312-50V7 Q&As

Ethical Hacking and Countermeasures (CEHv7)

Pass EC-COUNCIL 312-50V7 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.geekcert.com/312-50v7.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by EC-COUNCIL Official Exam Center

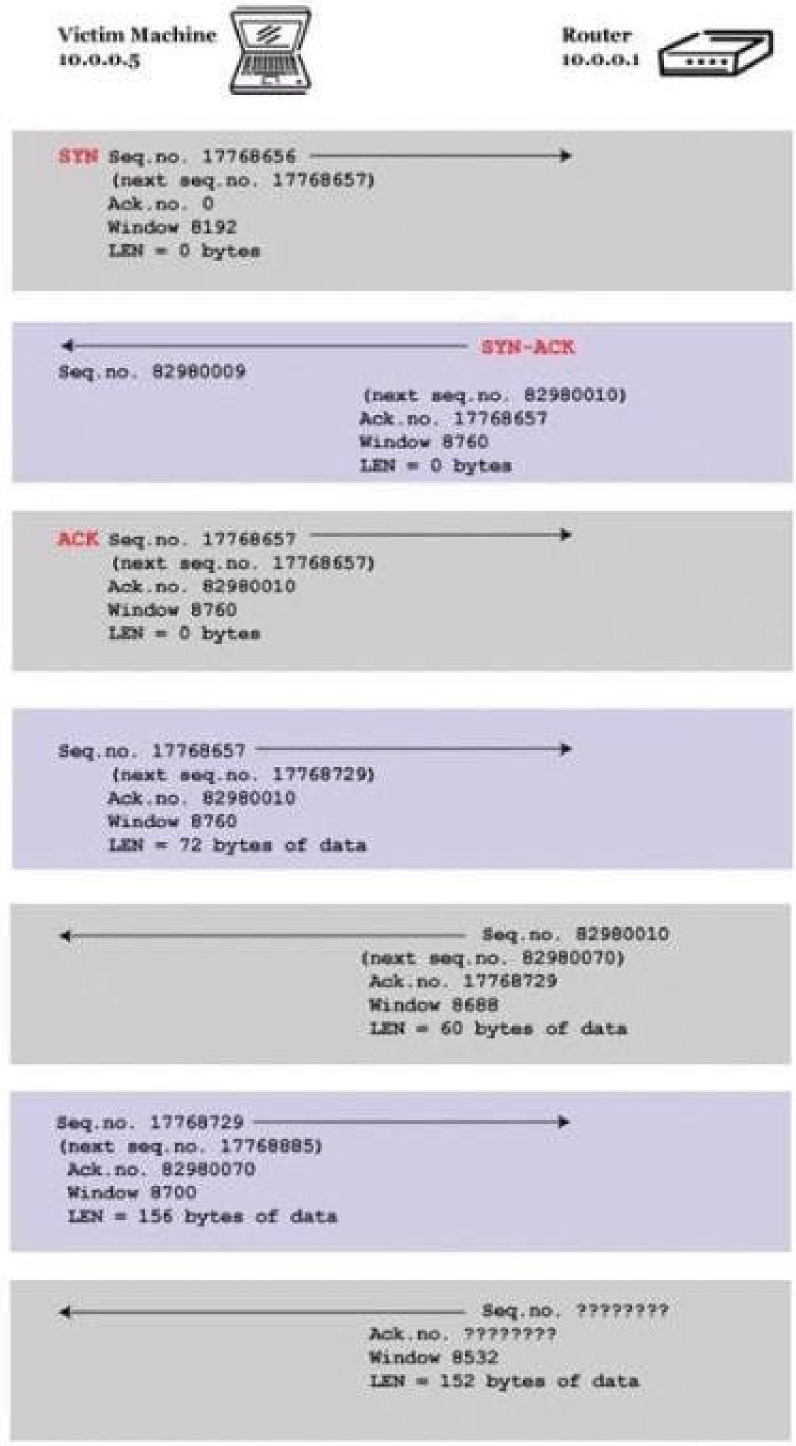
- Instant Download After Purchase
- 100% Money Back Guarantee
- 365 Days Free Update
- 800,000+ Satisfied Customers

SATISFACTION GUARANTEED
100%
SATISFACTION GUARANTEED

QUESTION 1

You are trying to hijack a telnet session from a victim machine with IP address 10.0.0.5 to Cisco router at 10.0.0.1. You sniff the traffic and attempt to predict the sequence and acknowledgement numbers to successfully hijack the telnet session.

