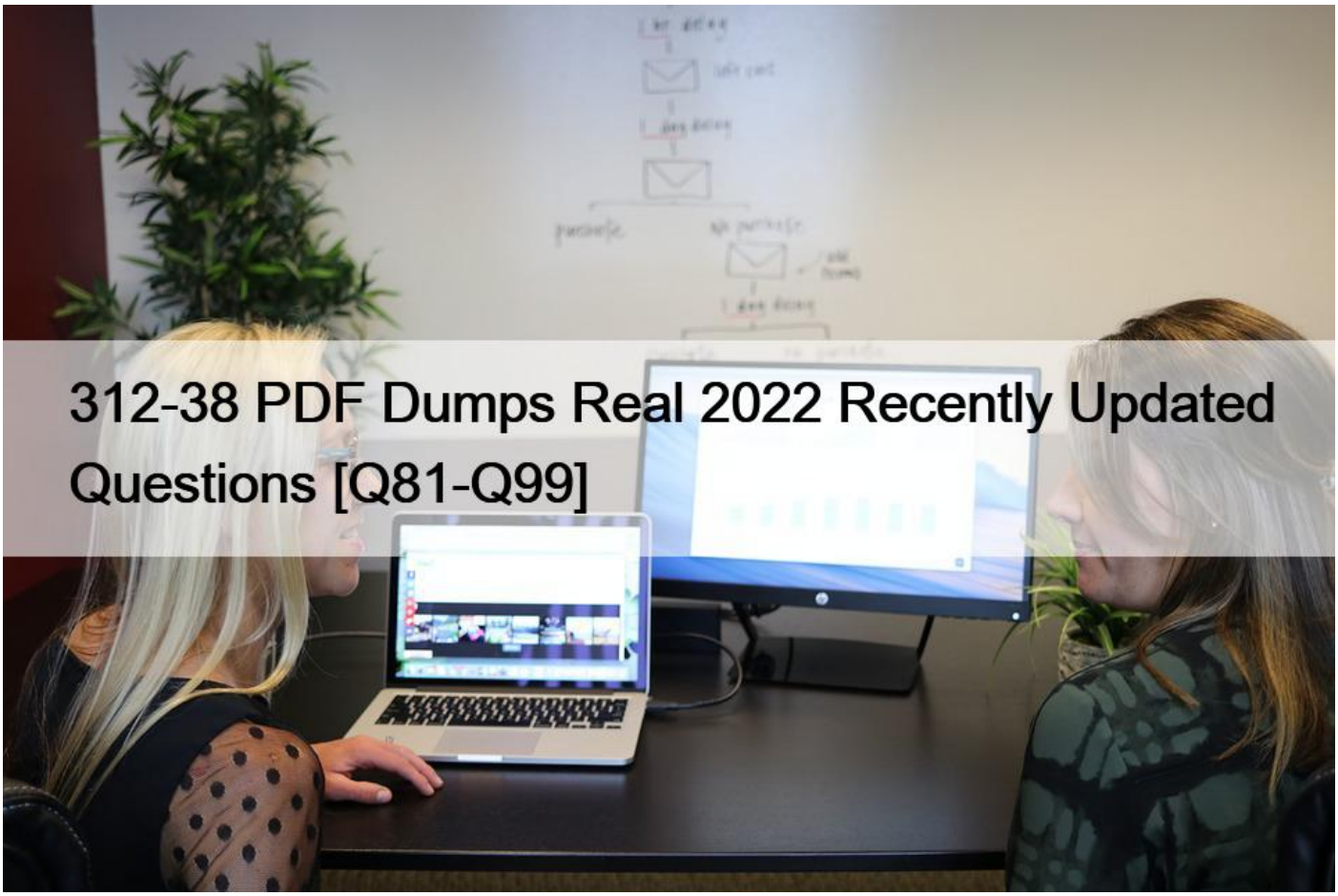
312-38 PDF Dumps Real 2022 Recently Updated Questions [Q81-Q99



312-38 PDF Dumps Real 2022 Recently Updated Questions
Released EC-COUNCIL 312-38 Updated Questions PDF

Prerequisites

The potential candidates must fulfill one of two options of eligibility criteria for this certification exam. The first thing is to complete the official training course, which can be taken as instructor-led training, academic learning, or online live training. The second variant is to opt for self-study. However, those who want to consider this option must have a minimum of two years of practical work experience in the domain of Information Technology. They should also have educational background that indicates a specialization in this area. To demonstrate this, they must submit a filled eligibility application form and pay the non-refundable application fee of $100.

