FUNDAMENTAL OF CYBER SECURITY

TCS-492

UNIT-1

KNOW YOUR MENTOR

SIDDHANT THAPLIYAL

B.Tech(C.S.E.),M.Tech(C.S.E.)

Ph.D.(Pursuing), Cyber Security in IoT Devices with Machine Learning

Profile Link : https://sites.google.com/view/siddhant-thapliyal/home

COURSE OUTCOME

After completion of the course the students will be able to:

CO1: Explain the three pillars of cyber security, types of hackers and penetration testing.

CO2: . Implement the scripting concepts used in cyber security.

CO3: Use the netcat, ping and wireshark tools to analyze the security of network.

CO4: Use the Javascript, php, sql to analyze the web security.

CO5: Explain the use of cyber security protocols for cyber threats.

CO6: Analyze the security level of web applications.

UNIT – I TOPICS

Unit 1: Introduction to Cyber Security What is Cyber security, Why we need Cyber security, The Zero Trust Model, Ethical Hacking Protect Against - Unauthorised Modification, Unauthorised Deletion and Unauthorised Access Three pillars of Cyber Security - Confidentiality, Availability and Integrity Steps to fix a crime - Identify Cyber Threats, Analyse and Evaluate Threat, Treatment Type of Hackers - White Hat, Great Hat, Black Hat Penetration Testing and its Phases - Reconnaissance, Scanning, Gaining Access, Maintaining Access, Covering Tracks

INTRODUCTION TO CYBER SECURITY

WHAT IS CYBER SECURITY?

•“ Cyber’ keyword came from “Cybernetic” from the Greek for “skilled in steering(governing)”,

•Cyber is a “ used in a growing number of terms to describe new things that are being made possible by the use of computers

•Anything related to the “ also falls under the cyber category.

What is Cyber Security?

Cyber security is a process of protecting and recovering networks, devices, and programs from any type of cyber attack.

- Cyber security is often confused with the definition of information security
- Information security, often referred to as ‘IT security’, looks to protect all information assets, whether as a hard copy or in digital form
- Cyber security is a subset of information security
- It specifically focuses on protecting computer systems and their components i e hardware software and data

Overview: Cyber security

- Overall protecting the digital infrastructure from attack, and unauthorized access
- In recent years, cyber security has come under focus of the society because of rapid development of cyber risks (i e attacks) and the degree of impact on individuals, governments organizations and other organizations

The three pillars of cyber security:

Robust cyber security involves implementing controls based on three pillars

- People
- Processes
- Technology

The three pillars of cyber security:

People

Every employee needs to be aware of their role in preventing and reducing cyber threats, and staff dedicated to cyber security need to keep up to date with the latest cyber risks and solutions

Processes

- Processes (process means day to day activates going in a organization)
- Processes are crucial in communicating the organization’s cyber security stance

The three pillars of cyber security:

Processes

- Documented processes should also clearly define roles and responsibilities, and specify the procedure to follow when (i e reporting a suspicious email)
- Processes should be regularly reviewed to account for the latest cyber threats and responses

Technology

- While organizational measures (i e protection methods) are a big part of cyber security, technical controls are just as essential
- For example use of access controls, installation of antivirus software, and other technology can be deployed to protect against cyber attacks

Need of cyber security

Increasingly sophisticated hackers

- Hacker (Internet attackers) are going smart day by day
- They use novel tools and technique to get access into a system
- Every organization has a website and externally exposed systems that could provide hackers a entry points into internal networks
- With the common highly sophisticated attacks, business organizations need to assume that they will be breached at some point
- So they need to implement controls which help to detect and respond to malicious activity before it causes damage and disruption

Need of cyber security

The rising cost of breaches

- The fact is that cyberattacks can be extremely expensive for an organization to suffer
- Recent statistics have suggested that the average cost of a data breach at a larger firm is 20 000.
- It is not just the financial damage suffered by the organization but also causes untold reputational damage
- Suffering a cyberattack can cause customers to lose trust in the organization So they try to spend their money elsewhere

