GOMYCODE Security+ MCQ - Ch02

Total des points 40/40

L'adresse e-mail du répondant (**anisnasri322@gmail.com**) a été enregistrée lors de l'envoi de ce formulaire.

✓ A public web service becomes unavailable due to a large volume of spoofed UDP requests causing responses to be amplified toward the target. Which of the following attacks is MOST likely occurring? *1/1

○ SYN flooding

○ Smurf attack

● Reflection/amplification DDoS ✓

○ Rogue DHCP

✓ A threat actor avoids dropping new binaries by using built-in tools like PowerShell and WMI to execute commands and move laterally. Which of the following BEST describes this approach? *1/1

● Living off the land ✓

○ Typosquatting

○ Evil twin

○ Supply chain compromise

✓ A rapidly spreading malware uses SMB to propagate laterally across multiple subnets. Which of the following is the BEST mitigation to reduce spread? *1/1

○ Allow inbound SMB from the internet for updates

○ Enable anonymous shares to reduce authentication failures

● Network segmentation and disabling legacy protocols such as SMBv1 where possible ✓

○ Move all servers to a single flat VLAN

✓ A cloud storage bucket containing internal documents is discovered to be publicly readable. Which of the following is the BEST immediate remediation? *1/1

● Block public access and restrict access via IAM least privilege ✓

○ Enable public access and rely on obscurity

○ Increase storage size to reduce errors

○ Rotate TLS certificates on endpoints

✓ A company notices users are being lured to a look-alike domain that differs by one character from the legitimate domain. Which of the following risks is MOST likely involved? *1/1

○ Domain fronting

○ DNSSEC validation

○ Certificate pinning failure

● Typosquatting ✓

✓ A vulnerability scanner reports many high-severity findings on a set of servers, but the administrator suspects false positives due to limited visibility. Which of the following actions would BEST improve accuracy? *1/1

○ Rely only on open-source intelligence

○ Increase scan speed to finish faster

● Run an authenticated (credentialed) vulnerability scan ✓

○ Disable the scanner to reduce noise

✓ Users consent to a third-party application that requests access to their cloud email and files. Shortly after, their mailboxes are accessed by an attacker without triggering password-based login alerts. Which of the following attacks is MOST likely? *1/1

○ Pass-the-ticket

● OAuth consent phishing ✓

○ Smishing

○ Watering hole attack

✓ An attacker uses a list of usernames and previously leaked passwords to attempt logins across many accounts on a cloud service. Which of the following attacks is occurring? *1/1

○ Password spraying

○ On-path attack

● Credential stuffing ✓

○ Rainbow table attack

✓ A server shows repeated login attempts against a single account with many different passwords per minute. Which of the following attacks is MOST likely? *1/1

○ Credential stuffing

● Online brute-force attack against one account ✓

○ Typosquatting

○ Password spraying

✓ An attacker requests ../../../../etc/passwd through a file-download endpoint and the server returns the file contents. Which of the following vulnerabilities is being exploited? *1/1

○ Command injection

● Directory traversal ✓

○ Buffer overflow

○ Race condition

✓ A user is logged into a banking site. When visiting a malicious site, the user's browser sends an unauthorized funds-transfer request to the bank using the existing session. Which of the following mitigations is BEST? *1/1

● Implement anti-CSRF tokens ✓

○ Use database encryption

○ Enable SMTP signing

○ Disable cookies

✓ A security audit finds several systems have outdated UEFI firmware and Secure Boot is disabled, increasing risk of boot-level malware. Which of the following is the BEST mitigation? *1/1

● Update firmware and enable Secure Boot with trusted keys ✓

○ Move the systems to a guest network only

○ Allow unsigned bootloaders for flexibility

○ Disable patching to reduce change risk

✓ An organization suspects an insider is copying sensitive files to removable media. Which of the following controls would BEST mitigate this? *1/1

● Disable USB mass storage and enforce endpoint DLP policies ✓

○ Enable WEP on wireless networks

○ Increase mailbox quotas

○ Disable DHCP on the LAN

✓ A forum application stores user comments and later displays them to other users. A malicious comment executes JavaScript in victims' browsers. Which of the following vulnerabilities is MOST likely present? *1/1

