SCHOOL OF CONTINUING AND DISTANCE EDUCATION

JAWAHARLAL NEHRU TECHNOLOGICALUNIVERSITY - HYDERABAD

Kukatpally, Hyderabad – 500 085, Telangana, India.

SIX MONTH ONLINE CERTIFICATE COURSES – 2023

CYBER SECURITY - ASSIGNMENT - 06

1) Define ethical hacking and distinguish it from malicious hacking. Highlighting the importance of ethical considerations.

Ans: 'Ethical hackers' are often identified with hackers that abide to a code of ethics privileging business-friendly values. However, there is no guarantee that respecting such values is always compatible with the all-things- considered morally best act. It is recognised, however, that in terms of assessment, it may be quite difficult to determine who is an ethical hacker in the 'all things considered' sense, while society may agree more easily on the determination of who is one in the 'business-friendly' limited sense.

Almost every week mass media communicates about hackers having stolen thousands of passwords and other sensitive private information. It is commonplace to read articles about hackers having taken advantage of system vulnerabilities to bypass security barriers in order to fraudulently access private and company networks.

Types of Hackers

Based on their motives and aims, hackers can be categorized into three types:

White Hat Hackers

White hat hackers are cybersecurity experts who breach in an 'official way.' They have been given permission or certification to hack the systems. These White Hat Hackers help governments and organizations by breaking into the system. They gain access to the system by exploiting the organization's cybersecurity flaws. They intend to see how secure the organization is from cyber attacks. They can recognize soft spots and correct them to prevent cyberattacks from outside sources. White hat hackers adhere to professional policies and standards and are called ethical hackers.

Black Hat Hackers

Black hat Hackers are indeed technology geniuses, but they have the wrong motive. They target other devices to gain access to systems to which they are not allowed. They may steal data or harm the system if they obtain unauthorized access. The hacker's ability and expertise determine the hacking techniques utilized by these hackers. Because of the hacker's criminal motives, often, you cannot determine their purpose or the degree of the intrusion.

Gray Hat Hackers

A gray hat hacker, as the name implies, is in between a white hat and a black hat hacker. Gray hat hacking is still unlawful, unlike Verified Ethical Hacking, because the hacker has not acquired authorization from an institution to attempt to enter their networks. However, the motives of a gray hat hacker aren't as nefarious as those of their black hat rivals. Gray hat hacking is occasionally carried out in the name of the public good. When a gray hat hacker discovers a hole and informs a firm, the corporation may often collaborate with the hacker to remedy the fault. Paying them similarly to a white hat hacker may motivate them to expose instead of exploiting the vulnerabilities.

Difference Between Hacking and Ethical Hacking

Parameter	Hacking	Ethical Hacking
INTENTION	A hacker targets a network, system, or app to collect personal information from users and may delete, change, or remove a corporation's records. They intend to steal your data.	An ethical hacker would strike a company's network for all the right reasons, such as detecting and repairing security flaws to protect the system, evaluating a company's security procedures and quality standards, and ensuring the data protection policies of an organization. In short, they protect your data.
LEGALITY	Hacking is when you access a company's network or technology without their knowledge or approval. It is entirely illegal, and anyone found guilty faces serious legal consequences.	Ethical hacking is authorized and permitted by the firm, and it is fully legal. Ethical hackers are covered by an agreement. This, in fact, is one of the highest-paying careers today.
COMPENSATION	A hacker or cyber attacker might be a single person, a community, or a government-sponsored cyber hacking squad. In either case, a hacker is looking to make money by unlawfully obtaining confidential material and marketing it or simply	Although an ethical hacker may operate alone or as part of the cyber security team of a company, they are a full-time employee. In return for his efforts in safeguarding the firm's data, they are guaranteed pay

	using your credit card information.	and all incentives.
TOOLS	They use the same tools as ethical hackers to exploit the vulnerabilities	They use the same tools as hackers to penetrate the system and seal the explored flaws.
TRAINING	Deep knowledge of networking, a thorough understanding of operating systems, a firm grip over network security control, and knowledge of programming languages such as Python, JavaScript, C, and C are some of the skills needed to be a hacker.	Ethical hackers receive the same fundamental training as hackers. After gaining some practical experience, you can pursue certifications such as the Certified Ethical Hacker (CEH) and work as an ethical hacker.
PROFESSIONAL DEVELOPMENT	A black hat hacker has no legit professional development. Instead, the individual is always at risk of being caught by the law.	Unlike black hat hacking, ethical hacking is a highly sought-after career with excellent pay. After acquiring your entry-level job, you can put yourself up for even more sophisticated computer security tasks like senior penetration tester or network administrator in a business.

2) Explain the concept of open source intelligence (OSINT) and its role in information gathering for ethical hacking.

Ans:

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.

There are three common uses of OSINT: by cybercriminals, by cyber defenders, and by those seeking to monitor and shape public opinion.

How Security Teams Use OSINT

For penetration testers and security teams, OSINT aims to reveal public information about internal assets and other information accessible outside the organization. Metadata accidentally published by your organization may contain sensitive information.

