312-38$^{\text{Q\&As}}$

Certified Network Defender (CND)

Pass EC-COUNCIL 312-38 Exam with 100% Guarantee

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

https://www.leads4pass.com/312-38.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

Which of the following is a session layer protocol?

A. RPC

B. SLP

C. RDP

D. ICMP

Correct Answer: A

QUESTION 2

Which of the following protocols is used by the Remote Authentication Dial In User Service (RADIUS) client/server protocol for data transmission?

A. DCCP

B. FTP

C. FCP

D. UDP

Correct Answer: D

QUESTION 3

John visits an online shop that stores the IDs and prices of the items to buy in a cookie. After selecting the items that he wants to buy, the attacker changes the price of the item to 1. Original cookie values:

ItemID1=2 ItemPrice1=900 ItemID2=1 ItemPrice2=200 Modified cookie values: ItemID1=2 ItemPrice1=1 ItemID2=1 ItemPrice2=1

Now, he clicks the Buy button, and the prices are sent to the server that calculates the total price. Which of the following hacking techniques is John performing?

A. Computer-based social engineering

B. Man-in-the-middle attack

C. Cookie poisoning

D. Cross site scripting

Correct Answer: C

John is performing cookie poisoning. In cookie poisoning, an attacker modifies the value of cookies before sending them back to the server. On modifying the cookie values, an attacker can log in to any other user account and can perform identity theft. The following figure explains how cookie poisoning occurs:

For example: The attacker visits an online shop that stores the IDs and prices of the items to buy in a cookie. After selecting the items that he wants to buy, the attacker changes the price of the item to 1. Original cookie values: ItemID1= 2 ItemPrice1=900 ItemID2=1 ItemPrice2=200 Modified cookie values: ItemID1= 2 ItemPrice1=1 ItemID2=1 ItemPrice2=1 Now, the attacker clicks the Buy button and the prices are sent to the server that calculates the total price. Another use of a Cookie Poisoning attack is to pretend to be another user after changing the username in the cookie values: Original cookie values: LoggedIn= True Username = Mark Modified cookie values: LoggedIn= True Username = Admin Now, after modifying the cookie values, the attacker can do the admin login. Answer option D is incorrect. A cross site scripting attack is one in which an attacker enters malicious data into a Website. For example, the attacker posts a message that contains malicious code to any newsgroup site. When another user views this message, the browser interprets this code and executes it and, as a result, the attacker is able to take control of the user\\'s system. Cross site scripting attacks require the execution of client-side languages such as JavaScript, Java, VBScript, ActiveX, Flash, etc. within a user\\'s Web environment. With the help of a cross site scripting attack, the attacker can perform cookie stealing, sessions hijacking, etc.

QUESTION 4

Which of the following tools is a free laptop tracker that helps in tracking a user\\'s laptop in case it gets stolen?

A. SAINT

B. Adeona

C. Snort

D. Nessus

Correct Answer: B

Adeona is a free laptop tracker that helps in tracking a user\\'s laptop in case it gets stolen. All it takes is to install the Adeona software client on the user\\'s laptop, pick a password, and make it run in the background. If at one point, the user\\'s laptop gets stolen and is connected to the Internet, the Adeona software sends the criminal\\'s IP address. Using the Adeona Recovery, the IP address can then be retrieved. Knowing the IP address helps in tracking the geographical location of the stolen device. Answer option D is incorrect. Nessus is proprietary comprehensive vulnerability scanning software. It is free of charge for personal use in a non-enterprise environment. Its goal is to detect potential vulnerabilities on tested systems. It is capable of checking various types of vulnerabilities, some of which are as follows: Vulnerabilities that allow a remote cracker to control or access sensitive data on a system Misconfiguration (e.g. open mail relay, missing patches, etc), Default passwords, a few common passwords, and blank/absent passwords on some system accounts. Nessus can also call Hydra (an external tool) to launch a dictionary attack. Denials of service against the TCP/IP stack by using mangled packets Answer option A is incorrect. SAINT stands for System Administrator\\'s Integrated Network Tool. It is computer software used for scanning computer networks for security vulnerabilities, and exploiting found vulnerabilities. The SAINT scanner screens every live system on a network for TCP and UDP services. For each service it finds running, it launches a set of probes designed to detect anything that could allow an attacker to gain unauthorized access, create a denial-of-service, or gain sensitive information about the network. Answer option C is incorrect. Snort is an open source network intrusion detection system. The Snort application analyzes network traffic in realtime mode. It performs packet sniffing, packet logging, protocol analysis, and a content search to detect a variety of potential attacks.

