312-38 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.pass4itsure.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

Instant Download After Purchase
100% Money Back Guarantee
365 Days Free Update
800,000+ Satisfied Customers

QUESTION 1

Which of the following tool is used for passive attacks to capture network traffic?

A. Intrusion prevention system

B. Intrusion detection system

C. Sniffer

D. warchalking

E. None

Correct Answer: C

QUESTION 2

The SNMP contains various commands that reduce the burden on the network administrators. Which of the following commands is used by SNMP agents to notify SNMP managers about an event occurring in the network?

A. INFORM

B. RESPONSE

C. TRAPS

D. SET

Correct Answer: C

QUESTION 3

Which of the following steps are required in an idle scan of a closed port? Each correct answer represents a part of the solution. Choose all that apply.

A. The attacker sends a SYN/ACK to the zombie.

B. The zombie\\'s IP ID increases by only 1.

C. In response to the SYN, the target sends a RST.

D. The zombie ignores the unsolicited RST, and the IP ID remains unchanged.

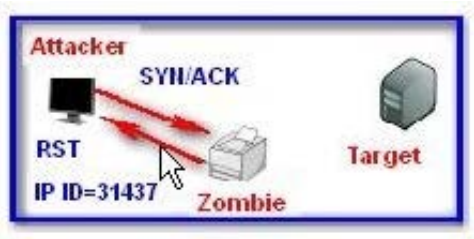
E. The zombie\\'s IP ID increases by 2.

Correct Answer: ACDB

Following are the steps required in an idle scan of a closed port:

1.Probe the zombie\\'s IP ID: The attacker sends a SYN/ACK to the zombie. The zombie, unaware of the SYN/ACK,

sends back a RST, thus disclosing its IP ID.



2.Forge a SYN packet from the zombie: In response to the SYN, the target sends a RST. The zombie ignores the unsolicited RST, and the IP ID remains unchanged.

3.Probe the zombie\\'s IP ID again: The zombie\\'s IP ID has increased by only 1 since step 1. So the port is closed.

QUESTION 4

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 5

Which of the following IEEE standards operates at 2.4 GHz bandwidth and transfers data at a rate of 54 Mbps?

A. 802.11r

B. 802.11n

C. 802.11g

D. 802.11a

Correct Answer: C

312-38 Study Guide 312-38 Exam Questions 312-38 Braindumps