For example, useful information that can be revealed through OSINT includes open ports; unpatched software with known vulnerabilities; publicly available IT information such as device names, IP addresses and configurations; and other leaked information belonging to the organization.

Websites outside of your organization, especially social media, contain huge amounts of relevant information, especially information about employees. Vendors and partners may also be sharing specific details about an organization's IT environment. When a company acquires other companies, their publicly available information becomes relevant as well.

How Threat Actors Use OSINT

A common use of OSINT by attackers is to retrieve personal and professional information about employees on social media. This can be used to craft spear-phishing campaigns, targeted at individuals who have privileged access to company resources.

LinkedIn is a great resource for this type of open source intelligence, because it reveals job titles and organizational structure. Other social networking sites are also highly valuable for attackers, because they disclose information such as dates of birth, names of family members and pets, all of which can be used in phishing and to guess passwords.

Another common tactic is to use cloud resources to scan public networks for unpatched assets, open ports, and misconfigured cloud datastores. If an attacker knows what they are looking for, they can also retrieve credentials and other leaked information from sites like GitHub. Developers who are not security conscious can embed passwords and encryption keys in their code, and attackers can identify these secrets through specialized searches.

Other Uses of OSINT

In addition to cybersecurity, OSINT is also frequently used by organizations or governments seeking to monitor and influence public opinion. OSINT can be used for marketing, political campaigns, and disaster management.

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, l hackingathering.

3) Discuss the legal and ethical considerations involved in conducting network scanning and enumeration during ethical hacking activities.

Ans:

Scanning could be basically of three types:

Port Scanning – Detecting open ports and running services on the target host.

Network Scanning – Discovering IP addresses, operating systems, topology, etc.

Vulnerability Scanning – Scanning to gather information about known vulnerabilities in a target.

Network scans fall into two categories: passive network scanning and active network scanning. Passive scanning, also known as "packet sniffing," tracks data packets moving through an organization's network.

Active scanning uses pings or test packets to search for specific irregularities and actively examines the results.

1. Vulnerability Scans

These types of scans look for vulnerabilities in your network and fall into two categories: external and internal.

External vulnerability scans look at your network from the hacker's perspective. They scan external IP addresses and domains, probing for vulnerabilities in internet-facing infrastructure to determine which ones can be exploited. These vulnerability scans are best used to verify the strength of your externally facing services. It helps identify weaknesses in your perimeter defenses, such as a firewall. These scans reveal not only your vulnerabilities, but also the list of ports that are open and exposed to the internet. While external scans are like external penetration tests, they are different in their methodologies.

Looking at your network from this point of view lets you easily identify the most pressing issues within your network, including any services or new servers that have been set up since the last scan to see if they present any new threats to your organization.

Internal vulnerability scans are performed from a location with access to the internal network, and are more complex than external ones, because there are also more potentially vulnerable assets within your organization. This scan will discover and catalog your core IP-connected endpoints, such as laptops, servers, peripherals, IoT-enabled machines, and mobile devices.

Internal vulnerability scanners check these endpoints for vulnerabilities due to misconfigurations or unpatched software, so you can prioritize the devices that require immediate attention to properly secure the network.

Internal scans are best used for patch verification, or when you need to provide a detailed report of vulnerabilities within the network. When analyzing the data, take note of trends such as the top missing patches and the most vulnerable machines.

Performing internal scans on a regular basis is a proactive approach to protecting your network from known vulnerabilities and helps you gain useful insight into your patch management process.

2. Endpoint Scans by Agent

An agent is installed on an endpoint itself and tracks active processes, applications, Wi-Fi networks, or USB devices that don't conform to company policies. It can then flag the user or IT team to fix the issue. In some cases, the agent can close the vulnerability by blocking the malicious action.

Endpoint agents monitor system activity for signs of suspicious behavior, including repeated failed login attempts, changes to the system registry, or backdoor installations.

A host-based agent is not a complete solution. That's because visibility is limited to a single host, and attacks aren't seen until they have already reached the host. You may have heard the concept that all attacks will ultimately end up on an endpoint, since this argument is often used to highlight the importance of endpoint security.

The truth is all threats will land on an endpoint — depending upon how you define an endpoint — as the attack progresses. You should ask yourself, however, if you are satisfied with detecting the threat as it lands, or would you prefer to detect the threat as it enters the environment and makes its way to the endpoint?

Therefore, the passive nature of endpoint agents means they are best suited to use in conjunction with the other types of security scans listed here to take advantage of complementary strengths.

3. Penetration Testing Tools

In penetration testing (often called pen tests) security experts simulate how malicious hackers may attempt to infiltrate your network.

These attacks help verify the effectiveness of your cybersecurity efforts, identify any potential weak spots, and test the human response capabilities of your security team and IT partners. Valuable and effective penetration testing tools are vital to gauge your system's security posture.

Types of penetration testing tools include:

Clear Box Tests. Your organization provides penetration testers with a variety of security information relating to your systems to help them easily find vulnerabilities.

