**ORGANIZATION 1**

I can provide you with a general overview of some common red team tools for **Angelonia Fashion** that are commonly used to exploit and compromise blue team defenses.

1-BloodHound: BloodHound is a tool that helps red teams identify and exploit Active Directory (AD) vulnerabilities. It maps out the AD environment and identifies potential attack paths, allowing red teams to identify high-value targets and plan their attacks accordingly.

2-Mimikatz: Mimikatz is a password-dumping tool that can be used by red teams to extract plaintext passwords and other sensitive information from target systems. It works by exploiting vulnerabilities in the Windows authentication system, and can be used to escalate privileges and gain access to additional systems and resources within the target network.

3-Metasploit: Metasploit is a popular penetration testing tool that can be used by red teams to identify and exploit vulnerabilities in target systems. It provides a range of exploit modules, payloads, and tools that can be used to compromise systems, gain access to sensitive information, and escalate privileges.

4-Cobalt Strike: Cobalt Strike is a powerful tool that enables red teams to simulate advanced persistent threats (APTs) and launch sophisticated attacks against target networks. It includes features like command-and-control (C2) servers, Beacon implants, and a range of post-exploitation tools that can be used to maintain persistence and evade detection.

3.2

Four (4) blue team tools **Angelonia Fashion** could use to protect the

Network from cyber-attacks are given below:

1-Firewalls: Firewalls are a type of security tool that monitor and control traffic between a network and the internet. Firewalls can block traffic from known malicious sources, prevent unauthorized access to the network, and help to identify and stop attacks in progress. **Angelonia Fashion** could use firewalls to protect their network from cyber-attacks by configuring them to block unauthorized traffic and limit access to sensitive information.

2-Intrusion Detection Systems (IDS): IDS are tools that monitor network traffic for signs of unauthorized access or suspicious activity. IDS can detect anomalies such as unusual network traffic patterns, unexpected data transfer, and unauthorized access attempts. **Angelonia Fashion** could use IDS to detect and respond to cyber-attacks in real-time, minimizing damage and preventing the attackers from gaining further access to the network.

3-Vulnerability Scanners: Vulnerability scanners are tools that identify security weaknesses in software, operating systems, and other network components. **Angelonia Fashion** could use vulnerability scanners to identify vulnerabilities and prioritize patching efforts. This could help to prevent attackers from exploiting known vulnerabilities and gaining access to the network.

4-Endpoint Protection: Endpoint protection tools are designed to secure individual devices such as laptops, desktops, and mobile devices. These tools can protect against malware, viruses, and other threats by scanning for malicious files and behavior. **Angelonia Fashion** could use endpoint protection tools to protect their devices and prevent them from becoming infected with malware, which could be used to gain access to the network.

**3.3**

A set of ethical practices employees can apply when using red and blue team tools in public networks for Angelonia Fashion Have been outlined.

Here are some ethical practices that employees can follow when using red and blue team tools in public networks for **Angelonia Fashion:**

1-Obtain proper authorization: Employees should only use red and blue team tools on public networks for **Angelonia Fashion** after obtaining proper authorization from the company. Unauthorized testing can be considered as hacking and may lead to legal consequences.

2-Use the tools only for intended purposes: Employees should use the red and blue team tools only for their intended purposes, which is to test the security of **Angelonia Fashion’s** public networks. Using these tools for any other purposes, such as personal gain or to harm other organizations, is unethical and illegal.

3-Respect privacy: Employees should respect the privacy of others while conducting security testing on public networks. They should avoid accessing or collecting any personal or sensitive information that is not related to the intended purpose of the testing.

3-Avoid damaging systems: Employees should take care not to cause any damage to the systems they are testing. They should ensure that they do not delete, modify or corrupt any data or files while conducting the testing.

4-Follow ethical guidelines: Employees should follow ethical guidelines while using red and blue team tools on public networks. They should not engage in any activity that could harm **Angelonia Fashion** or any other organizations, and should report any vulnerabilities or issues discovered during the testing to the appropriate authorities.

5-Document all findings: Employees should document all findings and keep accurate records of their testing activities. This documentation can be used to inform security policies and procedures, as well as to demonstrate compliance with ethical and legal standards.

6-Protect sensitive information: Employees should protect any sensitive information that they may come across while conducting security testing. They should not share this information with unauthorized individuals or organizations, and should take appropriate measures to secure it.

