Certified Ethical Hacker Exam (312-50v11 Japanese Version)

1. あなたは侵入テストを実行する任務を負っています。情報収集を行っているときに、Googleで従業員リストを見つけます。受付係の電子メールを見つけ、ソース電子メールを上司の電子メール（boss @ company）に変更する電子メールを彼女に送信します。このメールでは、情報が記載されたPDFを要求します。彼女はあなたのメールを読み、リンク付きのPDFを送り返します。悪意のあるリンク（これらのリンクにはマルウェアが含まれています）とpdfリンクを交換し、リンクが機能しないことを伝えて、変更されたpdfを送り返します。彼女はあなたの電子メールを読み、リンクを開き、彼女のマシンは感染します。これで、会社のネットワークにアクセスできます。どのようなテスト方法を使用しましたか？

A. テールゲート

B. 盗聴

C. ピギーバッキング

D. ソーシャルエンジニアリング

Answer(s): D

---

2. 匿名クエリからLDAPサービスを保護するために使用できるプロトコルは次のうちどれですか？

A. SSO

B. RADIUS

C. WPA

D. NTLM

Answer(s): D

---

3. プロのハッカーであるジョンは、分散ディレクトリサービスへのアクセスにLDAPを使用している組織を標的にしました。彼は自動化されたツールを使用して、ユーザー名などの機密情報をIDAPサービスに匿名で照会しました。標的組織へのさらなる攻撃を開始するためのアドレス、部門の詳細、およびサーバー名。

A. jxplorer

B. ザバサーチ

C. EarthExplorer

D. 池スキャン

Answer(s): A

---

4. 最近のセキュリティ評価中に、組織の非武装地帯（DMZ）に1つのドメインネームサーバー（DNS）があり、内部ネットワークに2つ目のDNSサーバーがあることがわかりました。

A. DNSスキーム

B. DNSSEC

C. DynDNS

D. スプリットDNS

Answer(s): D

---

5. スティーブンは自分のiPhoneを、攻撃者であるクラークに感染した公共のコンピューターに接続しました。パブリックコンピューターとの接続を確立した後、スティーブンはコンピューターでiTunes WI-FI同期を有効にして、デバイスが物理的に切断された後でもそのコンピューターとの通信を継続できるようにしました。

A. IOSトラストジャック

B. IOS脱獄

C. SS7の脆弱性を悪用する

D. Man-in-the-disk攻撃

Answer(s): A

---

6. 経営幹部が会社の資産と情報システムを適切に保護しなかった責任があると判明した場合、この状況ではどのような種類の法律が適用されますか？

A. 共通

B. 刑事

C. 土木

D. インターナショナル

Answer(s): C

---

7. どのDNSリソースレコードが、「DNSポイズニング」がどのくらい続く可能性があるかを示すことができますか？

A. MX

B. SOA

C. タイムアウト

D. NS

Answer(s): B

---

8. Gobusterツールを使用して特定のWebサーバーでコンテンツ列挙を実行する最速の方法は何でしょうか？

A. ブルートフォースモードと10スレッドを使用してコンテンツの列挙を実行する

B. 出荷SSL証明書の検証

C. ワードリストを使用してコンテンツの列挙を実行する

D. ブルートフォースモードとランダムなファイル拡張子を使用してコンテンツの列挙を実行する

Answer(s): A

---

9. Shellshockは、許可されていないユーザーがサーバーにアクセスすることを許可しました。多くのインターネット向けサービスに影響しましたが、どのOSに直接影響しませんでしたか？

A. Linux

B. Windows

C. OS X

D. Unix

Answer(s): B

---

10. Heartbleedバグは、2014年に発見され、MITREのCommon Vulnerabilities and Exposures（CVE）ではCVE-2014-0160と広く呼ばれています。このバグは、RFC6520で定義されているトランスポート層セキュリティ（TLS）プロトコルのOpenSSL実装に影響します。

