

**CYBER SECURITY ASSESSMENT TECHNIQUES: A CRITICAL
ANALYSIS OF FOOTPRINTING, VULNERABILITY
ASSESSMENT, PORT SCANNING, ENCRYPTION, AND
ETHICAL HACKING METHODOLOGIES**

Table of Contents

Part 1: Footprinting and DNS Enumeration.....	5
1.1 Footprinting in Cyber Security	5
1.1.1 Definition and Importance of Footprinting.....	5
1.1.2 Technical Footprinting Methods	5
1.1.3 Non-Technical Footprinting Methods.....	7
1.1.4 Organisational Measures to Prevent Information Disclosure	7
1.2 DNS Enumeration.....	8
1.2.1 Overview of DNS Enumeration.....	8
1.2.2 DNS Enumeration Techniques	8
1.2.3 DNS Enumeration Tool 1: DNSRecon	8
1.2.4 DNS Enumeration Tool 2: Fierce.....	8
Part 2: Vulnerability Assessment and Exploitation Concepts.....	10
2.1 Common Vulnerabilities and Exposures (CVE)	10
2.1.1 Definition of CVE.....	10
2.1.2 Structure of CVE Identifiers	10
2.1.3 Use of CVE Identifiers in Security Testing	10
2.2 Vulnerability Identification Approaches	11
2.2.1 Manual Vulnerability Identification.....	11
2.2.2 Automated Vulnerability Scanning	12
2.2.3 Advantages and Disadvantages of Both Methods.....	12
2.3 Privilege Escalation Techniques	12
2.3.1 Concept of Privilege Escalation.....	12
2.3.2 Technique 1: Exploiting Misconfigured Permissions	13

2.3.3 Technique 2: Exploiting Unpatched Vulnerabilities	13
2.4 Fuzzing in Security Testing.....	13
2.4.1 Definition of Fuzzing.....	13
2.4.2 Types of Fuzzing.....	14
2.4.3 Application of Fuzzing During Security Assessments.....	14
Part 3: Port Scanning and Cryptography	14
3.1 Port Scanning Methodology	14
3.1.1 Definition and Purpose of Port Scanning.....	14
3.1.2 Port Scanning Process.....	15
3.1.3 Practical Example Using Nmap	15
3.1.4 Open Ports.....	15
3.1.5 Closed Ports	15
3.1.6 Filtered Ports	16
3.2 Encryption for Service Protection.....	16
3.2.1 Importance of Encryption	16
3.2.2 Protecting Services from Unauthorised Access	16
3.2.3 Practical Examples of Encryption Usage.....	17
3.3 Comparison of Modern Encryption Algorithms	17
3.3.1 Advanced Encryption Standard (AES)	17
3.3.2 Rivest-Shamir-Adleman (RSA).....	18
3.3.3 Comparative Analysis of AES and RSA	18
Part 4: Ethical Hacking Process and Ethical Challenges	19
4.1 Ethical Hacking Methodology	19
4.1.1 Reconnaissance and Footprinting	19

4.1.2 Scanning and Enumeration	19
4.1.3 Gaining Access.....	20
4.1.4 Maintaining Access.....	20
4.1.5 Covering Tracks	20
4.1.6 Reporting and Remediation	21
4.2 Ethical Challenges Faced by Ethical Hackers	21
4.2.1 Challenge 1: Handling Sensitive Data and Privacy Concerns	21
4.2.2 Challenge 2: Scope Creep and Responsible Disclosure	21
References	23

Part 1: Footprinting and DNS Enumeration

1.1 Footprinting in Cyber Security

1.1.1 Definition and Importance of Footprinting

Footprinting refers to the collection of data about a target organisation, network, system or individual to later perform a security evaluation or attack. It is believed to be the first step towards ethical hacking and penetration testing since it offers valuable intelligence that assists security professionals in gaining knowledge of the target environment. Footprinting aims to find out data that might expose possible vulnerabilities, security flaws and entry points that can be utilized by attackers.

Footprinting is important as it provides a detailed profile of the target. Data gathered at this stage can consist of domain names, IP addresses, employee data, organisational structure, network infrastructure, technology stacks and publicly available resources. This information is used by ethical hackers to determine the level of security posture of an organisation and the areas that need to be improved.