Need of cyber security

Rapid growth in the deployment of IoT devices

- More smart devices (i e smart home appliances smart healthcare devices) than ever are connected to the internet
- These are known as Internet of Things IoT devices and are commonly use in homes and offices
- On the surface, these devices can simplify and speed up tasks, as well as offer greater levels of control and accessibility

Need of cyber security

Tighter regulations

- It is not just criminal attacks that mean organizations need to be more invested in cyber security than ever before
- The introduction of regulations such as the GDPR (EU General Data Protection Regulation) means that organizations need to take security more seriously than ever, or face heavy fines
- Among the requirements of the GDPR is the need for organizations to implement appropriate technical and organizational measures to protect personal data regularly review controls plus detect, investigate and report breaches

The Zero Trust Model

Ruled by the motto never trust, always verify

- Trust and trustworthiness
- Trust Firm belief in the reliability, truth, or ability of someone or something
- Trustworthiness The ability to be relied on as honest or truthful
- Trusting someone means that you think they are reliable, you have confidence in them and you feel safe with them physically and emotionally (In Cyber security You feel safe technically)

The Zero Trust Model

- When trying to create a safe network, organizations usually use a classic perimeter strategy
- This strategy assumes that all users, devices, and endpoints inside the perimeter are trusted by default, and only outsiders are treated as a potential threat
- But today, more and more companies are implementing Bring Your Own Device (policies, hiring remote employees, using cloud services and storage, and granting access to their networks to third party vendors

The Zero Trust Model

- In such an environment, the real threats come from within the network, increasing the risk of access misuse and devastating data breaches caused by insiders
- Therefore, securing remote access and ensuring a high level of perimeter protection isn’t enough anymore

The Zero Trust Model

- One possible solution to ensuring a better level of protection against insider threats is the so called zero trust security model
- In contrast to the classic perimeter model, this model doesn’t identify trusted users, devices, or endpoints based on the network they belong to
- Instead the zero trust model is ruled by the motto never trust, always verify
- It treats both insiders and outsiders as untrusted sources

The Zero Trust Model

- The term zero trust was first used by Forrester experts when describing a new security model in which users and devices were no longer split into trusted and untrusted groups
- Basically the zero trust model is designed to reduce the risk of insider threats
- In the zero trust security model, you grant access to critical applications, data, and endpoints only to those users and devices that have already been authenticated and verified.

The Zero Trust Model

Summary

- This approach is based on three essential steps
- Verifying users when they log in to the system (Use of strong authentication mechanism)
- Validating devices before they connect to the network (Use of strong device access control mechanism)
- Managing privileged access (Use of strong user access control mechanism)

The Zero Trust Model

Source: https:// www.ekransystem.com/en)

Possible suggestions

- User verification can be ensured with the help of such tools as multi factor authentication (i e 2 factor or 3
- Each time someone tries to access sensitive data, you have to make sure that the user requesting permission is who they claim to be (check the genuineness of a user)
- User behavior monitoring and analysis may also be helpful in verifying legitimate users and detecting insider threats
- For example, a login at an unusual time or from a suspicious location should be treated as a sign of a possible cybersecurity problem

Possible suggestions

- Also the least privilege approach must be applied wherever possible in order to make sure that no one can access data or assets which they are not authorized to access

Approaches for effective cyber security

1 Confidentiality

- Confidentiality means something which is secret and should not be disclosed to unintended people or entities
- Confidentiality ensures that sensitive information is accessed only by an authorized person and kept away from those who are not authorized
- Examples are Bank account statements, Personal information, Credit card numbers and Government documents
- Any data security approach is used should ensure customer’s data remains confidential at all times

Approaches for effective cyber security

Confidentiality

- Solution Use of data encryption techniques
- Data confidentiality in the network begins at the physical layer, where fiber tapping devices can be used to steal sensitive data
- To combat this, all your in transit data should be bulk encrypted from end to end which makes it undecipherable

