Understanding Cisco Cybersecurity Fundamentals (210-250 Japanese Version)

1. すべてのプロセスをroot / adminとして実行することにより、どのセキュリティ原則に違反するか

A. RBAC

B. Principle of least privilege

C. Segregation of duty

Answer(s): B

---

2. ネットワークレベルで暗号化されているテクノロジーは、ネイティブに組み込まれていないのですか？

A. TLS

B. SSL

C. IPsec

D. Kerberos

Answer(s): D

---

3. Runbookの有効性を測定できる指標は次のうちどれですか？

A. 修復の平均時間（MTTR）

B. 上記のすべて

C. 平均故障間隔 (MTBF)

D. セキュリティインシデントを発見する平均時間

Answer(s): B

---

4. 分析者がネットワークソースからのデータを確認する場合、どのオプションがデータ損失を構成しますか？

A. PNG ..... data stores

B. PK...1...client data.

C. PMOCCMOC...ZUser Guid

D. MS Portal

Answer(s): B

---

5. Linuxでの許可の定義はどれですか？

A. オブジェクトの所有権と制御の属性

B. テーブルメンテナンスプログラム

C. ネットワークトラフィックの出入りを許可するルール

D. システムを使用する前に署名する必要のある宣誓供述書

Answer(s): A

---

6. ゾンビプロセスは、次のどれが発生したときに発生しますか？

A. プロセスは、関連するメモリとリソースを保持しますが、エントリテーブルから解放されます。

B. プロセスは単独で実行を継続します。

C. プロセスはメモリを関連付けますが、リソースを解放します。

D. プロセスは関連するメモリとリソースを解放しますが、エントリテーブルに残ります。

Answer(s): D

---

7. イベントログやファイルシステムなどのテキストベースのデータへのユニバーサルクエリアクセスを提供するツールはどれですか。

A. Windows管理インストルメンテーション

B. サービスビューア

C. ハンドル

D. ログパーサー

Answer(s): D

---

8. RFC 1035により、DNSゾーン転送に使用されるトランスポート層プロトコルはどれですか？

A. RDP

B. UDP

C. TCP

D. HTTP

Answer(s): C

---

9. NTPは監視にどのように役立ちますか？

A. システム生成の電子メールを受信するには

B. 時刻を同期することにより、異なるシステムログからのイベントの相関が可能になります。

C. TCPを使用すると、サーバーとクライアント間のHTTP接続を表示できます。

D. FQDNを使用してシステムでIPアドレスを検索します。

Answer(s): B

---

10. NetFlowレコードでは、HTTP接続が完全に構築される前にファイアウォールなどのセキュリティアプライアンスによってHTTP接続が停止されたことを示すフラグはどれですか？

A. SYN ACK

B. RST

C. PSH、ACK

D. ACK

Answer(s): C

---

11. 捕鯨の例はどれですか？

A. 攻撃者が個人のグループを標的とする場合

B. 攻撃者がCEOを狙うとき

C. 攻撃者が正当なWebサイトのように見える詐欺Webサイトを使用する場合

D. 攻撃者が特定の個人を標的とする場合

Answer(s): B

---

12. NetFlowを使用してどのデータを取得できますか？

A. ネットワークのダウンタイム

B. セッションデータ

C. アプリケーションログ

D. 完全なパケットキャプチャを報告する

Answer(s): B

---

13. NGFWの2つの機能は何ですか：

A. データマイニング、

B. アプリケーションの可視性と制御

C. ホストベースのAV

D. SIEM

E. IDS

Answer(s): B,E

---

14. どの用語が、権限や許可なしに、割り当てられたものを超えてシステムの権利を取得するユーザーの行為を表しますか？

A. 管理上の悪用

B. 権限昇格

C. 認証トンネリング

D. 権利の搾取

Answer(s): B

---

15. コンピュータセキュリティでは、PHIという用語はどの情報を表すのに使用されていますか？

A. プライベートホスト情報

B. 個人の履歴情報

C. 保護されたホスト情報

D. 保護された健康情報

Answer(s): D

---

16. 適切な行動方針を促進するために関連情報を取得するために行わなければならない合理的な努力を表す用語はどれですか？

A. data mining.

B. ethical behavior

C. Due diligence

D. decision making

Answer(s): C

---

17. ネットワークトラフィックが外部に面したデバイスに大量に流入した後、サービス拒否攻撃と思われるものの調査を開始します。パケットキャプチャデータを確認すると、トラフィックが各ポートへの単一のSYNパケットであることがわかります。これはどのような攻撃ですか？

A. Traffic fragmentation.

B. Host porfiling.

C. Port scanning.

D. SYN flood.

Answer(s): D

---

18. ネットワークベースのアンチウイルスとホストベースのアンチウイルスを使用する利点はどれですか？

A. ネットワークベースには、管理されていないデバイスとサポートされていないオペレーティングシステムを保護する機能があります。

B. ホストベースのウイルス対策に比べて利点はありません。

C. ネットワークベースは、保存されている悪意のあるファイルからの感染から保護できます。

D. ホストベースのウイルス対策には、新しく作成された署名を収集する機能がありません。

Answer(s): A

---

19. FMCは、特定のイベントタイプに関連するHTML、Pdf、csvデータタイプを共有できます。

A. Intrusion

B. Netflow

C. connection

D. Host

Answer(s): A

---

20. どのセキュリティ監視データタイプがアプリケーションサーバーログに関連付けられていますか？

A. transaction data

B. statistical data

C. alert data

D. session data

Answer(s): A
