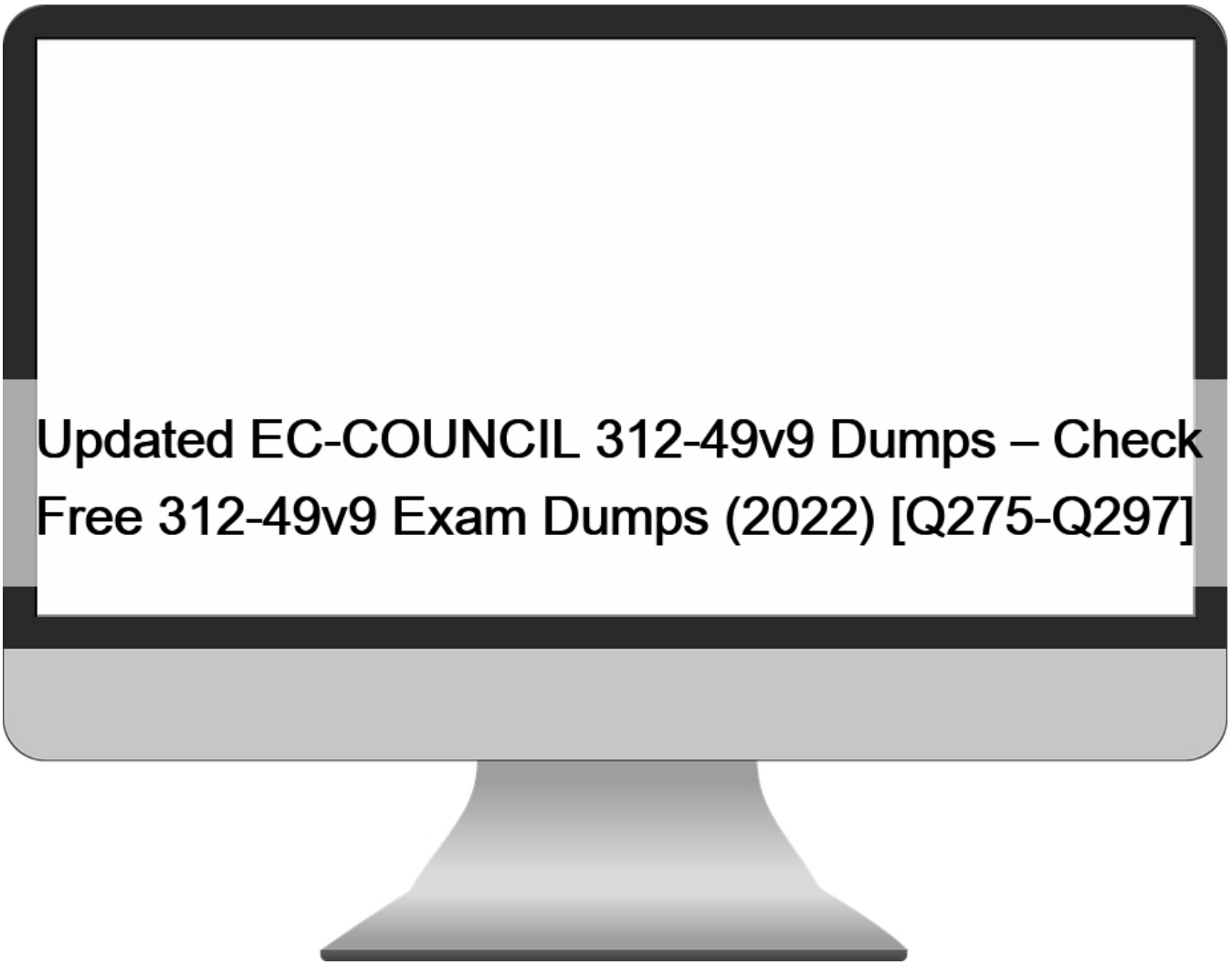
Updated EC-COUNCIL 312-49v9 Dumps ? Check Free 312-49v9 Exam Dumps (2022) [Q275-Q297



Updated EC-COUNCIL 312-49v9 Dumps – Check Free 312-49v9 Exam Dumps (2022) Updated 312-49v9 exam with EC-COUNCIL Real Exam Questions NO.275 How many possible sequence number combinations are there in TCP/IP protocol?