Here is the captured data in tcpdump.



```
SYN Seq.no. 17768656 ------------------------>
    (next seq.no. 17768657)
    Ack.no. 0
    Window 8192
    LEN = 0 bytes

<------------------------------------ SYN-ACK
Seq.no. 82980009
                          (next seq.no. 82980010)
                          Ack.no. 17768657
                          Window 8760
                          LEN = 0 bytes

ACK Seq.no. 17768657 ------------------------>
    (next seq.no. 17768657)
    Ack.no. 82980010
    Window 8760
    LEN = 0 bytes

Seq.no. 17768657 ---------------------------->
    (next seq.no. 17768729)
    Ack.no. 82980010
    Window 8760
    LEN = 72 bytes of data

<------------------------------------ Seq.no. 82980010
                          (next seq.no. 82980070)
                           Ack.no. 17768729
                           Window 8688
                           LEN = 60 bytes of data

Seq.no. 17768729 ---------------------------->
(next seq.no. 17768885)
 Ack.no. 82980070
 Window 8700
 LEN = 156 bytes of data

<------------------------------------ Seq.no. ????????
                           Ack.no. ????????
                           Window 8532
                           LEN = 152 bytes of data
```

What are the next sequence and acknowledgement numbers that the router will send to the victim machine?

A. Sequence number: 82980070 Acknowledgement number: 17768885A.

B. Sequence number: 17768729 Acknowledgement number: 82980070B.

C. Sequence number: 87000070 Acknowledgement number: 85320085C.

D. Sequence number: 82980010 Acknowledgement number: 17768885D.

Correct Answer: A

QUESTION 2

Jason works in the sales and marketing department for a very large advertising agency located in Atlanta. Jason is working on a very important marketing campaign for his company\\'s largest client. Before the project could be completed and implemented, a competing advertising company comes out with the exact same marketing materials and advertising, thus rendering all the work done for Jason\\'s client unusable. Jason is questioned about this and says he has no idea how all the material ended up in the hands of a competitor.

Without any proof, Jason\\'s company cannot do anything except move on. After working on another high profile client for about a month, all the marketing and sales material again ends up in the hands of another competitor and is released to the public before Jason\\'s company can finish the project. Once again, Jason says that he had nothing to do with it and does not know how this could have happened. Jason is given leave with pay until they can figure out what is going on.

Jason\\'s supervisor decides to go through his email and finds a number of emails that were sent to the competitors that ended up with the marketing material. The only items in the emails were attached jpg files, but nothing else. Jason\\'s supervisor opens the picture files, but cannot find anything out of the ordinary with them.

What technique has Jason most likely used?

A. Stealth Rootkit Technique

B. ADS Streams Technique

C. Snow Hiding Technique

D. Image Steganography Technique

Correct Answer: D

QUESTION 3

A pentester gains acess to a Windows application server and needs to determine the settings of the built-in Windows firewall. Which command would be used?

A. Netsh firewall show config

B. WMIC firewall show config

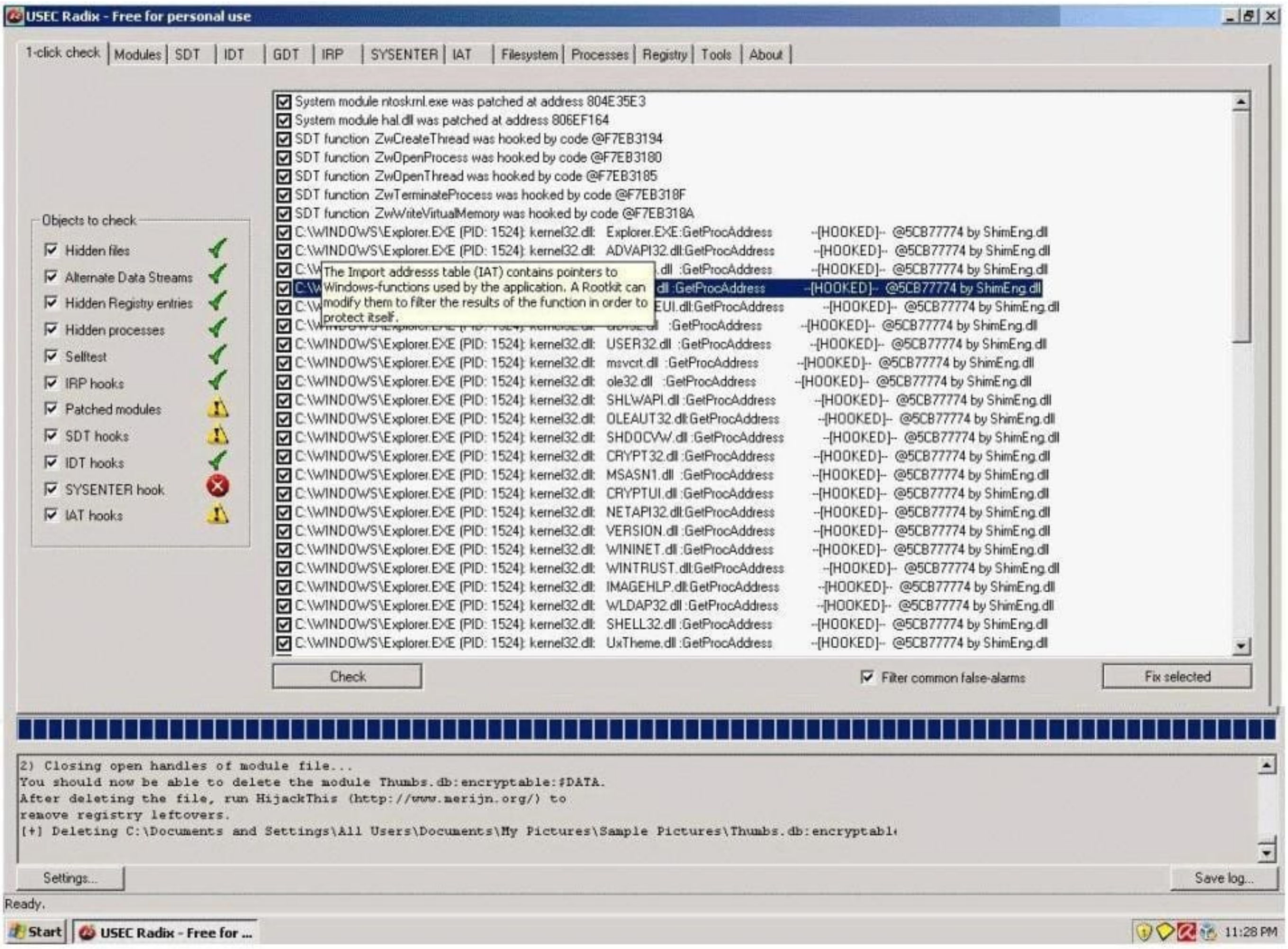
C. Net firewall show config

D. Ipconfig firewall show config

Correct Answer: A

QUESTION 4

A rootkit is a collection of tools (programs) that enable administrator-level access to a computer. This program hides itself deep into an operating system for malicious activity and is extremely difficult to detect. The malicious software operates in a stealth fashion by hiding its files, processes and registry keys and may be used to create a hidden directory or folder designed to keep out of view from a user\\'s operating system and security software.


USEC Radix - Free for personal use
1-click check | Modules | SDT | IDT | GDT | IRP | SYSENTER | IAT | Filesystem | Processes | Registry | Tools | About
Check
Fix selected
Settings...
Save log...
Start
USEC Radix - Free for ...
11:28 PM

