ASSIGNMENT -6

1. Define ethical hacking and distinguish it from malicious hacking, highlighting the importance of ethical considerations.

ANS:

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.

OR

An ethical hacker, also referred to as a *white hat hacker*, is an information security (infosec) expert who penetrates a computer system, network, application or other computing resource on behalf of its owners -- and with their authorization. Organizations call on ethical hackers to uncover potential security vulnerabilities that malicious hackers could exploit.

The purpose of ethical hacking is to evaluate the security of and identify vulnerabilities in target systems, networks or system infrastructure. The process entails finding and then attempting to exploit vulnerabilities to determine whether unauthorized access or other malicious activities are possible.

The importance of ethical hacking

- **Tools and methodologies:** The lessons learned from ethical hacking help with the creation of effective testing tools and methodologies. Such tools and methodologies further improve an organization’s cyber security posture.

- **Vulnerability identification:** White hat hackers can find critical security flaws in systems, applications, and websites. Patching vulnerabilities before a malicious hacker can exploit them can enhance different types of security, including Internet security. Vulnerability identification is also an important component of vulnerability management.

- **Incident Response:** Ethical hackers can run attack simulations using the same methods and tools as malicious hackers to help security teams prepare for cyber threats. With the aid of cyber attack exercises, security teams can improve their incident response plan and reduce their incident response time.

- **Anti-phishing:** Many modern ethical hacking teams offer anti-phishing training services. Here, they use emails, text messages, phone calls, and baiting to test the readiness of organizations against threats that utilize phishing. Read about this hacking prank for an example of a clever social engineering attack.

- **Secure development:** Some software developers hire ethical hackers to test their products during the development cycle. By ironing out vulnerabilities, developers can stop hackers from taking advantage of zero-day bugs.
- **Data security:** Modern organizations manage different types of sensitive data. Malicious hackers can access this data by using social engineering attacks or exploiting software vulnerabilities. Ethical hackers can improve data security by running penetration testing and simulating phishing attacks.
- **National security:** National organizations such as security agencies and public sector organizations face sophisticated threats from state-sponsored entities. They can mitigate the risk of terror threats and cyber attacks by using the lessons learned from ethical hacking to improve their cyber security.
- **Financial rewards:** Some ethical hackers rely on contracts and programs to generate income. They can find full-time or part-time employment with companies that develop software or need to reduce security vulnerabilities. They can also earn rewards by finding security vulnerabilities in bug bounty programs.
- **Financial losses:** Companies can suffer significant financial losses due to the exploitation of software vulnerabilities by hackers. Ethical hackers can reduce the risk of long-term losses by improving security.
- **Regulatory compliance**: Organizations must comply with regulations concerning privacy and security. They can comply with such regulations more easily by hiring white hat hackers to find bugs that can be exploited by attackers.

- **Reputational Damage:** A cyber security attack can dent a company’s reputation if it results in the loss of sensitive information. Running attack simulations and patching exploitable bugs with the assistance of ethical hacking can prevent incidents that damage an organization’s standing with its clients and partners.

Ethical Hacker vs. Malicious Hacker

In the world of cyber security, there are two primary players – the ethical hacker and the malicious hacker. While both may possess similar skills, their intentions and actions set them apart:

- An ethical hacker, also known as a white hat hacker, is someone who uses their expertise to identify vulnerabilities in computer systems with the permission of the system owner. They follow strict ethical guidelines and work within legal boundaries to help organizations strengthen their security defenses.
- On the other hand, a malicious hacker, often referred to as a black hat hacker or cybercriminal, exploits vulnerabilities in systems for personal gain or malice. Their actions can range from stealing sensitive data to disrupting digital infrastructures for financial or ideological reasons.
- The key difference between these two types lies in their motives. Ethical hackers use their knowledge and skills for good by proactively identifying weaknesses that could be exploited by cybercriminals. In contrast, malicious hackers exploit these weaknesses without any regard for legality or ethics.
- While an ethical hacker’s goal is to protect digital assets and safeguard user information, a malicious hacker’s objective revolves around personal gain at others’ expense.

