# Security Fundamental – Practice Exam Questions

1. **You are called by a person who is identifying as IT support and wants to follow up on an** **account compromise. You are asked to verify your user ID and password to validate the compromise. What specific type of attack is attempted?**
   1. Spear phishing
   2. **Vishing**
   3. Phishing
   4. Replication
2. **Which of the following are specifically used to spread influence, alter perceptions, and sway people toward a position favoured by those spreading it?**
   1. Identity fraud, invoice scams, credential harvesting
   2. Hoaxes, eliciting information, urgency
   3. **Influence campaigns, social media, hybrid warfare**
   4. Authority, intimidation, consensus
3. **Several computers in your organization are displaying a red screen with the message “Your files have been encrypted. You have to pay 100 bitcoin to**

**recover them.” These desktops have most likely been affected by what type of malware?**

* 1. Spyware
  2. Spraying
  3. **Ransomware**
  4. Crypto-malware

1. **When an attacker captures network traffic and retransmits it at a later time, what type of attack are they attempting?**
   1. Denial-of-service attack
   2. **Replay attack**
   3. Bluejacking attack
   4. Man in the middle attack
2. **You’re testing a web application and type a number in a text field. The application returns an error message containing filenames and the path of the application. This is an example of which of the following?**
   1. Resource exhaustion
   2. **Improper error handling**
   3. Generic error message
   4. Common misconfiguration
3. **While examining a laptop infected with malware, you notice the malware loads on startup and also loads a file called apputilities.dll each time Microsoft Word is opened. This is an example of which of the following?**
   1. Race condition
   2. **DLL injection**
   3. System infection
   4. Memory overflow
4. **A user reports “odd” certificate warnings on her web browser this morning whenever she visits Google. Looking at her browser, you see these certificate warnings. Looking at the network traffic, you notice that all HTTP and HTTPS requests from that system are being routed to the same IP regardless of destination. Which of the following attack types are you seeing in this case?**
   1. Evil twin
   2. **Man in the middle**
   3. Disassociation
   4. MAC cloning
5. **All of the wireless users on the third floor of your building are reporting issues with the network. Every 15 minutes, their devices disconnect from the network. Within a minute or so they are able to reconnect. What type of attack is most likely underway in this situation?**
   1. Evil twin
   2. Jamming
   3. Domain hijacking
   4. **Disassociation**
6. **Proper use of separation of duties with respect to privileged users on your systems is** **a defense against which type of hacker?**
   1. Nation-state actor
   2. **Insider**
   3. Criminal syndicate
   4. All of the above
7. **You use a “golden disk” to provision new machines from your vendors. As part of the incident response, you have discovered that the source of the malware you are seeing comes from this golden disk. This is an example of what vector?**
   1. Insider
   2. Direct access
   3. Removeable media
   4. **Supply chain**
8. **Understanding how an attacker operates so that you can develop a defensive posture is done through the use of which of the following?**
   1. Predictive analysis
   2. **TTPs**
   3. Threat maps
   4. Automated Indicator Sharing
9. **Common sources of vulnerability issues for systems include which of the following?**

**(Choose all that apply.)**

* 1. **Weak patch management**
  2. Data loss
  3. Identity theft
  4. **Weak configurations**

1. **What type of threat exploits system and application vulnerabilities that are unknown** **to software developers and even anti-malware manufacturers?**
   1. An on-premises attack
   2. **A zero-day attack**
   3. A cloud-based attack
   4. A legacy platform attack
2. **Who assumes the risk associated with a system or product after it has entered EOL** **status?**
   1. The original manufacturer
   2. The vendor
   3. **The organization**
   4. The supply chain manager
3. **Anti-malware software fails to detect a ransomware attack that is supposed to be** **within its capabilities of detecting. What is this an example of?**
   1. **False negative**
   2. False positive
   3. Measurement error
   4. Analysis failure
4. **Which of the following is NOT associated typically with SIEM processes?**
   1. **Applications**
   2. Syslog
   3. Log capture
   4. Log aggregation
5. **Which of the following are NOT typically scanned during a vulnerability scan?**
   1. **End users**
   2. Network
   3. Applications
   4. Web applications
6. **What is the most important first step in a penetration test?**
   1. OSINT
   2. **Rules of engagement**
   3. Reconnaissance
   4. Privilege escalation
7. **Which of the following is not a state of data in the enterprise?**
   1. At rest
   2. **In storage**
   3. In processing
   4. In transit/motion
8. **Which of the following can provide complete traceability to an original transaction** **without revealing any personal information if disclosed to an outside party?**
   1. **Tokenization**
   2. Data sovereignty
   3. Rights management
   4. Baseline configuration
9. **A system that is ready for immediate use in the event of an outage is called what?**
   1. Standby system
   2. Disaster recovery site
   3. Backup site
   4. **Hot site**
10. **Which of the following is important to consider when specifically examining** **configuration management?**
    1. Data loss prevention
    2. **Standard naming conventions**
    3. Rights management
    4. Hashing
11. **What is masking?**
    1. The use of stand-in data to replace real-time data
    2. The marking of regions where data is not allowed by policy
    3. The use of backups to preserve data during disruptive events
    4. **Redacting portions of data using a covering symbol such as \* or x**
12. **How does a hypervisor enable multiple guest operating systems to run concurrently** **on a host computer?**
    1. Via a specialized driver package
    2. **By abstracting the hardware from the guest operating system**
    3. By providing specific virtual hardware to each guest OS
    4. By hiding the underlying Linux operating system
13. **Your new application has multiple small processes that provide services to the** **network. You want to make this application run more efficiently by virtualizing it.** **What is the best approach for virtualization of this application?**
    1. Type II hypervisor
    2. Linux KVM
    3. **Containerisation**
    4. Type I hypervisor
14. **Problems in which phase will specifically stop continuous deployment but not necessarily continuous delivery?**
    1. **Continuous integration**
    2. Continuous monitoring
    3. Continuous validation
    4. Continuous development
15. **Which of the following algorithms uses a secret key with a current timestamp to generate a one-time password?**
    1. Hash-based Message Authentication Code
    2. Date-Hashed Message Authorization Password
    3. **Time-based One-Time Password**
    4. Single sign-on
16. **To ensure customers entering credentials in your website are valid and not someone with stolen credentials, your team is tasked with designing multifactor authentication. Which of the following would NOT be a good choice?**
    1. **Static code**
    2. Phone call
    3. Authentication application
    4. Short Message Service
17. **Which backup strategy includes only the files and software that have changed since** **the last full backup?**
    1. **Incremental**
    2. Full
    3. Snapshot
    4. Differential
18. **When discussing location for storage of backups, which of the following statements** **are true?**

**(Choose all that apply.)**

* 1. **The most recent copy should be stored offsite, as it is the one that is most** **current and is thus the most valuable.**
  2. Offsite storage is generally not necessary, except in cases where the possibility of a break-in at the main facility is high.
  3. **Offsite storage is a good idea so that you don’t lose your backup to the same** **event that caused you to lose your operational data and thus need the backup.**
  4. The most recent copy can be stored locally, as it is the most likely to be needed, while other copies can be kept at other locations.