QUESTION 5

Which type of wireless network threats an attacker stakes out the area from a nearby location with a high gain amplifier drowning out the legitimate access point?

A. Rogue access point attack

B. Jamming signal attack

C. Ad Hoc Connection attack

D. Unauthorized association

Correct Answer: B

QUESTION 6

John works as an Ethical Hacker for www.company.com Inc. He wants to find out the ports that are open in www.company.com\\'s server using a port scanner. However, he does not want to establish a full TCP connection. Which of the following scanning techniques will he use to accomplish this task?

A. TCP SYN

B. Xmas tree

C. TCP SYN/ACK

D. TCP FIN

Correct Answer: A

According to the scenario, John does not want to establish a full TCP connection. Therefore, he will use the TCP SYN scanning technique. TCP SYN scanning is also known as half-open scanning because in this type of scanning, a full TCP connection is never opened. The steps of TCP SYN scanning are as follows: 1.The attacker sends a SYN packet to the target port. 2.If the port is open, the attacker receives the SYN/ACK message. 3.Now the attacker breaks the connection by sending an RST packet. 4.If the RST packet is received, it indicates that the port is closed. This type of scanning is hard to trace because the attacker never establishes a full 3-way handshake connection and most sites do not create a log of incomplete TCP connections. Answer option C is incorrect. In TCP SYN/ACK scanning, an attacker sends a SYN/ACK packet to the target port. If the port is closed, the victim assumes that this packet was mistakenly sent by the attacker, and sends the RST packet to the attacker. If the port is open, the SYN/ACK packet will be ignored and the port will drop the packet. TCP SYN/ACK scanning is stealth scanning, but some intrusion detection systems can detect TCP SYN/ACK scanning. Answer option D is incorrect. TCP FIN scanning is a type of stealth scanning through which the attacker sends a FIN packet to the target port. If the port is closed, the victim assumes that this packet was sent mistakenly by the attacker and sends the RST packet to the attacker. If the port is open, the FIN packet will be ignored and the port will drop that packet. TCP FIN scanning is useful only for identifying ports of non-Windows operating systems because Windows operating systems send only RST packets irrespective of whether the port is open or closed. Answer option B is incorrect. Xmas Tree scanning is just the opposite of null scanning. In Xmas Tree scanning, all packets are turned on. If the target port is open, the service running on the target port discards the packets without any reply. According to RFC 793, if the port is closed, the remote system replies with the RST packet. Active monitoring of all incoming packets can help system network administrators detect an Xmas Tree scan.

QUESTION 7

Katie has implemented the RAID level that splits data into blocks and evenly writes the data to multiple hard drives but does not provide data redundancy. This type of RAID level requires a minimum of __________ in order to setup.

A. Two drives

B. Three drives

C. Six drives

D. Four drives

Correct Answer: A

QUESTION 8

Brendan wants to implement a hardware based RAID system in his network. He is thinking of choosing a suitable RAM type for the architectural setup in the system. The type he is interested in provides access times of up to 20 ns. Which type of RAM will he select for his RAID system?

A. NVRAM

B. SDRAM

C. NAND flash memory

D. SRAM

Correct Answer: D

QUESTION 9

James is a network administrator working at a student loan company in Minnesota. This company processes over 20,000 student loans a year from colleges all over the state. Most communication between the company, schools, and lenders is carried out through emails. Much of the email communication used at his company contains sensitive information such as social security numbers. For this reason, James wants to utilize email encryption. Since a server-based PKI is not an option for him, he is looking for a low/no cost solution to encrypt emails. What should James use?

A. James should utilize the free OTP software package.

B. James can enforce mandatory HTTPS in the email clients to encrypt emails.

C. James could use PGP as a free option for encrypting the company\\'s emails.

D. James can use MD5 algorithm to encrypt all the emails.

Correct Answer: C

QUESTION 10

Jason works as a System Administrator for www.company.com Inc. The company has a Windows-based network. Sam, an employee of the company, accidentally changes some of the applications and system settings. He complains to Jason that his system is not working properly. To troubleshoot the problem, Jason diagnoses the internals of his computer and observes that some changes have been made in Sam\\'s computer registry. To rectify the issue, Jason has to restore the registry. Which of the following utilities can Jason use to accomplish the task? Each correct answer represents a complete solution. Choose all that apply.

A. Reg.exe

B. EventCombMT

C. Regedit.exe

D. Resplendent registrar

Correct Answer: ACD

The resplendent registrar is a tool that offers a complete and safe solution to administrators and power users for maintaining the registry. It can be used for maintaining the registry of desktops and remote computers on the network. It offers a solution for backing up and restoring registries, fast background search and replace, adding descriptions to the registry keys, etc. This program is very attractive and easy to use, as it comes in an explorer-style interface. It can be used for Windows 2003/XP/2K/NT/ME/9x. Reg.exe is a command-line utility that is used to edit the Windows registry. It has the ability to import, export, back up, and restore keys, as well as to compare, modify, and delete keys. It can perform almost all tasks that can be done using the Windows-based Regedit.exe tool. Registry Editor (REGEDIT) is a registry editing utility that can be used to look at information in the registry. REGEDIT.EXE enables users to search for strings, values, keys, and subkeys and is useful to find a specific value or string. Users can also use REGEDIT.EXE to add, delete, or modify registry entries. Answer option B is incorrect. EventCombMT is a multithreaded tool that is used to search the event logs of several different computers for specific events, all from one central location. It is a little-known Microsoft tool to run searches for event IDs or text strings against Windows event logs for systems, applications, and security, as well as File Replication Service (FRS), domain name system (DNS), and Active Directory (AD) logs where applicable. The MT stands for multi-threaded. The program is part of the Account Lockout and Management Tools program package for Windows 2000, 2003, and XP.

QUESTION 11

Eric is receiving complaints from employees that their systems are very slow and experiencing odd issues including restarting automatically and frequent system hangs. Upon investigating, he is convinced the systems are infected with a virus that forces systems to shut down automatically after period of time. What type of security incident are the employees a victim of?

A. Scans and probes

B. Malicious Code

C. Denial of service

D. Distributed denial of service

Correct Answer: B

QUESTION 12

Which of the following help in estimating and totaling up the equivalent money value of the benefits and costs to the community of projects for establishing whether they are worthwhile? Each correct answer represents a complete solution. Choose all that apply.

A. Business Continuity Planning

B. Benefit-Cost Analysis

C. Disaster recovery

D. Cost-benefit analysis

Correct Answer: DB

Cost-benefit analysis is a process by which business decisions are analyzed. It is used to estimate and total up the equivalent money value of the benefits and costs to the community of projects for establishing whether they are worthwhile. It is a term that refers both to: helping to appraise, or assess, the case for a project, program, or policy proposal; an approach to making economic decisions of any kind. Under both definitions, the process involves, whether explicitly or implicitly, weighing the total expected costs against the total expected benefits of one or more actions in order to choose the best or most profitable option. The formal process is often referred to as either CBA (Cost-Benefit Analysis) or BCA (Benefit-Cost Analysis). Answer option A is incorrect. Business Continuity Planning (BCP) is the creation and validation of a practiced logistical plan that defines how an organization will recover and restore partially or completely interrupted critical (urgent) functions within a predetermined time after a disaster or extended disruption. The logistical plan is called a Business Continuity Plan. Answer option C is incorrect. Disaster recovery is the process, policies, and procedures related to preparing for recovery or continuation of technology infrastructure critical to an organization after a natural or human-induced disaster. Disaster recovery planning is a subset of a larger process known as business continuity planning and should include planning for resumption of applications, data, hardware, communications (such as networking) and other IT infrastructure. A business continuity plan (BCP) includes planning for non-IT related aspects such as key personnel, facilities, crisis communication and reputation protection, and should refer to the disaster recovery plan (DRP) for IT related infrastructure recovery / continuity.

