Ethical Hacker (CEH) Preparation Guide. Berkeley, CA: Apress.

Shital, M. M. (2023). *Network and Information Security*. Techknowledge Publication.

Singh, R., & Kumar, S. (2014). Vulnerable Security Aspects of Windows. *International Journal of Engineering Sciences & Research Technology*, *3*(8), 87-92.

Son, J. Y., & Kim, S. S. (2008). Internet Users' Information Privacy-Protective Responses: A Taxonomy and a Nomological Model. *MIS quarterly*, *32*(3), 503-529.

Stallings, W., & Brown, L., (2018). *Computer Security: Principles and Practice* (4th Ed.). United Kingdom: Pearson Education Limited.

Sterling, B. (1992). *The Hacker Crackdown: Law and Disorder on the Electronic Frontier*. Penguin, Bantam Books, New York.

Stone, B. (2008). Global Trail of an Online Crime Ring. *The New York Times*.

Teixeia, D. et al. (2021). *Metasploit Penetration Testing Cookbook*. Packt Publishing.

Tenable (2025). Tenable Nessus 10.7.x User Guide. Tenable Holdings, Inc.

Torraco, R. J. (2016). Writing Integrative Literature Reviews: Using the Past and Present to Explore the Future. *Human Resource Development Review*, *15*(4), 404-428.

Vest, J., & Tubberville, J., (2019). Red Team Development and Operations: A practical Guide. Independently published.

Wajahat, A., et al. (2019). A Novel Approach of Unprivileged Keyloggers Detection. Second IEEE International Conference on Computing, Mathematics and Engineering Technologies (iCoMET), Sukkur, Pakistan, 2019.

Wright, A. (2016). The Big Phish: Cyberattacks against US Healthcare Systems. *Journal of General Internal Medicine*, *31*(10), 1115-1118.

Yaacoub, J.-P. A., et al. (2021). Robotics Cyber Security: Vulnerabilities, Attacks, Countermeasures, and Recommendations. *Springer Nature International Journal of Information Security*, *21*(1), 115-158.

Yamauchi, T., et al. (2021). Additional Kernel Observer: Privilege Escalation Attack Prevention Mechanism Focusing on System Call Privilege Changes. *International Journal of Information Security*, *20*(4), 461-473.

Yan, J., et al. (2004). Password Memorability and Security: Empirical Results. *IEEE Security & Privacy*, *2*(5), 25-31.

Yiannis, C. (2013). Modern Password Cracking: A Hands-on Approach to Creating an Optimised and versatile attack. Surrey, Thesis.

Zuckerman, E, et al. (2011). Distributed Denial of Service Attacks Against Independent Media and Human Rights Sites. The Berkman Center for Internet & Society at Harvard University.