- It is crucial to understand this distinction because it highlights why organizations need ethical hacking services. By engaging with ethical hackers on a regular basis, companies can stay one step ahead of potential threats while ensuring they remain compliant with industry regulations.
- Moreover, businesses can benefit from proactive vulnerability assessments conducted by skilled professionals who prioritize security and adhere strictly to legal frameworks.
- By employing such measures against potential attacks before they occur rather than reacting after an incident takes place – organizations can save themselves significant time and resources that would otherwise be spent on recovery efforts post-breach.

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

ANS:

Open-Source Intelligence (OSINT) is defined as intelligence produced by collecting, evaluating and analyzing publicly available information with the purpose of answering a specific intelligence question.

OR

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.

How Is Open Source Intelligence Used?

1. Ethical Hacking and Penetration Testing

Security professionals use open source intelligence to identify potential weaknesses in friendly networks so that they can be remediated before they are exploited by threat actors. Commonly found weaknesses include:

- Accidental leaks of sensitive information, like through social media
- Open ports or unsecured internet-connected devices
- Un patched software, such as websites running old versions of common CMS products
- Leaked or exposed assets, such as proprietary code on paste bins

2. Identifying External Threats

The internet is an excellent source of insights into an organization’s most pressing emerging threats. From identifying which new vulnerabilities are being actively exploited to intercepting threat actor “chatter” about an upcoming attack, open source intelligence enables security professionals to prioritize their time and resources to address the most significant current threats.

Top OSINT Tools for Ethical Hacker

Ethical hackers and pen testers use OSINT tools to identify the potential vulnerabilities in the company's security system. The following is the list of top OSINT tools for ethical hackers.

Check Usernames: If you want to get any information about usernames seamlessly, then Check Usernames is one of the best tools. It is used to search for a specific username on 150 websites, and it helps to check the presence of the target on the website.

Google Dorks: Second on the list is Google Dorks, an online OSINT Tool that can help users get relevant information more efficiently. It helps to identify the Email Address Related to a Username and can collect information through social media.

If the user wants the search results in a PDF file for a username, then type 'Filetype: name of the information required in a pdf file in the google search bar. For instance, type "Jamie Oliver" filetype: pdf. in google search, you will get all the PDF files related to Jamie Oliver.

Maltego: Maltego is another OSINT tool for collecting and connecting information for graphical link analysis. It is used to map the relationship between two different kinds of information. Maltego helps mine the data from various sources, merges match information in one graph, and provides a visual map to explore the data effectively.

Metagoofil: Metagoofil is an information-gathering tool used for extracting metadata of public documents of the targeted company or organization that are readily available on websites. After extracting the data, the tool allows the user to generate a report containing software versions, servers or machine names, and usernames. It also helps to extract MAC addresses from Microsoft Office documents.

NexVision: NexVision is an advanced AI-powered OSINT tool that provides real-time intelligence from the Whole web (like on the Dark Web, Social Media, and Clear web). It uses artificial intelligence techniques to extract the most accurate intelligence to discard false positives. NexVision is the most comprehensive tool for many corporate companies, researchers, and governments.

Recon- Ng: Recon-ng is another free and open-source OSINT tool used for reconnaissance of the target. It is an in-built Kali Linux tool with many modules, functions, command completion, database interactions, and interactive help features termed as a complete package tool for information gathering.

Recon- Ng is used to identify IP addresses and can find sensitive files such as robots.txt. It also helps collect data about DNS lookup, sub-domain information, Geo-IP lookup, Banner grabbing, and reverse IP using WHOIS lookup.

How can OSINT help in launching a cyber-attack?

Once the information is gathered, the attack surface can be identified by classifying the data, and the same information can be used to launch potential attacks. There are numerous kinds of cyber-attacks that an attacker can plan and launch depending upon what kind of information he has gathered and his motive.

Following are some of the attacks that can be leveraged in planning some initial and low-high level attacks.

Social Engineering

Social Engineering is one type of cyber attack that does not include any high level of technical competencies and relies upon human manipulation techniques. In it, the attacker collects some vendors' information or employees' details such as designation, job roles, email addresses, etc. With the help of such information, he'd be able to launch different types of physical or digital social engineering attacks to invade the organization's remote or on-premises environment.