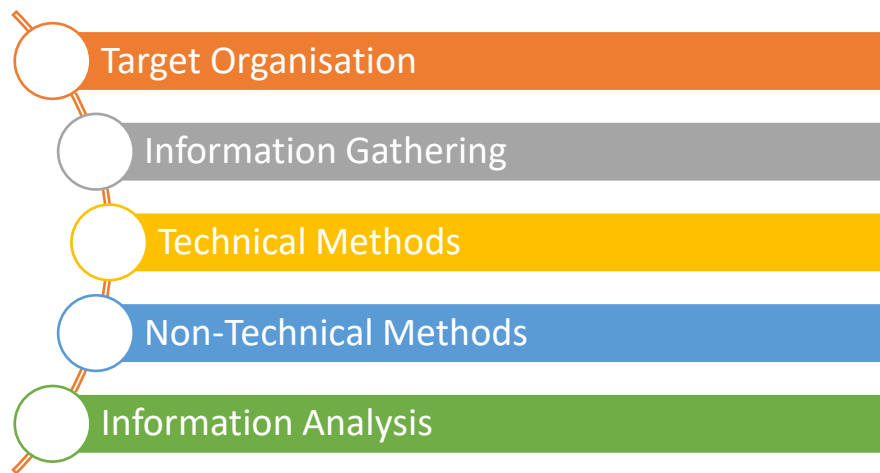


Figure 1: Foot printing Process

(source: Self-created)

1.1.2 Technical Footprinting Methods

Technical footprinting involves using technology tools and methods to collect data on a target system or network. A typical approach is to conduct domain analysis, in which attackers examine

domain registration history to determine ownership data, contact data, and hosting companies (Aishwarya et al., 2026). DNS interrogation is the other technique that gives information on domain names, mail servers, subdomains and network infrastructure.

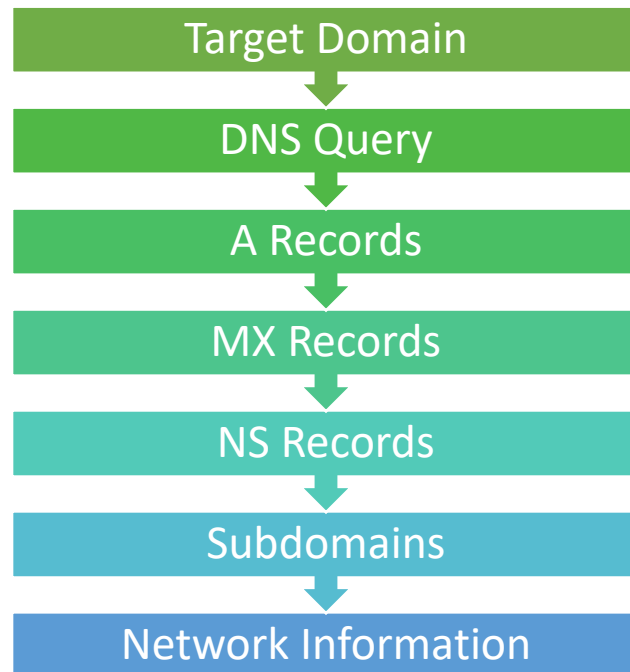


Figure 2: DNS Enumeration Process

(Source: self-created)

Technical footprinting also makes extensive use of network scanning. Nmap is one of the tools used by security professionals to report on the active hosts, open ports, and running services in a network. One can also use search engines to find publicly available information concerning websites, servers and databases (Banoth and Godishala, 2026). Also, attackers can examine source code, metadata and configuration files of websites to determine the versions of software and possible vulnerabilities.

Technical footprinting typically involves the collection of data in open repositories, cloud storage platforms, and databases. These techniques can be useful in understanding the technology environment of an organisation without having access to internal systems.

1.1.3 Non-Technical Footprinting Methods

Non-technical footprinting involves gathering data based on human contact and non-technical data publicly available. One of the most widespread is social engineering, in which attackers will use specific techniques to manipulate people to reveal confidential information. This can be via impersonation, fake emails, or phone calls to obtain confidential information (Bansal et al., 2023).

Another good source of information is social media. Employees always provide information regarding their work environment, organisational activities, technologies, and relations at businesses. This information may guide the attackers to know the organisational structure and possible targets.

