Introduction to Ethical Hacking

Ethical hacking is the practice of identifying and exploiting vulnerabilities in computer systems and networks with the goal of improving their security. This discipline requires a deep understanding of computer systems, networking, and security concepts, as well as a strong ethical framework. Ethical hackers use the same tools and techniques as malicious hackers, but with the intention of protecting organizations and individuals from cyber threats. This introduction will provide an overview of the ethical hacking process, the legal and ethical considerations involved, and the key skills and techniques required to become a successful ethical hacker.

P by PRAJAPATI MOHIT

Understanding the Ethical Hacking Process

1

Planning and Reconnaissance

The first step in the ethical hacking process is to gather as much information as possible about the target system or network. This includes identifying the network infrastructure, software and hardware used, and any known vulnerabilities or weaknesses.

2

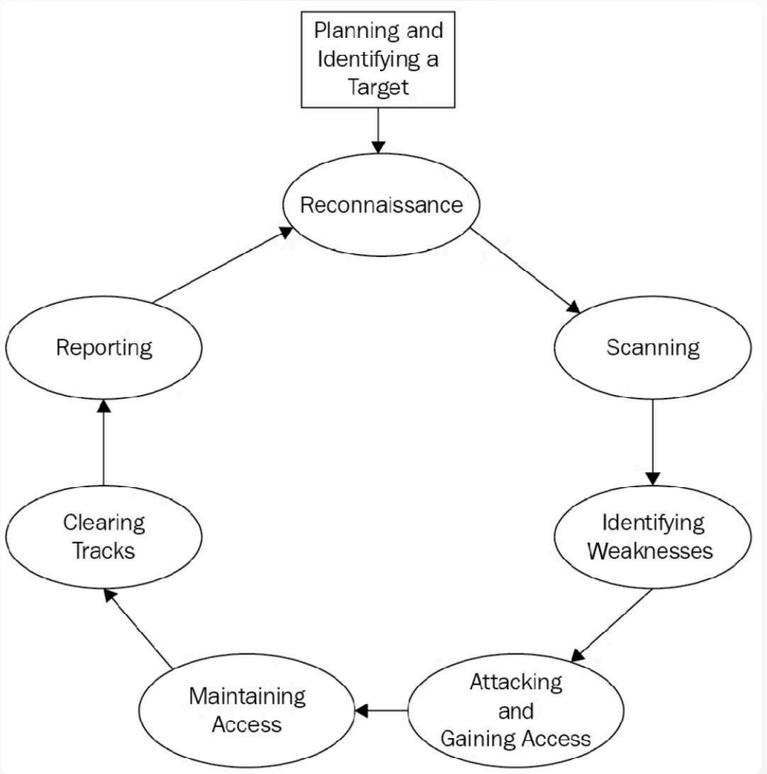
Vulnerability Identification

Once the reconnaissance phase is complete, the ethical hacker will use a variety of tools and techniques to identify vulnerabilities in the target system. This may include network scans, vulnerability assessments, and penetration testing.

3

Exploitation and Analysis

The ethical hacker will then attempt to exploit the identified vulnerabilities, but in a controlled and responsible manner. This allows them to understand the impact of the vulnerabilities and develop effective mitigation strategies.



Legal and Ethical Considerations

Legal Compliance

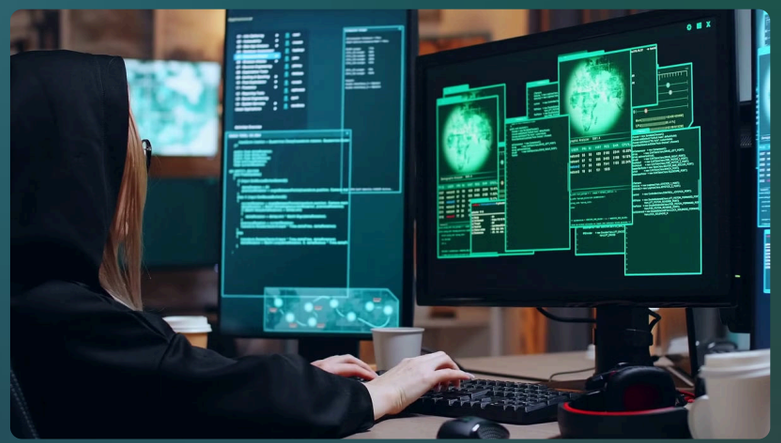
Ethical hacking must be conducted within the bounds of the law. Ethical hackers must obtain permission from the system owners and follow all relevant laws and regulations, such as the Computer Fraud and Abuse Act (CFAA) and the General Data Protection Regulation (GDPR).

