CERTFIED ETHICAL HACKING

by Durgesh Thakare

WHAT IS HACKING

Hacking means accessing any data, information or any system with & without the permission of individual.

Hacking is the practice of identifying vulnerabilities in computer systems, networks, or software applications, with the intention of improving security measures. Ethical hacking, also known as white hat hacking, is hacking conducted by authorized professionals in order to identify weaknesses in a system and provide solutions to enhance security. It involves a systematic approach of simulating attacks to uncover potential vulnerabilities and protect against malicious hackers.

Phase Of Hacking

VA --- Vulnerability Accessments---- weakness---- system/ network

PT---- Penetration Testing----Exploits----Payload-----Scripting Lang.-----Gaining Access----- system/network

Types of Hacking

Authorized Hacking

Performed with permission from the organization/owner.

Unauthorized Hacking

Performed without permission from the organization/owner.

System base hacking

System-based hacking refers to the act of exploiting vulnerabilities within an operating system in order to gain unauthorized access or control over a computer system. This type of hacking typically involves techniques such as exploiting software vulnerabilities, using malware or viruses, or bypassing security mechanisms to gain control over the targeted system. In order to mitigate system-based hacking, it is crucial to regularly update and patch operating systems, use strong authentication methods, and employ robust security measures to protect against potential attacks.

System

1 Mobile Base

Includes OS and IoT devices.

2 Linux

Android operating system built on the Linux kernel.

3 iOS

Unix-based operating system used in Apple devices.

4 Symbian

Java-based operating system widely used in older mobile devices.

5 Windows

Windows operating system for desktop and laptop computers.

Network base hacking

Network-based hacking involves exploiting vulnerabilities in network protocols, software, or devices to gain unauthorized access to a network or system. Attackers may use techniques such as packet sniffing, spoofing, and social engineering to infiltrate a network and compromise its security. To prevent network-based hacking, network administrators can implement strong access controls, use encryption to secure data in transit, and monitor network traffic for abnormal activity.

Network

1 IP Address

- Network Address: e.g., 192.168.0.23
- Physical Address: MAC Address
- Local Address: Local Host Address (127.0.0.1, 127.90.34.54)

2 Commands

- Windows: ipconfig
- Linux/Unix: ifconfig
- Windows: getmac

Hackers

WHO IS HACKER??

A hacker is a person who uses their technical computer skills to gain unauthorized access to computer systems or networks. Hackers can be classified into three types: white hat, black hat, and grey hat. White hat hackers use their skills to improve computer and network security, while black hat hackers use their skills to perform illegal activities like stealing data or spreading malware. Grey hat hackers are a combination of both.

Types of Hackers

1 **White Hat Hacker**

Ethical hacker who hacks with permission and helps improve security.

2 **Black Hat Hacker**

Hacker who engages in malicious activities for personal gain.

3 **Gray Hat Hacker**

Hacker who falls between white hat and black hat hackers, often engaging in vigilantism.

Other Types

Script Kiddies

Script kiddies are individuals who have limited programming or hacking skills and rely on pre-existing tools or scripts to carry out their hacking activities. They often engage in hacking out of curiosity or a desire for attention, but are generally less skilled and pose a lower level of threat compared to other types of hackers. It is common for script kiddies to target easily accessible or vulnerable targets, such as outdated systems or poorly secured websites.

Hacktivist

Hacktivists are hackers who use their skills to promote a political or social agenda. They often gain unauthorized access to websites or networks to spread a message or protest certain actions or policies. Script kiddies are also a type of hacker, but they differ from the other categories in that they lack the technical skills to create their own tools so they rely on pre-made ones.

Phreakers

Phreakers are hackers who specialize in exploiting vulnerabilities in telecommunication systems, such as phone lines and systems, to gain unauthorized access and control. They are often motivated by a desire for free phone calls or other telecommunication resources. Phreaking was first discovered in the 1970s when hackers realized that they could create tones that mimicked those used by the phone system to make free long-distance calls.

Noobz

Noobz refer to beginner hackers who have limited technical skills and knowledge. They usually rely on pre-packaged tools and tutorials to carry out their cyber attacks. Despite their lack of experience, noobz can still cause harm to computer systems and networks.

