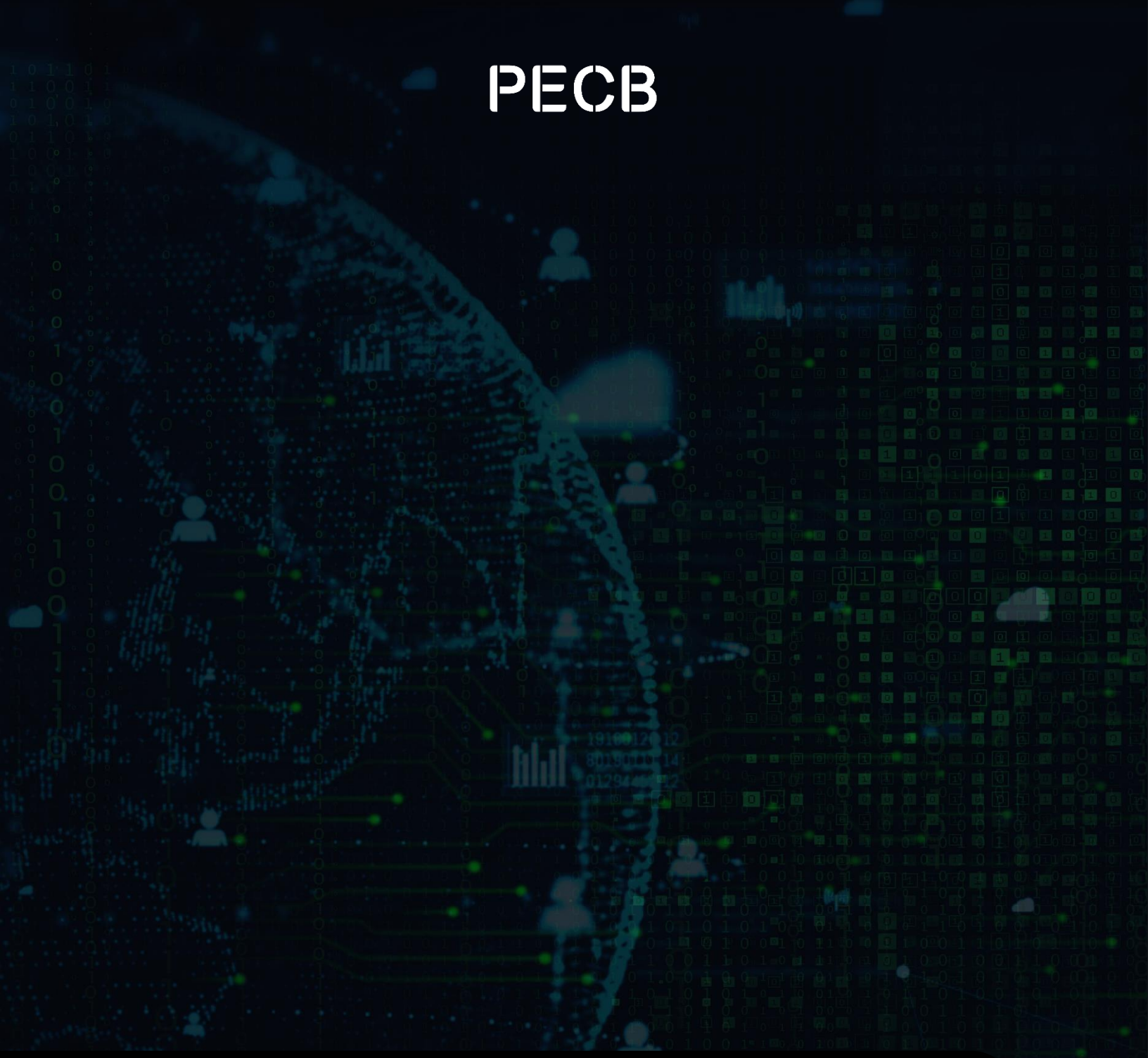
PECB



Ethical Hacking
Whitepaper

www.pecb.com

Table of contents

I. Introduction

Technological and digital progress is constantly evolving and the attack surface is ever-expanding. What used to be the Local Area Network (LAN), now includes mobile devices, wireless networks, and Internet of Things (IoT) devices. Organizations employ methods to secure their systems; however, many of them struggle to keep up with the ever-changing landscape.