Ethical Principles

Ethical hacking also requires adherence to a set of ethical principles, such as respecting privacy, minimizing harm, and acting in the best interests of the client. Ethical hackers must maintain a high level of integrity and professionalism throughout the engagement.

Responsible Disclosure

If vulnerabilities are discovered during the engagement, ethical hackers must follow a responsible disclosure process, informing the system owners and providing guidance on how to remediate the issues, without publicly sharing sensitive information that could be exploited by malicious actors.



Reconnaissance and Information Gathering

1

Open-Source Intelligence (OSINT)

Ethical hackers use a variety of open-source tools and techniques to gather information about the target system, such as searching public databases, social media, and online forums for relevant data.

2

Network Mapping

Ethical hackers will use network scanning tools to identify the target's network infrastructure, including devices, services, and potential entry points.

3

Vulnerability Scanning

Ethical hackers will use vulnerability scanning tools to identify known weaknesses in the target system's software, hardware, and configurations.

4

Social Engineering

Ethical hackers may also use social engineering techniques, such as phishing and impersonation, to gather sensitive information from employees or other stakeholders.

Vulnerability Identification and Analysis

1

Vulnerability Assessment

Ethical hackers will use a variety of tools and techniques to identify and assess the vulnerabilities present in the target system, including network scanners, web application scanners, and vulnerability databases.

2

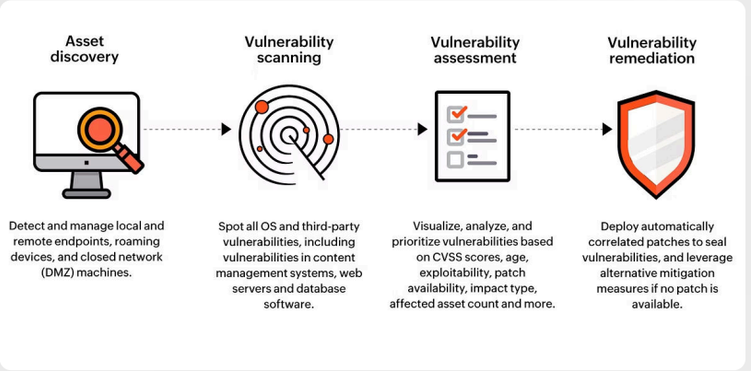
Risk Analysis

Once the vulnerabilities have been identified, ethical hackers will analyze the risks associated with each vulnerability, considering factors such as the likelihood of exploitation, the potential impact, and the ease of remediation.

3

Mitigation Strategies

Based on the risk analysis, ethical hackers will develop and recommend mitigation strategies to the client, including patches, configuration changes, and additional security controls.



Exploitation Techniques

Web Application Attacks

Ethical hackers may use techniques such as SQL injection, cross-site scripting (XSS), and cross-site request forgery (CSRF) to identify and exploit vulnerabilities in web-based applications.

Network Attacks

Ethical hackers may use techniques such as man-in-the-middle attacks, denial-of-service attacks, and wireless network attacks to identify and exploit vulnerabilities in network infrastructure.