○ SQL injection

○ Directory traversal

○ CSRF

● Stored XSS ✓

✓ Accounts payable receives an email from the CEO requesting an urgent change to bank account details for a vendor payment. Which of the following is the BEST next step to reduce the likelihood of fraud? *1/1

○ Reply to the email asking for confirmation

○ Forward the email to all staff for awareness

○ Proceed because the sender address matches the CEO

● Verify the request using an out-of-band method with known contact information ✓

✓ A company wants to reduce risk from vulnerable third-party libraries used in internal applications. Which of the following practices is MOST effective? *1/1

○ Using only HTTP for internal apps

○ Disabling code reviews

● Software composition analysis and dependency patching as part of secure SDLC ✓

○ Allowing developers to install any package without tracking

✓ A web application's CORS policy allows any origin and also allows credentials. Which of the following is the BEST fix? *1/1

● Restrict allowed origins to trusted domains and avoid allowing credentials broadly ✓

○ Set Access-Control-Allow-Origin to '*' and keep credentials enabled

○ Move the application behind NAT only

○ Disable TLS to simplify browser behavior

✓ A network admin suspects ARP spoofing is occurring on a switched LAN. Which of the following controls would BEST help prevent this? *1/1

○ Port mirroring on all switches

○ Disable IPv6 on endpoints

● Dynamic ARP inspection with DHCP snooping ✓

○ Enable Telnet for switch management

✓ A security analyst notices periodic outbound DNS queries to many unique, high-entropy subdomains of a single external domain. The queries occur even when users are idle. Which of the following is the MOST likely technique being used? *1/1

○ DNS cache poisoning

● DNS tunneling ✓

○ ARP spoofing

○ Domain hijacking

✓ A critical vulnerability is actively exploited, but the vendor has not released a patch yet. Which of the following compensating controls is MOST appropriate to implement immediately for a web-facing application? *1/1

○ Disable all user accounts permanently

● WAF rules or IPS signatures to block exploit patterns (virtual patching) ✓

○ Uninstall the operating system

○ Increase DHCP lease time

✓ A vendor distributes a software update that is later found to contain malicious code introduced before release. Which of the following controls would BEST help detect or prevent unauthorized updates? *1/1

● Code signing and signature verification ✓

○ MAC address filtering

○ Screen locking policies

○ Network time synchronization

✓ A developer uses serialized objects received from clients, and an attacker crafts a payload that results in remote code execution during deserialization. Which of the following mitigations is BEST? *1/1

○ Disable DNS on the server

● Avoid deserializing untrusted data and use allowlisting/signed objects ✓

○ Increase the server RAM

○ Use shorter session timeouts only

✓ A vulnerability is publicly disclosed and a vendor patch is available, but the organization has not yet applied it. Which of the following BEST describes this vulnerability status? *1/1

○ Unknown unknown

○ Logic bomb

○ Zero-day

● N-day ✓

✓ Security logs indicate large data transfers to an external site over HTTPS from a user workstation. Which of the following controls would BEST help prevent sensitive data exfiltration in this scenario? *1/1

○ Enable FTP over TLS

○ Disable VLANs

○ Replace all switches with hubs

● DLP with egress monitoring (including proxy/TLS inspection where permitted) ✓

✓ A developer wants to reduce the risk of session hijacking for users on untrusted Wi-Fi networks. Which of the following is the BEST web-application configuration to mitigate this? *1/1

○ Disable TLS and use HTTP for compatibility

● Enforce HSTS and set Secure and HttpOnly cookies ✓

○ Allow mixed content to reduce errors

○ Use FTP for session transport

✓ A security assessment finds multiple IoT devices still using default administrative credentials. Which of the following actions is the BEST immediate mitigation? *1/1

○ Disable logging to reduce storage usage

○ Enable SNMPv1 for easier monitoring

○ Move the devices to a public VLAN

● Enforce unique credential changes and disable default accounts ✓

✓ A security engineer wants to mitigate double-tagging VLAN hopping attacks. Which of the following switch configurations is BEST? *1/1