Suicide Hacker

Suicide Hacker, also known as a hacktivist, is a term used to describe hackers who engage in cyber attacks as a form of activism, often risking severe consequences for their actions. These hackers prioritize their cause over personal safety and are willing to face legal repercussions or retaliation for their activities. Their attacks are intended to raise awareness or retaliate against individuals, organizations, or governments they believe are engaged in unethical or oppressive practices.+++

State Sponsored Hacker

Hacker sponsored by a government or state agency with the purpose of carrying out cyber espionage or sabotage on behalf of the sponsoring nation. These hackers often target other nations, organizations, or individuals to gather intelligence or disrupt operations.

Hacktivist

A hacktivist is a term used to describe individuals or groups that use hacking techniques as a means of promoting a social or political cause. These hackers are known for their activism and often engage in cyber attacks or digital protests to raise awareness or bring about change. Hacktivists may target government institutions, corporations, or other entities that they believe are acting against their cause.

Cyber Terrorist

A cyber terrorist is an individual or group that seeks to cause harm or disruption to computer systems, with the aim of promoting a political or ideological agenda. These attacks are often carried out against key infrastructure or government targets, and can have serious consequences for public safety and security. Cyber terrorists may use a variety of techniques, including hacking, phishing, and malware, to achieve their goals.

HACKER CLASSES

1

HACKER TEAMS

Hacker teams, also known as hacker groups, are collections of individuals who come together to collaborate on hacking projects. These teams may have different goals and motivations for their activities, such as exploring new technology, exposing vulnerabilities, or perpetrating cyber attacks. Some of the most well-known hacker teams include Anonymous, LulzSec, and APT10.

2

INDESTRIAL SPIES

Industrial spies are hackers who are hired by businesses and corporations to gain unauthorized access to competitors' computer systems, steal valuable data and information, and sell them for monetary gain. These spies can be extremely dangerous and can cause significant harm to the targeted companies. To prevent such attacks, businesses must implement effective cybersecurity measures and remain vigilant against potential threats.

3

CRIMINAL SYNDICATES

Criminal syndicates are organized groups that engage in various illegal activities, including hacking. These syndicates often target financial institutions, government agencies, and individuals, seeking to obtain sensitive information such as credit card details or personally identifiable information to commit fraud or carry out other criminal activities. They operate on a large scale, often spanning across multiple countries, making them difficult to track and apprehend.

4

ORGANIZED HACKERS

Organized hackers, also known as hacktivist groups, are driven by specific agendas and ideologies, using their hacking skills to promote their causes and disrupt systems. These groups often carry out cyber attacks on organizations or governments they perceive as unjust or oppressive, aiming to expose secrets, deface websites, or disrupt services. Their actions can have significant political and social implications, challenging the traditional notions of hacking as purely criminal activity.

5

INSIDER THREATS

Insider threats are individuals with legitimate access who misuse that access to steal sensitive data or damage systems. They may be motivated by financial gain, revenge against the organization, or simply curiosity. Insider threats can be difficult to detect since they often have authorized access and knowledge of internal systems and procedures. Effective security measures, such as strict access controls and continuous monitoring, are necessary to prevent and identify insider threats.

Cyber Crime

CYBER CRIME

Cyber crime refers to criminal activities committed using computers or the internet. These crimes can include hacking, fraud, identity theft, and the distribution of malicious software. Cyber criminals are constantly evolving their tactics and techniques, making it necessary for individuals and organizations to stay vigilant and take proactive measures to protect themselves against these threats. With the increasing interconnectedness of our digital world, combating cyber crime has become a global challenge that requires collaboration and advanced security measures.

CYBER CRIME

1. Computer Fraud
   Deception or false representation
2. Privacy Violation
   Exposing data online
3. Identity Theft
   Stealing information
4. Sharing Copyrighted Files
   Leaking confidential data
5. Electronic Money Transfer
   Online transactions
6. Electronic Money Laundering
   Converting black money to white
7. ATM Fraud
   Cloning ATM cards
8. DOS Attack
   Denial of service
9. MITM Attack
   Capturing packets
10. Spam
    Fake mailing system

Cyber Terrorism

Cyber terrorism is a growing global concern, as it can wreak havoc on vital infrastructures such as power grids, transportation systems, and financial institutions. There is a need for increased international cooperation to combat cyber attacks and protect critical infrastructure. Additionally, educating the public on safe online practices could mitigate the risks of cyber terrorism.

Terrorist have found a new way for indulging into disruptive activities through digital space.

Ways:- Email conversation ---> telephonic conversation --> gaming platform.

Cyber terrorism means to damage information, computer systems and data that result in harm against non-combatant targets.