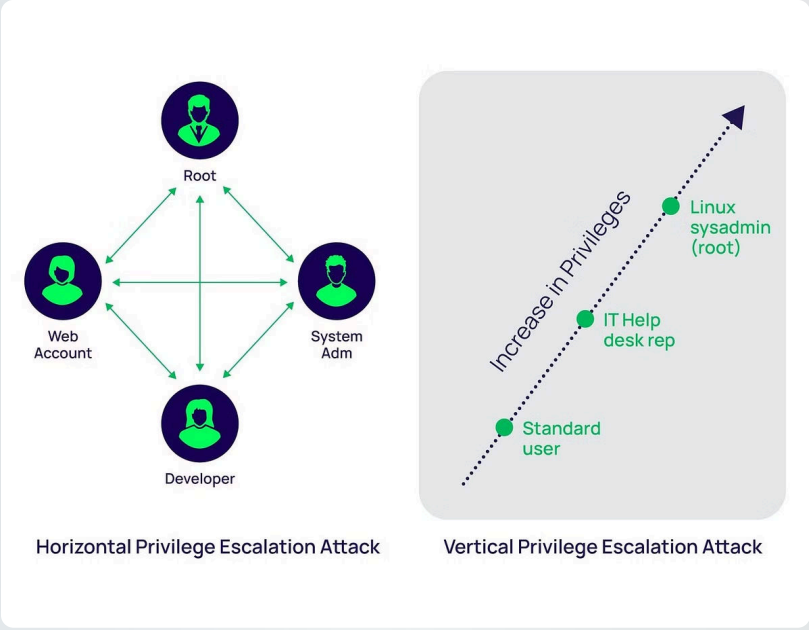
System Attacks

Ethical hackers may use techniques such as buffer overflow, privilege escalation, and malware injection to identify and exploit vulnerabilities in operating systems and software applications.

Social Engineering Attacks

Ethical hackers may use techniques such as phishing, impersonation, and baiting to identify and exploit vulnerabilities in human behavior and organizational policies.

Maintaining Access and Privilege Escalation



1

Backdoor Establishment

Ethical hackers may establish persistent access to the target system by creating backdoors or other mechanisms that allow them to regain access in the future.

2

Privilege Escalation

Ethical hackers may attempt to escalate their privileges within the target system, allowing them to access more sensitive data and resources.

3

Lateral Movement

Ethical hackers may move laterally within the target network, compromising additional systems and gaining a deeper understanding of the overall infrastructure.

Covering Tracks and Maintaining Persistence

Log Manipulation

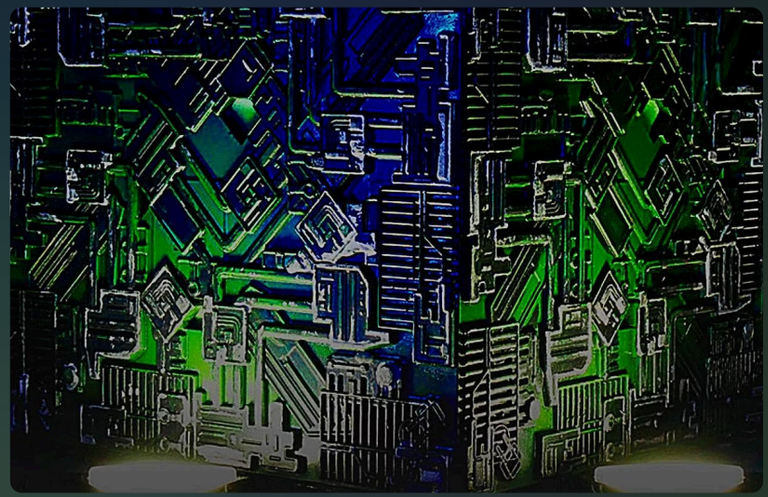
Ethical hackers may modify or delete system logs to cover their tracks and avoid detection by security monitoring systems.