○ Enable all trunk ports and allow all VLANs

○ Set all access ports to trunk mode

● Disable unused ports and avoid using VLAN 1 as the native VLAN ✓

○ Allow DTP negotiation on all ports

✓ A security team receives a SHA-256 hash of a known malicious file from a threat intelligence feed. Which of the following is the BEST immediate use of this information? *1/1

○ Replace all user passwords with the hash

● Add the hash to endpoint/network blocklists and alert on matches ✓

○ Disable hashing algorithms on endpoints

○ Publish the hash on social media

✓ Employees report occasionally connecting to a Wi-Fi network with the correct SSID, but their traffic is intercepted and credentials are stolen. Which of the following attacks is MOST likely? *1/1

○ Wardriving

○ Replay attack

○ Bluejacking

● Evil twin ✓

✓ Users report receiving repeated MFA push notifications that they did not initiate. One user eventually approves a prompt to stop the interruptions, and the account is compromised. Which of the following attacks BEST describes this? *1/1

○ SIM swapping

○ Pass-the-hash

○ Kerberoasting

● MFA fatigue (push bombing) ✓

✓ A workstation begins trusting a new root certificate authority that was not deployed by IT. Soon after, security tools observe interception of TLS connections. Which of the following is the MOST likely issue? *1/1

○ Downgrade attack caused by weak ciphers

○ ARP inspection failure

● Malicious local root CA enabling TLS interception ✓

○ DNSSEC misconfiguration

✓ A DevOps team deploys container images that later are found to contain known vulnerable libraries. Which of the following practices would BEST reduce this risk before deployment? *1/1

○ Use only larger instance types

● Container image scanning in CI/CD and enforcing signed images ✓

○ Allow developers to bypass checks for speed

○ Disable version control hooks

✓ A company discovers employees are uploading sensitive files to personal cloud drives that are not approved by IT. Which of the following controls would BEST reduce this risk? *1/1

○ SIEM

○ HIDS

● CASB ✓

○ NAC

✓ A caller claims to be from IT and pressures an employee to share a one-time passcode to 'fix' an urgent account issue. Which of the following social engineering techniques is being used? *1/1

○ Dumpster diving

○ Shoulder surfing

○ Tailgating

● Pretexting ✓

✓ A web application allows a user-supplied URL that the server fetches to generate previews. An attacker uses it to access http://169.254.169.254/ and retrieve instance credentials. Which of the following vulnerabilities is being exploited? *1/1

○ CSRF

○ SQL injection

● SSRF ✓

○ XSS

✓ A penetration tester enters ' OR 1=1 -- into a login field and gains access without valid credentials. Which of the following mitigations would BEST address this issue? *1/1

○ Disable user accounts after login

● Parameterized queries (prepared statements) ✓

○ Input length restrictions only

○ Add more database indexes

✓ A help desk reports users are being redirected to a malicious site even when they type the correct URL. Investigation shows the resolver cache contains forged entries. Which of the following controls would BEST mitigate this? *1/1

● DNSSEC validation ✓

○ UPnP enablement

○ WPA3-Personal

○ Telnet hardening

✓ A SIEM alert shows thousands of failed login attempts using the SAME password across many different usernames over a short period. Which of the following attacks is MOST likely? *1/1

○ Credential stuffing

● Password spraying ✓

○ Brute-force attack

○ Dictionary attack against one user

✓ After a ransomware incident, management requires a strategy to ensure data can be restored even if online backups are encrypted. Which of the following is the BEST approach? *1/1

○ Disable patching to avoid downtime

○ Increase file permissions to reduce access errors

○ Store backups on the same network share as production data

● Implement immutable or offline backups and regularly test restores ✓

✓ A Linux server compromise is traced to a misconfigured sudoers file that allows a service account to run any command as root. Which of the following is the BEST mitigation? *1/1

○ Move the server to a wireless network

○ Disable all user accounts on the server

○ Turn off logging to reduce attacker visibility

● Implement least privilege and restrict sudoers entries to required commands ✓