Classification Of Attacks

Passive Attacks

Passive attacks involve intercepting and monitoring network traffic and data flow on the target network and do not tamper with the data. Attackers perform reconnaissance on network activities using sniffers. These attacks are very difficult to detect as the attacker has no active interaction with the target system or network. Passive attacks allow attackers to capture the data or files being transmitted in the network without the consent of the user. For example, an attacker can obtain information such as unencrypted data in transit, clear-text credentials, or other sensitive information that is useful in performing active attacks. Examples of passive attacks:

- Footprinting
- Sniffing and eavesdropping
- Network traffic analysis
- Decryption of weakly encrypted traffic

Active Attacks

Active attacks, in contrast to passive attacks, involve directly manipulating or altering the target network or system. These attacks include activities such as injecting malicious code, unauthorized access to systems, modifying or deleting data, and performing network-based denial of service attacks. Active attacks pose a greater threat as they can directly disrupt normal operations, compromise sensitive information, and cause significant damage to the targeted entity.

Examples of active attacks

- Denial-of-service (DoS) attack
- Firewall and IDS attack
- Bypassing protection mechanisms
- Malware attacks (such as viruses, worms, ransomware)
- Modification of information
- Profiling
- Arbitrary code execution
- Privilege escalation
- Spoofing attacks
- Replay attacks

Close in Attack

Close-in attacks are a type of active attack that involves physical proximity. These attacks include actions such as gaining unauthorized access to an unattended machine or stealing information from an improperly secured device. Physical security measures such as locks, access controls, and surveillance cameras can help prevent close-in attacks.

Insider Attack

Insider attacks are another type of active attack that occur when a person with authorized access to systems or information misuses their privileges for personal gain or to harm the organization. These attacks can involve theft of sensitive data, sabotage of systems, or intentionally leaking confidential information. Implementing proper access controls, regular monitoring and auditing, and strong security awareness training are essential in preventing and mitigating the risk of insider attacks.

Distribution Attack

Distribution attacks are a type of active attack that aim to spread malware, viruses, or other malicious software across a network. These attacks can be initiated through a variety of means, including email attachments, social engineering, or compromised websites. Implementing strong anti-virus and anti-malware software, user education, and monitoring of network activity can help prevent and detect distribution attacks.

HACKING METHODOLOGY

Hacking Methodology

Hacking methodology refers to the systematic approach that hackers use to gain unauthorized access to a computer system or network. This process typically involves several stages, including reconnaissance, scanning, gaining access, maintaining access, and covering tracks. Understanding common hacking methodologies can help organizations identify vulnerabilities and implement appropriate security measures to protect against potential attacks.

Footprinting

Footprinting is the initial step in the hacking methodology process, where hackers gather information about their target through various means like searching online, using social engineering techniques, or conducting physical reconnaissance. By gathering this information, hackers can gain insight into the network infrastructure, potential vulnerabilities, and potential targets for further exploitation. Implementing measures to restrict the amount of information available to the public and regularly monitoring for suspicious activities can help organizations prevent or minimize the risks associated with footprinting.

Scanning

After the hackers have gathered information about their target through footprinting, the next step is scanning. During this stage, they use port scanning tools and vulnerability scanners to gather more information about the target infrastructure. By identifying open ports, operating systems used, and software versions running on those systems, hackers gain a better understanding of where the vulnerabilities lie and can prepare for possible attacks. Organizations can deploy security measures like firewalls and intrusion detection systems to monitor and block malicious traffic during this stage.

Enumeration

Enumerating is the next step in the hacking process after scanning. During enumeration, hackers use various techniques to gather more detailed information about the target network, such as usernames and system configurations. This information can be used to map out the network and identify potential points of entry. To mitigate the risks associated with enumeration, organizations can implement policies and procedures to restrict unauthorized access and regularly patch vulnerabilities.

Vulnerability Analysis

Vulnerability analysis involves identifying and assessing vulnerabilities in the software, systems, or network discovered during the scanning and enumeration stages. Hackers use various tools and techniques such as vulnerability scanners and manual testing to exploit the vulnerabilities and gain unauthorized access. Organizations can reduce the risk of successful attacks by regularly patching vulnerabilities and implementing security controls to prevent unauthorized access.

Gaining Access

The third step in the hacking process is gaining access. At this stage, hackers have enough information about the target system to attempt to exploit vulnerabilities and gain access to the system. This can be done through various methods such as password cracking, social engineering, or planting malware on the system. Organizations can take steps to prevent unauthorized access, such as using strong passwords, training employees on security awareness, and installing anti-malware software.