* 320 billion
* 1 billion
* 4 billion
* 32 million

NO.276 What advantage does the tool Evidor have over the built-in Windows search?

* It can find deleted files even after they have been physically removed
* It can find bad sectors on the hard drive
* It can search slack space
* It can find files hidden within ADS

NO.277 When an investigator contacts by telephone the domain administrator or controller listed by a Who is lookup to request all

e-mails sent and received for a user account be preserved, what U.S.C. statute authorizes this phone call and obligates the ISP to preserve e-mail records?
* Title 18, Section 1030
* Title 18, Section 2703(d)
* Title 18, Section Chapter 90
* Title 18, Section 2703(f)

NO.278 You have been given the task to investigate web attacks on a Windows-based server.

Which of the following commands will you use to look at which sessions the machine has opened with other systems?
* Net sessions
* Net use
* Net config
* Net share

NO.279 If a suspect computer is located in an area that may have toxic chemicals, you must:
* coordinate with the HAZMAT team
* determine a way to obtain the suspect computer
* assume the suspect machine is contaminated
* do not enter alone

NO.280 In which of these attacks will a steganalyst use a random message to generate a stego-object by using some steganography tool, to find the steganography algorithm used to hide the information?
* Chosen-message attack
* Known-cover attack
* Known-message attack
* Known-stego attack

NO.281 Study the log given below and answer the following question:

Apr 24 14:46:46 [4663]: spp_portscan: portscan detected from 194.222.156.169

Apr 24 14:46:46 [4663]: IDS27/FIN Scan: 194.222.156.169:56693 -> 172.16.1.107:482

Apr 24 18:01:05 [4663]: IDS/DNS-version-query: 212.244.97.121:3485 -> 172.16.1.107:53

Apr 24 19:04:01 [4663]: IDS213/ftp-passwd-retrieval: 194.222.156.169:1425 ->

172.16.1.107:21

Apr 25 08:02:41 [5875]: spp_portscan: PORTSCAN DETECTED from 24.9.255.53

Apr 25 02:08:07 [5875]: IDS277/DNS-version-query: 63.226.81.13:4499 ->

172.16.1.107:53

Apr 25 02:08:07 [5875]: IDS277/DNS-version-query: 63.226.81.13:4630 ->

1 72.16.1.101:53

Apr 25 02:38:17 [5875]: IDS/RPC-rpcinfo-query: 212.251.1.94:642 -> 172.16.1.107:111

Apr 25 19:37:32 [5875]: IDS230/web-cgi-space-wildcard: 198.173.35.164:4221 ->

172.16.1.107:80

Apr 26 05:45:12 [6283]: IDS212/dns-zone-transfer: 38.31.107.87:2291 -> 172.16.1.101:53

Apr 26 06:43:05 [6283]: IDS181/nops-x86: 63.226.81.13:1351 -> 172.16.1.107:53

Apr 26 06:44:25 victim7 PAM_pwdb[12509]: (login) session opened for user simple by

(uid=0)

Apr 26 06:44:36 victim7 PAM_pwdb[12521]: (su) session opened for user simon by simple(uid=506)

Apr 26 06:45:34 [6283]: IDS175/socks-probe: 24.112.167.35:20 -> 172.16.1.107:1080

Apr 26 06:52:10 [6283]: IDS127/telnet-login-incorrect: 172.16.1.107:23 ->

213.28.22.189:4558

Precautionary measures to prevent this attack would include writing firewall rules.

Of these firewall rules, which among the following would be appropriate?
* Disallow UDP 53 in from outside to DNS server
* Allow UDP 53 in from DNS server to outside
* Disallow TCP 53 in from secondaries or ISP server to DNS server
* Block all UDP traffic

NO.282 Which command line tool is used to determine active network connections?
* netsh
* nbstat
* nslookup
* netstat

NO.283 POP3 (Post Office Protocol 3) is a standard protocol for receiving an email that deletes mail on the server as soon as the user downloads it. When a message arrives, the POP3 server appends it to the bottom of the recipient’s account file, which can be retrieved by the email client at any preferred time. Email client connects to the POP3 server at _____ by default to fetch emails.
* Port 123
* Port 110
* Port 115
* Port 109

NO.284 companyXYZ has asked you to assess the security of their perimeter email gateway. From your office in New York you craft a specially formatted email message and send it across the Internet to an employee of CompanyXYZ. The employee of CompanyXYZ is aware.
* Source code review
* Reviewing the firewalls configuration

* Data items and vulnerability scanning
* Interviewing employees and network engineers

NO.285 George is a senior security analyst working for a state agency in Florida. His state’s congress just passed a bill mandating every state agency to undergo a security audit annually. After learning what will be required, George needs to implement an IDS as soon as possible before the first audit occurs. The state bill requires that an IDS with a “time-based induction machine” be used.

