Comptia Security+ Exam (SY0-601 German Version)

1. Ein Unternehmen erlebte kürzlich einen Angriff, bei dem seine Hauptwebsite auf den Webserver des Angreifers umgeleitet wurde, wodurch der Angreifer Anmeldeinformationen von ahnungslosen Kunden erbeuten konnte. Welche der folgenden Maßnahmen sollte das Unternehmen umsetzen, um diese Art von Angriffen in Zukunft zu verhindern?

A. IPsec

B. SSL/TLS

C. ONSSEC

D. LÄCHELN

Answer(s): B

---

2. Ein Sicherheitsadministrator untersucht die ARP-Tabelle eines Zugriffsschalters und sieht die folgende Ausgabe:

A. DDoSonFa02-Port

B. MAG-Überschwemmung am Fa0/2-Anschluss

C. ARP-Poisoning am Fa0/1-Port

D. DNS-Vergiftung auf Port Fa0/1

Answer(s): C

---

3. Ein Sicherheitsadministrator hat einen neuen Webserver installiert. Der Administrator hat dies getan, um die Kapazität für eine Anwendung zu erhöhen, da die Ressourcen auf einem anderen

Server erschöpft waren. Welchen der folgenden Algorithmen sollte der Administrator verwenden, um die Anzahl der Verbindungen auf jedem Server zu halbieren?

A. Gewichtete Antwort

B. Round-Robin

C. Geringste Verbindung

D. Gewichtete geringste Verbindung

Answer(s): B

---

4. Welches der folgenden Systeme umfasst am ehesten ein SCADA-System?

A. Smartwatch

B. Wi-Fi-fähiger Thermostat

C. Wasseraufbereitungsanlage

D. Überwachungssystem

Answer(s): C

---

5. Ein Ingenieur hat kürzlich eine Gruppe von 100 Webservern in einer Cloud-Umgebung bereitgestellt. Gemäß der Sicherheitsrichtlinie sollten alle Webserver-Ports außer 443 deaktiviert werden. Welche der folgenden Methoden können verwendet werden, um diese Aufgabe zu erfüllen?

A. Anwendungszulassungsliste

B. Load Balancer

C. Hostbasierte Firewall

D. VPN

Answer(s): C

---

6. Ein Mitarbeiter erhält eine Textnachricht, die offenbar von der Lohn- und Gehaltsabrechnung gesendet wurde und in der er um eine Überprüfung seiner Anmeldedaten bittet. Welche der folgenden Social-Engineering-Techniken werden versucht? (Wählen Sie zwei aus).

A. Fehlinformation

B. Phishing

C. Schmunzelnd

D. Vishing

E. Tippfehler

F. Identitätswechsel

Answer(s): C,F

---

7. Ein Cybersicherheitsanalyst bei Unternehmen A arbeitet daran, einen sicheren Kommunikationskanal mit einem Gegenstück bei Unternehmen B einzurichten, das 3.000 Meilen (4,828 Kilometer) entfernt ist. Welches der folgenden Konzepte würde dem Analysten helfen, dieses Ziel auf sichere Weise zu erreichen?

A. Digitale Signaturen

B. Schlüsselaustausch

C. Salzen

D. PPTP

Answer(s): B

---

8. Ein Unternehmen muss seine Protokolle zentralisieren, um eine Basis zu schaffen und Einblick in seine Sicherheitsereignisse zu haben. Welche der folgenden Technologien wird dieses Ziel

erreichen?

A. Sicherheitsinformations- und Ereignismanagement

B. Eine Webanwendungs-Firewall

C. Ein Schwachstellenscanner

D. Eine Firewall der nächsten Generation

Answer(s): A

---

9. Ein Systemadministrator prüft alle Unternehmensserver, um sicherzustellen, dass sie die Mindestsicherheitsgrundlinie erfüllen. Bei der Prüfung eines Linux-Servers stellt der Systemadministrator fest, dass die Datei /etc/ahadow über Berechtigungen verfügt, die über die Grundempfehlung hinausgehen. Welchen der folgenden Befehle sollte der Systemadministrator verwenden, um dieses Problem zu beheben?

A. chmod

B. grep

C. dd

D. Passwort

Answer(s): A

---

10. Ein Sicherheitsanalyst möchte überprüfen, ob eine Client-Server-Anwendung (nicht Web) verschlüsselten Datenverkehr sendet.

A. openssl

B. hping

C. netcat

D. tcpdump

Answer(s): A

---

11. Welcher der folgenden Gründe ist der beste, eine Prüfung im Bankenumfeld durchzuführen?

A. Selbstbewertungsanforderung

B. Regulatorische Anforderung

C. Organisatorische Änderung

D. Service-Level-Anforderung

Answer(s): B

---

12. Ein Cybersicherheitsadministrator muss mobilen BYOD-Geräten den Zugriff auf Netzwerkressourcen ermöglichen. Welche der folgenden Best Practices für Authentifizierung und Infrastruktursicherheit gelten, da die Geräte nicht in der Domäne registriert sind und keine Richtlinien auf sie angewendet werden? (Wählen Sie ZWEI).