Non-technical footprinting also uses public documents, company websites, press releases, annual reports, and job advertisements (Barman et al., 2023). Advertisements, such as job descriptions, can indicate the type of software platforms, security technology, and network infrastructure that an organisation utilises.

1.1.4 Organisational Measures to Prevent Information Disclosure

There are several practices which organisations can employ to make footprinting activities less effective. The training of employees on awareness is necessary since most of the footprinting methods depend on human error and information leakage. Employees are to be informed about social engineering attacks, phishing attacks and information-sharing safety.

The organisations must also come up with stringent regulations on the posting of information on websites and social media. Unless it is necessary, sensitive technical information must not be publicized. Periodic reviews of the publicly available information can be used to detect and eliminate the unnecessary exposure to data.

Information leakage can be further minimized with technical controls, including privacy protection services to domain registration, secure DNS configurations, and access controls (Faki and Egenti, 2024). Patrolling web sites where organisational information is leaked without authorisation also helps in enhancing better security stance.

1.2 DNS Enumeration

1.2.1 Overview of DNS Enumeration

The Domain Name System (DNS) enumeration is the act of collecting data about the Domain Name System (DNS) to determine the hosts, services, and network resources of a target domain. DNS is very important in resolving the domain names into IP addresses and because of this reason, it is a very interesting target of attackers as well as security professionals.

1.2.2 DNS Enumeration Techniques

DNS enumeration is performed using several techniques. A popular way is by making queries to DNS records to get information on a domain. Such records consist of A records, which are domain names to IP address mappings, MX records, which are mail servers, and NS records, which are authoritative name servers (Hartman, 2024).

Another significant test is zone transfer testing. Sometimes, DNS servers permit zone-transfers among authorised systems, to copy DNS data. When misconfigured, an attacker can access the complete DNS database revealing detailed information about the network resources.

1.2.3 DNS Enumeration Tool 1: DNSRecon

DNSRecon is a popular DNS enumeration tool that is used to automate DNS-related information gathering. It also facilitates a wide range of enumeration methods such as typical DNS record queries, reverse lookups, zone transfers, and subdomain brute-forcing.

DNSRecon is especially useful in reconnaissance since it offers an in-depth view of the DNS infrastructure, and less time is wasted on manual investigations. It is also popular among penetration testers and security researchers due to its flexibility and comprehensive functionality (Hasan et al., 2024).

1.2.4 DNS Enumeration Tool 2: Fierce

Another popular DNS reconnaissance tool used is fierce, which is aimed at finding concealed subdomains and locating network resources related to a target domain. It is programmed to do specific DNS enumeration with minimum traffic on the network, which has a low chance of being detected.

Part 2: Vulnerability Assessment and Exploitation Concepts

2.1 Common Vulnerabilities and Exposures (CVE)

2.1.1 Definition of CVE

The Common Vulnerabilities and Exposures (CVE) is an internationally recognised scheme that identifies, lists, and monitors publicly reported vulnerabilities in cybersecurity. The CVE system offers a standardised way of making references to the security weaknesses identified in software, hardware, operating systems and network applications. CVE allows security experts, software vendors, and researchers to talk about security problems in a consistent manner by assigning unique identifiers to vulnerabilities.

2.1.2 Structure of CVE Identifiers

Every CVE record has a unique identifier based on a standard format. A standard CVE identifier is composed of three parts: the CVE prefix, the year of publication and a distinct numerical sequence.

The standardised format enables vulnerabilities to be easily monitored in various databases, security tools, and vendor advisories (Kumar et al., 2024). The CVE identifier of a particular vulnerability can be quickly searched by security professionals to find information regarding the vulnerability.

2.1.3 Use of CVE Identifiers in Security Testing

CVE identifiers are commonly employed by security testers in the process of vulnerability testing and penetration testing. A vulnerability scanner can match the results with pertinent CVE entries when it detects outdated software or misconfigured services. This allows testers to explore the known vulnerabilities to the security and determine their effects on the target environment.

CVE identifiers can also be used to prioritise remediation activities as organisations can tell whether the vulnerabilities they have identified are actively exploited or present significant risks. CVE databases are also used by security teams to keep track of vulnerabilities that are being publicly disclosed and that impact systems deployed into their infrastructure (Kushwah, 2024).