With the advent of SMACIT (Social, Mobile, Analytics, Cloud, and Internet of Things), it is critical to note that any system can be digitally invaded if there is any issue or weakness in its architecture, design, implementation, or operation. Cyberattacks are an ever-growing threat that can cause financial and reputational loss, privacy violation, and data breaches. As a result, the need for ethical hacking is on the top agenda for most organizations. Regular conduct of ethical hacking adds value and helps increase the effectiveness of an organization's security practices by reducing the risk of unauthorized information disclosure.

Ethical hacking is the authorized process of simulating a real cyberattack on a client environment to detect and find ways of exploiting potential vulnerabilities. The simulated cyberattacks can either be carried out via a third party organization or by internal staff. It is one of the most efficient ways to find weaknesses and prevent threats from exploiting them. Ethical hacking helps discover system bugs that may not be in the realm of regular expectations.

In conclusion, ethical hacking is evolving to become one of the key pillars for ensuring security, data protection, and a good cybersecurity posture.

II. Ethical Hacking and Penetration Testing

Ethical hacking, also known as penetration testing (pen testing), is performed by cybersecurity experts in a similar way as black hat hacking, but with prior authorization from the client and in compliance with applicable laws and regulations.

Ethical hacking includes information gathering, identification and exploitation of vulnerabilities, and a detailed report of the entire process. The weaknesses detected are documented and communicated to the organization's top management and other stakeholders along with recommendations on how to prevent such vulnerabilities being exploited by attackers.

To ensure the security of their IT environments, organizations nowadays regularly conduct vulnerability assessments. Vulnerability assessment is the process of identifying, evaluating, and mitigating the weaknesses of an information system. It helps the organization to discover security weaknesses but does not provide information on the damage that the exploitation of these weaknesses could cause. Therefore, organizations perform pen testing.

Pen testing can find gaps in systems that may not be detected during regular tests, audits, or risk assessments. Depending on the scope, it can offer an in-depth analysis of the IT infrastructure and existing security measures against various threat actors and scenarios, including social engineering attacks. It also helps ensure confidentiality, integrity, and availability of the information, as well as developing strategies for reducing the impact of an attack. Pen testing and vulnerability assessment are often performed jointly to provide a comprehensive understanding of the security posture of an organization.

A pen test can be external or internal. External pen testing is gaining access to an internal network or system by attacking

remotely. External pen testing exploits external vulnerabilities and finds externally exposed systems. Internal pen testing is the process of simulating an attack from a person that has access to the internal infrastructure of the organization. It is focused on issues such as privilege escalation or inbound attacks. Internal threats typically cause greater damage since the attackers usually have both a good knowledge of the internal network and processes as well as key access privileges.

Pen tests are either announced or unannounced. Announced pen testing is performed by informing the involved parties. Unannounced pen testing is performed without informing the involved parties. The main objective of unannounced testing is to test the incident response process and find out if the system or network administrators notice the intrusion of the hacker.

Ethical hackers have the same skills and mindset and use the same tools of a real hacker; however, they perform attacks in a non-destructive manner.

There are three types of hackers: black hat hacker, gray hat hacker, and white hat hacker. Black hat hackers, also known as cybercriminals, are individuals with malicious intentions that exploit system vulnerabilities and use them to their advantage. Gray hat hackers are individuals who do not have the malicious intents of a black hat hacker; however, they hack systems or networks. They may both fix and exploit system vulnerabilities, usually not for financial gain. White hat hackers, known as ethical hackers, are individuals that conduct pen tests to find vulnerabilities only after the owner’s consent is given.

Similar to the types of hackers, there are three main pen testing strategies: black box, white box, and gray box.

PENETRATION STRATEGIES
Black box, also known as zero-knowledge testing, simulates the actions and procedures of a malicious attacker who has no prior knowledge about the target. Black box testing is further classified into blind testing and double-blind testing.
White box, also known as complete-knowledge testing, simulates the actions and procedures of an attacker who has prior knowledge on the target. It provides a much more cost-effective way to quickly reveal misconfigurations and vulnerabilities, as well as assuring complete testing coverage.
Grey box, also known as partial-knowledge testing, combines the methodologies of both black box and white box testing. It consists of a methodical attack that simulates testing with limited information on the target.

III. Top Cyber Threats

As our technological dependence continually increases, especially during the times of the pandemic, so does the possibility of cyber threats. Many hackers have been able to steal information from less secured organizations, causing them huge financial loss. According to the International Criminal Police Organization (INTERPOL), due to the Covid-19 pandemic, there has been a "significant target shift" from individuals and small businesses to major organizations, governments, and critical infrastructure.

ENISA Threat Landscape 2020 Report states that important changes occurred in the cyber threat landscape in 2019 and 2020, mostly due to the Covid-19 pandemic and working remotely. Another factor that has affected the threat landscape is the advanced adversary tactics used by threat actors. The picture below represents what are the trends of top threats and how they have changed throughout the years.

Top Threats 2019-2020		Assessed Trends	Change in Ranking
1	Malware	—	—
2	Web-based Attacks	—	↗
3	Phishing	↗	↗
4	Web application attacks	—	↙
5	Spam	↙	↗
6	Denial of service	↙	↙
7	Identity theft	↗	↗
8	Data breaches	—	—
9	Insider threat	↗	—
10	Botnets	↙	↙
11	Physical manipulation, damage, theft and loss	—	↙
12	Information leakage	↗	↙
13	Ransomware	↗	↗
14	Cyberespionage	↙	↗
15	Crytojacking	↙	↙

Legend: Trends: ↙ Declining, — Stable, ↗ Increasing **Ranking:** ↗ Going up, — Same, ↙ Going down

Some of the top cyber threats to look out for in 2021 include ransomware attacks, web-based attacks, attacks on cloud services, social engineering, supply chain attacks, DDoS attacks, IoT attacks, and insider attacks.

A. Ransomware

Ransomware attacks have grown to become a major threat over the years. In 2020, the number of ransomware attacks raised highly in almost all industries due to new techniques in the technology landscape. According to Cybersecurity Ventures predictions, a ransomware attack happens globally every 11 seconds in 2021. Usually, ransomware attacks happen in larger organizations. However, small and medium organizations are highly affected by it as well, resulting in the loss of vital information and operations.

A ransomware tactic that has spread in 2021 is “double extortion.” Rather than only encrypting the files and demanding ransom, attackers first exfiltrate the sensitive information of victims. In case the ransom is not paid, they post the information online, exposing it to millions of people.

According to Sophos State of Ransomware 2021 global survey, in terms of countries, Poland and Japan remain the countries with the lowest levels of ransomware attacks. India, on the other hand, remains the country that was hit the most by ransomware attacks. Based on the same report, the average cost of remediating from a ransomware attack in 2021 reached up to 1.85 million dollars, while in 2020 it was $761,106. In addition, the average ransom paid is $170,404.

B. Web-Based Attacks

Web-based attacks use web systems or services to gain access to valuable information. Through malicious scripts or URLs, hackers are able to direct the user to open or download malicious content. Web-based attacks may affect the availability of websites and applications and result in data breach. Some forms of web-based

attacks include SQL injection, cross-site scripting (XSS), directory traversal, and local file inclusion.

An example of a web-based attack is the *LoadPCBanker* malware found in Google Sites. The hacker first created a webpage using Classic Google Site and then used it to host payloads. Through SQL service, the hacker was able to send the compromised users' data to the server. According to Netskope, the company that reported the malware, it has been around since 2014 and was discovered only in 2019.

C. Social Engineering

In 2020, social engineering was the most reported form of cyberattack. This method focuses in human interaction and manipulates users into giving out confidential information.

Phishing, one of the most common social engineering techniques, sends emails camouflaged as being sent from reliable sources in an attempt to trick victims to provide their sensitive information or get unauthorized remote access. If opened, they give access to different types of malware that allows hackers to access data, encrypt data, or hide in your network. Business email compromise (BEC) attacks, also known as email account compromise (EAC), are a common form of phishing. BEC attacks use email fraud to attack organizations or individuals. Other forms of social engineering include baiting, tailgating, and piggybacking.

Social engineering is often the gateway to a ransomware attack.

D. Attacks on Cloud Services

According to McAfee report "Cloud Adoption & Risk Report – Work from Home Edition," since the onset of the Covid-19 pandemic, the demand for cloud services has increased by 50% in all industries.

Thus, there has been an increase in the number of malicious attacks on cloud services.

A recent example is *Blackbaud*, a cloud service provider that was attacked and had their clients' payment information stolen. They had to pay large fines and suffered other legal consequences.

To mitigate cyber threats when using cloud desktop devices, organizations must give attention to their security as they do with physical desktops.

E. Supply Chain Attacks

In 2020, several organizations had their crucial operations completely disrupted from supply chain attacks. Supply chain attacks exploit the vulnerabilities of the suppliers or vendors of an organization in order to have access to the organization's systems. Over the past years, there have been many supply chain attacks including those that target the hardware level or those that modify the software.

A massive supply chain attack known as *Sunburst* happened recently. *Sunburst* is a malware installed in *SolarWinds Orion Platform*, a platform used to manage and monitor networks of large organizations. The attackers modified the source code of *SolarWinds* which allowed them to gain access to other organizations that used the platform. Several public, governmental, and private organizations, including high-tech giants, were infected with this malware without prior knowledge.

F. Distributed Denial-of-Service (DDoS) Attacks

DDoS is a network attack that disrupts the normal operation of servers, systems, or services by flooding them with traffic from multiple sources. Recently, hackers have been using internet-connected smart devices such as surveillance cameras, smart door lock, or smart TV to perform these attacks.

In 2020, a DDoS attack happened to Amazon Web Services (AWS), one of largest cloud computing providers. With a peak traffic volume of 2.3 Tbps, AWS attack was the largest DDoS attack ever recorded. The attack targeted one of AWS's customers using hijacked web servers. AWS reported that the attack lasted for three days but it was mitigated.

Compared to other attacks, the cost of DDoS is lesser. There is an increase in awareness of DDoS services to ensure protection and reduce any potential attack. In addition, there are various solutions available to address possible attack vectors.

G. IoT Attacks

The use of smart devices which are operated through the internet at homes and organizations is continuously increasing, resulting in IoT attacks rising rapidly. A major issue of smart devices is the lack of security measures installed in them. According to the FBI, many smart TVs are vulnerable to these attacks as their manufacturers do not consider the security and privacy risks when producing them. If compromised, these devices allow hackers to watch and listen at your home, using the integrated camera and microphone.

H. Insider Attacks

Insider attacks are performed by people within the organization who use their inside access or privilege for personal gain. Insider

threats are faced by many organizations regardless of their size. Small organizations, however, are at higher risk as employees often have access to more parts of the internal network. Insider attacks may result in devastating losses for organizations. According to Verizon’s 2019 report on data breaches, 57% of database breaches involved insider threats.

IV. Steps for Planning a Penetration Test

The first stage of pen testing is planning. The organization should spend sufficient time in planning the pen test so it achieves tenable results. The following steps can ensure a good preparation for a pen test.

1. Understand the environment
2. Set test objectives
3. Define the test scope
4. Assess the risks
5. Define the methodology
6. Ensure management approval
7. Decide who is going to conduct the tests and when
8. Allocate the resources
9. Inform the IT team
10. Define what the report should include

1. **Understand the environment:** The organization should inform the pen tester about the critical assets of the organization and the asset inventory. They are used to identify the most critical assets, classify the risk severity of those assets against cyberattacks, and determine the systems to be tested. The needs and expectations of the interested parties regarding the pen test should also be analyzed.

2. **Set test objectives:** The organization should define the purpose of pen testing. The test objectives should be defined based on the organization's requirements.
3. **Define the test scope:** The pen test scope outlines the boundaries, rules of engagement, environment, and resources of pen testing. The scope should be clear and include systems, networks, applications, and services that will be tested and any exclusion.
4. **Assess the risks:** It is a good practice that the organization conducts a risk assessment to identify risks related to pen testing. It should focus on mitigating risks that may potentially impact the objective and scope of the test.
5. **Define the methodology:** The organization should define the pen testing methodology based on the test objectives. The most popular pen testing methodologies are NIST, OSSTMM, OWASP, PTES, and ISSAF. The organization should determine whether black, gray, or white box testing will be conducted.
6. **Ensure management approval:** The organization's management should be informed of the purpose, objectives, and scope of the pen test. Conducting pen testing requires approval from the organization's management, preferably senior executive level.
7. **Decide who is going to conduct the tests and when:** The organization should decide whether the pen testing will be conducted by internal staff or a third party. In both cases, pen testing should be undertaken by trained professionals who are aware of the latest hacking tools and techniques. Organizations should also define an appropriate time for the test (e.g., non-office hours).
8. **Allocate the resources:** Based on the outcomes of previous steps, the organization should allocate the resources required for the pen test.
9. **Inform the IT team:** When performing white-box pen testing, the organization should communicate the pen testing plan to all members of the IT Department and ensure their availability for

resolving technical issues that may occur during the testing process. In addition, teams working for the organization's crisis management should also be informed. In the case of black-box penetration testing, also known as double-blind or covert testing, the IT team should not be informed.

10. **Define what the report should include:** During the planning process, the organization should determine the information to be included in the pen testing report. The organization's requirements regarding the report may include mapping the findings to an international security standard and prioritizing the risks in terms of business perspective.

V. Phases of Conducting a Penetration Test

In today's increasingly risky information technology environment, every organization should prioritize addressing IT vulnerabilities and securing it from all forms of threats, including data breaches.

There are six important phases to conduct a pen test.

A. Information Gathering (Reconnaissance)

Reconnaissance, otherwise known as recon, is the first step of pen testing. The more valuable the information one has on a target, the more likely they are to discover weaknesses or vulnerabilities. To start a pen test, it is important to collect as much information as possible.

This can be done by looking for publicly available information about the system and the organization and determining the best way to use it. Information gathering is more than just a single step in the security testing process; it is a skill that every pen tester should master for a better experience.

Reconnaissance is considered to be the most important phase of ethical hacking. Information can be gathered through active reconnaissance and passive reconnaissance. Passive reconnaissance is performed by gathering publicly available information about the target without interacting with the target. Active reconnaissance,

on the other hand, requires the ethical hacker to have some level of interaction with the target.

The information about an organization's network architecture, operating systems, applications, and users can be determined during reconnaissance.

Footprinting is a strategy for gathering as much information about a targeted network, system, or person as possible. It aids pen testers in gaining access to an organization's computer system in a variety of methods. Tools for footprinting include *Whois Lookup*, *NS lookup*, and *IP lookup*. There are different types or branches of footprinting:

- **Open-source footprinting** is the safest type of footprinting because it respects all legal limitations. Examples include finding someone's password, phone number, email address, home address, etc.
- **Network-based footprinting** is used to recover information such as user name, shared data among individuals, network services, and network topology.
- **Domain Name Servers (DNS) interrogation** gathers the needed information and then queries DNS using pre-existing tools. A DNS query is an information request sent from the user's computer to DNS servers.

B. Scanning and Enumeration

Scanning includes techniques and procedures used to identify hosts, ports, and various services within a network. Network scanning is an information-gathering retrieval mechanism used to generate an overview scenario of the target organization. For each type of scan, different tools are used. For example, a network scanning tool cannot be used for scanning the vulnerabilities of a web application. Among others, tools used for scanning and information gathering include *nmap*, *wireshark*, *OWASP ZAP*, and *nslookup*.

Vulnerability scanning is an automated process that checks your systems for known flaws and potential risks.

Enumeration is used to gather information such as usernames, group names, hostnames, IP tables and routing tables, and applications and banners.

Vulnerability scanning and enumeration are generally performed using automated tools which report the existence of vulnerabilities, without taking further action. Therefore, among automated tools, the pen tester should use the human element to analyze vulnerabilities and penetrate to a network or server.

C. Gaining Access

Having identified all possible vulnerabilities and entry points, pen testers use exploitation tactics to gain access to the targets. In this phase, pen testers actively attack the security weaknesses of the system, using numerous attack methods. The identified vulnerabilities are compared based on their CVSS (Common Vulnerability Scoring System) scores. The higher the CVSS score, the easier will be to exploit the vulnerability.

Techniques for gaining access are defined based on the pen testing scope. The main objective of this phase is to understand the level of damage that a hacker can cause. Once initial access is established, pen testers will attempt to escalate their access privileges and pivot or access other parts of the network.

Through privilege escalation, pen testers are able to use captured existing credentials to gain access to other systems, thus avoiding detection. Methods for privilege escalation include credential harvesting and structured passwords.

