



Security Testing

Vathna.lay@cadt.edu.kh

Becoming the Hacker to Beat the Hacker

- **The need for Hacker Savvy:** To protect against cyber threats, security professionals must understand the hacker's mindset & tactics.
- **Ethical Hacking, The difference:** Same tools, techniques but with the target's permission and a professional focus.
- **The goal of Vulnerability and Penetration Testing:** proactively identify weaknesses from a hacker's perspective to strengthen security
- **Part of a comprehensive Security Strategy:** Ethical hacking complements risk management and helps validate vendor claims





Security Testing vs. Auditing

- **Security Auditing**

- **Focus:** Evaluating if security policies and controls are in place as required by standards or regulations
- **Method:** Often involves reviewing processes, documentation, and sometimes technical check
- **Intent:** Validate compliance and existing security Measure



Security Testing vs. Auditing

- **Vulnerability and Penetration Testing**
 - **Focus:** Finding and exploiting weaknesses in systems and security controls
 - **Method:** Highly technical, using the mindset and tools of hackers to simulate real-world attack
 - **Intent:** Identify vulnerabilities that could be exploited by malicious actors



Policy & Compliance

- **Document Policy:**
 - Outlines who conducts the tests, types of testing, frequency, & procedures.
 - Establishes standards for tools and personnel.
 - Sets clear expectations for security testing activities.
- **Compliance and Regulations:**
 - Consider state, federal, and international laws (e.g., DMCA, HIPAA, GLBA, NERC CIP, PCI DSS, CMMC, GDPR). Ensure the testing is align with the regulations
 - Integrating security testing into your compliance program can strengthen overall security and privacy





Think Like a Thief to Catch a Thief

- **Understanding the Enemy:** Knowing hacker tactics is key to defending against them.
- **The Reality of Vulnerability:** All systems are potentially susceptible to attack.
- **Beyond Security Products:** Testing uncovers weaknesses that even expensive tools can miss.





Think Like a Thief to Catch a Thief

- **Addressing the Low-Hanging Fruit:** Focus on the common vulnerabilities that cause most problems.
- **Prioritization and Risk Reduction:** Identify and fix the most critical issues first.
- **Continuous Improvement:** As hackers evolve, so must your security practices.





Beyond the Code: The Human Element of Security

- **The Weakest Link:** Humans are often the most vulnerable point in a security system due to trust and susceptibility to manipulation.
- **Physical Attacks:**
 - Breaking into facilities to steal equipment or information.
 - Dumpster diving for discarded sensitive documents.
 - Simple yet effective ways to bypass technical security measures.





Vulnerabilities in Network Infrastructure

- **Widespread Access:** Networks connected to the Internet are exposed to global threats.
- **Common Network Infrastructure Attacks:**
 - **Unsecured Wireless Access:** Bypassing firewalls through open Wi-Fi networks.
 - **Protocol Weaknesses:** Exploiting vulnerabilities in FTP, SSL, or other network protocols.
 - **Denial of Service (DoS):** Overwhelming networks with traffic to disrupt legitimate use.
 - **Packet Capture:** Intercepting unencrypted data to expose sensitive information.



Operating Systems & Applications Attack

- **Operating Systems (os): Popular Targets**
- **Applications:**
 - **Shadow IT:** Hidden applications increase the attack surface and risk.
 - **Web Applications:** Ubiquitous and often targeted due to vulnerabilities in code or configuration.
 - **Mobile Apps:** Increasingly used for business, making them a growing target.
 - **Unsecured Files:** Sensitive data stored in shared folders or cloud services is at risk.
 - **Databases:** Can contain valuable information and may have exploitable vulnerabilities.



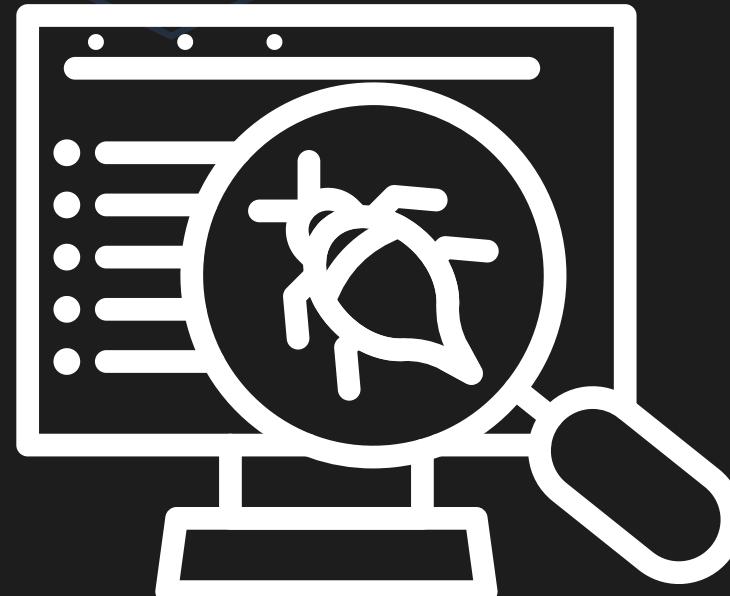
Principles of Ethical Hacking: The Right Way to Test

- **Work Ethically:**
- **Respect Privacy:**
 - Treat all information gathered with the utmost confidentiality.
 - Avoid snooping into unrelated corporate or personal data.
 - Implement peer review or oversight for increased transparency and trust.
- **Avoid System Disruption:** Don't crash the systems you're trying to protect.



