DUMPSARENA

Certified Ethical Hacker (CEH)

GAQM CEH-001

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

Take a look at the following attack on a Web Server using obstructed URL:

```
http://www.certifiedhacker.com/script.ext?
template=%2e%2e%2f%2e%2e%2f%2e%2e%2f%65%74%63%2f%70%61%73%73%77%64
This request is made up of:
%2e%2e%2f%2e%2e%2f%2e%2e%2f = ../../../
%65%74%63 = etc
%2f = /
%70%61%73%73%77%64 = passwd
```

How would you protect from these attacks?

A. Configure the Web Server to deny requests involving "hex encoded" characters

B. Create rules in IDS to alert on strange Unicode requests

C. Use SSL authentication on Web Servers

D. Enable Active Scripts Detection at the firewall and routers

ANSWER: B

QUESTION NO: 2

The programmers on your team are analyzing the free, open source software being used to run FTP services on a server. They notice that there is an excessive number of fgets() and gets() on the source code. These C++ functions do not check bounds.

What kind of attack is this program susceptible to?

A. Buffer of Overflow

B. Denial of Service

C. Shatter Attack

D. Password Attack

ANSWER: A

QUESTION NO: 3

E-mail scams and mail fraud are regulated by which of the following?

A. 18 U.S.C. par. 1030 Fraud and Related activity in connection with Computers

B. 18 U.S.C. par. 1029 Fraud and Related activity in connection with Access Devices

C. 18 U.S.par. 1362 Communication Lines, Stations, or Systems

D. 18 U.S.C. par. 2510 Wire and Electronic Communications Interception and Interception of Oral Communication

ANSWER: A

QUESTION NO: 4

Liza has forgotten her password to an online bookstore. The web application asks her to key in her email so that they can send her the password. Liza enters her email liza@yahoo.com'. The application displays server error. What is wrong with the web application?

A. The email is not valid

B. User input is not sanitized

C. The web server may be down

D. The ISP connection is not reliable

ANSWER: B

Explanation:

http://www.cert.org/advisories/CA-1997-25.html

http://www.cert.org/advisories/CA-2000-02.html

QUESTION NO: 5

How do you defend against Privilege Escalation?

A. Use encryption to protect sensitive data

B. Restrict the interactive logon privileges

C. Run services as unprivileged accounts

D. Allow security settings of IE to zero or Low

E. Run users and applications on the least privileges

ANSWER: A B C E

QUESTION NO: 6

Which of the following settings enables Nessus to detect when it is sending too many packets and the network pipe is approaching capacity?

A. Netstat WMI Scan

B. Silent Dependencies

C. Consider unscanned ports as closed

D. Reduce parallel connections on congestion

ANSWER: D

QUESTION NO: 7

The SYN flood attack sends TCP connections requests faster than a machine can process them.

How do you protect your network against SYN Flood attacks?

A. SYN cookies. Instead of allocating a record, send a SYN-ACK with a carefully constructed sequence number generated as a hash of the clients IP address, port number, and other information. When the client responds with a normal ACK, that special sequence number will be included, which the server then verifies. Thus, the server first allocates memory on the third packet of the handshake, not the first.

B. RST cookies - The server sends a wrong SYN/ACK back to the client. The client should then generate a RST packet telling the server that something is wrong. At this point, the server knows the client is valid and will now accept incoming connections from that client normally

C. Check the incoming packet's IP address with the SPAM database on the Internet and enable the filter using ACLs at the Firewall

D. Stack Tweaking. TCP stacks can be tweaked in order to reduce the effect of SYN floods. Reduce the timeout before a stack frees up the memory allocated for a connection

E. Micro Blocks. Instead of allocating a complete connection, simply allocate a micro record of 16-bytes for the incoming SYN object

ANSWER: A B D E

QUESTION NO: 8

Which of the following types of firewall inspects only header information in network traffic?

A. Packet filter

B. Stateful inspection

C. Circuit-level gateway

D. Application-level gateway

ANSWER: A

QUESTION NO: 9

Peter, a Network Administrator, has come to you looking for advice on a tool that would help him perform SNMP enquires over the network. Which of these tools would do the SNMP enumeration he is looking for?

Select the best answers.

A. SNMPUtil

B. SNScan

C. SNMPScan

D. Solarwinds IP Network Browser

E. NMap

ANSWER: A B D

QUESTION NO: 10

Buffer X in an Accounting application module for Brownies Inc. can contain 200 characters. The programmer makes an assumption that 200 characters are more than enough. Because there were no proper boundary checks being conducted, Bob decided to insert 400 characters into the 200-character buffer. (Overflows the buffer). Below is the code snippet:

```
Void func (void)
{
int I; char buffer [200];
for (I=0; I<400; I++)
buffer [I]= 'A';
return;
}
```

How can you protect/fix the problem of your application as shown above?

A. Because the counter starts with 0, we would stop when the counter is less than 200

B. Because the counter starts with 0, we would stop when the counter is more than 200

C. Add a separate statement to signify that if we have written less than 200 characters to the buffer, the stack should stop because it cannot hold any more data

D. Add a separate statement to signify that if we have written 200 characters to the buffer, the stack should stop because it cannot hold any more data

ANSWER: A D

QUESTION NO: 11

Frederickson Security Consultants is currently conducting a security audit on the networks of Hawthorn Enterprises, a contractor for the Department of Defense. Since Hawthorn Enterprises conducts business daily with the federal government, they must abide by very stringent security policies. Frederickson is testing all of Hawthorn's physical and logical security measures including biometrics, passwords, and permissions. The federal government requires that all users must utilize random, non-dictionary passwords that must take at least 30 days to crack. Frederickson has confirmed that all Hawthorn employees use a random password generator for their network passwords. The Frederickson consultants have saved off numerous SAM files from Hawthorn's servers using Pwdump6 and are going to try and crack the network passwords. What method of attack is best suited to crack these passwords in the shortest amount of time?

A. Brute force attack

B. Birthday attack

C. Dictionary attack

D. Brute service attack

ANSWER: A

QUESTION NO: 12

Blane is a network security analyst for his company. From an outside IP, Blane performs an XMAS scan using Nmap. Almost every port scanned does not illicit a response. What can he infer from this kind of response?

A. These ports are open because they do not illicit a response.

B. He can tell that these ports are in stealth mode.

C. If a port does not respond to an XMAS scan using NMAP, that port is closed.

D. The scan was not performed correctly using NMAP since all ports, no matter what their state, will illicit some sort of response from an XMAS scan.

ANSWER: A

QUESTION NO: 13

Which of the following are potential attacks on cryptography? (Select 3)

A. One-Time-Pad Attack

B. Chosen-Ciphertext Attack

C. Man-in-the-Middle Attack

D. Known-Ciphertext Attack

E. