Certified Ethical Hacker Exam (312-50v12 Japanese Version)

1. クライアントの侵入テストを実行していて、内部ネットワーク上のWindowsマシンへのシェルアクセスを取得しました。DNSサーバーが次の場所にある場合、内部ドメインのすべてのDNSレコードを取得するつもりです。

A. is-d abccorp.local

B. List domain=Abccorp.local type=zone

C. list server=192.168.10.2 type=all

D. Iserver 192.168.10.2-t all

Answer(s): A

---

2. SSL/TLS で対称暗号化と非対称暗号化の両方を使用する利点の 1 つは何ですか?

A. 両方のタイプのアルゴリズムをサポートすることで、携帯電話などの性能の低いデバイスでも代わりに対称暗号化を使用できるようになります。

B. 対称暗号化により、サーバーはセッション キーを帯域外で安全に送信できます。

C. AES などの対称アルゴリズムは、非対称メソッドが失敗した場合にフェイルセーフを提供します。

D. 非対称暗号化は、それに比べると計算コストが高くなります。ただし、対称暗号化で使用するキーを安全にネゴシエートするには適しています。

Answer(s): A

---

3. 「サーバーサイドインクルード」攻撃とは、HTML ページにスクリプトを挿入したり、任意のコードをリモートで実行したりして、Web アプリケーションを悪用することを指します。

A. .stm

B. .html

C. .rss

D. .cms

Answer(s): A

---

4. これは、ユーザーが提供したデータがサニタイズされていないコンテンツがサイトに表示されるという Web サイトの脆弱性を悪用した攻撃です。

A. クロスサイトスクリプティング攻撃

B. SQLインジェクション

C. バッファオーバーフロー攻撃

D. URLトラバーサル攻撃

Answer(s): A

---

5. 大胆な攻撃者が、あなたが管理するウェブサーバーを狙っています。攻撃者は、HTTP接続を操作して、Slow HTTP POST攻撃を実行しようとしています。各接続は、1秒ごとに1バイトのデータを転送し、実質的に接続を長時間にわたって停止させます。サーバーは1秒あたりm個の接続を処理するように設計されていますが、この数を超える接続はシステムを圧倒する傾向があります。

A. m=110、b=20: 攻撃者が100の接続を送信したにもかかわらず、サーバーは1秒あたり110の接続を処理できるため、接続ごとのホールドアップ時間に関係なく、動作を継続する可能性があります。

B. m=90、b=15: サーバーは1秒あたり90の接続を処理できますが、攻撃者の100の接続はこれを超えており、各接続が15秒間保持されるため、攻撃の持続時間はかなり長くなる可能性があります。

C. 95, b=10: ここで、サーバーは1秒あたり95の接続を処理できますが、接続あたりのホールドアップ時間は短いものの、攻撃者の100の接続には及びません。

D. m=105、b=12: サーバーは 1 秒あたり 105 の接続を処理できます。これは攻撃者の 100 の接続よりも多いため、中程度のホールドアップ時間にもかかわらず動作が維持される可能性があります。

Answer(s): B

---

6. 攻撃者が Web サーバーをどのように悪用するかを考えるとき、Web サーバー フットプリントとは何でしょうか。

A. 攻撃者が脆弱性スキャナを実装して弱点を特定する場合

B. 攻撃者がアカウントの詳細やサーバー名などのシステムレベルのデータを収集する場合

C. 攻撃者がブルートフォース攻撃を使用してWebサーバーのパスワードを解読する場合

D. 攻撃者がサイトの外部リンクとファイル構造の完全なプロファイルを作成すると、

Answer(s): B

---

7. ケイトは携帯電話を落とし、その後携帯電話の内蔵スピーカーに問題が発生しました。そのため、彼女は電話の通話やその他の活動に携帯電話のスピーカーを使用しています。攻撃者のボブは、この脆弱性を利用してケイトの携帯電話のハードウェアを密かに悪用し、悪意のあるアプリを使用して音声アシスタント、マルチメディア メッセージ、オーディオ ファイルなどのデータソースからのスピーカー出力を監視し、スピーチのプライバシーを侵害します。上記のシナリオでボブがケイトに対して行った攻撃の種類は何ですか?

A. SIMカード攻撃

B. ディスク侵入攻撃

C. aLTEr 攻撃

D. スピアフォン攻撃

Answer(s): D

---

8. 次のどれが GUI ベースの Wireshark に似たコマンドライン パケット アナライザーですか?

A. ネサス

B. tcpdump

C. エーテル

D. 切り裂きジャック

Answer(s): B

---

9. 自宅のルーターでワイヤレスを設定する際、JavikはSSIDブロードキャストを無効にし、認証はそのままにしておく。

A. Javik のルーターは、アクセス ポイントのハードウェア アドレスに送信される特別に細工されたパケットを使用して SSID ブロードキャスト設定を有効にすることができるため、ワイヤレス ハッキング攻撃に対して依然として脆弱です。

B. ハッカーが、成功したワイヤレス接続から SSID をスニッフィングした後でも、ネットワークに接続できる可能性があります。

C. SSID ブロードキャストを無効にすると、アクセス ポイントから 802.11 ビーコンが送信されなくなり、「セキュリティによる隠蔽」を活用した有効なセットアップが実現します。

D. 接続には SSID が必要なので、ブルートフォース攻撃を防ぐには 32 文字の文字列で十分です。

Answer(s): B

---

10. 攻撃者の Dayn は、ターゲット ネットワークにハニーポットがインストールされているかどうかを検出したいと考えていました。この目的のために、彼は時間ベースの TCP フィンガープリント法を使用して、通常のコンピュータへの応答と、手動 SYN 要求に対するハニーポットの応答を検証しました。ハニーポットを検出するために Dayn が使用している技術は次のどれですか。

