DUMPSQUEEN

Hacker Tools, Techniques, Exploits and Incident Handling

SANS SEC504

Version Demo

Total Demo Questions: 15

Total Premium Questions: 328

Buy Premium PDF

https://dumpsqueen.com

support@dumpsqueen.com

Topic Break Down

Topic	No. of Questions
Topic 1, Volume A	97
Topic 2, Volume B	96
Topic 3, Volume C	135
Total	328

QUESTION NO: 1

OutGuess is used for _____ attack.

A. Steganography

B. Web password cracking

C. SQL injection

D. Man-in-the-middle

ANSWER: A

QUESTION NO: 2

Which of the following is a technique for creating Internet maps?

Each correct answer represents a complete solution. Choose two.

A. Active Probing

B. AS PATH Inference

C. Object Relational Mapping

D. Network Quota

ANSWER: A B

QUESTION NO: 3

Session splicing is an IDS evasion technique in which an attacker delivers data in multiple small-sized packets to the target computer. Hence, it becomes very difficult for an IDS to detect the attack signatures of such attacks. Which of the following tools can be used to perform session splicing attacks?

Each correct answer represents a complete solution. Choose all that apply.

A. Whisker

B. Fragroute

C. Nessus

D. Y.A.T.

ANSWER: A C

QUESTION NO: 4

Your friend plans to install a Trojan on your computer. He knows that if he gives you a new version of chess.exe, you will definitely install the game on your computer. He picks up a Trojan and joins it with chess.exe. Which of the following tools are required in such a scenario?

Each correct answer represents a part of the solution. Choose three.

A. NetBus

B. Absinthe

C. Yet Another Binder

D. Chess.exe

ANSWER: A C D

QUESTION NO: 5

Which of the following tools is described in the statement given below?

"It has a database containing signatures to be able to detect hundreds of vulnerabilities in UNIX, Windows, and commonly used web CGI scripts. Moreover, the database detects DdoS zombies and Trojans as well."

A. SARA

B. Nessus

C. Anti-x

D. Nmap

ANSWER: B

QUESTION NO: 6

Which of the following statements are true about firewalking?

Each correct answer represents a complete solution. Choose all that apply.

A. 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.

B. In this technique, an attacker sends a crafted packet with a TTL value that is set to expire one hop past the firewall.

C. A malicious attacker can use firewalking to determine the types of ports/protocols that can bypass the firewall.

D. Firewalking works on the UDP packets.

ANSWER: A B C

QUESTION NO: 7

In the DNS Zone transfer enumeration, an attacker attempts to retrieve a copy of the entire zone file for a domain from a DNS server. The information provided by the DNS zone can help an attacker gather user names, passwords, and other valuable information. To attempt a zone transfer, an attacker must be connected to a DNS server that is the authoritative server for that zone. Besides this, an attacker can launch a Denial of Service attack against the zone's DNS servers by flooding them with a lot of requests. Which of the following tools can an attacker use to perform a DNS zone transfer?

Each correct answer represents a complete solution. Choose all that apply.

A. Host

B. Dig

C. DSniff

D. NSLookup

ANSWER: A B D

QUESTION NO: 8

Which of the following types of attacks is mounted with the objective of causing a negative impact on the performance of a computer or network?

A. Vulnerability attack

B. Man-in-the-middle attack

C. Denial-of-Service (DoS) attack

D. Impersonation attack

ANSWER: C

QUESTION NO: 9 - (FILL BLANK)

Fill in the blank with the appropriate name of the attack.

_____ takes best advantage of an existing authenticated connection

Answer: session hijacking

ANSWER: session hijacking

QUESTION NO: 10

Which of the following Incident handling process phases is responsible for defining rules, collaborating human workforce, creating a back-up plan, and testing the plans for an enterprise?

A. Preparation phase

B. Eradication phase

C. Identification phase

D. Recovery phase

E. Containment phase

ANSWER: A

QUESTION NO: 11

Which of the following systems is used in the United States to coordinate emergency preparedness and incident management among various federal, state, and local agencies?

A. US Incident Management System (USIMS)

B. National Disaster Management System (NDMS)

C. National Emergency Management System (NEMS)

D. National Incident Management System (NIMS)

ANSWER: D

QUESTION NO: 12

You are concerned about rootkits on your network communicating with attackers outside your network. Without using an IDS how can you detect this sort of activity?

A. By examining your domain controller server logs.

B. You cannot, you need an IDS.

C. By examining your firewall logs.

D. By setting up a DMZ.

ANSWER: C

QUESTION NO: 13

Which of the following attacks can be overcome by applying cryptography?

A. Buffer overflow

B. Web ripping

C. Sniffing

D. DoS

ANSWER: C

QUESTION NO: 14

Which of the following tools can be used to perform brute force attack on a remote database?

Each correct answer represents a complete solution. Choose all that apply.

A. SQLBF

B. SQLDict

C. FindSA

D. nmap

ANSWER: A B C

QUESTION NO: 15

Which of the following types of attacks is only intended to make a computer resource unavailable to its users?

A. Denial of Service attack

B. Replay attack

C. Teardrop attack

D. Land attack

ANSWER: A