2.2 Vulnerability Identification Approaches

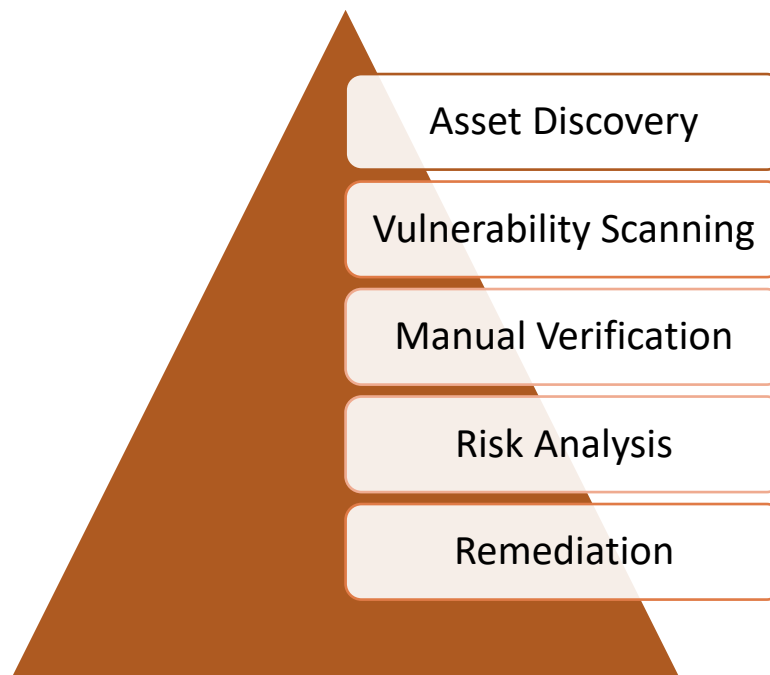


Figure 3: Vulnerability Assessment Workflow

(Source: Self-Created)

2.2.1 Manual Vulnerability Identification

Manual vulnerability discovery is the practice of security professionals manually inspecting systems, applications, and networks. This is done by using human knowledge, critical thinking, and testing methods to identify security vulnerabilities that might be missed by automated tools.

Security testers examine system settings, code, authentication, access policies, and application behaviour to discover vulnerabilities. They can strive to tamper with inputs, probe business logic and examine security controls in different scenarios. Such a strategy allows complex vulnerabilities to be discovered, including paths of privilege escalation, logic bugs, and problems with authentication.

Context-aware analysis is one of the key benefits of manual testing. Having experienced professionals enables them to assess the interaction of vulnerabilities within the target environment and identify realistic attack scenarios. Nonetheless, manual evaluation is time-

consuming, knowledge-intensive, and resource intensive, which is not very efficient when it comes to large-scale settings (Nasir and Pomeroy, 2025).

2.2.2 Automated Vulnerability Scanning

Automated vulnerability scanning involves the use of specialised software to detect familiar security vulnerabilities in systems and networks. Nessus is one of the frequently used vulnerability scanners and it automatically scans hosts, services, operating systems, and applications to find security problems.

Scanners with automation can be used to match configurations found with large databases of vulnerabilities and produce reports about the likely threats. They can detect patches that are missing, configurations that are not secure, software that is out of date, weak encryption protocols, as well as known vulnerabilities that are associated with CVE entries.

2.2.3 Advantages and Disadvantages of Both Methods

Manual vulnerability identification offers more information to the security of the system and allows identifying complicated vulnerabilities that could be overlooked by automated tools. People testers are better than automated systems to test business logic, user interface, and contextual security concerns (Rabnawaz, 2023).

Vulnerability scanning can be done automatically and provides an opportunity to quickly identify known security vulnerabilities and conduct large-scale evaluations. It enhances productivity, minimizes tasks, and facilitates periodic checks of systems.

2.3 Privilege Escalation Techniques

2.3.1 Concept of Privilege Escalation

Privilege escalation happens when an attacker can obtain greater access privileges within a system by compromising a low-privilege account. The goal is to gain administrative or root access, which allows unlimited access to sensitive data, system settings and important resources.

Effective privilege escalation greatly amplifies the effects of a security attack as attackers can overcome security measures, deploy malware, and have continued access into compromised systems.

2.3.2 Technique 1: Exploiting Misconfigured Permissions

A typical privilege escalation technique is to take advantage of poorly configured file, directory, or service privileges. System administrators can also give too much authority to normal users without their intentions, and this will allow attackers to acquire higher privileges.