QUESTION 13

Which of the following intrusion detection techniques observes the network for abnormal usage patterns by determining the performance parameters for regular activities and monitoring for actions beyond the normal parameters?

A. Statistical anomaly detection

B. Signature/Pattern matching

C. None of these

D. Stateful protocol analysis

Correct Answer: A

QUESTION 14

Which of the following is a worldwide organization that aims to establish, refine, and promote Internet security standards?

A. ANSI

B. WASC

C. IEEE

D. ITU

Correct Answer: B

Web Application Security Consortium (WASC) is a worldwide organization that aims to establish, refine, and promote Internet security standards. WASC is vendor-neutral, although members may belong to corporations involved in the

research, development, design, and distribution of Web security-related products.

Answer option A is incorrect. ANSI (American National Standards Institute) is the primary organization for fostering the development of technology standards in the United States. ANSI works with industry groups and is the U.S. member of the

International Organization for Standardization (ISO) and the International Electro-technical Commission (IEC). Long-established computer standards from ANSI include the American Standard Code for Information Interchange (ASCII) and the

Small Computer System Interface (SCSI).

Answer option D is incorrect. The International Telecommunication Union (ITU) is an organization established to standardize and regulate international radio and telecommunications. Its main tasks include standardization, allocation of the

radio spectrum, and organizing interconnection arrangements between different countries to allow international phone calls. ITU sets standards for global telecom networks. The ITU\\'s telecommunications division (ITU-T) produces more than

200 standard recommendations each year in the converging areas of telecommunications, information technology, consumer electronics, broadcasting and multimedia communications. ITU was streamlined into the following three sectors:

ITU-D (Telecommunication Development)

ITU-R (Radio communication)

ITU-T (Telecommunication Standardization)

Answer option C is incorrect. The Institute of Electrical and Electronic Engineers (IEEE) is a society of technical professionals. It promotes the development and application of electro-technology and allied sciences. IEEE develops

communications and network standards, among other activities. The organization publishes number of journals, has many local chapters, and societies in specialized areas.

QUESTION 15

Which of the following steps of the OPSEC process examines each aspect of the planned operation to identify OPSEC indicators that could reveal critical information and then compare those indicators with the adversary\\'s intelligence collection capabilities identified in the previous action?

A. Analysis of Threats

B. Application of Appropriate OPSEC Measures

C. Identification of Critical Information

D. Analysis of Vulnerabilities

E. Assessment of Risk

Correct Answer: D

OPSEC is a 5-step process that helps in developing protection mechanisms in order to safeguard sensitive information and preserve essential secrecy.

The OPSEC process has five steps, which are as follows:

1.Identification of Critical Information: This step includes identifying information vitally needed by an adversary, which focuses the remainder of the OPSEC process on protecting vital information, rather than attempting to protect all classified

or sensitive unclassified information.

2.Analysis of Threats: This step includes the research and analysis of intelligence, counter-intelligence, and open source information to identify likely adversaries to a planned operation. 3.Analysis of Vulnerabilities: It includes examining each

aspect of the planned operation to identify OPSEC indicators that could reveal critical information and then comparing those indicators with the adversary\\'s intelligence collection capabilities identified in the previous action.

4.Assessment of Risk: Firstly, planners analyze the vulnerabilities identified in the previous action and identify possible OPSEC measures for each vulnerability. Secondly, specific OPSEC measures are selected for execution based upon a

risk assessment done by the commander and staff.

5.Application of Appropriate OPSEC Measures: The command implements the OPSEC measures selected in the assessment of risk action or, in the case of planned future operations and activities, includes the measures in specific OPSEC

plans.