The most common social engineering techniques involve:

Phishing attack

A phishing attack is usually carried out through deceptive emails forged with malicious URLs, attachments, or fake scenarios to manipulate humans in downloading the files, opening links, or giving away sensitive information and credentials . To carry out a phishing campaign, little research on the target is beneficial. Let's understand it this way.

In phishing emails, the cybercriminals use leaked or breached resources to collect emails, phone numbers, and relevant organization resources to send phishing emails. Phishing emails have hidden malicious software in the form of URLs and attached documents or images. Once the user clicks a link or opens the phishing email file, the malicious software activates itself to steal credentials (user name, password), bypass the security measures, or take the system hostage by utilizing the system owner access.

Open-source software

Many businesses and applications integrate open-source software into their infrastructure. In open-source software, all issues are publicly available, and it is easy to find out loopholes and issues in them. As the source code is available, threat actors can easily exploit or modify it to perform illegal activities by changing code or inserting malware to steal sensitive data or carry supply chain attacks.

Simultaneously, many legitimate extensions and applications scan the website and reveal the platform and technology on which websites or applications are built. This helps the attacker to know about web technology while crafting their attack plans.

Unpatched System

Unpatched vulnerabilities impose high risk over the applications, network, and overall IT infrastructure. Every other day vulnerabilities are awarded CVEs, whose exploits and related information are made publically for organizations to understand the severity and patches. With the same information, any malicious hacker can also exploit the bug instead of patching it.

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

ANS:

Ethical Hacking -

Ethical hacking, also known as white hat hacking, is the practice of testing a system for security vulnerabilities. It can be done for many reasons, including assessing the security of a system or helping identify weaknesses that can be addressed before an attacker discovers and exploits them.

Ethical hackers use their knowledge and expertise to test the organization's security without causing any damage or loss of data. They will try to find loopholes in your system and report them to you so that remedial measures can get taken before any harm is done.

The goal of ethical hacking is not to cause damage or steal data like a malicious hacker would but to test the security of a system, network, or application. Ethical hackers use the same tools and techniques as malicious hackers, including social engineering, password cracking, and port scanning. Still, they do so to expose vulnerabilities so they can get fixed before they're exploited by someone looking to cause harm.

Ethical and Legal Considerations

While active reconnaissance can be a powerful tool in the arsenal of an ethical hacker, it comes with significant ethical and legal considerations.

1. **Permission and Authorization**: Always ensure you have explicit permission and appropriate authorizations before engaging in active reconnaissance against any network or system.
2. **Respecting Privacy**: Avoid accessing or retrieving personal data unless it is necessary and authorized as part of the engagement.
3. **Minimizing Impact**: Efforts should be made to minimize the impact on the target system. This includes avoiding denial of service conditions or any actions that could disrupt normal operations.
4. **Compliance with Laws**: Be aware of and comply with all relevant laws and regulations. Illegal hacking activities can lead to severe legal consequences.

Tools and Technologies :

Several tools and technologies are commonly used in active reconnaissance:

- **Nmap**: for network scanning and reconnaissance
- **Burp Suite**: for web application security testing
- **Metasploit Framework**: for simulating real-world attacks
- **Wireshark**: for network traffic analysis
- **Nessus**: for vulnerability scanning and reporting
- **John the Ripper**: for password cracking
- **Aircrack-ng:** for wireless network auditing
- **OWASP Zap**: for web application security assessment
- **Sqlmap**: for detecting SQL injection vulnerabilities
- **Hydra**: for password brute-forcing

Phase 1: Passive and Active Reconnaissance

Passive reconnaissance involves gathering information about a potential target without the targeted individual’s or company’s knowledge. Passive reconnaissance can be as simple as watching a building to identify what time employees enter the building and when they leave. However, most reconnaissance is done sitting in front of a computer. When hackers are looking for information on a potential target, they commonly run an Internet search on an individual or company to gain information. I’m sure many of you have performed the same search on your own name or a potential employer, or just to gather information on a topic. This process when used to gather information regarding a TOE is generally called information gathering. Social engineering and dumpster diving are also considered passive information-gathering methods

Active reconnaissance involves probing the network to discover individual hosts, IP addresses, and services on the network. This process involves more risk of detection than passive reconnaissance and is sometimes called rattling the doorknobs. Active reconnaissance can give a hacker an indication of security measures in place (is the front door locked?), but the process also increases the chance of being caught or at least raising suspicion. Many software tools that perform active reconnaissance can be traced back to the computer that is running the tools, thus increasing the chance of detection for the hacker.