Likewise, the control systems of access to important configuration files can be insecure, which can provide the attacker with control over the system's behaviour and access to higher privileges. Routine checks of authorizations and compliance with the principle of least privilege are also crucial steps to preventing this kind of attack.

2.3.3 Technique 2: Exploiting Unpatched Vulnerabilities

Attackers often use unpatched software vulnerabilities to attain privilege escalation. Applications and operating systems sometimes have vulnerabilities that enable low-privileged users to execute highly-permissions code.

After a vulnerability is publicly disclosed, attackers can create exploit code that can be used to take advantage of vulnerability. When organisations do not use security updates in a timely manner, attackers are able to use the vulnerabilities to acquire administrative control over the systems (Rawashdeh and Al-Haija, 2025).

Privilege escalation vulnerabilities can be in kernel components, device drivers, authentication mechanisms or privileged services. It is thus important to ensure that an efficient patch management programme is in place to minimise exposures to privilege escalation attacks and safeguard organisational assets.

2.4 Fuzzing in Security Testing

2.4.1 Definition of Fuzzing

Fuzzing is an automated method of software testing where malformed, unexpected, random or invalid inputs are given to applications aiming to detect security vulnerabilities and stability bugs. This is aimed at monitoring software behavior when handling abnormal data and finding out whether it makes errors.

Should an application crash, freeze, or consume memory or behave in any way that is not predictable during testing, the behaviour can be symptomatic of vulnerability. Fuzzing is

popularly employed to discover vulnerabilities that might be exploited by the attackers (Sarker et al., 2023).

2.4.2 Types of Fuzzing

There are various kinds of fuzzing that are common in cybersecurity testing. Black-box fuzzing does not require any knowledge of the internal composition of the application and only concentrates on inputs and outputs. This method emulates the way that a hacker would engage with the system.

White-box fuzzing uses information about the application source code that allows testers to fuzz functions and execution paths. This is a technique that can often cover more and detect vulnerabilities better (Srikanth, 2022).

Grey-box fuzzing is a unification of the two methods by relying on a partial knowledge about the application, but with efficient automated testing. It is widely used in contemporary security tests as it is both effective and practical.

2.4.3 Application of Fuzzing During Security Assessments

Fuzzing is significant in the process of vulnerability discovery that otherwise would not be revealed by conventional testing. Fuzzing is done by security professionals to test web applications, network services, operating systems, communication protocols, and software interfaces.

Part 3: Port Scanning and Cryptography

3.1 Port Scanning Methodology

3.1.1 Definition and Purpose of Port Scanning

Port scanning is a network reconnaissance method that is employed to determine open ports, running services, and available systems in a network. Each network service is communicating because of ports, and by scanning these ports, security experts can ascertain what services are in operation on a victim system. Port scanning is a crucial part of ethical hacking, penetration testing, and vulnerability tests as it assists in determining possible vulnerability points that can be used by attackers.

3.1.2 Port Scanning Process

The port scanning process normally starts with the detection of active hosts in a network. After identifying a target system, the scanner will transmit network packets to different ports and compare the responses to the packets. The answers give out an indication of whether a port is open, closed, or filtered by a firewall or security device (Tariq et al., 2023).

This can be done using several scanning techniques. TCP Connect Scanning completes a full connection with the target port to figure out the status. Half-open scanning (alternatively known as SYN scanning) is a type of scanning that establishes a connection but does not finish, thereby limiting the scan.

3.1.3 Practical Example Using Nmap

Nmap is a popular port scanner in the cybersecurity arena. It allows security experts to discover open ports, running services, operating systems, and network settings. In a standard test, a tester can scan a target host and find out which services can be accessed by the network using Nmap.

Nmap is also able to detect service versions, fingerprinting the operating system and discovery of vulnerabilities. These features render it a crucial tool used in reconnaissance of the network and security testing. Nmap is often used by organisations to confirm firewall rules, detect unauthorised services, and enhance the security of their entire network.

3.1.4 Open Ports

Open ports refer to ports which are actively waiting to accept network connections. In the case of an open port, the application in the port listens to communication requests by external systems. Examples are web servers on port 80 or secure shell services on port 22.

3.1.5 Closed Ports

Closed ports are those ports that are available on the target system but are not currently serving a running service. The target system usually reacts when a scanner is probing a closed port by showing that no service is available (Teotia et al., 2026).