Approaches for effective cyber security

Integrity

- Integrity means that when a sender sends data, the receiver must receive exactly the same data as sent by the sender
- Data must not be changed in transit i e if someone sends a message “then the receiver must receive “
- That is, it must be exactly the same data as sent by the sender
- Any addition or subtraction of data during transit would mean the ntegrity has been compromised
- Example are Data modification attacks and Man in the middle (attack
- Solution Use of hashing algorithms i e SHA 256

Approaches for effective cyber security

Availability

- Availability implies that information should be available to authorized parties whenever required
- It is essential to have plans and procedures in place to prevent or mitigate data loss as a result of a disaster
- A disaster recovery plan must include unpredictable events such as natural disasters and fire

Approaches for effective cyber security

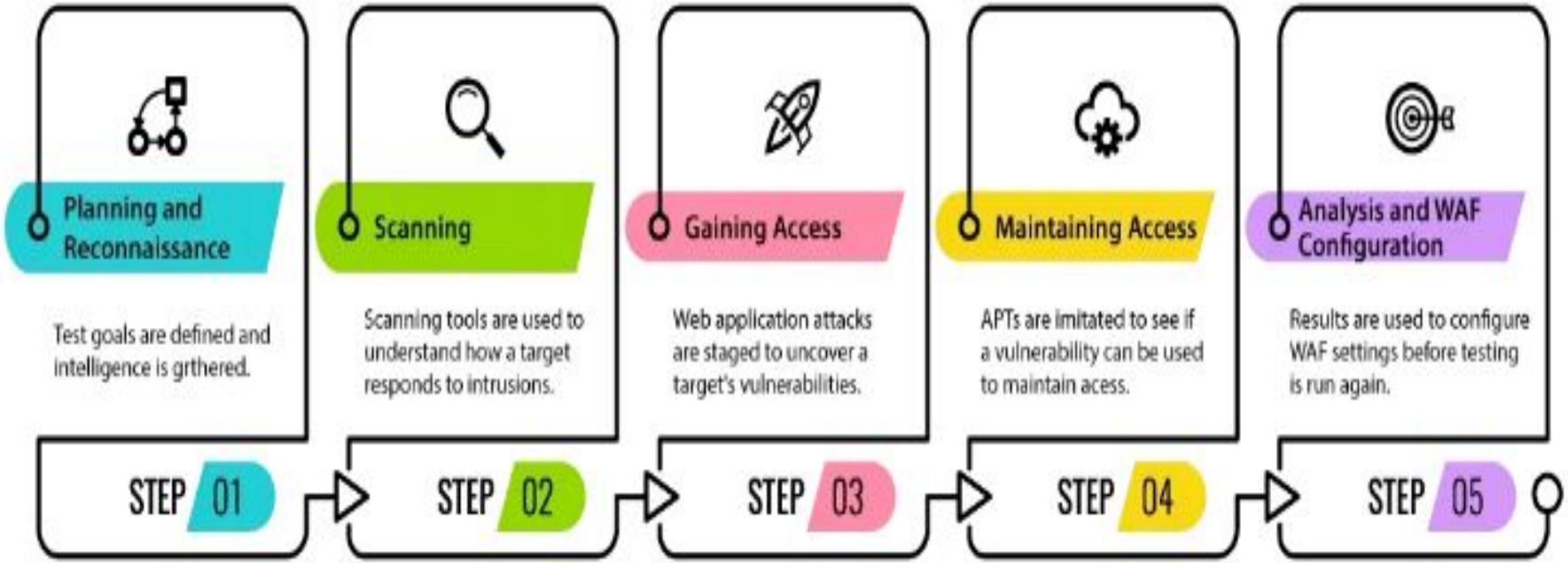
Availability

- Solution A routine backup job is advised in order to prevent or minimize total data loss from such occurrences
- Also extra security equipment or software such as firewalls and proxy servers can guard against downtime and unreachable data due to malicious actions such as denial of service DoS attacks and network intrusions (i e malware)
- Example Attacks that affect Availability DoS and DDoS attacks (i e Hello flood attack)

ETHICAL HACKING

Ethical hacking involves an authorized attempt to gain unauthorized access to a computer system, application, or data. Carrying out an ethical hack involves duplicating strategies and actions of malicious attackers. This practice helps to identify security vulnerabilities which can then be resolved before a malicious attacker has the opportunity to exploit them.