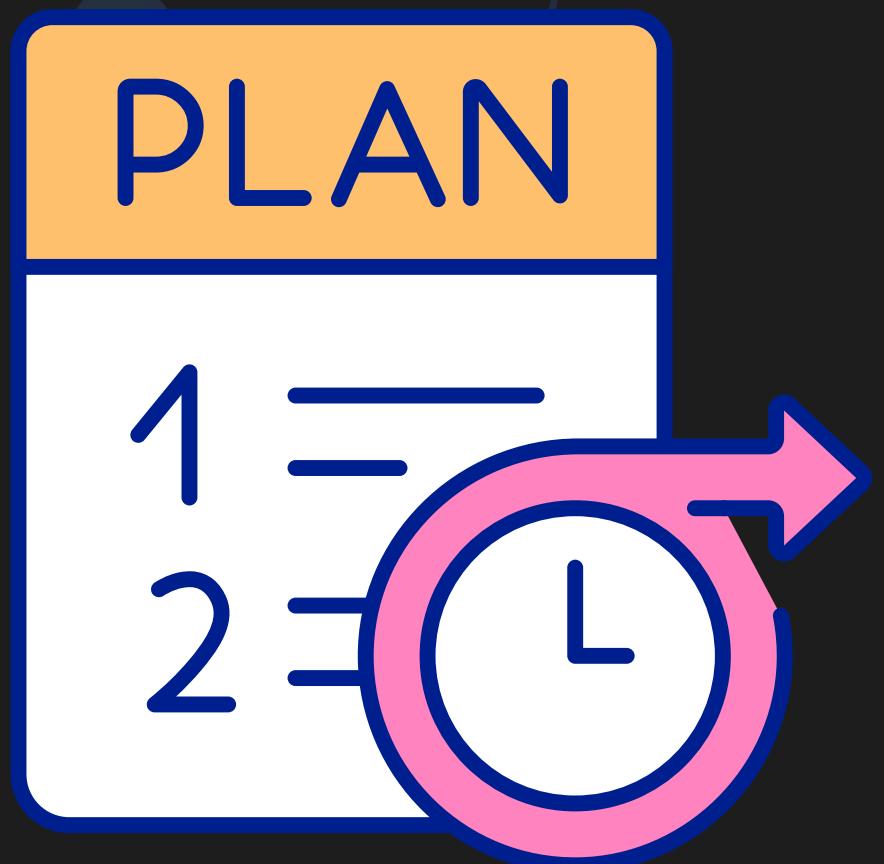
Embarking on the V&P Testing Journey

- **The Importance of Planning:**
- **The Reformed Hacker Question: (Should we hire a hacker?)**
 - **Potential Benefits:** Deep expertise, insights into attacker mindset.
 - **Risks:** Trustworthiness concerns, potential for misuse of information.
 - **Questions to Consider:**
 - Do you want to reward past malicious behavior?
 - Can you trust the individual's reformation?
 - How will you protect sensitive information?
 - **Decision:** Weigh the risks and benefits carefully before making a decision.



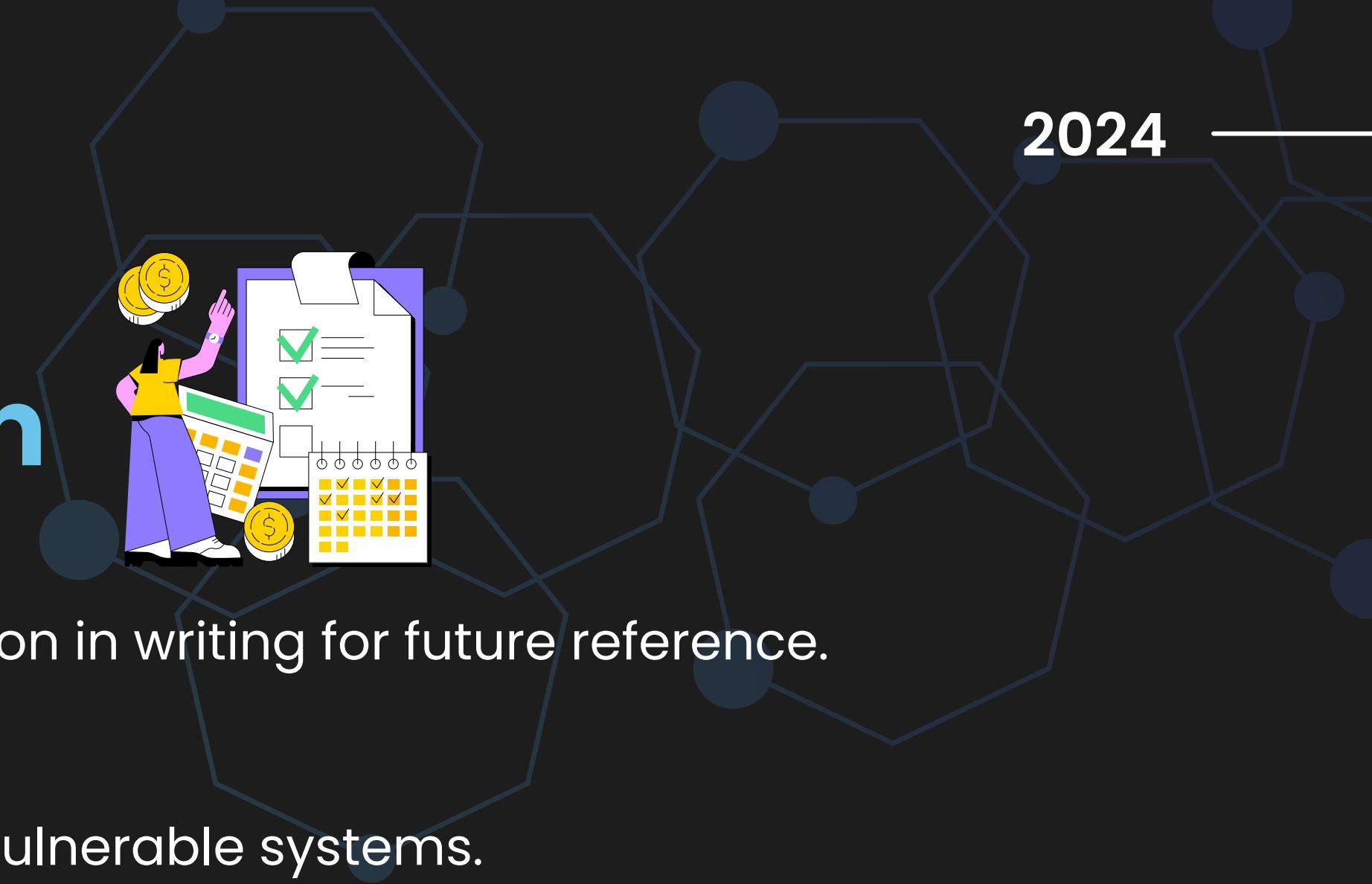
Vulnerability and Penetration Testing Process

- Formulating your plan
- Selecting tools
- Executing the plan
- Evaluating results
- Moving on





Formulating your plan



- **Obtain approval:** Document the authorization in writing for future reference.
- **Define the scope**
 - **Specific Systems:** Prioritize critical and vulnerable systems.
 - **Risks:** Have a contingency plan for potential disruptions or downtime.
 - **Timeline:** Determine optimal testing times to minimize business impact.
- **Other consideration: Detection, Security Control, System Knowledge, Major vulnerabilities response**
 - **Deliverables:** Define the reports and documentation to be provided upon completion.

Selecting Tools

- **The Right Tool for the Job**
- **Understand Your Tools**
 - Many tools have a learning curve and may generate false positives or negatives.
 - Familiarize yourself with the tools' documentation, user guides, and tutorials.
 - Practice using the tools in a lab or test environment.
- **Look for this features**
 - Industry acceptance and regular updates
 - Detailed vulnerability reports with remediation guidance
 - High-level reports for management or non-technical audiences



Executing the plan

- **Gather Intelligence (Reconnaissance):**
 - **External:** Search the internet for information about your organization, systems, and IP addresses.
 - **Internal:** Conduct casual assessments to gain initial insights into systems and potential vulnerabilities.
- **Narrow Your Focus:**
 - Target the specific systems identified in your plan.
 - Start with broad scans and gradually move towards more detailed tests.
- **Execute Attacks and Exploits:**
 - If authorized, attempt to exploit identified vulnerabilities to assess their real-world impact.
 - Proceed with caution and ensure you have a clear understanding of potential consequences.

Evaluating results

- **Assess Your Results:**
 - Analyze the vulnerabilities discovered during testing.
 - Prioritize based on severity and potential impact.
- **Knowledge is Power:** With experience, you'll gain deeper insights into your systems' weaknesses.
- **Report to Management/Client:**
 - Provide a formal, detailed report outlining:
 - Identified vulnerabilities
 - Severity assessment
 - Recommended remediation steps
 - Keep stakeholders informed to demonstrate the value of your work and maintain transparency.