By following these ethical practices, employees can conduct red and blue team testing on public networks for **Angelonia Fashion** in a responsible and professional manner.

**3.4**

Consequences of unethical behaviour in Angelonia Fashion :

1. The legal consequences of misusing skills gained using red and blue team tools and the potential data breaches that can occur when using these skills unauthorized can be severe. Misusing these tools could result in criminal charges for violating various laws, including the Computer Fraud and Abuse Act, the Electronic Communications Privacy Act, and state laws governing unauthorized access to computer systems. Such violations could lead to fines, imprisonment, or both. Additionally, if **Angelonia Fashion** stores personal data of its customers, a data breach resulting from unauthorized use of these tools could lead to civil liability for damages, regulatory fines, and loss of reputation.
2. Unauthorised access to network devices can result in significant consequences for **Angelonia Fashion.** The unauthorized access can lead to the loss of confidential information, data breaches, or even theft of intellectual property. In addition, unauthorized access can allow attackers to install malware or modify the configuration of network devices, resulting in system downtime or a complete system failure. Such an attack can have significant financial implications for the company, including loss of revenue, legal costs, and expenses associated with repairing the system.
3. Bypassing copyright media and applications can result in legal consequences for **Angelonia Fashion.** The company could face legal action for copyright infringement, which could result in significant financial penalties, including damages and legal fees. Additionally, Angelonia Fashion could face loss of reputation and potential loss of customers who do not wish to associate with a company that engages in unethical behavior. Finally, bypassing copyright media and applications may also be a violation of the terms of service of the software or media, which could result in the loss of the right to use the software or media.

.

**3.5**

**A** minimum of four (4) examples of unethical behaviour that could happen in the **Angelonia Fashion** by the hand of cyber security technicians have been identified. Are given below:

1-Unauthorized Access: A cyber security technician could intentionally access confidential or sensitive data without proper authorization. This unethical behavior can lead to serious implications, such as theft of personal information, financial loss, and damage to the reputation of **Angelonia Fashion.** It can also lead to legal consequences if the unauthorized access violates any regulations or laws.

2-Data Manipulation: A cyber security technician could manipulate data to create false information or hide information from the management. This unethical behavior can lead to incorrect business decisions, loss of reputation, and financial loss. Moreover, it can also violate regulations or laws, leading to legal consequences.

3-Data Breach: A cyber security technician may intentionally or unintentionally cause a data breach, allowing hackers or other unauthorized parties to gain access to sensitive or confidential data. This unethical behavior can lead to serious implications, such as financial loss, reputation damage, and legal consequences. Moreover, it can also violate regulations or laws, leading to further legal consequences.

4-Cyber Espionage: A cyber security technician may engage in cyber espionage to gain an unfair advantage over competitors. This unethical behavior can lead to serious implications, such as loss of intellectual property, damage to the reputation of **Angelonia Fashion**, and legal consequences. Moreover, it can also lead to the loss of trust and confidence from clients and partners.

In summary, any unethical behavior by cyber security technicians can have severe implications on the overall network and data security of **Angelonia Fashion.** Such unethical behavior can lead to financial loss, reputation damage, legal consequences, and loss of trust from clients and partners. It is crucial to implement strict policies, procedures, and training to prevent such unethical behavior and maintain the integrity of **Angelonia Fashion’s** network and data security.

**ORGANIZATION 2**

3.1

I can provide a general overview of some tools that are commonly used by red teams to test and assess the security of an **TURTLE MOVERS** defenses. It is important to note that these tools should only be used with proper authorization and under controlled circumstances.

1-Metasploit Framework: This is a popular open-source exploitation framework that allows red teams to launch attacks against various types of systems and applications. It has a wide range of modules and exploits that can be customized to suit different attack scenarios, making it a powerful tool for testing and identifying vulnerabilities in an organization’s defenses.

2-Cobalt Strike: This is a commercial penetration testing tool that enables red teams to simulate advanced threat actors and launch targeted attacks against a company’s network infrastructure. It has features such as beaconing, social engineering, and phishing that can be used to compromise user credentials and gain access to sensitive information.

3-Empire: This is another open-source tool that provides a modular framework for red teams to launch post-exploitation attacks against Windows, macOS, and Linux systems. It includes features such as keylogging, credential theft, and lateral movement that can be used to pivot through a network and gain deeper access to target systems.