Before you start the registration process, you should check if you qualify as one of the target audiences for this path. The intended candidates for EC-Council 312-38 are the security operators, network administrators, security analysts, network defense technicians, network security engineers, network security administrators, as well as any professionals who work with network operations.

QUESTION 81

Which of the following systems is formed by a group of honeypots?

* Research honeypot
* Honeyfarm
* Honeynet
* Production honeypot

QUESTION 82

Which of the following standards defines Logical Link Control (LLC)?
* 802.2
* 802.3
* 802.5
* 802.4

QUESTION 83

Each of the following is a network layer protocol used for a particular (MAC) address to obtain an IP address?
* ARP
* None
* RARP
* P.M
* PIM

QUESTION 84

Which of the following is a technique for gathering information about a remote network protected by a firewall?
* Firewalking
* Warchalking
* Wardriving
* Wardialing

Explanation

Explanation:

Fire walking is a technique for gathering information about a remote network protected by a firewall. This technique can be used effectively to perform information gathering attacks. In this technique, an attacker sends a crafted packet with a TTL value that is set to expire one hop past the firewall. If the firewall allows this crafted packet through, it forwards the packet to the next hop. On the next hop, the packet expires and elicits an ICMP

“TTL expired in transit” message to the attacker. If the firewall does not allow the traffic, there should be no response, or an ICMP “administratively prohibited” message should be returned to the attacker. A malicious attacker can use firewalking to determine the types of ports/protocols that can bypass the firewall. To use firewalking, the attacker needs the IP address of the last known gateway before the firewall and the IP address of a host located behind the firewall. The main drawback of this technique is that if an administrator blocks ICMP packets from leaving the network, it is ineffective.

Answer option B is incorrect. Warchalking is the drawing of symbols in public places to advertise an open Wi-Fi wireless network. Having found a Wi-Fi node, the warchalker draws a special symbol on a nearby object, such as a wall, the pavement, or a lamp post. The name warchalking is derived from the cracker terms war dialing and war driving.

Answer option C is incorrect. War driving, also called access point mapping, is the act of locating and possibly exploiting connections to wireless local area networks while driving around a city or elsewhere. To do war driving, one needs a vehicle, a

computer (which can be a laptop), a wireless Ethernet card set to work in promiscuous mode, and some kind of an antenna which can be mounted on top of or positioned inside the car.

Because a wireless LAN may have a range that extends beyond an office building, an outside user may be able to intrude into the network, obtain a free Internet connection, and possibly gain access to company records and other resources.

Answer option D is incorrect. War dialing or wardialing is a technique of using a modem to automatically scan a list of telephone numbers, usually dialing every number in a local area code to search for computers, Bulletin board systems, and fax machines. Hackers use the resulting lists for various purposes, hobbyists for exploration, and crackers – hackers that specialize in computer security – for password guessing.

QUESTION 85

Which of the following analyzes network traffic to trace specific transactions and can intercept and log traffic passing over a digital network? Each correct answer represents a complete solution. Choose all that apply.
* Wireless sniffer
* Spectrum analyzer
* Protocol analyzer
* Performance Monitor

Protocol analyzer (also known as a network analyzer, packet analyzer or sniffer, or for particular types of networks, an Ethernet sniffer or wireless sniffer) is computer software or computer hardware that can intercept and log traffic passing over a digital network. As data streams flow across the network, the sniffer captures each packet and, if needed, decodes and analyzes its content according to the appropriate RFC or other specifications.

Answer option D is incorrect. Performance Monitor is used to get statistical information about the hardware and software components of a server.

Answer option B is incorrect. A spectrum analyzer, or spectral analyzer, is a device that is used to examine the spectral composition of an electrical, acoustic, or optical waveform. It may also measure the power spectrum.