What IDS feature must George implement to meet this requirement?
* Signature-based anomaly detection
* Pattern matching
* Real-time anomaly detection
* Statistical-based anomaly detection

NO.286 Harold wants to set up a firewall on his network but is not sure which one would be the most appropriate. He knows he needs to allow FTP traffic to one of the servers on his network, but he wants to only allow FTP-PUT. Which firewall would be most appropriate for

Harold? needs?
* Packet filtering firewall
* Circuit-level proxy firewall
* Application-level proxy firewall
* Data link layer firewall

NO.287 Where does the Windows 10 system store the metadata of the deleted files?
* INFO file
* INFO2 file
* Recycle Bin
* Deletes it permanently

NO.288 The need for computer forensics is highlighted by an exponential increase in the number of cybercrimes and litigations where large organizations were involved. Computer forensics plays an important role in tracking the cyber criminals. The main role of computer forensics is to:
* Maximize the investigative potential by maximizing the costs
* Harden organization perimeter security
* Document monitoring processes of employees of the organization
* Extract, process, and interpret the factual evidence so that it proves the attacker’s actions in the court

NO.289 Which command can provide the investigators with details of all the loaded modules on a Linux-based system?
* lsmod
* lsof -m
* list modules -a
* plist mod -a

NO.290 Which of the following Linux command searches through the current processes and lists the process IDs those match the selection criteria to stdout?
* pstree
* pgrep
* ps
* grep

NO.291 One way to identify the presence of hidden partitions on a suspect’s hard drive is to:
* Add up the total size of all known partitions and compare it to the total size of the hard drive
* Examine the FAT and identify hidden partitions by noting an H in the partition Type field
* Examine the LILO and note an H in the partition Type field
* It is not possible to have hidden partitions on a hard drive

NO.292 Which among the following U.S. laws requires financial institutions/companies that offer consumers financial products or services such as loans, financial or investment advice, or insurance to protect their customers’ information against security threats?
* HIPAA
* FISMA
* GLBA
* SOX

NO.293 You are working in the security Department of law firm. One of the attorneys asks you about the topic of sending fake email because he has a client who has been charged with doing just that. His client alleges that he is innocent and that there is no way for a fake email to actually be sent. You inform the attorney that his client is mistaken and that fake email is possibility and that you can prove it. You return to your desk and craft a fake email to the attorney that appears to come from his boss. What port do you send the email to on the company SMTP server?
* 10
* 25
* 110
* 135

NO.294 If you see the files Zer0.tar.gz and copy.tar.gz on a Linux system while doing an investigation, what can you conclude?
* The system files have been copied by a remote attacker
* The system administrator has created an incremental backup
* The system has been compromised using a t0rnrootkit
* Nothing in particular as these can be operational files

NO.295 How do you define forensic computing?
* It is the science of capturing, processing, and investigating data security incidents and making it acceptable to a court of law.
* It is a methodology of guidelines that deals with the process of cyber investigation
* It Is a preliminary and mandatory course necessary to pursue and understand fundamental principles of ethical hacking
* It is the administrative and legal proceeding in the process of forensic investigation

NO.296 Wireless access control attacks aim to penetrate a network by evading WLAN access control measures such as AP MAC filters and Wi-Fi port access controls. Which of the following wireless access control attacks allow the attacker to set up a rogue access point outside the corporate perimeter and then lure the employees of the organization to connect to it?
* Ad hoc associations
* Client mis-association
* MAC spoofing
* Rogue access points

NO.297 John is working on his company policies and guidelines. The section he is currently working on covers company documents; how they should be handled, stored, and eventually destroyed. John is concerned about the process whereby outdated documents are destroyed. What type of shredder should John write in the guidelines to be used when destroying documents?
* Strip-cut shredder
* Cross-cut shredder

* Cross-hatch shredder
* Cris-cross shredder

Actual 312-49v9 Exam Recently Updated Questions with Free Demo: https://www.vceprep.com/312-49v9-latest-vce-prep.html]