Phases of Ethical Hacking/Penetration Testing



Source: https://www.eccouncil.org/cybersecurity-exchange/ethical-hacking/what-is-ethical-hacking/

Reconnaissance

First in the ethical hacking methodology steps is reconnaissance, also known as the footprint or information gathering phase. The goal of this preparatory phase is to collect as much information as possible. Before launching an attack, the attacker collects all the necessary information about the target. The data is likely to contain passwords, essential details of employees, etc. An attacker can collect the information by using tools such as HTTPTrack to download an entire website to gather information about an individual or using search engines such as Maltego to research about an individual through various links, job profile, news, etc.

Reconnaissance is an essential phase of ethical hacking. It helps identify which attacks can be launched and how likely the organization's systems fall vulnerable to those attacks.

Footprinting collects data from areas such as:

- TCP and UDP services
- Vulnerabilities
- Through specific IP addresses
- Host of a network

In ethical hacking, footprinting is of two types:

Active: This footprinting method involves gathering information from the target directly using Nmap tools to scan the target's network.

Passive: The second footprinting method is collecting information without directly accessing the target in any way. Attackers or ethical hackers can collect the report through social media accounts, public websites, etc.

Scanning

Second step in the hacking methodology is scanning, where attackers try to find different ways to gain the target's information. The attacker looks for information such as user accounts, credentials, IP addresses, etc. This step of ethical hacking involves finding easy and quick ways to access the network and skim for information. Tools such as dialers, port scanners, network mappers, sweepers, and vulnerability scanners are used in the scanning phase to scan data and records. In ethical hacking methodology, four different types of scanning practices are used, they are as follows:

Vulnerability Scanning: This scanning practice targets the vulnerabilities and weak points of a target and tries various ways to exploit those weaknesses. It is conducted using automated tools such as Netsparker, OpenVAS, Nmap, etc.

Port Scanning: This involves using port scanners, dialers, and other data-gathering tools or software to listen to open TCP and UDP ports, running services, live systems on the target host. Penetration testers or attackers use this scanning to find open doors to access an organization's systems.

Network Scanning: This practice is used to detect active devices on a network and find ways to exploit a network. It could be an organizational network where all employee systems are connected to a single network. Ethical hackers use network scanning to strengthen a company's network by identifying vulnerabilities and open doors.

Gaining Access

The next step in hacking is where an attacker uses all means to get unauthorized access to the target's systems, applications, or networks. An attacker can use various tools and methods to gain access and enter a system. This hacking phase attempts to get into the system and exploit the system by downloading malicious software or application, stealing sensitive information, getting unauthorized access, asking for ransom, etc. Metasploit is one of the most common tools used to gain access, and social engineering is a widely used attack to exploit a target.

Ethical hackers and penetration testers can secure potential entry points, ensure all systems and applications are password-protected, and secure the network infrastructure using a firewall. They can send fake social engineering emails to the employees and identify which employee is likely to fall victim to cyberattacks.

Maintaining Access

Once the attacker manages to access the target's system, they try their best to maintain that access. In this stage, the hacker continuously exploits the system, launches DDoS attacks, uses the hijacked system as a launching pad, or steals the entire database. A backdoor and Trojan are tools used to exploit a vulnerable system and steal credentials, essential records, and more. In this phase, the attacker aims to maintain their unauthorized access until they complete their malicious activities without the user finding out.

Ethical hackers or penetration testers can utilize this phase by scanning the entire organization's infrastructure to get hold of malicious activities and find their root cause to avoid the systems from being exploited.

Clearing Track

The last phase of ethical hacking requires hackers to clear their track as no attacker wants to get caught. This step ensures that the attackers leave no clues or evidence behind that could be traced back. It is crucial as ethical hackers need to maintain their connection in the system without getting identified by incident response or the forensics team. It includes editing, corrupting, or deleting logs or registry values. The attacker also deletes or uninstalls folders, applications, and software or ensures that the changed files are traced back to their original value.