3.1.6 Filtered Ports

Filtered ports are where communication between a scanner and target port is blocked by a firewall, intrusion prevention system, or network security device. When this happens, the scanner will respond with little or no response, and it will be hard to tell what the real state of the port is.

3.2 Encryption for Service Protection

3.2.1 Importance of Encryption

Encryption refers to a security system that encodes decipherable information into an indecipherable form that is only decipherable with the help of the right key. It is very important to safeguard the confidentiality, integrity and privacy of data when transmitting and storing data.

Services detected via a port scan in modern networks can include sensitive data like usernames, passwords, financial statements, and sensitive messages (Wisdom et al., 2024).



Figure 4: Encryption for Service Protection

(Source: sealpath.com, 2026)

3.2.2 Protecting Services from Unauthorised Access

Encryption is used to secure network services by securing communication between the clients and servers. Any type of service transmitting information via the internet typically depends on encryption protocols to avoid eavesdropping and tampering. As an illustration, secure communication protocols involve cryptographic algorithms to create encrypted connections and authenticate the identity of communicating participants.

Encryption prevents the exploitation of intercepted traffic by attackers when they detect services during port scanning (Delgado et al., 2023). Attackers who get access to network communications will not understand any of the data since encrypted data is presented as a ciphertext.

3.2.3 Practical Examples of Encryption Usage

One of the typical encryptions is the secure web communications over the use of HTTPS. In HTTPS, data that is exchanged between web browsers and the server is encrypted preventing sensitive information like the login credentials and payment details.

Secure Shell (SSH) offers secure remote administration services to replace the insecure protocols which send information in plain text. Encryption is also used in Virtual Private Networks (VPNs) to protect communications over the public networks to guarantee confidentiality and integrity.

3.3 Comparison of Modern Encryption Algorithms

Table 1: AES vs RSA Comparison

Feature	AES	RSA
Type	Symmetric	Asymmetric
Speed	Fast	Slower
Key Usage	Same Key	Public/Private Keys
Primary Use	Data Encryption	Key Exchange
Performance	High	Moderate

3.3.1 Advanced Encryption Standard (AES)

Advanced Encryption Standard (AES) is a symmetric encryption algorithm that is commonly applied in the protection of digital information. Symmetric encryption implies that we encrypt and decrypt using the same key. AES has been known to be efficient, fast and highly secure.

AES has key lengths of 128, 192 and 256 bits, with longer keys offering higher resistance to brute-force attacks. The algorithm uses several substitution and permutation operations to

convert plaintext into ciphertext. AES is widely employed in the encryption of files, wireless security, cloud computing, database security, and secure communications because of its high performance.

3.3.2 Rivest-Shamir-Adleman (RSA)

RSA is an asymmetric encryption algorithm, where two different keys are used: the encryption key which is the public key and the decryption key which is the private key. In this way, a safe interaction between the parties is possible without the need to exchange a common secret key (Arsat et al., 2025).

RSA is widely used for secure key exchange, digital signatures, and authentication systems. RSA relies on the mathematical challenge of factoring large prime numbers and is thus secure.

3.3.3 Comparative Analysis of AES and RSA

AES and RSA are applicable in different contexts of modern cybersecurity. AES is a symmetric encryption algorithm that is highly performance based and effective in protecting a vast volume of data. RSA is an asymmetric encryption algorithm that has majorly been used in authentication, digital signatures and secure key exchange.

AES is more appropriate in assuring data confidentiality because it is much faster and does not require a lot of computation. RSA provides secure key management and identity verification at the cost of more processing power.

Part 4: Ethical Hacking Process and Ethical Challenges

4.1 Ethical Hacking Methodology

4.1.1 Reconnaissance and Footprinting

The initial step of the ethical hacking process is known as reconnaissance, also known as footprinting. The main aim is to collect data on target organisation, network, systems as well as employees. By gathering data, ethical hackers can assist in determining areas of vulnerability and attack points without disrupting business.

Data collected at this stage can comprise domain names, IP addresses, contact information on employees, network structure, technology platforms, and available resources (Jinta et al., 2025). There are passive and active reconnaissance. Passive reconnaissance is the gathering of information without direct communication with the target and active reconnaissance is the communication with the systems to obtain more fine-tuned information.