QUESTION 86

Identify the correct statements regarding a DMZ zone:
* It is a file integrity monitoring mechanism
* It is a Neutral zone between a trusted network and an untrusted network
* It serves as a proxy
* It includes sensitive internal servers such as database servers

QUESTION 87

What is the range for well known ports?
* 49152 through 65535
* 1024 through 49151
* Above 65535
* 0 through 1023

QUESTION 88

Which of the following techniques is used for drawing symbols in public places for advertising an open Wi-Fi

wireless network?
* Spamming
* War driving
* War dialing
* Warchalking

Warchalking is the drawing of symbols in public places to advertise an open Wi-Fi wireless network. Having found a Wi-Fi node, the warchalker draws a special symbol on a nearby object, such as a wall, the pavement, or a lamp post. The name warchalking is derived from the cracker terms war dialing and war driving.

Answer option B is incorrect. War driving, also called access point mapping, is the act of locating and possibly exploiting connections to wireless local area networks while driving around a city or elsewhere. To do war driving, one needs a vehicle, a computer (which can be a laptop), a wireless Ethernet card set to work in promiscuous mode, and some kind of an antenna which can be mounted on top of or positioned inside the car. Because a wireless LAN may have a range that extends beyond an office building, an outside user may be able to intrude into the network, obtain a free Internet connection, and possibly gain access to company records and other resources.

Answer option C is incorrect. War dialing is a technique of using a modem to automatically scan a list of telephone numbers, usually dialing every number in a local area code to search for computers, BBS systems, and fax machines. Hackers use the resulting lists for various purposes, hobbyists for exploration, and crackers (hackers that specialize in computer security) for password guessing.

Answer option A is incorrect. Spamming is the technique of flooding the Internet with a number of copies of the same message. The most widely recognized form of spams are e-mail spam, instant messaging spam, Usenet newsgroup spam, Web search engine spam, spam in blogs, online classified ads spam, mobile phone messaging spam, Internet forum spam, junk fax transmissions, social networking spam, television advertising and file sharing network spam.

QUESTION 89

Management asked Adam to implement a system allowing employees to use the same credentials to access multiple applications. Adam should implement the————————–authentication technique to satisfy the management request.
* Two-factor Authentication
* Smart Card Authentication

* Single-sign-on
* Biometric

QUESTION 90

Which of the following can be used to suppress fire from Class K sources?
* Water
* Carbon dioxide
* Foam
* Dry Chemical

QUESTION 91

Which of the following is a computer networking protocol used by hosts to retrieve IP address assignments and other configuration information?
* SNMP
* ARP
* DHCP
* Telnet

The Dynamic Host Configuration Protocol (DHCP) is a computer networking protocol used by hosts (DHCP clients) to retrieve IP address assignments and other configuration information. DHCP uses a client-server architecture. The client sends a broadcast request for configuration information. The DHCP server receives the request and responds with configuration information from its configuration database. In the absence of DHCP, all hosts on a network must be manually configured individually – a time-consuming and often error-prone undertaking. DHCP is popular with ISP’s because it allows a host to obtain a temporary IP address. Answer option B is incorrect. Address Resolution Protocol (ARP) is a network maintenance protocol of the TCP/IP protocol suite. It is responsible for the resolution of IP addresses to media access control (MAC) addresses of a network interface card (NIC). The ARP cache is used to maintain a correlation between a MAC address and its corresponding IP address. ARP provides the protocol rules for making this correlation and providing address conversion in both directions. ARP is limited to physical network systems that support broadcast packets. Answer option A is incorrect. The Simple Network Management Protocol (SNMP) allows a monitored device (for example, a router or a switch) to run an SNMP agent. This protocol is used for managing many network devices remotely. When a monitored device runs an SNMP agent, an SNMP server can then query the SNMP agent running on the device to collect information such as utilization statistics or device configuration information. An SNMP-managed network typically consists of three components: managed devices, agents, and one or more network management systems. Answer option D is incorrect. Telnet (Telecommunication network) is a network protocol used on the Internet or local area networks to provide a bidirectional interactive communications facility. Typically, Telnet provides access to a command-line interface on a remote host via a virtual terminal connection which consists of an 8-bit byte oriented data connection over the Transmission Control Protocol (TCP). User data is interspersed in-band with TELNET control information. Typically, the Telnet protocol is used to establish a connection to Transmission Control Protocol (TCP) port number 23.