Phase 2: Scanning

Scanning involves taking the information discovered during reconnaissance and using it to examine the network. Tools that a hacker may employ during the scanning phase include ,

Dialers

Port scanners

Internet Control Message Protocol (ICMP) scanners

Ping sweeps

Network mappers

Simple Network Management Protocol (SNMP) sweepers

Vulnerability scanners- Hackers are seeking any information that can help them perpetrate an attack on a target, such as the following:

Computer names

Operating system (OS)

Installed software

IP addresses

User accounts

4. How does Google Hacking contribute to footprinting and information gathering in ethical hacking?

ANS:

Google hacking refers to the utilization of advanced Google search operators to create complex search queries and extract sensitive or hidden information. Attackers employ Google hacking techniques to find vulnerable targets that can be exploited. The Google Hacking Database (GHDB) is a valuable resource that provides a database of queries to identify sensitive data. By leveraging advanced Google operators, attackers can pinpoint specific strings of text, such as vulnerable web application versions, within search results.

When conducting a query using standard search operators, Google traces the search terms across various parts of a webpage, including the title, text, URL, digital files, and more. However, to narrow down a search and obtain the most relevant and accurate output, Google offers advanced search operators. These operators play a crucial role in confining a search and optimizing the search query's output.

Footprinting Techniques Using Google Hacking

1**. Email Footprinting**

Email foot printing, also known as email tracking, is a technique that allows hackers to monitor email deliveries and gather information about the target for potential attacks. This technique can provide valuable insights such as the recipient's IP address, geo location, time of receiving and reading the email, interactions with email links, and even the recipient's browser and operating system. By leveraging email foot printing, attackers can gather crucial information for launching targeted attacks.

2. **Google Hacking**

Google hacking techniques involve the use of advanced search operators to extract specific information from Google search results. By crafting complex search queries, hackers can identify vulnerable websites and discover sensitive data. The GHDB serves as a valuable resource for finding relevant queries to uncover potential vulnerabilities. Advanced operators like “inurl,” “intitle,” and “filetype” help narrow down search results and find specific strings of text or versions of vulnerable web applications.

3. **Network Scanning**

Network scanning is an essential footprinting technique that enables attackers to identify and map out the network infrastructure of a target organization. By utilizing Google search operators like “ip,” “port,” and “link,” hackers can search for specific IP addresses, open ports, or external links associated with the target network. This information can help them identify potential entry points or vulnerabilities within the network.

4. **Enumeration**

Enumeration is a technique used to gather detailed information about a target, such as usernames, system configurations, or network resources. By leveraging advanced Google operators like “intext” and “site,” attackers can search for specific text within webpages or confine their search to a particular website. This information can be used to gain a better understanding of the target’s infrastructure and potential vulnerabilities.

5. **Vulnerability Analysis**

Vulnerability analysis plays a crucial role in footprinting, as it helps identify potential vulnerabilities within a target’s systems or applications. By using advanced search operators like “intext” and “filetype,” hackers can search for specific keywords or file types associated with known vulnerabilities. This information can be used to exploit weaknesses and gain unauthorized access to the target’s systems or sensitive data.

Footprinting Tools in Ethical Hacking

1. **TheHarvester**

The Harvester is a powerful reconnaissance tool used to gather information about email addresses, sub domains, hosts, employee names, open ports, and more. By leveraging various data sources, such as search engines, PGP key servers, and SHODAN, The Harvester can provide a comprehensive view of a target’s online presence. This tool is particularly useful for email foot printing and gathering information about a target’s digital footprint.

2. **Maltego**

Maltego is a robust data mining and visualization tool that enables ethical hackers to gather and analyze information from various sources, such as social media platforms, online databases, and DNS records. The tool provides a graphical interface to visualize relationships between different entities, helping hackers identify potential vulnerabilities or connections that can aid in their reconnaissance efforts.