Moving On

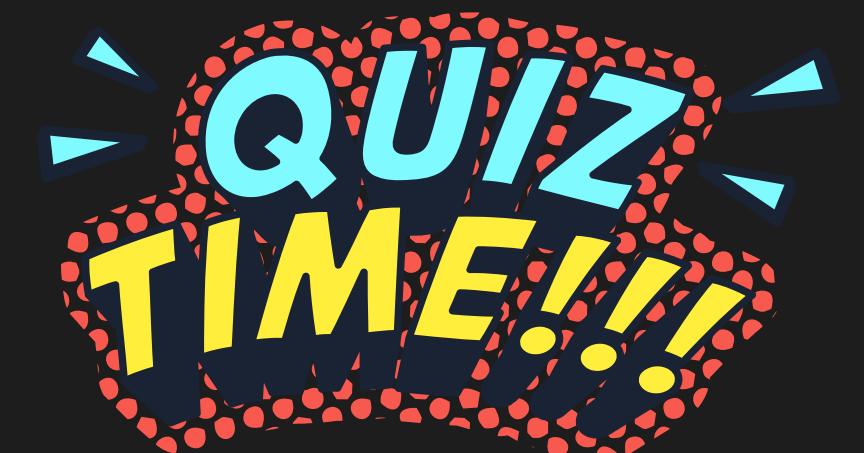
- **Implement Recommendations:**
 - Security testing is just the first step. Take action to remediate the identified vulnerabilities.
 - Prioritize fixes based on the severity and potential impact of each issue.
 - Track and document progress for accountability and future reference.
- **Stay Vigilant:**
- **Adapt to Change:**
 - New systems, software updates, and patches can introduce new vulnerabilities.
 - Reassess your security posture after significant changes to your environment.
 - Adjust your security strategy as needed to keep pace with evolving threats.

Question

What is the PRIMARY difference between ethical hacking

and malicious hacking?

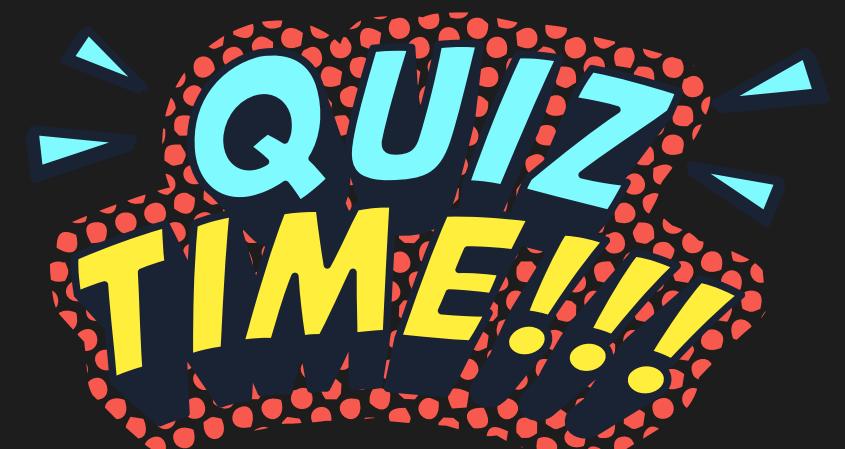
- (A) The tools and techniques used.
- (B) The level of technical skill required.
- (C) The target's permission and the intent behind the actions.
- (D) The potential financial gain for the hacker.



Question

Which of the following is NOT a common type of non-technical attack?

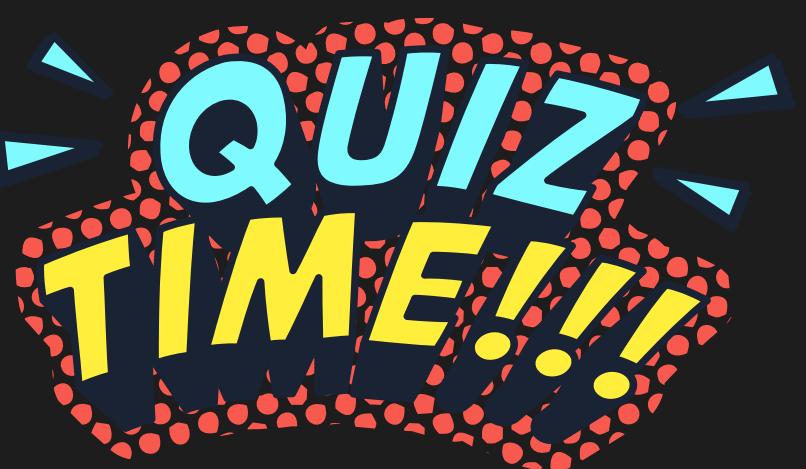
- (A) Phishing emails
- (B) Dumpster diving
- (C) SQL injection
- (D) Social engineering



Question

What is the main purpose of a security audit?

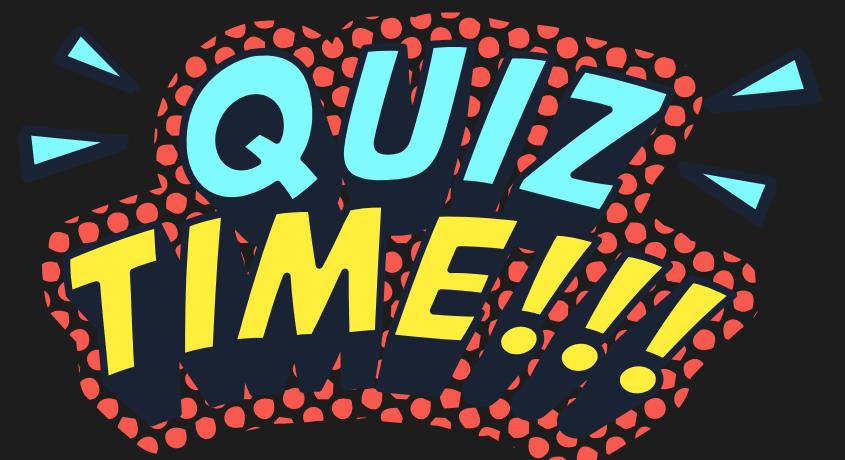
- (A) To find and exploit vulnerabilities in systems.
- (B) To simulate real-world attacks on a network.
- (C) To evaluate the effectiveness of existing security controls.
- (D) To validate compliance with security policies and regulations.



Question

When considering hiring a reformed hacker, which question is NOT a primary concern?