In ethical hacking, ethical hackers can use the following ways to erase their tracks:

- Using reverse HTTP Shells
- Deleting cache and history to erase the digital footprint
- Using ICMP (Internet Control Message Protocol) Tunnels

What are the key concepts of ethical hacking?

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.

How are 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.

How are ethical hackers different than malicious hackers?

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.

How are ethical hackers different than malicious hackers?

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 organization's security posture.

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

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).

Protection Against

- Unauthorised Modification

- Unauthorised Deletion

- Unauthorised Access

Protecting against unauthorized modification

It involves implementing a combination of technical and procedural measures to safeguard your systems, data, and networks.

Access Controls:

- Implement role-based access control (RBAC) to ensure that users only have the necessary permissions for their roles.
- Regularly review and update access rights based on job responsibilities.

File Integrity Monitoring (FIM)

•Use FIM tools to monitor critical system files and detect any unauthorized changes.

•Set up alerts or notifications for suspicious activities related to file modifications.

Version Control:

•Use version control systems for critical files and code repositories to track changes and roll back to previous versions if necessary.

Encryption:

•Encrypt sensitive data to protect it from unauthorized modifications, both in transit and at rest.

Protecting against Unauthorized Deletion:

Regular Backups

•Perform regular backups of critical data and systems to ensure that data can be restored in case of unauthorized deletion.

•Store backups in a secure, offsite location.

Access Controls

•Implement strong access controls to prevent unauthorized users from deleting critical files or data.

•Use audit logs to monitor and review deletion activities.

Data Retention Policies

•Establish and enforce data retention policies to ensure that important data is not deleted prematurely.

Monitoring and Alerts

•Set up monitoring systems to detect unusual or suspicious deletion activities.

•Configure alerts to notify administrators of any potentially harmful actions.

Protecting against Unauthorized Access:

Strong Authentication

•Implement multi-factor authentication (MFA) to add an extra layer of security to user accounts.

•Encourage the use of strong, unique passwords.

Network Segmentation

•Segment your network to limit lateral movement in case of a breach, preventing unauthorized access to sensitive areas.

Regular Audits and Reviews:

Conduct regular security audits to identify and address potential vulnerabilities.

Review user accounts, permissions, and access logs on a periodic basis.

Intrusion Detection/Prevention Systems (IDS/IPS)

Deploy IDS/IPS to monitor network traffic and detect and prevent unauthorized access attempts.

Security Awareness Training

Educate users and employees about the importance of security best practices and the risks associated with unauthorized access.

Incident Response Plan

Develop and regularly test an incident response plan to ensure a swift and effective response in the event of unauthorized access.