Maintaining Access

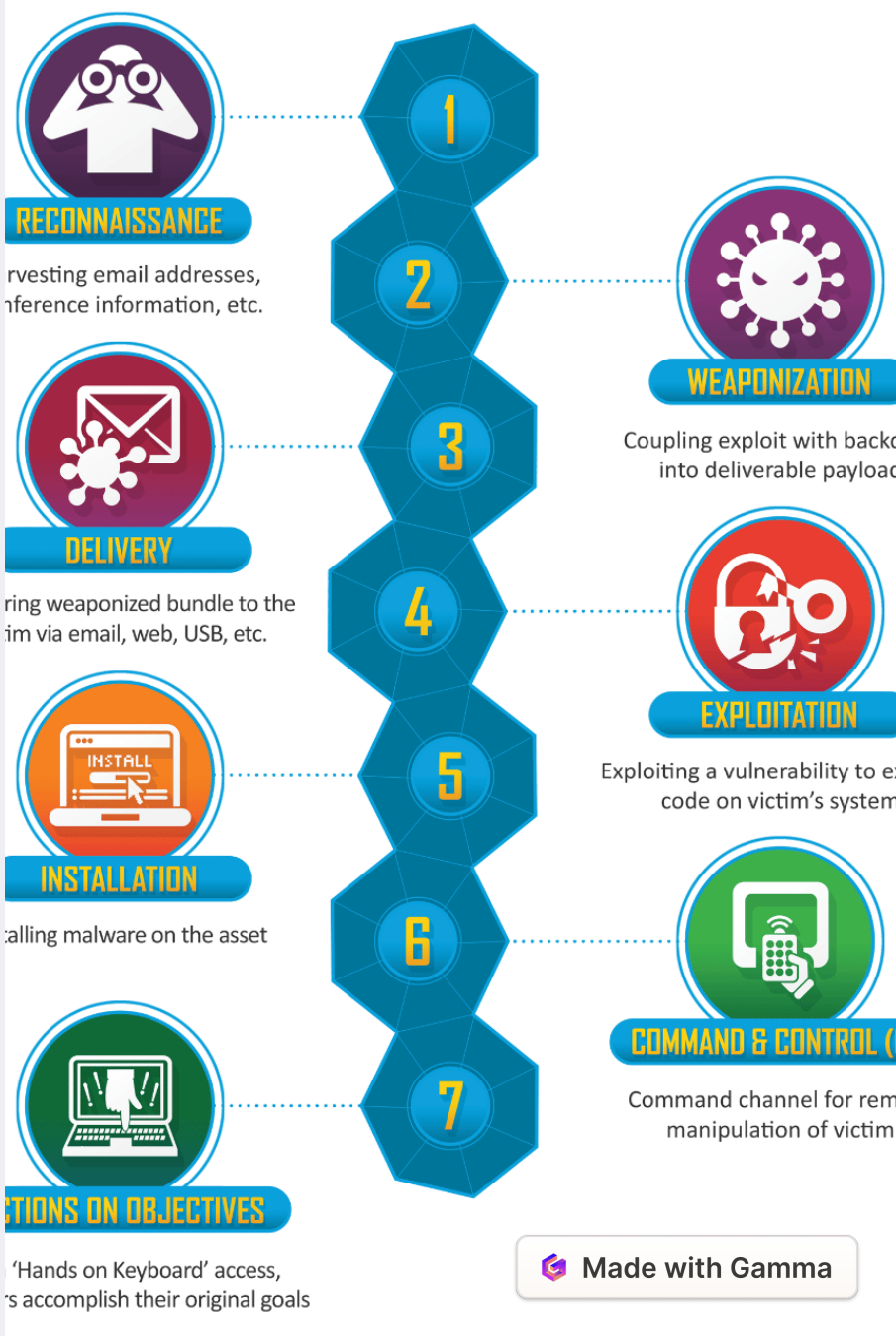
Once hackers have successfully gained access to a system, they aim to maintain that access for as long as possible. This involves establishing persistence by installing backdoors, rootkits, or other malware that allows them to continue accessing the system even after remediation attempts. Hackers may also create multiple accounts or elevate their privileges to maintain a foothold in the system. To counter this, organizations should regularly monitor their systems for suspicious activity, use network segmentation to limit lateral movement, and enforce least privilege access controls.