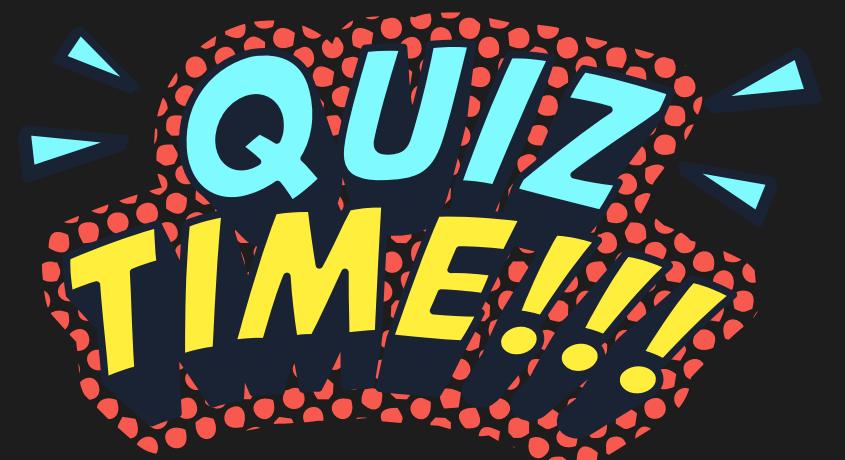
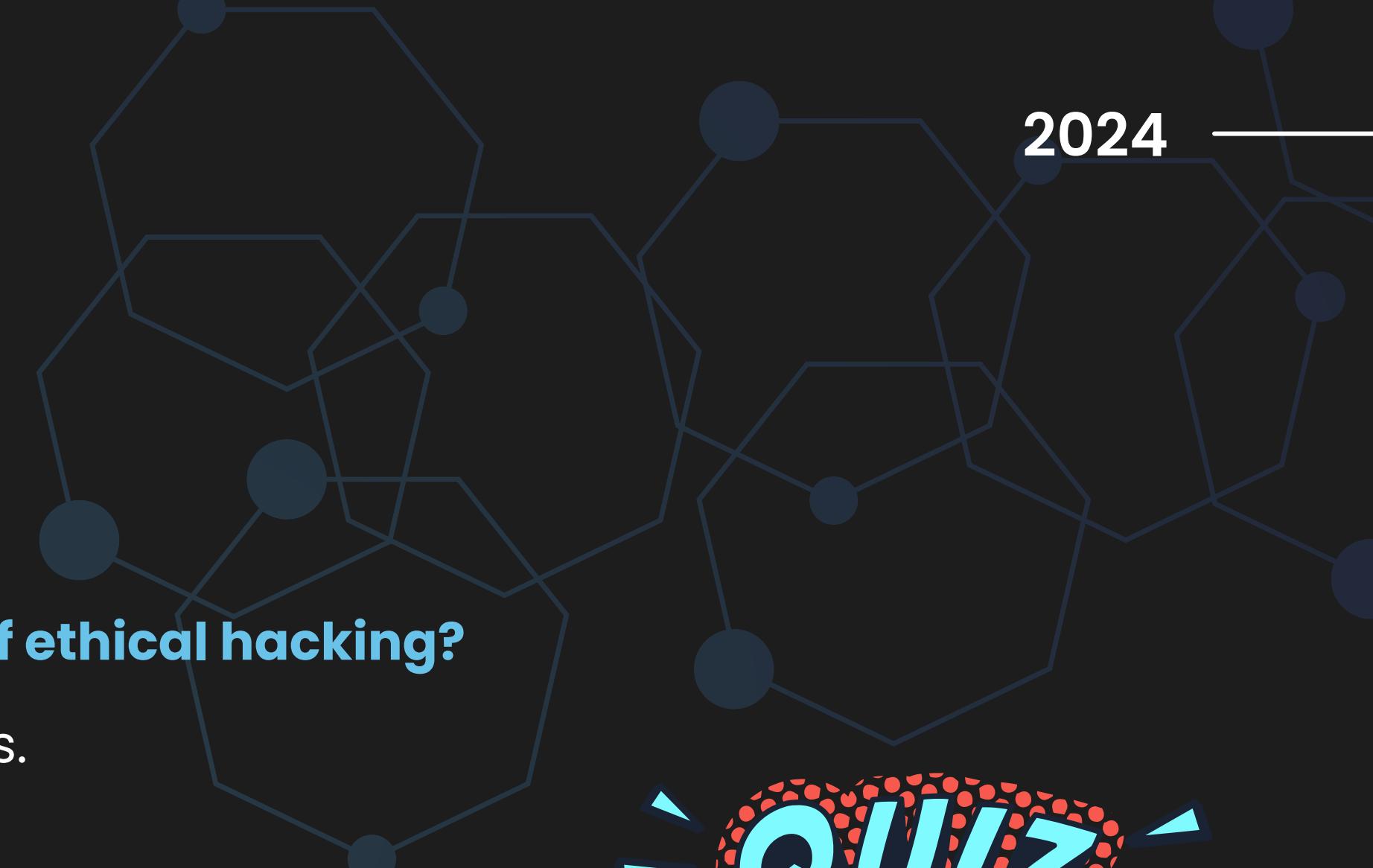
- (A) Do they have the technical skills to perform the job?
- (B) Do you want to reward past malicious behavior?
- (C) Can you trust the individual's reformation?
- (D) How will you protect sensitive information?



Question

Which of the following is NOT a key principle of ethical hacking?

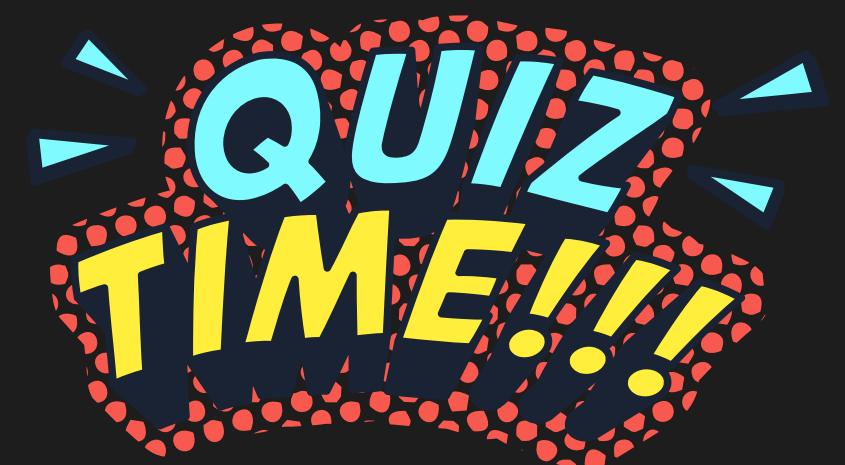
- (A) Work ethically and maintain trustworthiness.
- (B) Respect privacy and confidentiality.
- (C) Maximize disruption to test system resilience.
- (D) Avoid causing harm or damage to systems.



Question

What is the first step in formulating a vulnerability and penetration testing plan?

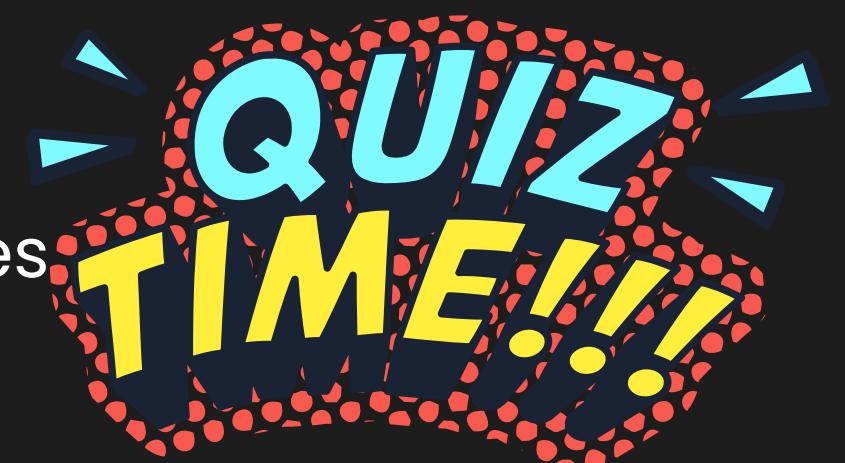
- (A) Selecting the right tools for the job.
- (B) Obtaining approval from stakeholders.
- (C) Defining the scope of the assessment.
- (D) Identifying potential vulnerabilities.