4-Nmap: This is a network exploration and reconnaissance tool that can be used to map an organization’s network topology, identify open ports, and discover potential vulnerabilities. It can be used to gather valuable intelligence that can be used by red teams to plan and execute targeted attacks.

5-Again, it is important to emphasize that the use of these tools should only be done with the explicit permission and guidance of an authorized entity or organization, and not for any malicious or illegal activities.

3.2

I can provide an overview of four blue team tools that **TURTLE MOVERS** commonly use to protect their network from cyber-attacks:

1-Intrusion Detection System (IDS): An IDS monitors network traffic for suspicious activity and alerts security personnel when potential threats are detected. IDS can be host-based or network-based, and they use various methods to detect attacks such as signature-based, anomaly-based, and heuristic-based techniques.

2-Security Information and Event Management (SIEM): A SIEM system collects, analyzes, and correlates security events from various sources such as firewalls, IDS, antivirus, and other security devices. SIEM systems can provide real-time alerts and detailed reports that help security teams to identify and respond to security incidents.

3-Endpoint Detection and Response (EDR): EDR tools protect endpoints such as servers, desktops, and laptops from advanced threats such as malware, ransomware, and fileless attacks. EDR solutions use behavioral analysis, threat intelligence, and machine learning to detect and respond to threats in real-time.

4-Vulnerability Management (VM): VM tools scan the network and endpoints to identify vulnerabilities and provide prioritized recommendations for remediation. VM solutions can automate the patching process and ensure that the network is up-to-date with the latest security patches.

Overall, these blue team tools can help **TURTLE MOVERS**  to detect, prevent and respond to cyber-attacks effectively. However, each organization’s needs are unique, and it’s crucial to choose the right tools that align with their security requirements and budget.

3.3

Red and blue team tools can be valuable for testing the security of public networks, but they should be used responsibly and ethically. Here are some ethical practices that employees can follow when using these tools:

1-Obtain proper authorization: Employees should obtain proper authorization before using red and blue team tools on public networks. They should ensure that they have the necessary permissions to perform security testing.

2-Use the tools only for security testing: Employees should use the tools only for security testing purposes and not for any other purposes.

3-Respect privacy: Employees should respect the privacy of others when using red and blue team tools. They should not access or collect any personal information unless it is necessary for security testing and they have obtained proper authorization.

4-Avoid causing harm: Employees should avoid causing any harm to the network or its users while using red and blue team tools. They should ensure that their testing activities do not disrupt the network or cause any damage.

5-Report vulnerabilities: If employees find any vulnerabilities during their testing activities, they should report them to the appropriate authorities immediately. They should not exploit the vulnerabilities or share them with unauthorized parties.

6-Keep the testing activities confidential: Employees should keep the details of their testing activities confidential. They should not disclose any information about their testing activities to unauthorized parties.

7-Use secure communication channels: Employees should use secure communication channels when discussing the results of their testing activities. They should ensure that the communication is encrypted and that only authorized parties have access to it.

By following these ethical practices, employees can use red and blue team tools responsibly and help to improve the security of public networks of **TURTLE MOVERS**  without causing any harm or violating anyone’s privacy.

3.4

1-Misusing skills gained using red and blue team tools and engaging in unauthorized data breaches can lead to severe legal consequences. Individuals who engage in such unethical behavior may be subject to criminal prosecution, fines, and imprisonment. Additionally, the affected parties may sue them for damages resulting from the breach, leading to civil lawsuits.

2-Unauthorized access to network devices can lead to several consequences. Firstly, the individual may be breaking the law, leading to criminal charges, fines, and imprisonment. Secondly, unauthorized access may disrupt the network’s functionality, leading to downtime, financial loss, and reputational damage. Lastly, it can compromise sensitive data stored on the network, leading to data breaches and exposure of private information.

3-Bypassing copyright media and applications obtained via file sharing or downloading can lead to both legal and reputational consequences. The individuals can face legal charges for violating copyright laws, leading to fines and criminal prosecution. Additionally, it can lead to reputational damage for the individuals, such as loss of credibility, trust, and respect in the industry. Furthermore, the copyright owner may sue the individuals for damages resulting from copyright infringement, leading to civil lawsuits.