Clearing Log

To cover their tracks and make it difficult for organizations to detect their presence, hackers often attempt to clear log files and erase any evidence of their activities. By deleting or modifying log entries, they can hide their malicious actions and make it more challenging for incident responders to investigate security incidents. Organizations can mitigate this risk by implementing log monitoring and analysis tools, ensuring that logs are stored securely and cannot be easily manipulated or deleted. Regular backups of log files can also be helpful in case of tampering or deletion attempts.

Cyber kill chain Methodology

The Cyber Kill Chain Methodology is a framework used by many organizations to help identify and prevent cyber attacks. It consists of seven different stages, including reconnaissance, weaponization, delivery, exploitation, installation, command and control, and finally, actions on objectives. By understanding and analyzing each stage of the kill chain, organizations can better protect their systems and data from a wide variety of threats.



Tactics, Techniques, and Procedures (TTPs)

Tactics, Techniques, and Procedures (TTPs) are the tools and methods used by threat actors during cyber attacks. By identifying and understanding these TTPs, organizations can enhance their detection and response capabilities. This includes mapping out the various tactics employed, such as social engineering or SQL injection, as well as the specific techniques utilized within each tactic, such as phishing emails or code injection. By staying informed about the latest TTPs, organizations can proactively adapt their security measures to stay one step ahead of potential attackers.

TACTICS: Tactics are the overall approach and strategy that a threat actor employs during a cyber attack, such as infiltration or data exfiltration. Techniques, on the other hand, are specific methods and procedures used within those tactics, such as malware propagation or brute force attacks. Understanding both tactics and techniques allows organizations to better detect and prevent attacks at each stage of the kill chain. By focusing on the complete picture of TTPs, organizations can better defend against even the most advanced cyber threats.

TECHNIQUES: Techniques are specific methods and procedures used by cyber attackers to achieve their objectives, such as password spraying or spear phishing. By having a comprehensive understanding of the different techniques, organizations can more effectively identify and respond to attacks. Additionally, relying on best practices and applying security updates in a timely manner can help prevent successful exploitation of vulnerabilities and limit the effectiveness of different techniques.

PROCEDURES: Procedures are predefined sequences of actions or steps followed by cyber attackers during an attack. These can include steps like reconnaissance, initial compromise, privilege escalation, and lateral movement. Understanding the procedures used by threat actors can help organizations build effective defense strategies and implement countermeasures at each stage of an attack. By continuously monitoring and updating these procedures, organizations can enhance their cybersecurity posture and mitigate the risk of successful attacks.

MITRE ATT&CK FRAMEWORK

The MITRE ATT&CK Framework is a valuable resource that can help organizations understand the procedures used by various threat actors. It provides insights into the tactics, techniques, and procedures (TTPs) used in cyber attacks and can aid in the development of security measures that can help organizations detect and respond to threats more effectively. By leveraging the MITRE ATT&CK Framework, organizations can build a more robust cybersecurity strategy and stay ahead of potential attackers.

ETHICAL HACKING CONCEPT

Ethical hacking, also known as white hat hacking, is a practice in which an authorized individual attempts to exploit system vulnerabilities and weaknesses to identify and report on potential security risks. It mimics the actions of a malicious hacker but is undertaken for defensive purposes. Organizations can use ethical hacking to identify weaknesses in their security infrastructure and take corrective action before an actual attack can take place.

WHY ETHICAL HACKING IS NECESSARY

Ethical hacking is necessary for several reasons. Firstly, it allows organizations to proactively identify vulnerabilities in their systems and infrastructure before malicious attackers can exploit them. By conducting ethical hacking assessments, organizations can assess the effectiveness of their security measures and make necessary improvements. Additionally, ethical hacking helps organizations stay up to date with evolving threat landscapes and emerging attack techniques, ensuring their defenses remain robust and effective.

SCOPE of ETHICAL HACKING

Ethical hacking is a crucial component of risk assessment, auditing, counter fraud, and information systems security best practices It is used to identify risks and highlight remedial actions. It also reduces ICT costs by resolving vulnerabilities

LIMITATION OF ETHICAL HACKING

Gain authorization from the client and have a signed contract giving the tester permission to perform the test

Maintain confidentiality when performing the test and follow a Nondisclosure Agreement (NDA) with the client for the confidential information disclosed during the test. The information gathered might contain sensitive information, and the ethical hacker must not disclose any information about the test or the confidential company data to a third party

Perform the test up to but not beyond the agreed-upon limits. For example, ethical hackers should perform DoS attacks only if they have previously agreed upon this with the client. Loss of revenue, goodwill, and worse consequences could befall an organization whose servers or applications are unavailable to customers because of the testing.