312-38Q&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.geekcert.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

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 2

Which of the following is not part of the recommended first response steps for network defenders?

A. Restrict yourself from doing the investigation

B. Extract relevant data from the suspected devices as early as possible

C. Disable virus protection

D. Do not change the state of the suspected device

Correct Answer: D

QUESTION 3

Which of the following data security technology can ensure information protection by obscuring specific areas of information?

A. Data retention

B. Data encryption

C. Data hashing

D. Data masking

Correct Answer: D

QUESTION 4

The IP addresses reserved for experimental purposes belong to which of the following classes?

A. Class E

B. Class C

C. Class A

D. Class D

Correct Answer: A

QUESTION 5

Alice wants to prove her identity to Bob. Bob requests her password as proof of identity, which Alice dutifully provides (possibly after some transformation like a hash function); meanwhile, Eve is eavesdropping the conversation and keeps the password. After the interchange is over, Eve connects to Bob posing as Alice; when asked for a proof of identity, Eve sends Alice\\'s password read from the last session, which Bob accepts. Which of the following attacks is being used by Eve?

A. Replay

B. Fire walking

C. Cross site scripting

D. Session fixation

Correct Answer: A

Eve is using Replay attack. A replay attack is a type of attack in which attackers capture packets containing passwords or digital signatures whenever packets pass between two hosts on a network. In an attempt to obtain an authenticated connection, the attackers then resend the captured packet to the system. In this type of attack, the attacker does not know the actual password, but can simply replay the captured packet. Session tokens can be used to avoid replay attacks. Bob sends a one-time token to Alice, which Alice uses to transform the password and send the result to Bob (e.g. computing a hash function of the session token appended to the password). On his side Bob performs the same computation; if and only if both values match, the login is successful. Now suppose Mallory has captured this value and tries to use it on another session; Bob sends a different session token, and when Mallory replies with the captured value

it will be different from Bob\\'s computation. Answer option C is incorrect. In the cross site scripting attack, an attacker tricks the user\\'s computer into running code, which is treated as trustworthy because it appears to belong to the server, allowing the attacker to obtain a copy of the cookie or perform other operations. Answer option B is incorrect. Firewalking 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. Answer option D is incorrect. In session fixation, an attacker sets a user\\'s session id to one known to him, for example by sending the user an email with a link that contains a particular session id. The attacker now only has to wait until the user logs in.