Question

Why is it important to perform reconnaissance before conducting a security assessment?

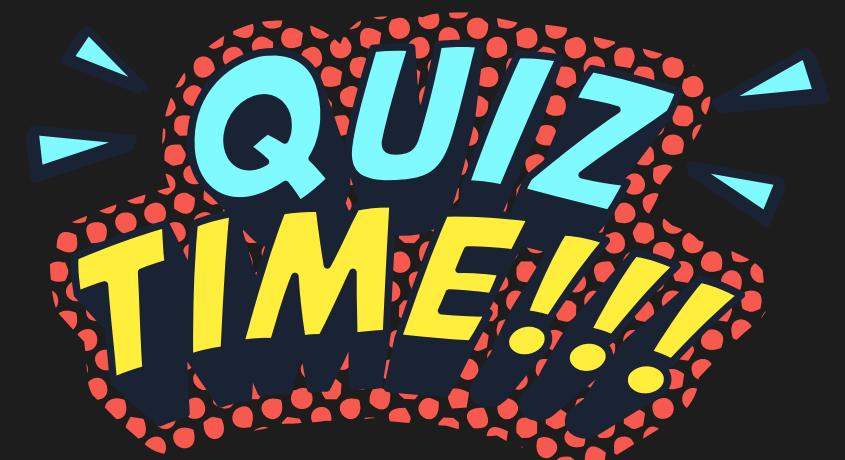
- (A) To identify potential targets for attack.
- (B) To gather information about the target's systems and vulnerabilities.
- (C) To test the effectiveness of existing security controls.
- (D) To determine the scope of the assessment.



Question

Which of the following is NOT a common type of network infrastructure attack?

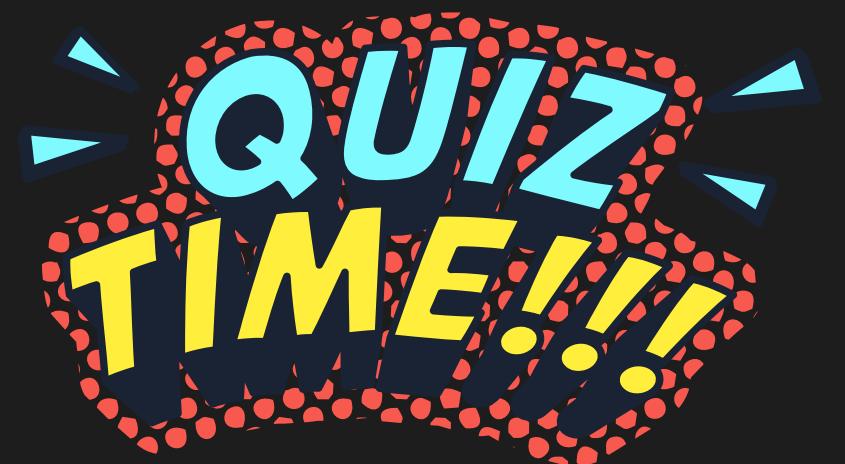
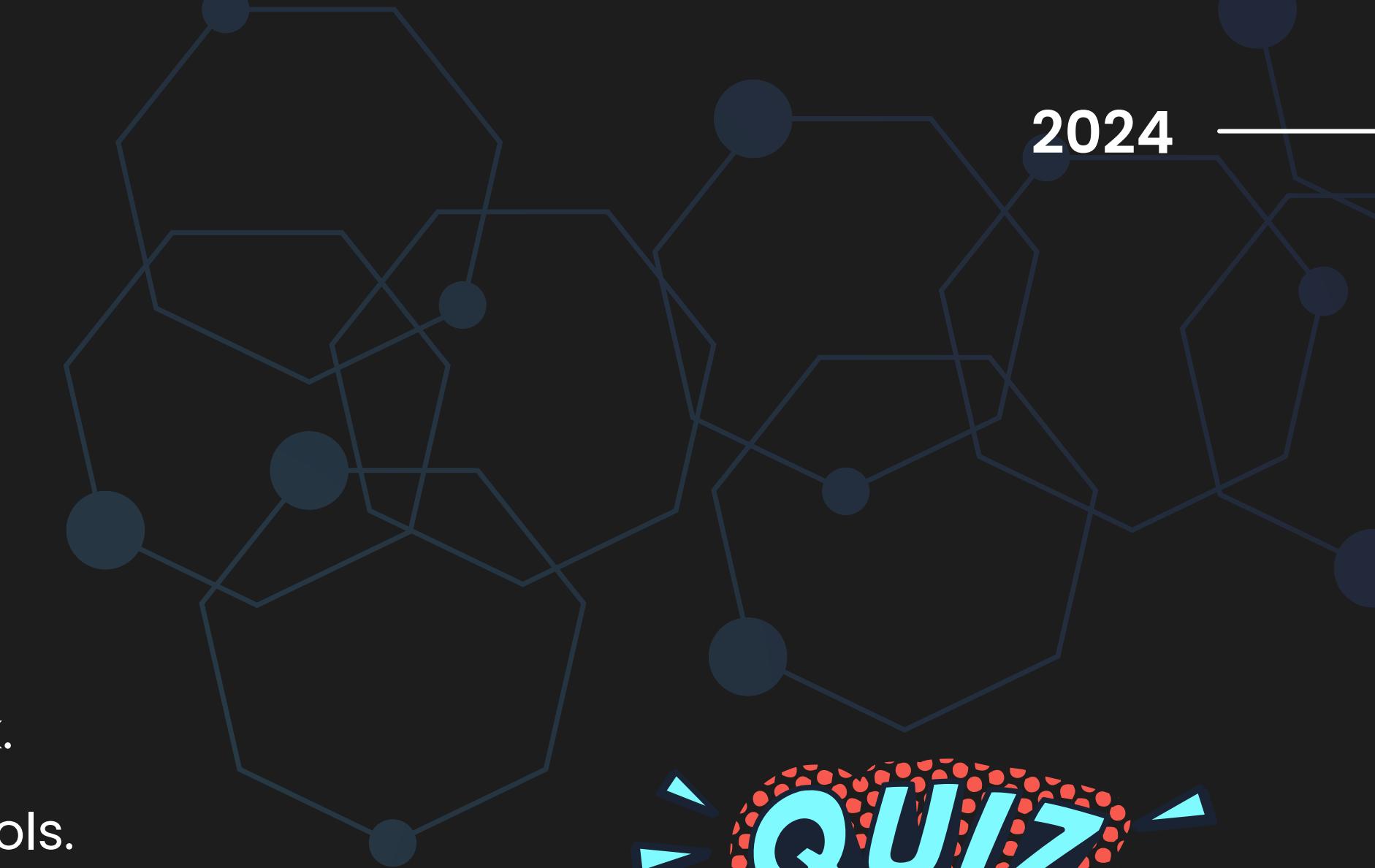
- (A) Unsecured wireless access
- (B) Protocol weaknesses (e.g., FTP, SSL)
- (C) Denial of Service (Dos) attacks
- (D) Social engineering



Question

What is shadow IT?

