1)

ETHICAL HACKER:

Also known as "white hats," ethical hackers are security experts that perform these security assessments. The proactive work they do helps to improve an organization's security posture. With prior approval from the organization or owner of the IT asset, the mission of ethical hacking is opposite from malicious hacking.

Hacking experts follow four key protocol concepts:

1. ***Stay legal**. Obtain proper approval before accessing and performing a security assessment.*
2. ***Define the scope**. Determine the scope of the assessment so that the ethical hacker's work remains legal and within the organization's approved boundaries.*
3. ***Report vulnerabilities**. Notify the organization of all vulnerabilities discovered during the assessment. Provide remediation advice for resolving these vulnerabilities.*
4. ***Respect data sensitivity**. Depending on the data sensitivity, ethical hackers may have to agree to a non-disclosure agreement, in addition to other terms and conditions required by the assessed organization.*

ethical hackers different than malicious hackers:

Ethical hackers use their knowledge to secure and improve the technology of organizations. They provide an essential service to these organizations by looking for vulnerabilities that can lead to a security breach.

An ethical hacker reports the identified vulnerabilities to the organization. Additionally, they provide remediation advice. In many cases, with the organization's consent, the ethical hacker performs a re-test to ensure the vulnerabilities are fully resolved.

Malicious hackers intend to gain unauthorized access to a resource (the more sensitive the better) for financial gain or personal recognition. Some malicious hackers deface websites or crash backend servers for fun, reputation damage, or to cause financial loss. The methods used and vulnerabilities found remain unreported. They aren't concerned with improving the organizations security posture.

hacking identify:

While assessing the security of an organization's IT asset(s), ethical hacking aims to mimic an attacker. In doing so, they look for attack vectors against the target. The initial goal is to perform reconnaissance, gaining as much information as possible.

Once the ethical hacker gathers enough information, they use it to look for vulnerabilities against the asset. They perform this assessment with a combination of automated and manual testing. Even sophisticated systems may have complex countermeasure technologies which may be vulnerable.

They don't stop at uncovering vulnerabilities. Ethical hackers use exploits against the vulnerabilities to prove how a malicious attacker could exploit it.

Some of the most common vulnerabilities discovered by ethical hackers include:

- *Injection attacks*
- *Broken authentication*
- *Security misconfigurations*
- *Use of components with known vulnerabilities*
- *Sensitive data exposure*

After the testing period, ethical hackers prepare a detailed report. This documentation includes steps to compromise the discovered vulnerabilities and steps to patch or mitigate them

some limitations of ethical hacking:

- ***Limited scope***. *Ethical hackers cannot progress beyond a defined scope to make an attack successful. However, it's not unreasonable to discuss out of scope attack potential with the organization.*
- ***Resource constraints***. *Malicious hackers don't have time constraints that ethical hackers often face. Computing power and budget are additional constraints of ethical hackers.*
- ***Restricted methods***. *Some organizations ask experts to avoid test cases that lead the servers to crash (e.g., Denial of Service (DoS) attacks).*

2)

Open-Source Intelligence (OSINT):

Open Source Intelligence (OSINT) is a method of gathering information from public or other open sources, which can be used by security experts, national intelligence agencies, or cybercriminals. When used by cyber defenders, the goal is to discover publicly available information related to their organization that could be used by attackers, and take steps to prevent those future attacks.

OSINT leverages advanced technology to discover and analyze massive amounts of data, obtained by scanning public networks, from publicly available sources like social media networks, and from the deep web—content that is not crawled by search engines, but is still publicly accessible.

OSINT tools may be open source or proprietary: the distinction should be made between open source code and open source content. Even if the tool itself is not open source, as an OSINT tool, it provides access to openly available content, known as open source intelligence.

OSINT Gathering Techniques

Here are three methods commonly used to gain open intelligence data.

Passive Collection

This is the most commonly used way to gather OSINT intelligence. It involves scraping publicly available websites, retrieving data from open APIs such as the Twitter API, or pulling data from deep web information sources. The data is then parsed and organized for consumption.

Semi-Passive

This type of collection requires more expertise. It directs traffic to a target server to obtain information about the server. Scanner traffic must be similar to normal Internet traffic to avoid detection.

Active Collection

This type of information collection interacts directly with a system to gather information about it. Active collection systems use advanced technologies to access open ports, and scan servers or web applications for vulnerabilities.

This type of data collection can be detected by the target and reveals the reconnaissance process. It leaves a trail in the target's firewall, Intrusion Detection System (IDS), or Intrusion Prevention System (IPS). Social engineering attacks on targets are also considered a form of active intelligence gathering.

OSINT Tools

Here are some of the most popular OSINT tools.

Maltego

Maltego is part of the Kali Linux operating system, commonly used by network penetration testers and hackers. It is open source, but requires registration with Paterva, the solution vendor. Users can run a "machine", a type of scripting mechanism, against a target, configuring it according to the information they want to collect.

Main features include:

- *Built-in data transformations.*
- *Ability to write custom transformations.*
- *Built-in footprints that can collect information from sources and create a visualization of data about a target.*

Spiderfoot

Spiderfoot is a free OSINT tool available on Github. It integrates with multiple data sources, and can be used to gather information about an organization including network addresses, contact details, and credentials.

Main features include:

- *Gathers and analyzes network data including IP addresses, classless inter-domain routing (CIDR) ranges, domains and subdomains.*
- *Gathers email addresses, phone numbers, and other contact details.*
- *Collects usernames for accounts operated by an organization.*
- *Collects Bitcoin addresses.*

Intelligence X

Intelligence X is an archival service that preserves historical versions of web pages that were removed for legal reasons or due to content censorship. It preserves any type of content, no matter how dark or controversial. This includes not only data censored from the public Internet but also data from the dark web, wikileaks, government sites of nations known to engage in cyber attacks, and many other data leaks.

Main features include:

- *Search on email addresses or other contact details.*
- *Advanced search on domains and URLs.*
- *Search for IPs and CIDR ranges, with support for IPv4 and IPv6.*
- *Search for MAC addresses and IPFS Hashes.*
- *Search for financial data such as account numbers and credit card numbers*
- *Search for personally identifiable information*
- *Darknet: Tor and I2P*
- *Wikileaks & Cryptome*
- *Government sites of North Korea and Russia*
- *Public and Private Data Leaks*
- *Whois Data*
- *Dumpster: Everything else*
- *Public Web*

BuiltWith

BuiltWith maintains a large database of websites, which includes information on the technology stacks used by each site. You can combine BuiltWith with security scanners to identify specific vulnerabilities affecting a website.

Main features include:

- *Reporting on the content management system (CMS) in use by a website, its version, and plugins currently in use.*
- *Reporting on other infrastructure components used by a website, such as a CDN.*
- *Providing a list of JavaScript and CSS libraries used by the website.*
- *Providing information about the web server running the website.*
- *Providing details of analytics and tracking tools deployed by a website.*

Shodan

Shodan is a security monitoring solution that makes it possible to search the deep web and IoT networks. It makes it possible to discover any type of device connected to a network, including servers, smart electronics devices, and webcams.

Main features include:

- *Easy to use search engine interface.*
- *Provides information on devices operating on protocols like HTTP, SSH, FTP, SNMP, Telnet, RTSP, and IMAP.*
- *Results can be filtered and ordered by protocol, network ports, region, and operating system.*
- *Access to a huge range of connected devices, including home appliances and public utilities such as traffic lights and water control systems.*

HaveIbeenPwned

HaveIbeenPwned is a service that can be used directly by consumers who were impacted by data breaches. It was developed by security researcher Troy Hunt.

3)

As ethical hacking is likely to be done with the permission of the victim or the targeted system, the only way to tackle black hat hacking is tackling it through ethical hacking, the techniques used in penetration are created in a way to emulate the real attacks without causing any damage and safeguard the organization or an individual against the cyber attacks. After it is discovered how the attackers work the Network administrators, engineers and security professional emulate the environment of security level to conduct a penetration test. The things important to know are what the victim is looking for, to make the tests easy and effective.

The Steps that are involved in Penetration tests are as follows:
*• **Ground rules should be established**: to set the expectation, to identify the parties involved, written permissions or an agreement of access mainly known as Statement of work in the United state*
*• **Passive Scanning**: Gathering information about the target without his knowledge also known as Open Source Intelligence, information such as Social Networking Site, Online databases etc.*
*• **Active Scanning and Enumeration**: Using investigating tools to scan the target's public exposure.*
*• **Fingerprinting**: Performing investigation of the target systems to identify, operating system, applications, and patch level open ports, user accounts etc.*
• Selecting a target system.
*• **Exploiting the uncovered vulnerabilities**: executing the appropriate tools targeted at the suspected exposures.*
*• **Escalating privilege**: escalate the security context so the ethical hacker has more control like gaining root or administrative rights, using cracked passwords for unauthorized access*

*• **Documenting and reporting**: A file shall be maintained about every technique used or every tool that was used, vulnerabilities that were exploited and much more.*

The term Hacking become legal:

The increased use of internet the word hacking has lost its worth and is seen more of illegal activity or as a cybercrime, unethical hackers or commonly known as black hat hackers are responsible for the darker side of hacking as they are the one who breaches the cybersecurity with their skills and techniques. To tackle cyber criminals like black hat hackers there is a need of law as well as of ethical hackers.
The white hat hackers work according to the ethics of hacking and protect the interest of individuals on the internet as they are the cybersecurity professional. Ethical hacking is the authorized way of gaining permission for the same.

1. Web Application Hacking

Evidently, web application hacking focuses on securing websites and online services. Therefore, ethical hackers might use tools like OWASP ZAP and Burp Suite to test web applications for vulnerabilities like SQL injection or cross-site scripting.

2. System Hacking

System hacking involves penetrating computer systems to identify and rectify security flaws. They play a critical role in ensuring the security of essential IT infrastructure.

3. Network Hacking

This type of hacking focuses on securing the networks that connect various digital systems. Ethical hackers might employ tools like Wireshark and Aircrack-ng to analyze network traffic and identify potential security breaches. In essence, their work is crucial in maintaining the integrity and safety of data transmission across networks.

4. Wireless Security Hacking

In the wireless domain, this profession is increasingly important due to the proliferation of wireless devices. Moreover, their efforts ensure the safety of wireless communications in both public and private settings.

5. Social Engineering

It involves testing security protocols by understanding and manipulating human behavior to share personal information.

The Key Steps Involved in Ethical Hacking:

1. Reconnaissance

The first step in ethical hacking is reconnaissance or information gathering. Ethical hackers might use tools like Maltego or Shodan to gather critical information about the target. Consequently, this step lays the groundwork for all subsequent hacking activities.

2. Scanning

Following reconnaissance, scanning is the next critical step. It involves using tools like Nessus or Nmap to scan the target for open ports and vulnerabilities. As a matter of fact, this phase helps ethical hackers understand potential entry points in the system.

3. Gaining Access

Gaining access is often considered the heart of this. Ethical hackers use various methods, like exploiting vulnerabilities or social engineering, to gain unauthorized access.

4. Maintaining Access

Once access is gained, maintaining that access is essential for thorough testing. This step allows for the in-depth analysis of vulnerabilities and their potential impact.

5. Covering Tracks

Finally, covering one's tracks is an ethical imperative in ethical hacking. It not only involves erasing all traces of the hacking process but also entails ensuring that the system remains secure. Accordingly. tools like CCleaner or codes like custom scripts are often used to clean logs and temporary files.

4)

Footprinting through Search Engines:

This is a passive information gathering process where we gather information about the target from social media, search engines, various websites etc. Information gathered includes name, personal details, geographical location detrails, login pages, intranet portals etc. Even some target specific information like Operating system details, IP details, Netblock information, technologies behind web application etc can be gathered by searching through search engines

Eg: collecting information from Google, Bingo etc

Google Hacking:

Google hacking refers to collecting information using google dorks (keywords) by constructing search queries which result in finding sensitive information.details collected include compromised passwords, default credentials, competitor information, information related to a particular topic etc.

Eg:inurl:, site:, allintitle etc

Examining HTML Source and Examining Cookies:

Html source codes of a web application may give us an understanding of the application functionality, hidden fields, comments, variable names etc. Cookies are used to identify a user in his session. these cookies may be stored in the browser or passed in the URL, or in the HTTP header.

The entire website can be mirrored using tools like HTTtracker to gather information at our own phase.

Extract website Archives: older versions of website can be obtained

which may reveal some information related to the target.

eg: www.archive.org

Email Footprinting:

email header reveals information about the mail server, original sender's email id, internal IP addressing scheme, as well as the possible architecture of the target network

Competitive Intelligence:

Competitive intelligence gathering is the process of gathering information about the competitors from resources such as the Internet.

Eg: company website, search engine, internet, online databases, press releases, annual reports, trade journals

Google Hacking/Google Dorks:

This is a process of creating search queries to extract hidden information by using Google operators to search specific strings of text inside the search results.

Some google operators, site, allinurl, inurl, allintitle

DNS Footprinting:

DNS is a naming system for computers that converts human-readable domain names into computer readable IP-addresses and vice versa.DNS uses UDP port 53 to serve its requests. A zone subsequently stores all information, or resource records, associated with a particular domain into a zone file; Resource records responded by the name servers should have the following fields:

Domain Name — Identifying the domain name or owner of the records

Record Types — Specifying the type of data in the resource record

Record Class — Identifying a class of network or protocol family in use

Time to Live (TTL) — Specifying the amount of time a record can be stored in cache before discarded.

Record Data — Providing the type and class dependent data to describe the resources.

A (address)—Maps a hostname to an IP address

SOA (Start of Authority)—Identifies the DNS server responsible for the domain information

CNAME (canonical name)—Provides additional names or aliases for the address record

MX (mail exchange)—Identifies the mail server for the domain

SRV (service)—Identifies services such as directory services

PTR (pointer)—Maps IP addresses to hostnames

NS (name server)—Identifies other name servers for the domain

HINFO = Host Information Records

\DNS servers perform zone transfers to keep themselves up to date with the latest information. A zone transfer of a target domain gives a list of all public hosts, their respective IP addresses, and the record type.

Footprinting through Social Engineering:

Social media like twitter, facebook are searched to collect information like personal details, user credentials, other sensitive information using various social engineering techniques. Some of the techniques include

Eavesdropping: It is the process of intercepting unauthorized communication to gather information

Shoulder surfing: Secretly observing the target to gather sensitive information like passwords, personal identification information, account information etc

Dumpster Diving: This is a process of collecting sensitive information by looking into the trash bin. Many of the documents are not shredded before disposing them into the trash bin . Retrieving these documents from trash bin may reveal sensitive information regarding contact information, financial information, tender information etc.

Footprinting countermeasures:

Creating awareness among the employees and users about the dangers of social engineering

Limiting the sensitive information

encrypting sensitive information

using privacy services on whois lookup database

Disable directory listings in the web servers

Enforcing security policies

Ethical Hacking

Introduction to Ethical Hacking

Footprinting and Reconnaissance

Scanning

Enumeration

System Hacking

Malware Threats

Sniffing

Social Engineering

Denial of Service

Session Hijacking

Hacking Web Servers

Web Application Attacks

SQL Injection

Hacking Wireless Networks

Hacking Mobile Devices

Evading Firewall/IDS and Honey Bots

Cryptography

Cloud Computing

5)

Incident Response Plan(IRP):

An incident response plan is a comprehensive, structured approach that outlines the steps an organization must take in the event of a cybersecurity breach or attack. It includes guidelines for detecting, containing, eradicating, and recovering from security incidents, as well as the roles and responsibilities of various stakeholders involved in the process.

1. ***Minimizing the Impact of Incidents****: A well-structured incident response plan enables organizations to act quickly and efficiently when faced with a cyber threat. By following a predefined set of procedures, organizations can minimize downtime, financial losses, and reputational damage.*

2. ***Improving Incident Detection****: An effective incident response plan includes continuous monitoring and regular reviews of security systems, which can help organizations detect threats earlier and take proactive measures to prevent breaches.*

3. ***Streamlining Communication****: A key component of any incident response plan is clear communication among all stakeholders, including IT staff, management, and employees. This ensures that everyone is on the same page during an incident, reducing confusion and enabling a faster recovery.*

4. ***Legal and Regulatory Compliance****: Many industries are subject to strict regulations regarding data protection and cybersecurity. Having a well-documented incident response plan in place can help organizations demonstrate their commitment to compliance and avoid potential penalties.*

5. ***Building Resilience****: Developing and maintaining an incident response plan promotes a culture of security awareness within an organization. As employees become more knowledgeable about potential threats and the proper steps to take during a security incident, the organization as a whole becomes more resilient to cyberattacks.*