A. Erstellen Sie ein neues Netzwerk für die Mobilgeräte und blockieren Sie die Kommunikation zum internen Netzwerk und zu den Servern

B. Verwenden Sie ein Captive-Portal für die Benutzerauthentifizierung.

C. Authentifizieren Sie Benutzer mit OAuth für mehr Ausfallsicherheit

D. Implementieren Sie SSO und erlauben Sie die Kommunikation mit dem internen Netzwerk

E. Das vorhandene Netzwerk nutzen und die Kommunikation mit dem internen Netzwerk und den Servern zulassen.

F. Verwenden Sie einen neuen und aktualisierten RADIUS-Server, um die beste Lösung beizubehalten

Answer(s): B,C

---

13. Endbenutzer eines Unternehmens berichten, dass sie externe Websites nicht erreichen können. Nach Überprüfung der Leistungsdaten für die DNS-Server stellt der Analyst fest, dass die CPU-, Festplatten- und Speicherauslastung minimal ist, die Netzwerkschnittstelle jedoch mit eingehendem Datenverkehr überflutet ist. Netzwerkprotokolle zeigen nur eine kleine Anzahl an an diesen Server gesendeten DNS-Anfragen. Welche der folgenden Aussagen beschreibt am besten, was der Sicherheitsanalyst sieht?

A. Sicheres kryptografisches DNS-Downgrade

B. Reflektierter Denial-of-Service

C. Gleichzeitige Sitzungsnutzung

D. Ressourcenverbrauch auf dem Pfad

Answer(s): B

---

14. Ein Sicherheitsadministrator sammelt Informationen von allen Geräten im lokalen Netzwerk, um einen besseren Einblick in die Benutzeraktivitäten zu erhalten. Welche der folgenden Lösungen ist die beste, um dieses Ziel zu erreichen?

A. JA

B. HIDS

C. CASB

D. EDR

Answer(s): A

---

15. Im vergangenen Jahr kam es in einer Organisation zu mehreren Lecks von geistigem Eigentum durch eine unbekannte Quelle. Welche der folgenden Risikomanagementrichtlinien helfen dem Unternehmen dabei, die Ursache dieses Problems zu ermitteln?

A. Anwenden von Datenaufbewahrungsstandards auf alle Datenbanken

B. Alle Mitarbeiter müssen eine Richtlinie zur akzeptablen Nutzung unterzeichnen

C. Durchführung von kriminalpolizeilichen Hintergrundüberprüfungen

D. Einführung von Pflichturlauben

Answer(s): D

---

16. Eine Organisation rüstet ihr drahtloses System auf und möchte MFA verlangen, damit Benutzer eine Verbindung zu Wi-Fi herstellen können. Neue Access Points wurden installiert und an den Controller angeschlossen. Welche der folgenden Technologien ist als nächstes erforderlich, um MFA zu ermöglichen?

A. CBC-MAC

B. RADIUS

C. HSM

D. BWPA3

E. PSK

Answer(s): B

---

17. Ein Sicherheitsanalyst überprüft die Authentifizierungsprotokolle eines Unternehmens und stellt mehrere Authentifizierungsfehler fest. Die Authentifizierungsfehler stammen von verschiedenen Benutzernamen, die dieselbe Quell-IP-Adresse haben. Welcher der Passwortangriffe findet am wahrscheinlichsten statt?

A. Wörterbuch

B. Regenbogentisch

C. Sprühen

D. Brutale Gewalt

Answer(s): C

---

18. Ein Benutzer versucht erfolglos, Bilder per SMS zu senden. Der Benutzer hat die Bilder von einem Firmen-E-Mail-Konto auf ein Arbeitstelefon heruntergeladen. Welche der folgenden Richtlinien verhindert, dass der Benutzer diese Aktion ausführt?

A. Anwendungsmanagement

B. Content-Management

C. Containerisierung

D. Vollständige Festplattenverschlüsselung

Answer(s): B

---

19. Ein Prüfbericht weist darauf hin, dass mehrere verdächtige Versuche unternommen wurden, auf Unternehmensressourcen zuzugreifen. Diese Versuche wurden vom Unternehmen nicht entdeckt. Welche der folgenden Lösungen wäre am besten für die Implementierung im Unternehmensnetzwerk geeignet?

A. Intrusion-Prevention-System

B. Proxyserver

C. Jump-Server

D. Sicherheitszonen

Answer(s): A

---

20. Eine Organisation stellte fest, dass ein verärgerter Mitarbeiter durch das Hochladen von Dateien eine große Menge an PII-Daten herausgefiltert hatte. Welche der folgenden Kontrollen sollte die Organisation berücksichtigen, um dieses Risiko zu mindern?

A. EDR

B. Firewall

C. HÜFTEN

D. DLP

Answer(s): D