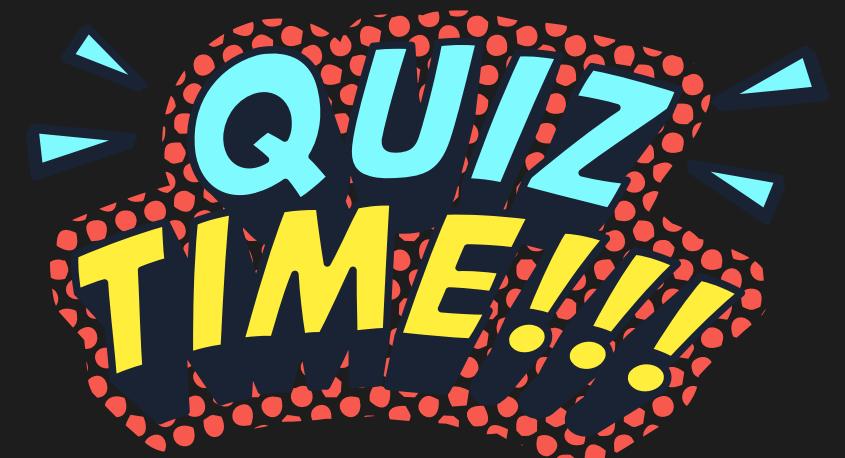
- (A) A type of malware that hides on a network.
- (B) A technique used to bypass security controls.
- (C) The use of unauthorized applications or devices within an organization.
- (D) A method for testing security vulnerabilities.



Question

Why is it essential to keep security tools updated?

- (A) To ensure compatibility with the latest operating systems.
- (B) To take advantage of new features and functionalities.
- (C) To address newly discovered vulnerabilities and exploits.
- (D) All of the above



Understanding Your **Adversary**

- **The Changing Face of Hacking**
- **The Hacker Mindset**
- **The Insider Threat**
- **The Dual Role of Hackers**
 - Hackers drive technological advancement by uncovering vulnerabilities and pushing the boundaries of security.
 - They also pose a constant threat, requiring organizations to stay vigilant and adapt their defenses.



The Hacker's Arsenal

The Hacker tactic

- **Technical Evasion**
 - Changing MAC or IP addresses to avoid intrusion detection.
 - Exploiting vulnerabilities in web pages and login mechanisms.
 - Altering default ports to bypass firewall restrictions.
- **Physical Exploitation:**
 - Targeting offices that are temporarily unoccupied.
 - Disabling security cameras monitoring sensitive areas.



The Hacker's Arsenal

The Hacker tactic

- **Social Engineering:**
 - Using fake Wi-Fi hotspots (evil twins) to lure unsuspecting users.
 - Taking advantage of trusting colleagues' credentials.
- **Network Attacks:**
 - Performing SQL injection or password cracking attacks through anonymous networks.



the Hacker's Motives: What Drives the Attack?

- Thrill and Challenge
- Notoriety and Recognition
- Ideology and Activism
- Financial Gain
- Revenge and Malice



WHY?

Hacker Tactics & Timing

- **Attack Styles Vary:**
 - **Methodical Hackers:** Carefully plan and gather information before executing their attacks.
 - **Impulsive Hackers:** Act rashly, often making mistakes that lead to their discovery.
 - **Malicious Insiders:** Range from sophisticated to opportunistic, exploiting access to sensitive information.





Hacker Tactics & Timing

- **The Hacker's Advantage: Time and Anonymity**
 - **Time:** Attacks can be carried out slowly and deliberately, often after business hours when defenses are weaker.
 - **Anonymity:** The internet and lack of effective monitoring provide cover for attackers.



Hacker Tactics & Timing

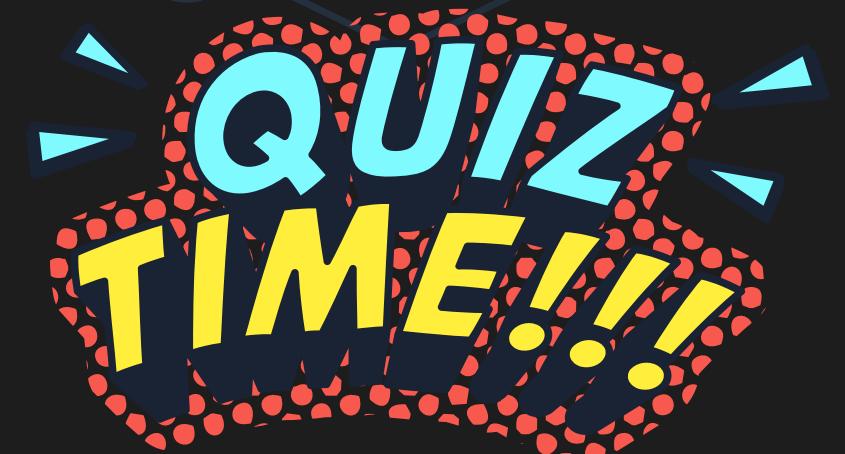
- **Prey on Ignorance:** Exploit the lack of proper system management, patch management, and awareness among administrators.
- **Exploit Complexity:** Take advantage of the increasing complexity of networks, cloud services, and mobile devices.
- **Leverage Anonymity:** Use tools and techniques to mask their identity and location.



Question

Which of the following is NOT a typical motivation for malicious hackers?