Key Components of an Effective Incident Response Plan

- ***Preparation****: Establish a dedicated incident response team, define roles and responsibilities, and provide regular training to ensure that all team members are well-equipped to handle security incidents.*

- ***Detection and Analysis****: Implement continuous monitoring and threat detection tools, and establish procedures for reporting and analyzing potential security incidents.*

- ***Containment, Eradication, and Recovery****: Develop strategies for containing and eradicating threats, as well as restoring affected systems and data.*

- ***Post-Incident Review****: Conduct a thorough review after each incident to identify lessons learned, update the incident response plan, and improve future response efforts.*

It's important for organizations to remember that creating an incident response plan is only one part of a comprehensive security strategy; organizations also need to ensure that they have the right tools, processes, and resources in place to effectively respond to any security incidents. This may include having access to a qualified team of security professionals, outsourcing monitoring and incident response services, or maintaining strong relationships with trusted partners who can provide specialized assistance during an attack. Taking these steps can help organizations quickly identify and mitigate potential threats before they cause serious damage.

Ultimately, developing a well-defined incident response plan is essential for helping organizations remain secure in the face of cyber threats. Having clear guidelines and protocols in place that are updated regularly ensures organizations are prepared to swiftly address any potential security risks they may face. By taking the time to create an effective incident response plan, businesses will be better positioned to manage their risk exposure and protect their digital environment.

Furthermore, an incident response plan is also beneficial for improving operational efficiency and streamlining processes. By having a clear roadmap of specific steps to follow in the event of an incident, teams can quickly identify any threats they are facing and determine the best course of action. This eliminates redundancies and ensures that all stakeholders involved in the process know what their roles are in mitigating cyber risks. Incident response plans also allow organizations to track progress on security incidents and provide valuable lessons learned that may be used as reference points going forward.

Overall, creating a comprehensive incident response plan is invaluable for protecting businesses from potential cyber threats. By preparing ahead of time with well-defined protocols, organizations can better manage their risk exposure and ensure they are able to respond quickly and effectively in the event of a security incident. Documenting all steps involved in the process also helps to reduce response time and streamline processes, giving teams the best chance of success in mitigating risk and responding appropriately. Furthermore, having an incident response plan can help organizations better understand their cyber security posture and provide insight into potential areas for improvement. Having a documented plan also serves as evidence that organizations have taken reasonable steps to prevent and manage data breaches or other cyber-related issues.

Therefore, it is essential for businesses to invest the time into creating a detailed incident response plan that outlines exactly how they will handle each step of the process if a breach were to occur. By taking proactive measures before any security incidents arise, organizations can be better prepared to respond swiftly and effectively, minimizing the damage done and helping them to maintain customer trust. This plan should include information on how to report *an incident, who is responsible for responding, and what steps will be taken to contain the breach. It should also address any legal requirements or regulatory compliance considerations that may come into play during the incident response process. Ultimately, having a well-defined incident response plan in place can significantly reduce the amount of time it takes to define and execute corrective actions when an incident does occur. This can ultimately result in fewer losses and a smoother overall recovery. Having an incident response plan is essential for organizations that depend on the security of their data and systems, as it will help ensure that they are prepared to handle any type of security incident. By taking the time to create an effective plan, organizations can be confident in their ability to quickly identify and address potential threats.*

In order to fully leverage the value of an incident response plan, organizations should also consider implementing preventative measures before an incident ever takes place. This could include regular risk assessments, employee training on cyber security best practices, and the implementation of necessary tools such as firewalls and antivirus software. Additionally, companies should implement processes to detect anomalous activity within their network. By proactively monitoring for suspicious activity, organizations can significantly reduce the amount of time it takes to identify and respond to a security incident.

In conclusion, an incident response plan is essential in order to properly address and mitigate any cyber security threats an organization might face. While implementing preventative measures can help reduce the risk of a security breach, having an effective plan in place is key to ensuring a quick and successful recovery from any incidents that may occur. With the right preparation and procedures in place, businesses can protect their systems and data while continuing operations with minimal disruption. By taking the time to create a detailed plan and train everyone involved in its implementation, organizations can dramatically reduce the amount of time it takes to identify and respond to a security incident. This not only saves precious time but also reduces the overall impact a security breach could have on operations. Investing in an effective incident response plan is key to keeping your business safe and secure.