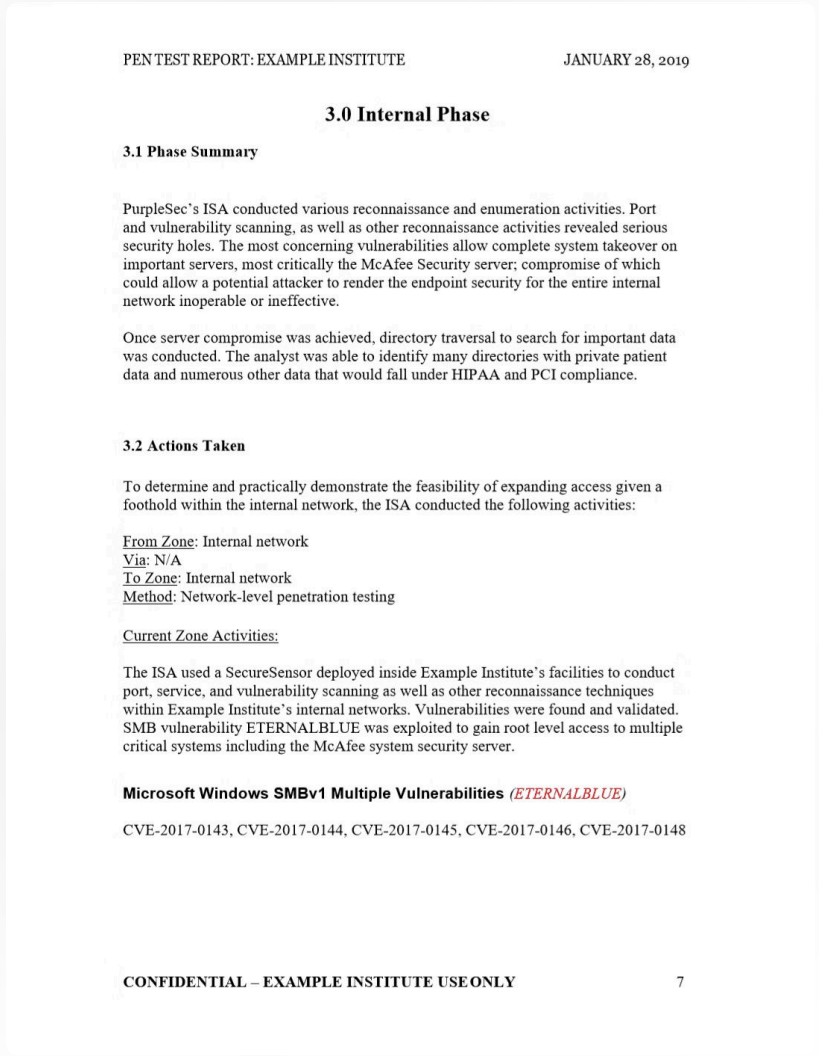
Malware Implantation

Ethical hackers may deploy malware or other persistent mechanisms that allow them to maintain access to the target system even after the initial engagement is complete.

Anti-Forensics Techniques

Ethical hackers may use a variety of anti-forensics techniques, such as data wiping, file obfuscation, and network traffic anonymization, to avoid leaving behind evidence of their activities.





PEN TEST REPORT: EXAMPLE INSTITUTE JANUARY 28, 2019

3.0 Internal Phase

3.1 Phase Summary

PurpleSec's ISA conducted various reconnaissance and enumeration activities. Port and vulnerability scanning, as well as other reconnaissance activities revealed serious security holes. The most concerning vulnerabilities allow complete system takeover on important servers, most critically the McAfee Security server; compromise of which could allow a potential attacker to render the endpoint security for the entire internal network inoperable or ineffective.

Once server compromise was achieved, directory traversal to search for important data was conducted. The analyst was able to identify many directories with private patient data and numerous other data that would fall under HIPAA and PCI compliance.

3.2 Actions Taken

To determine and practically demonstrate the feasibility of expanding access given a foothold within the internal network, the ISA conducted the following activities:

From Zone: Internal network
Via: N/A
To Zone: Internal network
Method: Network-level penetration testing

Current Zone Activities:

The ISA used a SecureSensor deployed inside Example Institute's facilities to conduct port, service, and vulnerability scanning as well as other reconnaissance techniques within Example Institute's internal networks. Vulnerabilities were found and validated. SMB vulnerability ETERNALBLUE was exploited to gain root level access to multiple critical systems including the McAfee system security server.

Microsoft Windows SMBv1 Multiple Vulnerabilities *(ETERNALBLUE)*

CVE-2017-0143, CVE-2017-0144, CVE-2017-0145, CVE-2017-0146, CVE-2017-0148

CONFIDENTIAL – EXAMPLE INSTITUTE USE ONLY 7

Reporting and Remediation Strategies

Vulnerability	Severity	Remediation
Unpatched software vulnerability	High	Apply latest security patches
Weak password policy	Medium	Implement strong password requirements
Misconfigured firewall rules	High	Review and update firewall rules
Lack of network segmentation	High	Implement network segmentation and access controls

Conclusion and Next Steps

Continuous Improvement

Ethical hacking is an ongoing process that requires continuous improvement and adaptation. Ethical hackers must stay up-to-date with the latest threats, vulnerabilities, and mitigation strategies to ensure the long-term effectiveness of their efforts.

Ethical Hacking Careers

Ethical hacking is a rapidly growing field with a high demand for skilled professionals. Individuals interested in pursuing a career in ethical hacking can consider options such as penetration testing, vulnerability assessment, and security consulting.

Ethical Hacking Certifications

There are several industry-recognized certifications, such as the Certified Ethical Hacker (CEH) and the Offensive Security Certified Professional (OSCP), that can help aspiring ethical hackers demonstrate their skills and expertise.