Figure 5: Ethical Hacking Methodology

(Source: sankalppatil12112001.medium.com, 2026)

4.1.2 Scanning and Enumeration

Once preliminary information is collected, ethical hackers move on to the scanning and enumeration stage. This stage aims to discover active systems, open ports, running services, operating systems as well as user accounts in the target environment.

Scanning techniques assist in finding out the available systems and services. Network scanners and vulnerability scanners are some of the tools that are widely used to gather technical data on the hosts and network infrastructure (Tariq et al., 2023). Enumeration goes further to extract detailed data of services that have been identified, such as usernames, shared resources, domain data, and application settings.

4.1.3 Gaining Access

The gaining access stage entails making efforts to compromise the target systems to gain access to the systems based on known vulnerabilities. Authorised testing techniques are employed by ethical hackers to ascertain whether any weaknesses that are found can be exploited by them successfully under controlled conditions.

Software vulnerabilities, poor authentication systems, improperly configured services, and unprotected network configurations are common attack vectors. In this stage, the ethical hackers replicate real-life attack situations to test the performance of the security controls in place.

4.1.4 Maintaining Access

After gaining access, ethical hackers evaluate the possibility of an attacker being able to sustain access to the compromised system. This level measures the capability of the organisation in the detection, prevention and response to long-term unauthorised access.

In the case of real-world cyberattacks, attackers frequently implement persistence mechanisms which enable them to re-access again after system restart or a security update. To test the capabilities of current security measures to detect and eliminate lingering threats, ethical hackers can mimic these tricks within the scope of the approved engagement.

4.1.5 Covering Tracks

Covering tracks are methods employed by attackers to conceal traces of their actions and prevent detection. In the context of a real-life cyberattack, an attacker may destroy logs, modify documentation, or manipulate the data in the system to cover the tracks of their existence within a network.

Ethical hackers test the ability of the current logging, monitoring and auditing systems to detect suspicious behaviour and maintain forensic evidence. Ethical hackers do not literally destroy

logs or disrupt operations but are used to assess the efficiency of security controls to detect such an activity.

4.1.6 Reporting and Remediation

The last and the most significant stage of the ethical hacking is reporting and remediation. Once the assessment is done, ethical hackers record all the findings, such as the vulnerabilities identified, the outcome of exploitation, the level of risks, and the corrective measures.

A detailed report gives the management and other technical teams a clear picture of the security posture of the organisation. The priorities of vulnerabilities are usually based on the possible effect, as well as the probability of exploitation. The recommendations can involve the implementation of security patches, enhancing configuration, improving authentication mechanisms, and training of employees on awareness (Wisdom et al., 2024).

4.2 Ethical Challenges Faced by Ethical Hackers

4.2.1 Challenge 1: Handling Sensitive Data and Privacy Concerns

When dealing with sensitive information during security assessments, one of the greatest ethical issues that ethical hackers must deal with is such. Ethical hackers usually get access to confidential data, such as personal data, financial information, intellectual data, and business communication. Access is authorised, but the task of guarding this information is of paramount importance.

4.2.2 Challenge 2: Scope Creep and Responsible Disclosure

Scopes creep happens when testing activities go out of the systems, applications or networks that are explicitly approved to be assessed. During testing, ethical hackers might discover other systems or vulnerabilities that are out of scope. There is a significant ethical dilemma in deciding how to act in this kind of situation.

Any breach of the limits of testing can result in contravention of the contractual agreements, disruption of the operations, and legal troubles. Ethical hackers are thus required to strictly follow specified parameters of engagement and consult before exploring systems that are not in the original scope.

Another issue of significance in ethical considerations is responsible disclosure. In case of critical vulnerabilities, ethical hackers should make sure that the results are promptly disclosed to the impacted organization (Aishwarya et al., 2026). The level of disclosure must be enough to allow remediation but not too much that could allow unwarranted exposure to predatory use.