A. Public

B. Root

C. Shared

D. Private

Answer(s): D

---

11. ベンは新しいスマートフォンを購入し、OTA方式でいくつかのアップデートを受け取りました。彼は2つのメッセージを受け取りました。1つはネットワークオペレーターからのPINで、もう1つはオペレーターから受け取ったPINの入力を求めています。 PINを入力するとすぐに、スマートフォンが異常に機能し始めました。上記のシナリオでベンに対して実行される攻撃のタイプは何ですか？

A. 'nゴーストアタックをタップ

B. SSLピン留めをバイパスする

C. 高度なSMSフィッシング

D. フィッシング

Answer(s): C

---

12. チャンドラーは、ニューヨークのIT企業で侵入テストを行っています。彼は、システム内のウイルスを検出する一環として、アンチウイルスが仮想マシン上で悪意のあるコードを実行してCPUとメモリのアクティビティをシミュレートする検出方法を使用しています。このコンテキストでチャンドラーはどのタイプのウイルス検出方法を使用しましたか？

A. ヒューリスティック分析

B. 整合性チェック

C. コードエミュレーション

D. スキャン

Answer(s): C

---

13. アクセス可能なディスクドライブを備えたWindows2008R2サーバーに物理的にアクセスできるようになりました。サーバーを起動してログインしようとすると、パスワードを推測できません。ツールキットには、Ubuntu 9.10 LinuxLiveCDが含まれています。どのLinuxベースのツールがユーザーのパスワードを変更したり、無効になっているWindowsアカウントをアクティブ化したりできますか？

A. カインとアベル

B. SET

C. ジョン・ザ・リッパー

D. CHNTPW

Answer(s): D

---

14. 検出されることを心配せず、非常に高速なスキャンを実行したい場合は、どのNmapオプションを使用しますか？

A. -T5

B. -O

C. -A

D. -T0

Answer(s): A

---

15. Nmapでスキャンしているときに、Patinはインクリメンタルシーケンスの IPIDを持ついくつかのホストを見つけました。その後、彼は次のことを行うことにしました：nmap -Pn -p- -si kiosk.adobe.comwww.riaa.com。 kiosk.adobe.comは、増分IPIDシーケンスを持つホストです。Nmapで「-si」を使用する目的は何ですか？

A. ステルススキャンを実行します

B. ICMPスキャンを実行します

C. IDLEスキャンを実行します

D. サイレントスキャンを実行します

Answer(s): C

---

16. Common Vulnerability Scoring System（CVSS）v3.1の重大度評価では、中程度の脆弱性はどの範囲に含まれますか？

A. 3.0-6.9

B. 40-6.0

C. 4.0-6.9

D. 3.9-6.9

Answer(s): C

---

17. ネットワークには、ワイヤレスネットワークコンポーネントの安全性が十分でないという懸念があります。ワイヤレスネットワークの脆弱性スキャンを実行し、有線暗号化を模倣するように設計された古い暗号化プロトコルを使用していることがわかりました。どの暗号化プロトコルが使用されていますか？

A. WEP

B. RADIUS

C. WPA

D. WPA3

Answer(s): A

---

18. ネットワークタイムプロトコル（NTP）が主要な通信手段として使用するUDPポートを特定しますか？

A. 69

B. 161

C. 123

D. 113

Answer(s): C

---

19. パスワードについて話し合うとき、ブルートフォース攻撃と見なされるものは何ですか？

A. パスワードの有効期限が切れるまで待ちます

B. パスワードを明かさない限り、誰かにゴムホースを使用すると脅迫する

C. 多数の単語のハッシュを作成し、暗号化されたパスワードと比較します

D. 単語の辞書をクラッキングプログラムにロードします

E. 考えられるすべての組み合わせを使い果たすか、パスワードを見つけるまで、すべての可能性を試みます

Answer(s): E

---

20. 攻撃者が動的に生成されたWebページの脆弱性を悪用して、他のユーザーが表示するWebページにクライアント側のスクリプトを挿入するWebアプリケーション攻撃を特定します。

A. クロスサイトリクエストフォージェリ（CSRF）

B. LDAPインジェクション攻撃

C. SQLインジェクション攻撃

D. クロスサイトスクリプティング（XSS）

Answer(s): D