A. Sebekベースのハニーポットの存在を検出する

B. VMware 上で実行されているハニーポットの検出

C. Honeyd ハニーポットの存在を検出する

D. Snort_inline ハニーポットの存在を検出する

Answer(s): D

---

11. Vlady は漁業会社で働いていますが、従業員の大半は IT セキュリティどころか IT についてもほとんど理解していません。Vlady がよく目にする情報セキュリティの問題には、従業員がパスワードを共有している、ポストイットにパスワードを書いてデスクに貼っている、コンピューターのロックを解除したままにしている、電子メールやその他のソーシャル メディア アカウントからログアウトしていない、などがあります。

A. 付箋にパスワードを書いて机に貼っている人への警告

B. 情報セキュリティ意識向上トレーニング

C. 厳格な情報セキュリティポリシーの策定

D. 情報セキュリティの重要性について他の従業員と1対1で話し合う

Answer(s): A

---

12. ソフトウェア開発者の Calvin は、手動操作なしで Web ページのコンテンツを自動生成する機能を使用しており、SSI ディレクティブと統合されています。この機能はリモート ユーザーの入力を受け入れてページで使用するため、開発された Web アプリケーションに脆弱性が生じます。ハッカーはこの機能を悪用し、悪意のある SSI ディレクティブを入力値として渡し、サーバー ファイルの変更や消去などの悪意のあるアクティビティを実行する可能性があります。Calvin の Web アプリケーションが影響を受けやすいインジェクション攻撃の種類は何ですか?

A. サーバーサイドインクルードインジェクション

B. サーバーサイド JS インジェクション

C. サーバー側テンプレートインジェクション

D. CRLF挿入

Answer(s): A

---

13. ビルはネットワーク管理者です。彼は会社のネットワーク内の暗号化されていないトラフィックを排除したいと考えています。彼は SPAN ポートを設定し、データセンターへのすべてのトラフィックをキャプチャすることにしました。彼はすぐにポート UDP 161 で暗号化されていないトラフィックを発見しました。このポートはどのプロトコルを使用しており、そのトラフィックをどのように保護できるでしょうか。

A. SNMP は重要な情報を伝送しないため、アクションを実行する必要はありません。

B. SNMP なので、SNMP V3 に変更する必要があります。

C. RPCであり、ベストプラクティスはRPCを完全に無効にすることです

D. SNMP なので、暗号化された SNMP v2 に変更する必要があります。

Answer(s): B

---

14. プロのハッカーであるメイソンは、ある組織を標的にし、悪意のあるスクリプトを通じて Emotet マルウェアを拡散します。

A. NetPass.exe

B. Outlook スクレーパー

C. Webブラウザパスビュー

D. 資格情報列挙子

Answer(s): D

---

15. 攻撃者はホストにRATをインストールしました。攻撃者は、ユーザーが

A. スドーユーザー

B. ネットワーク

C. ホスト

D. Boot.ini

Answer(s): C

---

16. スーザンは会社のネットワークに接続し、上司のセッションをファイル サーバーのセッションと同期させました。そして、上司がサーバーに送るトラフィックを傍受し、自分の希望どおりに変更して、サーバーの上司のホーム ディレクトリに配置しました。

A. スニッフィング攻撃

B. 中間者攻撃

C. サービス拒否攻撃

D. なりすまし攻撃

Answer(s): B

---

17. セキュリティ専門家の Abel は、セキュリティの抜け穴がないか確認するために、クライアント組織で侵入テストを実施しています。彼は、偽造された DHCP 要求をブロードキャストして DHCP サーバーに攻撃を仕掛け、DHCP スコープで使用可能なすべての DHCP アドレスを、サーバーが IP アドレスを発行できなくなるまでリースしました。これにより DoS 攻撃が発生し、結果として、正当な従業員がクライアント ネットワークにアクセスできなくなりました。上記のシナリオで Abel が実行した攻撃は次のうちどれですか。

A. VLANホッピング

B. DHCP 不足

C. 不正なDHCPサーバー攻撃

D. STP攻撃

Answer(s): B

---

18. トロイの木馬の用語では、秘密チャネルとは何ですか?

A. HTTPプロトコルの代わりにHTTPSプロトコルを使用して接続を確立するリバーストンネリング技術です。

B. ブートプロセスとサービスを隠すカーネル操作で、検出をマスクします。

C. コンピュータシステムまたはネットワーク内でデータを転送するための正当な通信経路

D. セキュリティポリシーに違反する方法でコンピュータシステムまたはネットワーク内で情報を転送するチャネル

Answer(s): D

---

19. netcat の次のコマンドは何をしますか?

A. UDP ポート 55555 に接続したときに /etc/passwd ファイルを削除します。

B. 着信接続を/etc/passwdファイルに記録します

C. UDP ポート 55555 に接続したときに /etc/passwd ファイルを取得します。

D. /etc/passwdファイルをUDPポート55555にロードします。

Answer(s): C

---

20. ペン テスターがテスト用に Windows ラップトップを構成しています。Wireshark を設定する場合、NIC がプロミスキャス モードで動作できるようにするには、どのリバーとライブラリが必要ですか。

A. ウィンプロム

B. libpcap

C. アウィンキャップ

D. ウィンキャップ

Answer(s): D