Type of Hackers

- White Hat

- Grey Hat

- Black Hat

White Hat Attackers

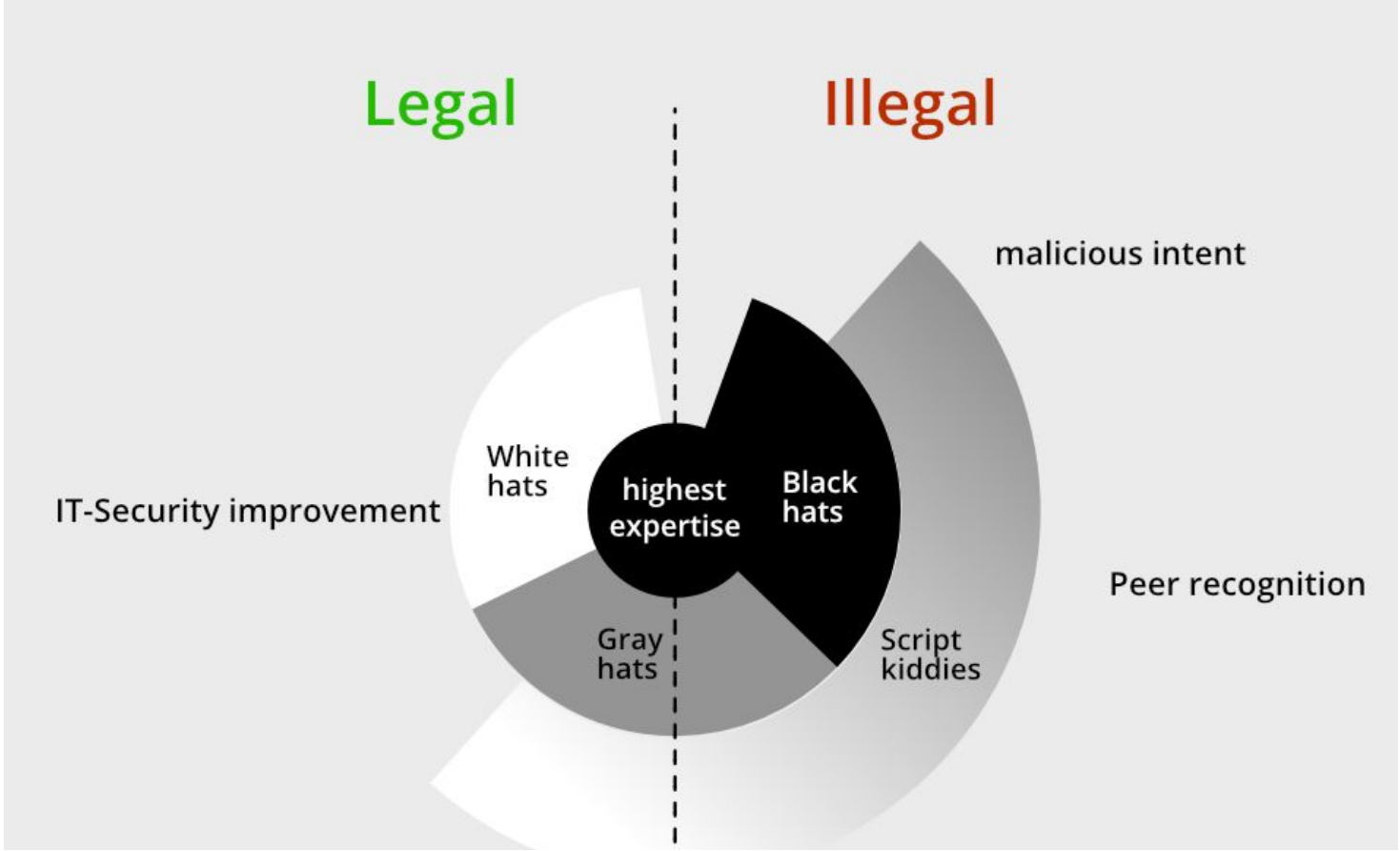
White hat hackers are the one who is authorized or the certified hackers who work for the government and organizations by performing penetration testing and identifying loopholes in their cybersecurity. They also ensure the protection from the malicious cyber crimes. They work under the rules and regulations provided by the government, that's why they are called ***Ethical hackers*** **or** ***Cybersecurity experts*****.**

Black Hat Attackers

They are often called ***Crackers***. Black Hat Hackers can gain the unauthorized access of your system and destroy your vital data. The method of attacking they use common hacking practices they have learned earlier. They are considered to be as criminals and can be easily identified because of their malicious actions.

Gray Hat Attackers

Gray hat hackers fall somewhere in the category between white hat and black hat hackers. They are not legally authorized hackers. They work with both good and bad intentions; they can use their skills for personal gain. It all depends upon the hacker. If a gray hat hacker uses his skill for his personal gains, he/she is considered as black hat hackers.



Source: https://www.geeksforgeeks.org/what-are-white-hat-gray-hat-and-black-hat-hackers/

Difference between White-Hat, Black-Hat, and Gray-Hat Hackers:

S No.	White-Hat Hackers	Black-Hat Hackers	Gray-Hat Hackers
1.	White-Hat Hacking is done by White Hat Hackers.	Black-Hat Hacking is done by Black Hat Hackers.	Gray-Hat Hacking is done by Gray Hat Hackers.
2.	White-Hat Hackers are individual who finds vulnerabilities in computer networks.	Black-Hat Hackers are highly skilled individuals who hack a system illegally.	Gray-Hat Hackers work both Defensively and aggressively.