3.5

1-Unauthorized Access: An unethical behavior by a cyber security technician could be to access confidential data or networks without permission. This could have a severe impact on overall network and data security as it could lead to data theft, unauthorized modification or deletion of data, and exposure of sensitive information to unauthorized individuals. Such unethical behavior could also compromise the integrity and confidentiality of the data, leading to legal and financial repercussions.

2-Neglecting Security Patches: Another unethical behavior is to neglect security patches that are critical for the security of the system. This could lead to vulnerabilities in the system that can be exploited by hackers, resulting in data breaches, theft, or even complete loss of data. Neglecting security patches could also have a severe impact on the overall network and data security, as it could leave the system exposed to various forms of cyber attacks.

3-Selling Sensitive Information: An unethical behavior by a cyber security technician could be to sell sensitive information to unauthorized individuals or organizations. This could lead to data breaches, theft, and other forms of cyber attacks that could have a severe impact on the overall network and data security. Selling sensitive information could also compromise the integrity and confidentiality of the data, leading to legal and financial repercussions for the organization.

4-Sabotage: An unethical behavior by a cyber security technician could be to intentionally sabotage the system, either by disabling security measures or by introducing malware or viruses. This could have a severe impact on the overall network and data security, as it could compromise the confidentiality, integrity, and availability of the data. Sabotage could also lead to significant financial and reputational losses for the organization, as well as legal consequences.

For anyone organization

3.6

Ethic code practice for **TURTLE MOVERS** are given:

✓Hold paramount the safety, health, and welfare of the public.

✓Perform services only in areas of their competence.

✓Issue public statements only in an objective and truthful manner.

✓Act for each employer or client as faithful agents or trustees.

✓Avoid deceptive acts.

That’s great to hear that an Ethics Code of Practice has been developed for the cyber security technicians of **THE TURTLE MOVERS**. Here are some considerations for the distribution and implementation of the code:

1-Distribution: The code should be distributed to all cyber security technicians within the organization. This can be done through email, company-wide announcements, or even a physical copy of the code.

2-Acknowledgement: Technicians should be required to acknowledge that they have read and understand the code. This can be done through a signature or online confirmation.

3-Training: In addition to distributing the code, it is important to provide training to the technicians on how to apply the principles of the code in their work. This can be done through workshops or online training sessions.

4-Enforcement: The code should be enforced through a disciplinary process for any violations. The disciplinary process should be clearly outlined in the code and communicated to all technicians.

5-Review and Update: The code should be periodically reviewed and updated to ensure that it remains relevant and effective. This can be done through a review committee or a designated person in charge of the code.

Overall, the distribution and implementation of the Ethics Code of Practice for the cyber security technicians should be taken seriously and done in a comprehensive and thorough manner to ensure its effectiveness in promoting ethical behavior within the organization.

3.7

Three (3) downloading file-sharing services have been identified for the TURTLE MOVERS ,their suitability and security risks are given below

1-Google Drive

Suitability: Google Drive is a cloud-based file-sharing service that allows users to upload, store and share files. It is suitable for individuals, small businesses and large organizations as it offers a range of features and storage options. It has a user-friendly interface and can be accessed from multiple devices.

Security Risks: One of the security risks associated with Google Drive is data breaches, where sensitive information can be accessed by unauthorized users. Another risk is the potential for malware or viruses to be uploaded to the platform. Users must also be cautious of sharing files publicly, as it can lead to data leaks.

2-Dropbox

Suitability: Dropbox is a popular cloud-based file-sharing service that allows users to store and share files. It is suitable for individuals, small businesses, and large organizations as it offers various features such as file syncing, collaboration tools, and mobile apps.

Security Risks: One of the security risks associated with Dropbox is data breaches. Another risk is the potential for sensitive information to be accessed by unauthorized users due to weak passwords or shared links. Additionally, Dropbox’s mobile app has been known to have vulnerabilities that can be exploited by hackers.

3-WeTransfer

Suitability: WeTransfer is a file-sharing service that allows users to send files up to 2GB for free. It is suitable for individuals who need to share large files quickly and easily.

Security Risks: One of the security risks associated with WeTransfer is the potential for sensitive information to be accessed by unauthorized users. Another risk is the potential for malware or viruses to be uploaded to the platform. Users must also be cautious of phishing scams, where attackers can use fake WeTransfer emails to trick users into downloading malware or providing login credentials.