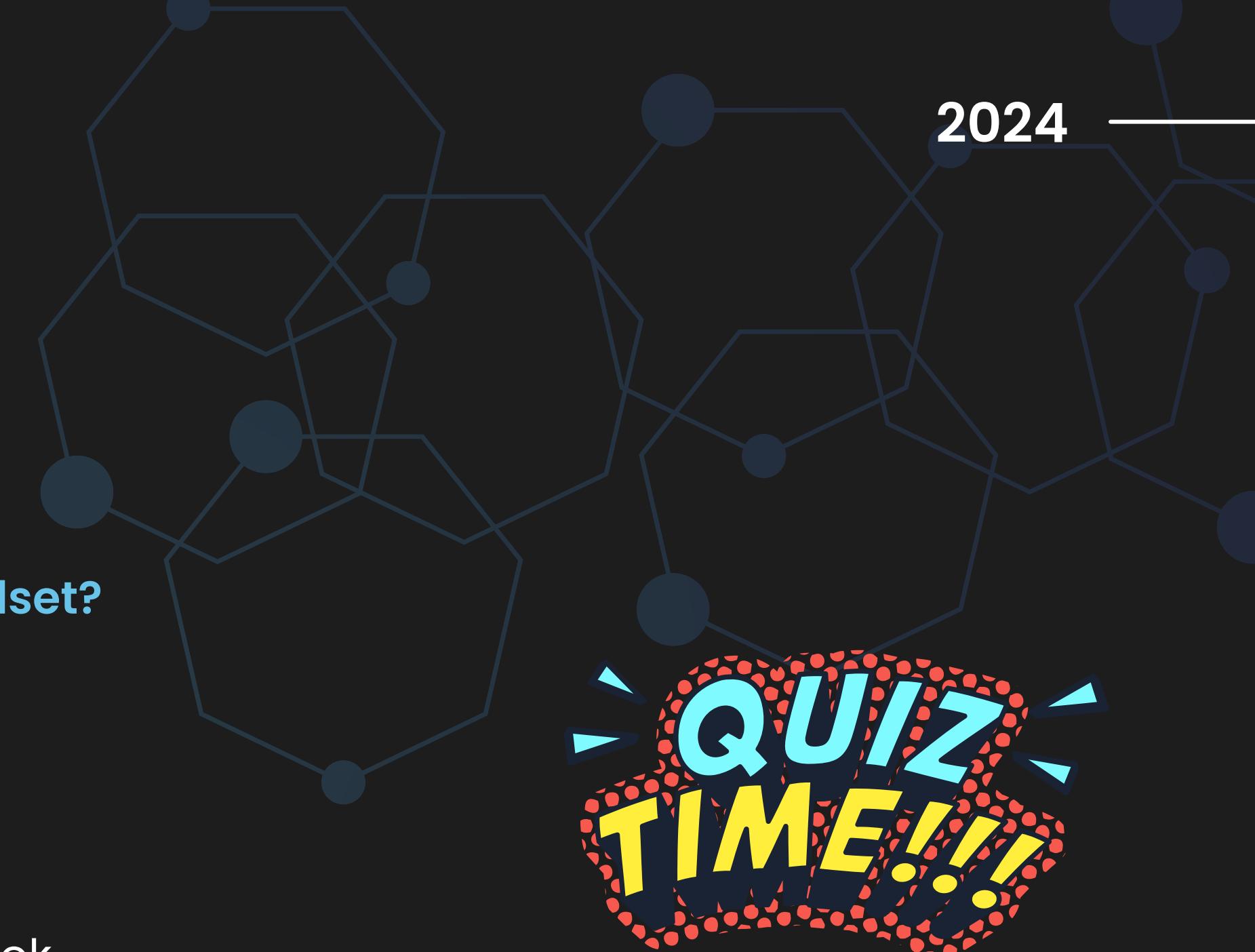
- A. Financial gain
- B. Notoriety and recognition
- C. Desire to improve system security
- D. Boredom or curiosity



Question

What is a common characteristic of the hacker mindset?

- A. A strong desire to follow rules and regulations.
- B. An aversion to risk and challenges.
- C. A preference for teamwork and collaboration.
- D. Curiosity and a tendency to see what others overlook.

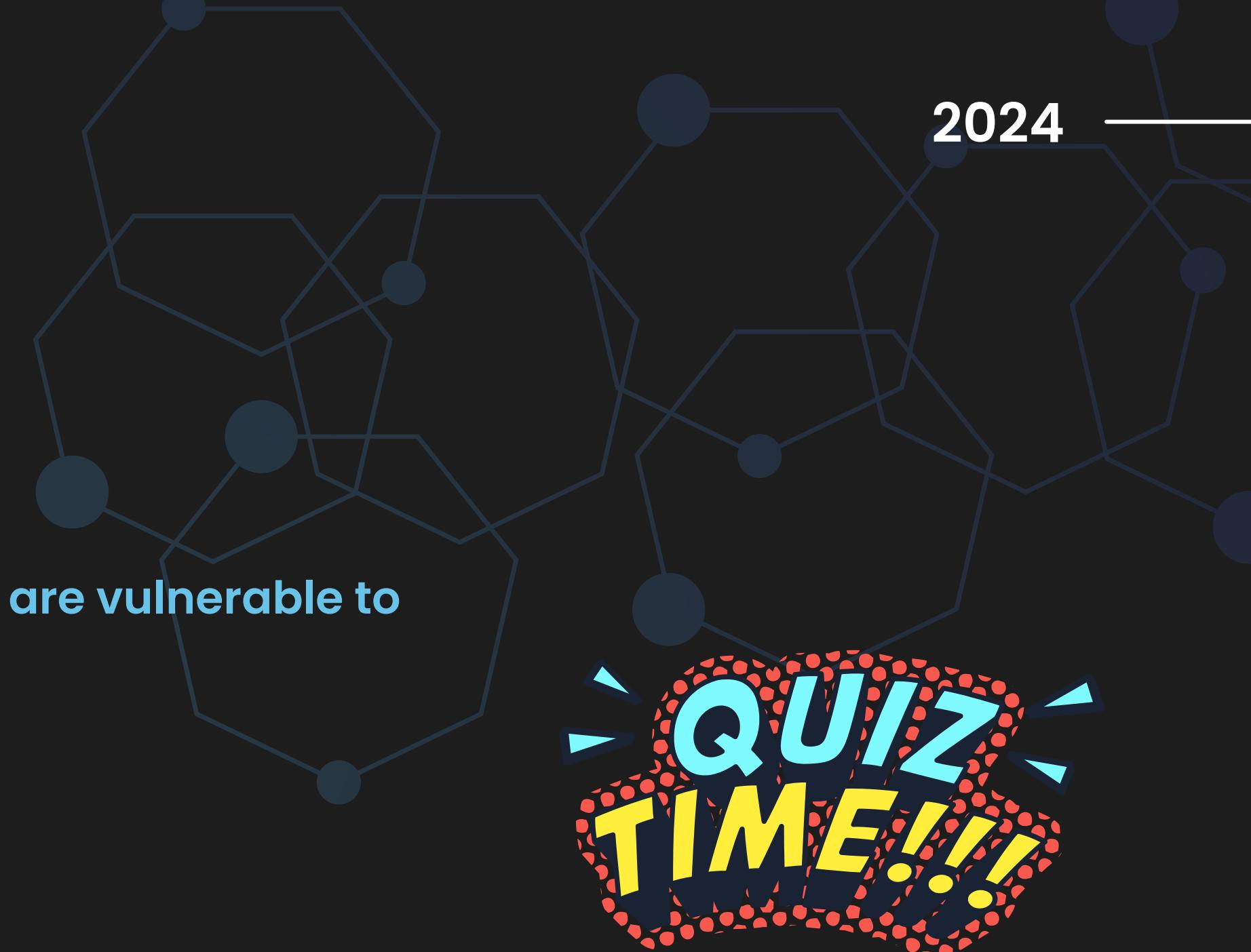




Question

What is the primary reason why many organizations are vulnerable to attacks?

- A. The high cost of security tools and software.
- B. The lack of awareness about cybersecurity threats.
- C. The increasing complexity of information systems.
- D. The widespread use of outdated technology.





Question

What is the term for unauthorized applications or devices used within an organization?

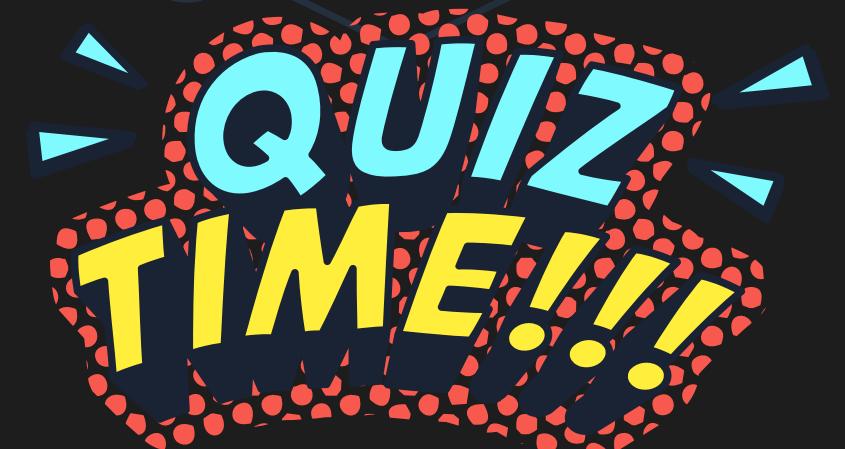
- A. Ransomware
- B. Shadow IT
- C. Malware
- D. Phishing

**QUIZ
TIME!!!**

Question

Which of the following is NOT a tactic used by malicious hackers to evade detection?