D. Maintaining Access

Once the access to systems and networks is achieved, pen testers, similar to what black-hat hackers would do, try to maintain that access. In this phase, the system is already breached. The objective now is to remain in the system as long as possible. This phase allows pen testers to acquire adequate time to extract valuable information, pivot to other areas, or further exploit the

environment. This also enables the identification of other hidden vulnerabilities in the system.

E. Cleaning Up

After achieving the objectives of the pen test, the pen tester should clean and destroy any artifacts created during the test. This is done to prevent potential hackers from using the actions or findings of the pen tester. Artifacts that should be removed by the pen tester include, but are not limited to, agents, scripts, backdoors, temporary files, and shell sessions. Cleaning up and destroying artifacts help the pen tester think like a hacker and define actions that potential hackers could take for removing their footprints.

F. Reporting

The findings of the pen test are analyzed and documented in a written report. Pen testers keep track of every action they take during all phases of the test. The main objective of this phase is to provide information on how entry points and security issues were discovered.

The report should include specific vulnerabilities that were exploited, the rating scale of the risk related to the identified vulnerabilities, and detailed explanations on the recommendations for mitigating each of them. It may also discuss possible modus operandi of cyber criminals and how to manage them. In addition, screen captures for exploited vulnerabilities are added in the report as evidence.

VI. Ethical Hacking Tools

Ethical hacking tools are computer programs or scripts that help ethical hackers to find and exploit vulnerabilities. There are many open-source and commercial tools utilized by ethical hackers that simplify their activities through automation.

Nmap

Network Mapper (Nmap) is an open-source tool that is used for network discovery and vulnerability scanning. Through Nmap, ethical hackers gather information on the target and detect open ports on remote hosts. Nmap supports most operating systems, including Linux, Windows, and Mac OS.

Acunetix

Acunetix is an automated tool used for scanning vulnerabilities of web applications. Acunetix detects SQL injection and cross-site scripting (XSS) as well as other vulnerabilities. Acunetix is available as a cloud or on-premise solution.

Metasploit

Metasploit is an open-source framework mainly used for pen tests. It verifies vulnerabilities mitigation and helps in managing security assessments and IDS signature development.

Wireshark

Wireshark is a network protocol analyzer. It captures network packets on the local network and allows ethical hackers to analyze network traffic and detect vulnerabilities. It supports leading operating systems such as Linux and Windows.

John the Ripper

John the Ripper is an open-source password cracking tool. It is used to find passwords based on the dictionary method preferred by real hackers. John the Ripper offers three modes of operation: wordlist, single crack, and incremental mode.

VII. Red Teaming

Nowadays, organizations employ red teaming to assess their security defense. Red teaming is a group of ethical hackers who have been authorized to simulate a potential adversary attack against an organization's security posture. A red team can be a contracted external party or an internal group that employs strategies to encourage an outsider viewpoint. Red teams are primarily concerned with offensive security. They simulate a real attack on cybersecurity defense. Blue teams, on the other hand, are cybersecurity professionals that are concerned with defense security. They design and maintain the internal cybersecurity infrastructure.

For a comprehensive test of the organization, the red team imitates adversaries' tactics, techniques, and procedures (TTPs) and control (C2) framework. TTPs are known actions taken by real malicious actors who actively target organizations and they are used to identify and close gaps in the organization's security posture. Red teams develop payload for the chosen TTPs. They execute the same TTP as many times as the blue team requires to tune their defenses in real time.

Adversary emulation is carried out by an ethical hacking team that has been hired and authorized to simulate and mimic known threats. During adversary emulation, the red team imitates the actions of an attacker, leveraging frameworks such as MITRE ATT & CK to identify TTPs.

While blue teams test and probe defenses, red teams have the tradecraft and skill set to perform malicious actions to circumvent defenses. During the adversary emulation, the team will use cyber threat intelligence (CTI) to identify adversaries who have the intent, opportunity, and capability to attack.

The collaboration of multiple cybersecurity domains of expertise, particularly red team and CTI professionals, is required for successful adversary emulation.