Blind Tests. Your company provides penetration testers with no security information about the system being penetrated with the goal of exposing vulnerabilities that would otherwise go undetected.

Double-Blind Tests. Penetration testers attempt to find vulnerabilities in external-facing applications, such as websites, that can be accessed remotely.

Internal Tests. Penetration testing takes place on-premises and focuses on security vulnerabilities that someone within your organization may use for their advantage.

API Penetration Testing. Simulating attacks via your application program interface (API) will let you simulate the steps a cybercriminal can take toward exploit.

Penetration testing, the most active form of network scanning, can be critical to reducing cyber risk and patching vulnerabilities. It shows your organization where and how a malicious attacker might exploit your network, allowing you to mitigate weaknesses before a real attack occurs. While some IT and security teams may search for open-source penetration testing tools, experts recommend you engage the services of a professional third-party to conduct any penetration testing.

4) How does google hacking contribute to footprinting and information gathering in ethical hacking ?

Ans:

Footprinting using advanced Google hacking techniques involves locating specific strings of text within search results using advanced operators in the Google search engine.

Types of Footprints

a) Active Footprinting: It means performing footprinting by getting indirect touch with target machine.

b) Passive Footprinting: It means collecting information about a system located at remote distance from the attacker.

These are information gathered from footprinting

- Operating System from target machine
- IP address
- Firewall
- Network Map
- Security configurations of the target machine
- Email ID
- Password
- Server Configuration
- URL's (Uniform Resource Locator)
- VPN (Virtual Private Network)

Performing footprinting using google hacking:

To gather the information hackers may use search engines like Google. Google may be used to know the information of target system. If hackers know how to use search engines or google then hackers collect more information like company details, company policies, careers etc. This is passive information gathering method it includes name, personal details, geographical location, login pages, internet portal information and sometime target system operating system, internet protocol (IP) address of that system, Netblock information, web technologies used, different web application used by that system all this information gathered through search engine.

5) Describe the significance of networking fundamentals in the context of ethical hacking and incident respone planning?

Ans:

Network protocols and traffic analysis are essential skills for ethical hackers who want to understand how systems communicate, identify vulnerabilities, and perform penetration testing. However, the network landscape is constantly evolving, with new technologies, standards, and threats emerging every day.

simple introduction to the most important network concepts for ethical hacking

Topologies

There are many different types of network, which can be used for different purposes and by different types of people and organization. Here are some of the network types that you might come across:

LAN - Local Area Network

A LAN is a network that has a logical and physical borders that a computer can broadcast

WAN - Wide Area Network

WAN is a multiple LANs or additional WANs with routing functionality for interconnectivity.

Internet

Connecting WANs through WANs until complete the entire world = Internet.

- The protocol which runs the internet is TCP/IP
- As long you're using legitimate IPv4 address or IPv6

Intranet

If you're using the TCP/IP stack and making your own LAN or WAN = Intranet.

- Intranet is a private network which still runs TCP/IP

Common Terms in Networking

IP (internet protocol) address: the network address of the system across the network, which is also known as the Logical Address).

MAC address: the MAC address or physical address uniquely identifies each host. It is associated with the Network Interface Card (NIC).

Open system: an open system is connected to the network and prepared for communication.

Closed system: a closed system is not connected to the network and so can't be communicated with.

Port: a port is a channel through which data is sent and received.

Nodes: nodes is a term used to refer to any computing devices such as computers that send and receive network packets across the network.

Network packets: the data that is sent to and from the nodes in a network.

Routers: Routers are pieces of hardware that manage router packets. They determine which node the information came from and where to send it to. A router has a routing protocol which defines how it communicates with other routers.

Network address translation (NAT): a technique that routers use to provide internet service to more devices using fewer public IPs. A router has a public IP address but devices connected to it are assigned private IPs that others outside of the network can't see.

NAT - Network Address Translation

NAT stands for network address translation. It's a way to map multiple local private addresses to a public one before transferring the information. Organizations that want multiple devices to employ a single IP address use NAT, as do most home routers.

Static NAT

When the local address is converted to a public one, this NAT chooses the same one. This means there will be a consistent public IP address associated with that router or NAT device.

Dynamic NAT

Instead of choosing the same IP address every time, this NAT goes through a pool of public IP addresses. This results in the router or NAT device getting a different address each time the router translates the local address to a public address.

MAC Addresses

- MAC (Media Access Control) address is provided by NIC Card'd manufacturer and gives the physical address of a computer.

Ports & Protocols

In computer networking, a port is a communication endpoint. At the software level, within an operating system, a port is a logical construct that identifies a specific process or a type of network service.

The most common ports

As a penetration tester or ethical hacker you should be familiar with the common ports and protocols used by popular services.

Port Numbers

Internet Assigned Numbers Authority (IANA) - maintains Service Name and Transport Protocol Port Number Registry which lists all port number reservations

Ranges

Well-known ports - 0 - 1023

Registered ports - 1024 - 49,151

Dynamic ports - 49,152 - 65,535