3. **Shodan**

Shodan is a specialized search engine that focuses on internet-connected devices, including servers, routers, webcams, and IoT devices. By utilizing Shodan, ethical hackers can search for specific devices or vulnerabilities associated with a target organization. This information can be instrumental in identifying potential entry points or weaknesses within the target's infrastructure.

4. **Recon-ng**

Recon-ng is a powerful reconnaissance framework that automates various footprinting techniques. The framework supports multiple modules and allows ethical hackers to gather information from different sources, such as search engines, social media platforms, and DNS records. Recon-ng simplifies the footprinting process by automating repetitive tasks and providing a centralized platform for managing reconnaissance activities.

Best Practices for Ethical Footprinting :

1. Obtain proper authorization: Always ensure that you have the necessary permissions and authorizations before conducting any footprinting activities. Unauthorized access to systems or networks can have serious legal consequences.

2. Respect privacy and confidentiality: When conducting footprinting activities, respect the privacy and confidentiality of individuals and organizations. Avoid disclosing or misusing any sensitive information obtained during the process.
3. Keep records and document findings: Maintain detailed records of your footprinting activities, including the tools used, search queries, and findings. This documentation can be valuable for analysis, reporting, and future reference.
4. Stay up-to-date with legal and ethical guidelines: Stay informed about the legal and ethical guidelines governing ethical hacking and footprinting activities in your jurisdiction. Compliance with these guidelines is essential to maintain ethical conduct and avoid legal implications.
5. Continuously enhance your skills: Ethical hacking and footprinting techniques evolve rapidly, and new vulnerabilities emerge regularly. Stay updated with the latest tools, techniques, and security trends to enhance your skills and effectively identify

5. Describe the significance of networking fundamentals in the context of ethical hacking and incident response planning (IRP).

Ans:

What is an Incident Response Plan?

An incident response plan is defined as a "documentation of a predetermined set of instructions or procedures to detect, respond to, and limit consequences of malicious cyber attacks against an organization's information systems."

OR

Establishes procedures to address cyber attacks against an organization's information system(s). These procedures are designed to enable security personnel to identify, mitigate, and recover from malicious computer incidents, such as unauthorized access to a system or data, denial of service, or unauthorized changes to system hardware, software, or data (e.g., malicious logic, such as a virus, worm, or Trojan horse).

When done right, an incident response plan will include the necessary processes, procedures, and documentation needed to detect, respond to, and recover from cyber-related incidents. The action steps outlined in an IRP will cover how an organization and its cyber security team respond to the following:

- Cyber threats (both active and passive)
- Natural disasters
- Unplanned Internet or general connectivity outages

The Importance of an Incident Response Plan

- With notable organizations such as, but not included to, Indigo, Uber, NATO, and MSI reporting significant data breaches, businesses of all sizes should note the importance of an incident response plan… and either A) get one in place, or B) refine any pre-existing IRPs that may have already been drafted.
- A thorough IRP process gives your organization instructions regarding how to effectively minimize losses, remedy exploitable vulnerabilities in your cyber infrastructure, restore all impacted systems and devices, and shut down the attack vector that was used to guarantee that no similar attack will succeed in the future.
- IRPs are integral to preventing cyber-related incidents, protecting sensitive data, pinpointing the root causes of security breaches, and how to recover in the worst-case scenario. They cement the best practices for cyber security incident handling and outline a step-by-step breakdown of how your organization should notify law enforcement, employees, staff, and any impacted clients.

Incident Response Steps

A systematic approach to managing a cyber attack can guide organizations through an otherwise catastrophic event and prevent future attacks. Here are the typical steps involved in incident response:

1. **Preparation**

Preparing against a cyberattack typically requires:

- Identifying a security team of critical people and developing a written set of an organization’s information security policies.
- Ensuring everyone understands their roles and responsibilities in an IR plan.
- Creating a list of assets, including the people, processes, and technology that ensure the success of a critical project.
- Gathering contact information for key personnel provides immediate access when a cyber event occurs.