VIII. Ethical Hacking and Legal Implications

Ethical hacking is the approach of legally compromising systems and networks owned by other parties. It is only permissible when the owner has given their permission, which should be given in a written form. It is also a good practice to establish a contractual agreement between both parties before any test is conducted. This is usually mandatory for the testing organization particularly in relation to professional indemnity insurance. In addition, it is recommended to have a single point of contact during testing in case of emergency.

Pen testing can only be conducted within the pre-defined scope. Tests outside the agreed scope without a formal authorization from the organization will most likely breach laws and regulations. In these cases, the organization has the right to take legal action against pen testers that participate in such activities. The same is applicable for pen testers that alter, destroy, or expose confidential information of organizations found during the pen tests.

IX. Training Course and Certification

Cybersecurity professionals should not consider security strategies as a mechanistic approach. As San Tzu, author of the book "Art of War," states "all warfare is based on deception," cybersecurity professionals must consider possible deceptive actions of the cybercriminals. PECB's training course, the Certified Lead Ethical Hacker, is one step toward that direction for gaining insights on ethical hacking.

The Certified Lead Ethical Hacker training course has been recently added under the PECB information security portfolio. The training course is designed to provide all the grounding knowledge and practical skills needed to start a career in ethical hacking. It provides information on how to plan, manage, and conduct pen tests and prepares candidates for the certification exam.

After passing the exam, candidates receive an internationally recognized PECB certificate. The certificate demonstrates that candidates have the required knowledge and skills for the process and are aware of the ethical responsibilities of being an ethical hacker.

More details on this and other training courses and certification may be found on our website: https://pecb.com.

X. Conclusion

One single vulnerability is all an attacker needs. – Window Snyder

Information and information systems nowadays are essential for managing the operations of organizations. This is enough reason to make information one of the most valuable assets of an organization and a top target for hackers. In a world where cybercrime is always on the rise, ethical hacking has a crucial role in securing systems and networks. This way, organizations are one-step ahead in discovering their own weaknesses.

Furthermore, through ethical hacking, cybersecurity professionals can start a career that is currently in high demand. Using their hacker skills in an ethical manner, they help organizations and the overall cyberspace.

Principal Authors

Arta Haxhixhemajli, PECB
Era Mustafa, PECB
Fjolla Muhadri, PECB

Contributors

Argita Canhasi, PECB
Adeniyi Odefunso, DeepHow Corporation (Nigeria)
Aletta Terblanche, The Caridon Group (Australia)
Alex Ryals, Global VP, Security Solutions - TechData (United States)
B M Zahid ul Haque, BRAC Bank Ltd (Bangladesh)
Bledar Mexhiti, PECB
Bolaji Bankole, PwC Nigeria (Nigeria)
Carl Carpenter (United States)
Carlos Flores, CONCEPTA TRAINING - GRUPO CONCEPTA (Perú)
Christodoulos Papadopoulos, geevo® (Cyprus)
Dr Nilakshi Jain, Shah and anchor Kutchhi engineering college (India)
Dr. Peter Adewale Obadare, DIGITAL ENCODE LIMITED (Nigeria)
Egzon Bunjaku, PECB
Enis Shala, PECB
Eric Jhessim, Zenith Bank (Ghana) Ltd (Ghana)
Forster Chiu, IBSL Auditing and Compliance Limited (Hong Kong)
Goodness Okpani, ETHNOS IT SOLUTIONS (Nigeria)
Graeme Parker, Parker Solutions Group (United Kingdom)
Guy Cohen (Israel)
Jan Carroll, Fortify Institute (Ireland)
Kavish Dabee Ramnarain (Mauritius)
Kester Ewere Irabor, CONSILIUM HOUSE CONSULTING (Bahrain)
Pablo Barrera Guzmán, ES Consulting (Guatemala)
Paulo Garcia Miguel, PGM CONSULTORES (Portugal)
Rajib Subba, University of Agder, Norway (Nepal)
Ranjeet Ambarte (India)
Romain Hennion, Directeur Formind Consulting (France)
Rowena Gladys Aguirre, Freelance Management System Conultant/Trainer (Philippines)
S M Mahabubul Alam, COO, SPEQTA Limited (Bangladesh)
Tchamdjo David, Electricy Sector Regulatory Agency (ARSEL) (Cameroon)
William Falcon, BDO (Dominican Republic)
Yassia Savadogo, ARCEP (Burkina Faso)