Objects to check

- ☑ Hidden files ✓
- ☑ Alternate Data Streams ✓
- ☑ Hidden Registry entries ✓
- ☑ Hidden processes ✓
- ☑ Selftest ✓
- ☑ IRP hooks ✓
- ☑ Patched modules ⚠
- ☑ SDT hooks ⚠
- ☑ IDT hooks ✓
- ☑ SYSENTER hook ✖
- ☑ IAT hooks ⚠

```
☑ System module ntoskrnl.exe was patched at address 804E35E3
☑ System module hal.dll was patched at address 806EF164
☑ SDT function  ZwCreateThread was hooked by code @F7EB3194
☑ SDT function  ZwOpenProcess was hooked by code @F7EB3180
☑ SDT function  ZwOpenThread was hooked by code @F7EB3185
☑ SDT function  ZwTerminateProcess was hooked by code @F7EB318F
☑ SDT function  ZwWriteVirtualMemory was hooked by code @F7EB318A
☑ C:\WINDOWS\Explorer.EXE (PID: 1524): kernel32.dll:  Explorer.EXE:GetProcAddress   --[HOOKED]--  @5CB77774 by ShimEng.dll
☑ C:\WINDOWS\Explorer.EXE (PID: 1524): kernel32.dll:  ADVAPI32.dll:GetProcAddress   --[HOOKED]--  @5CB77774 by ShimEng.dll
☑ C:\W                                                .dll  :GetProcAddress   --[HOOKED]--  @5CB77774 by ShimEng.dll
☑ C:\W                                                 dll :GetProcAddress    --[HOOKED]--  @5CB77774 by ShimEng.dll
☑ C:\W                                                EUI.dll:GetProcAddress   --[HOOKED]--  @5CB77774 by ShimEng.dll
☑ C:\W                                                     :GetProcAddress   --[HOOKED]--  @5CB77774 by ShimEng.dll
☑ C:\WINDOWS\Explorer.EXE (PID: 1524): kernel32.dll:  USER32.dll  :GetProcAddress   --[HOOKED]--  @5CB77774 by ShimEng.dll
☑ C:\WINDOWS\Explorer.EXE (PID: 1524): kernel32.dll:  msvcrt.dll  :GetProcAddress   --[HOOKED]--  @5CB77774 by ShimEng.dll
☑ C:\WINDOWS\Explorer.EXE (PID: 1524): kernel32.dll:  ole32.dll   :GetProcAddress   --[HOOKED]--  @5CB77774 by ShimEng.dll
☑ C:\WINDOWS\Explorer.EXE (PID: 1524): kernel32.dll:  SHLWAPI.dll :GetProcAddress   --[HOOKED]--  @5CB77774 by ShimEng.dll
☑ C:\WINDOWS\Explorer.EXE (PID: 1524): kernel32.dll:  OLEAUT32.dll:GetProcAddress   --[HOOKED]--  @5CB77774 by ShimEng.dll
☑ C:\WINDOWS\Explorer.EXE (PID: 1524): kernel32.dll:  SHDOCVW.dll :GetProcAddress   --[HOOKED]--  @5CB77774 by ShimEng.dll
☑ C:\WINDOWS\Explorer.EXE (PID: 1524): kernel32.dll:  CRYPT32.dll :GetProcAddress   --[HOOKED]--  @5CB77774 by ShimEng.dll
☑ C:\WINDOWS\Explorer.EXE (PID: 1524): kernel32.dll:  MSASN1.dll  :GetProcAddress   --[HOOKED]--  @5CB77774 by ShimEng.dll
☑ C:\WINDOWS\Explorer.EXE (PID: 1524): kernel32.dll:  CRYPTUI.dll :GetProcAddress   --[HOOKED]--  @5CB77774 by ShimEng.dll
☑ C:\WINDOWS\Explorer.EXE (PID: 1524): kernel32.dll:  NETAPI32.dll:GetProcAddress   --[HOOKED]--  @5CB77774 by ShimEng.dll
☑ C:\WINDOWS\Explorer.EXE (PID: 1524): kernel32.dll:  VERSION.dll :GetProcAddress   --[HOOKED]--  @5CB77774 by ShimEng.dll
☑ C:\WINDOWS\Explorer.EXE (PID: 1524): kernel32.dll:  WININET.dll :GetProcAddress   --[HOOKED]--  @5CB77774 by ShimEng.dll
☑ C:\WINDOWS\Explorer.EXE (PID: 1524): kernel32.dll:  WINTRUST.dll:GetProcAddress   --[HOOKED]--  @5CB77774 by ShimEng.dll
☑ C:\WINDOWS\Explorer.EXE (PID: 1524): kernel32.dll:  IMAGEHLP.dll:GetProcAddress   --[HOOKED]--  @5CB77774 by ShimEng.dll
☑ C:\WINDOWS\Explorer.EXE (PID: 1524): kernel32.dll:  WLDAP32.dll :GetProcAddress   --[HOOKED]--  @5CB77774 by ShimEng.dll
☑ C:\WINDOWS\Explorer.EXE (PID: 1524): kernel32.dll:  SHELL32.dll :GetProcAddress   --[HOOKED]--  @5CB77774 by ShimEng.dll
☑ C:\WINDOWS\Explorer.EXE (PID: 1524): kernel32.dll:  UxTheme.dll :GetProcAddress   --[HOOKED]--  @5CB77774 by ShimEng.dll
```

The Import addresss table (IAT) contains pointers to Windows-functions used by the application. A Rootkit can modify them to filter the results of the function in order to protect itself.

☑ Filter common false-alarms

```
2) Closing open handles of module file...
You should now be able to delete the module Thumbs.db:encryptable:$DATA.
After deleting the file, run HijackThis (http://www.merijn.org/) to
remove registry leftovers.
[+] Deleting C:\Documents and Settings\All Users\Documents\My Pictures\Sample Pictures\Thumbs.db:encryptabl
```

Ready.

What privilege level does a rootkit require to infect successfully on a Victim\\'s machine?

A. User level privileges

B. Ring 3 Privileges

C. System level privileges

D. Kernel level privileges

Correct Answer: D

QUESTION 5

Least privilege is a security concept that requires that a user is

A. limited to those functions required to do the job.

B. given root or administrative privileges.

C. trusted to keep all data and access to that data under their sole control.

D. given privileges equal to everyone else in the department.

Correct Answer: A

312-50V7 PDF Dumps 312-50V7 Practice Test 312-50V7 Exam Questions