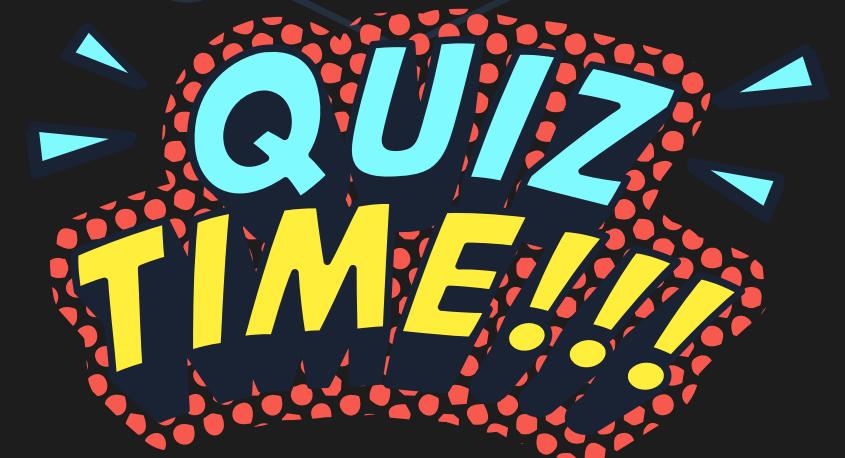
- A. Changing MAC or IP addresses
- B. Regularly patching and updating systems
- C. Exploiting vulnerabilities in web applications
- D. Altering default ports to bypass firewalls



Question

Why is time often considered an attacker's friend?

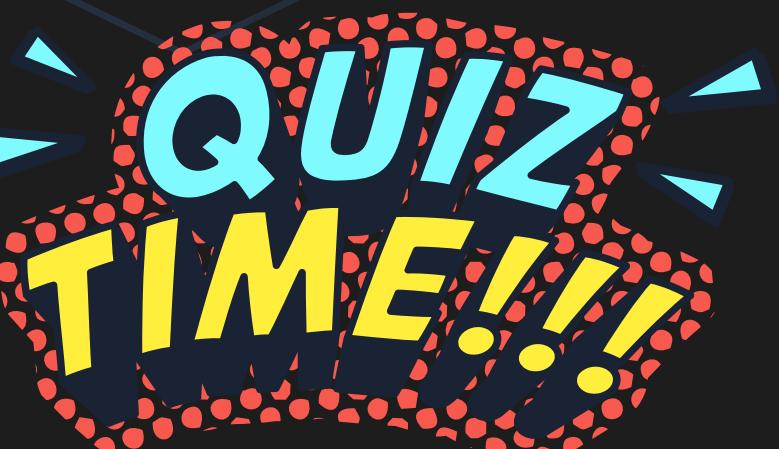
- A. They can plan and execute attacks at their convenience.
- B. They can remain anonymous while conducting their activities.
- C. They can slowly probe systems over time, making detection difficult.
- D. All



Question

What is the main difference between a malicious hacker and a malicious insider?

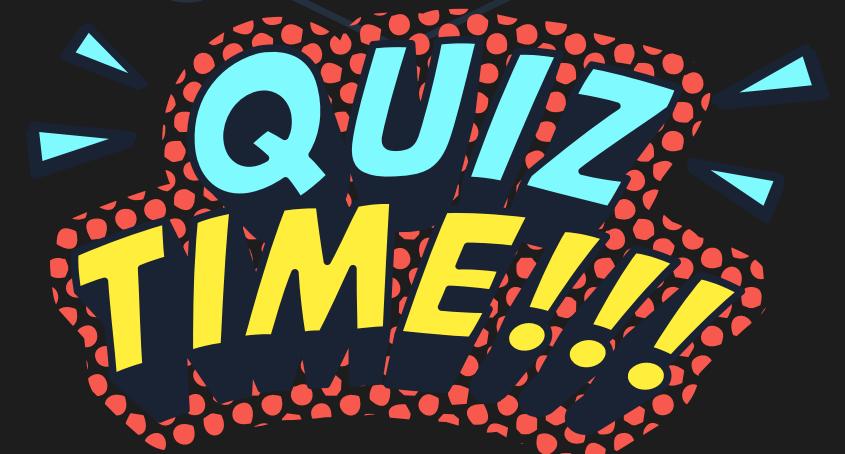
- A. A malicious hacker operates from outside the organization, while a malicious insider works within the organization.
- B. A malicious hacker uses technical skills, while a malicious insider relies on social engineering.
- C. A malicious hacker is motivated by financial gain, while a malicious insider seeks revenge.
- D. There is no difference; they are interchangeable terms.



Question

How can organizations mitigate the risk of insider threats?

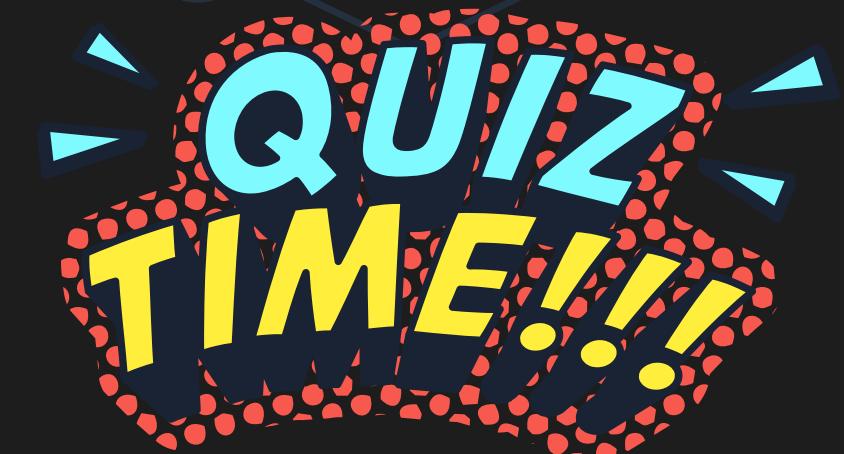
- A. Implement strict access controls and least privilege principles.
- B. Conduct regular security awareness training for employees.
- C. Monitor user activity and investigate anomalies.
- D. All of the above.



Question

What is the ultimate goal of understanding the hacker mindset?

- A. To become a hacker oneself.
- B. To predict and prevent future attacks.
- C. To develop more sophisticated hacking tools.
- D. To infiltrate hacker communities.



Question

Which of the following best describes a "defense-in-depth" approach to security?

- A. Relying solely on a single, powerful security tool.
- B. Leaving all security controls disabled during testing to find more vulnerabilities.
- C. Implementing multiple layers of security measures to protect against a variety of threats.
- D. Focusing exclusively on technical vulnerabilities while ignoring social engineering.