2. **Detection**

Recognizing malicious activity can include:

- Assessing system data to determine whether a cyber intrusion occurred. Not every anomaly in computer system behavior indicates a cyber issue, which makes identification a crucial decision point.

- Responding promptly to system error messages, firewall alerts, and log files indicating a cyber attack.
- Notifying security teams assigned to handle incidents immediately so they can implement the IR plan's next steps as quickly as possible.

3**. Identification**

Identifying security incidents for response often requires:

- Training both security and non-security teams to quickly identify a variety of dynamic threats, including:
    - Phishing: A social engineering tactic used to manipulate users into clicking a malicious link or downloading a malicious file via email
    - Man-in-the-middle (MITM) attacks: Cyber attacks wherein an invisible, malicious actor sits between or facilitates communication between two unaware individuals, skimming sensitive information contained within
    - Trojans: Viruses that look like reliable software to users, tricking them into downloading and installing malicious files that invade systems
    - Ransomware: This type of malware blocks access or encrypts assets, often forcing the user to pay ransom to regain access to their device, files, or system. In many cases, paying ransom to malicious actors doesn't help. Although payment has been made, users may still be unable to gain access to their files. Some data extortionists now demand a ransom in

return for not leaking the user's data. Today's ransomware actors have turned toward data theft instead of time-expensive encryption, and importantly, the anatomy of modern extortion attacks involves operators taking different approaches to data destruction from full encryption to partial encryption to no encryption – and, thus, no ransomware – at all.

- Denial-of-Service (DoS) attacks: Cyber attacks designed to shut down machines or networks by flooding targets with traffic or sending information that triggers a crash, making them inaccessible to intended users
- Protecting the organization against the above and other constant threats to the security of data and financial information.
- Organizations often face a constant threat to the security of data and financial information. Incident response examples may be malware that installs viruses such as Trojans, worms, adware, spyware, and ransomware.

4. **Containment**

Once a threat is detected and identified, containing it involves:

- Determining the threat's size and scope.
- Implementing containment measures to prevent the threat from spreading and creating an additional impact on data systems.
- Establishing boundaries around the existing damage to prevent more destruction and loss of data.

- Avoiding mistakes that can erase evidence.
- Addressing areas most likely to suffer from a cyber attack via:

1. Short-term containment: This is intended to curtail damage immediately. Identifying infected machines and removing them from a system network can quickly prevent spread. In some cases, promptly addressing containment issues may require disabling an organization's servers until a damage assessment can define further actions.
2. Long-term containment: Long-term containment addresses lingering effects after the initial onset of an attack. For example, while security teams fix infected systems and prepare them for service, backups or additional equipment can help organizations maintain business continuity while vulnerabilities are patched or removed.
3. Continuous monitoring: Monitoring software can provide ongoing visibility into an organization's information systems, providing information about when and where attacks occur. This helps security teams patch existing vulnerabilities, identify new vulnerabilities in real time, and in some cases, predict where future intrusions might occur.

5. **Eradication**

Eliminating all traces of contamination from a security intrusion often requires:

- Thoroughly inspecting all systems to ensure the eradication of vulnerabilities.
- Documenting all research efforts to provide stakeholders with critical information for informing future incident response guides.
- Creating a detailed account of the breach and assessing the impact of the incident, including data on resources spent on remediation efforts.
- Improving security defenses and eliminating vulnerabilities.
- Informing decision makers with all the necessary data for choosing a well-informed path using best practices.
- Planning for undetected artifacts, which can cause reinfection and require repeating the steps in an IR framework.

6. **Recovery and Restoration**

Returning to business as usual after an attack can include:

- Removing malicious content from infected systems
- Rechecking, testing, and verifying all components for functionality
- Enacting extreme care during the recovery and restoration process so information systems are reliable once more

- Implementing a systematic approach to testing, monitoring, and validating data systems to avoid future compromise
- Designing procedures that help return information systems to full functionality (e.g., establishing an agreed-upon timeframe to restore data systems for use)
- Creating a written record of platforms and processes for testing and verification of restored systems to provide guidelines for managing another intrusion should it occur.

----------------------------000000-----------------------------