References

- Aishwarya, S., Selvamurugan, C., Parthiban, K.G., Athulya, A.K., Sangeetha, G. and Amrutha, V.J., 2026. Ethical Hacking and Penetration Testing in Cyber Security. In *Ethical Hacking and Penetration Testing in Cybersecurity* (pp. 145-186). IGI Global Scientific Publishing.
- Banoth, R. and Godishala, A.K., 2026. Information Gathering and Vulnerability Scanning. In *Cybersecurity Red Teamin: Penetration Testing Strategies* (pp. 75-136). Cham: Springer Nature Switzerland.
- Bansal, D., Bhatia, M., Atrey, A. and Yadav, A.K., 2023. Perspective of cybersecurity and ethical hacking with vulnerability assessment and exploitation tools. In *Big data analytics framework for smart grids* (pp. 98-111). CRC Press.
- Barman, F., Alkaabi, N., Alshedi, M., Ikuesan, R. and Almenhali, H., 2023, June. A methodical framework for conducting reconnaissance and enumeration in the ethical hacking lifecycle. In *European Conference on Cyber Warfare and Security*.
- Faki, A.S. and Egenti, G., 2024. Vulnerability Assessment of Online Market Infrastructure: A Simulated Approach. *Available at SSRN 4980813*.
- Hartman, S., 2024. *Hands-On Ethical Hacking Tactics: Strategies, tools, and techniques for effective cyber defense*. Packt Publishing Ltd.
- Hasan, M., Khan, M.A.R., Hussain, M.I., Al Mamun, M.A., Hossain, M.M., Islam, S.M. and Nurazzaman, K.M., 2024. A comprehensive investigation of reconnaissance threats and its remediation. *International Journal of Advanced Research*, 13(11).
- Kumar, J.R.R., Bhalke, D., Nikam, S., Chobe, S., Khidse, S. and Kale, K., 2024. Original research article evaluation of the extent and demanding roles of ethical hacking in cybersecurity. *J Auton Intell*, 7(1).
- Kushwah, R., 2024. Navigating the Cybersecurity Landscape: Vulnerabilities, Mitigation Strategies and Future Outlooks. *International Journal of Performability Engineering*, 20(11), p.688.
- Nasir, M. and Pomeroy, J., 2025. Ethical Hacking Meets AI: Revolutionizing Vulnerability Assessments and Penetration Testing.

Rabnawaz, M., 2023. *Performance Analysis of Ethical Hacking Tools and Its Approaches* (Master's thesis, Üzküdar University (Turkey)).

Rawashdeh, M. and Al-Haija, Q.A., 2025. Cybersecurity, Forensic Tools, and Risk Mitigation Techniques. In *Cyber Security, Forensics and National Security* (pp. 17-39). CRC Press.

Sarker, K.U., Yunus, F. and Deraman, A., 2023. Penetration taxonomy: A systematic review on the penetration process, framework, standards, tools, and scoring methods. *Sustainability*, 15(13), p.10471.

Srikanth, B., 2022. Ethical Hacking in Network Security: Assessing Vulnerabilities to Improve Defenses.

Tariq, U., Ahmed, I., Bashir, A.K. and Shaukat, K., 2023. A critical cybersecurity analysis and future research directions for the internet of things: a comprehensive review. *sensors*, 23(8), p.4117.

Teotia, S., Sharma, V., Kumar, A., Vashishth, T.K. and Chauhan, P., 2026. Advancing Cybersecurity Through Network Vulnerability Assessment and Exploitation. In *Advanced Cybersecurity for Threats Exploitation and Digital Risk* (pp. 61-86). IGI Global Scientific Publishing.

Wisdom, D.D., Vincent, O.R., Adebayo, A.A., Olusegun, F. and Ayetuoma, I.O., 2024. Security Measures in Computational Modeling and Simulations. *Computational Modeling and Simulation of Advanced Wireless Communication Systems*, pp.112-148.

Delgado, I., Sancristobal, E., Martin, S. and Robles-Gómez, A., 2023. Exploring iot vulnerabilities in a comprehensive remote cybersecurity laboratory. *Sensors*, 23(22), p.9279.

Arsat, N., Daoud, H.I., Zainol, Z. and Kumar, G., 2025, January. The Role and Impact of Ethical Hacking in Modern Society's Economy. In *International Conference on Mathematical Modeling and Computational Science* (pp. 310-326). Cham: Springer Nature Switzerland.

Jinta, K., Sethi, K. and Anand, A., 2025, November. Network Penetration Testing: A Comprehensive Review of Tools, Vulnerabilities, and AI-Driven Solutions. In *2025 IEEE 3rd International Symposium on Sustainable Energy, Signal Processing and Cybersecurity* (pp. 1-6). IEEE.