QUESTION 92

Which of the following is a session layer protocol?
* RPC
* SLP
* RDP
* ICMP

QUESTION 93

Which of the following represents a network that connects two or more LANs in the same geographic area?

* PAN
* WAN
* MAN
* SAN

QUESTION 94

If a network is at risk resulting from misconfiguration performed by unskilled and/or unqualified individuals, what type of threat is this?
* External Threats
* Unstructured Threats
* Structured Threats
* Internal Threats

QUESTION 95

Which of the following statements are true about a wireless network?

Each correct answer represents a complete solution. Choose all that apply.
* Data can be shared easily between wireless devices.
* It provides mobility to users to access a network.
* Data can be transmitted in different ways by using Cellular Networks, Mobitex, DataTAC, etc.
* It is easy to connect.

The advantages of a wireless network are as follows:

It provides mobility to users to access a network.

It is easy to connect.

The initial cost to set up a wireless network is low as compared to that of manual cable

network.Data can be transmitted in different ways by using Cellular Networks, Mobitex, DataTAC,

etc.Data can be shared easily between the wireless devices.

QUESTION 96

What is the bit size of the Next Header field in the IPv6 header format?
* 2 bits
* 4 bits
* 8 bits
* 20 bits

QUESTION 97

Which of the following encryption techniques do digital signatures use?
* MD5
* RSA
* Blowfish
* IDEA

QUESTION 98

Which of the following is a term to describe the use of inert gases and chemical agents to extinguish a fire?
* Gaseous fire suppression
* Fire alarm system
* Fire sprinkler
* Fire suppression system

QUESTION 99

FILL BLANK

Fill in the blank with the appropriate term. _____ is the complete network configuration

and information toolkit that uses multi-threaded and multi-connection technologies in order to be very fast and

efficient.
NetRanger

Explanation:

NetRanger is the complete network configuration and information toolkit that includes the following tools: a

Ping tool, Trace Route tool, Host Lookup tool, Internet time synchronizer, Whois tool, Finger Unix hosts tool,

Host and port scanning tool, check multiple POP3 mail accounts tool, manage dialup connections tool, Quote

of the day tool, and monitor Network Settings tool. These tools are integrated in order to use an application

interface with full online help. NetRanger is designed for both new and experienced users. This tool is used to

help diagnose network problems and to get information about users, hosts, and networks on the Internet or on

a user computer network. NetRanger uses multi-threaded and multi-connection technologies in order to be

very fast and efficient.

How to study the Certified Network Defender

This is exam is very difficult for those candidates who don't practice during preparation and candidates need a lab for practicing. If you have completed CND training (online, instructor-led, or academia learning), you are eligible to attempt the CEH examination.

Once approved, the applicant will be sent instructions on purchasing a voucher from EC-Council store directly. EC-Council will then send the candidate the voucher code which candidate can use to register and schedule the test. Then practical exposure is much required to understand the contents of the exam. So, if anyone is associated with some kinds of an organization where he has opportunities to practice but if you can't afford the lab and don't have time to practice. So, ValidBraindumps is the solution to this problem. We provide the best **ECCOUNCIL EC 312-38 exam dumps** and practice test for your preparation. **ECCOUNCIL EC 312-38 exam dumps** to ensure your success in BCS Exam at first attempt. Our EC 312-38 exam dumps are updated on regular basis. ValidBraindumps has the combination of PDF and VCE file that will be much helpful for candidates in passing the exam. ValidBraindumps provides verified questions with relevant answers which will be asked from candidates in their final exam. So, it makes it for candidates to get good grades in the final exam and one of the best features is we also provide **ECCOUNCIL EC 312-38 exam dumps** in PDF format which is candidates can download and study offline. Use our **ECCOUNCIL EC 312-38 practice exams** and **ECCOUNCIL EC 312-38 practice exams** for preparing these topics.

312-38 Dumps and Practice Test (171 Exam Questions): https://www.validbraindumps.com/312-38-exam-prep.html]