S No.	White-Hat Hackers	Black-Hat Hackers	Gray-Hat Hackers
3.	White-Hat Hackers works for the organizations and government.	Black -Hat Hackers are criminals who violate computer security for their owner's personal gain.	Gray-Hat Hackers find issues in a system without the owner's permission.
4.	In some cases, white-hat hackers are paid, employees.	Black-Hat hackers make money by carding and selling information to other criminals.	Gray-Hat hackers find issues and report the owner, sometimes requesting a small amount of money to fix that issue.
5.	White-Hat Hacking is legal.	Black-Hat Hacking is illegal.	Sometimes Gray-Hat Hackers violate Laws.

Few More Types of Attackers

- **Script Kiddies:** They are the most dangerous people in terms of hackers. A Script kiddie is an unskilled person who uses scripts or downloads tools available for hacking provided by other hackers. They attempt to attack computer systems and networks and deface websites. Their main purpose is to impress their friends and society. Generally, Script Kiddies are juveniles who are unskilled about hacking.
- **Green Hat Hackers:** They are also amateurs in the world of hacking but they are bit different from script kiddies. They care about hacking and strive to become full-blown hackers. They are inspired by the hackers and ask them few questions about. While hackers are answering their question they will listen to its novelty.

- **State/Nation Sponsored Hackers:** State or Nation sponsored hackers are those who are appointed by the government to provide them cybersecurity and to gain confidential information from other countries to stay at the top or to avoid any kind of danger to the country. They are highly paid government workers.
- **Hacktivist:** These are also called the online versions of the activists. Hacktivist is a hacker or a group of anonymous hackers who gain unauthorized access to government's computer files and networks for further social or political ends.

- **Red Hat Hackers:** They are also known as the eagle-eyed hackers. Like white hat hackers, red hat hackers also aims to halt the black hat hackers. There is a major difference in the way they operate. They become ruthless while dealing with malware actions of the black hat hackers. Red hat hacker will keep on attacking the hacker aggressively that the hacker may know it as well have to replace the whole system.

- **Malicious Insider or Whistleblower:** A malicious insider or a whistleblower could be an employee of a company or a government agency with a grudge or a strategic employee who becomes aware of any illegal activities happening within the organization and can blackmail the organization for his/her personal gain.

- **Blue Hat Hackers:** They are much like the white hat hackers; they work for companies for security testing of their software right before the product launch. Blue hat hackers are outsourced by the company unlike white hat hackers which are employed by the (part of the) company.

Steps to fix a Cyber crime

- Identify Cyber Threats
- Analyse and Evaluate Threat
- Treatment

Identify The Cyber Threat

- **Penetration testing.** By thinking the way a cyber criminal would, security experts can scan their IT environments for vulnerabilities, such as unpatched software, authentication errors, and more.

- **Automated monitoring systems**. Alongside manual processes, organizations can enhance their cybersecurity by integrating automated threat detection systems. These platforms can help organizations by tracking device performance and activity, monitoring web traffic, and notifying the cybersecurity team when irregularities are detected.

- **User behavior analytics.** By analyzing user behavior, an organization can better understand what normal behavior for an employee would look like. This includes the kind of data they access, the time of day during which they log on, and their physical location. That way, any outlying behavior will stand out as unusual, and it will be easier for a security analyst to know what behavior to investigate.

Endpoint Detection and Response (EDR): EDR solutions monitor endpoint devices (e.g., computers, servers, mobile devices) for suspicious activity and potential threats. They collect data on processes, file activities, network connections, and user behavior to identify malicious behavior.

Network Intrusion Detection Systems (NIDS): NIDS monitor network traffic for suspicious patterns or signatures indicative of known threats or attacks. They inspect packets passing through the network and generate alerts for potential threats such as malware, intrusion attempts, or abnormal traffic.

Security Information and Event Management (SIEM): SIEM platforms aggregate and analyze log data from various sources across the IT environment, including network devices, servers, applications, and security tools. By correlating events and identifying anomalies, SIEM solutions help detect potential security incidents and threats.

Threat Intelligence Feeds: Subscribing to threat intelligence feeds provides access to real-time information about emerging threats, vulnerabilities, and indicators of compromise (IOCs). Integrating threat intelligence feeds with security solutions enables proactive identification and blocking of known malicious entities.

Behavioral Analytics: Behavioral analytics solutions analyze user and entity behavior to identify deviations from normal patterns that may indicate a security threat. By establishing baselines of normal behavior, these tools can detect anomalies such as unusual file access, privilege escalation, or data exfiltration.

Web Application Firewalls (WAF): WAFs inspect and filter HTTP requests to web applications, identifying and blocking potentially malicious traffic such as SQL injection, cross-site scripting (XSS), or other web-based attacks.

Email Security Gateways: Email security gateways employ various techniques, including spam filtering, antivirus scanning, and URL reputation checks, to detect and block phishing emails, malware attachments, and other email-based threats.

File Integrity Monitoring (FIM): FIM solutions monitor changes to critical system files and configurations, alerting administrators to unauthorized modifications that may indicate a security breach or malware infection.

Honeypots and Honeynets: Deploying honeypots or honeynets—decoy systems designed to attract and deceive attackers—can help identify and study the tactics, techniques, and procedures (TTPs) used by threat actors targeting your organization.

Continuous Security Monitoring: Implementing continuous security monitoring practices allows for ongoing assessment of the IT environment, enabling timely detection of security incidents and threats. Automated tools and manual oversight combine to provide comprehensive coverage and response capabilities.

Analyse and Evaluate Threat

- VirusTotal
- Nmap (Network Mapper)
- Wireshark
- Snort
- Metasploit Framework
- OpenVAS (Open Vulnerability Assessment System):
- MISP (Malware Information Sharing Platform)

Treatment

- **Incident Response:** Activate incident response plans to contain, investigate, and mitigate cybersecurity incidents promptly. This includes coordinating response efforts, preserving evidence, and restoring affected systems and data.
- **Forensic Analysis:** Conduct forensic analysis to determine the root cause of security incidents, identify compromised systems or data, and gather evidence for potential legal or law enforcement action.

- **Communication and Reporting:** Communicate effectively with stakeholders, including employees, customers, regulators, and law enforcement, about the incident, its impact, and the steps taken to address it.
- **Remediation and Recovery:** Take remedial actions to address security vulnerabilities, implement additional security controls, and enhance cybersecurity defenses to prevent similar incidents in the future. Also, restore affected systems and data from backups and verify their integrity to ensure business continuity.
- **Lessons Learned:** Conduct post-incident reviews to analyze the incident response process, identify areas for improvement, and incorporate lessons learned into future security strategies and policies.

References

1. https://www.synopsys.com/glossary/what-is-ethical-hacking.html
2. https://www.eccouncil.org/cybersecurity-exchange/ethical-hacking/what-is-ethical-hacking/
3. https://www.geeksforgeeks.org/what-are-white-hat-gray-hat-and-black-hat-hackers/
4. https://www.geeksforgeeks.org/types-of-hackers/
5. Zero Trust Model Can Trusting No One Be the Answer to Your Cybersecurity Problems (Information available at https www ekransystem com/en/blog/zero trust security model

References

7. Textbook Penetration Testing A Hands on Introduction to Hacking by Georgia Weidman

8. Textbook Cyber Security Understanding Cyber Crimes, Computer Forensics And Legal Perspectives by Sunit Belapure and Nina Godbole

9. Michael E Whitman and Herbert J Mattord Principles of Information Security, 2 e), Thomson Learning, 2007

10. psu.edu

11. Pen test Information available at https ://www imperva com/learn/application security/penetration testing/

12. Identifying, Analyzing, and Evaluating Cyber risks Information available at https ://www securityforum org/ uploads/ 2017 05 /ISF_c 07 pdf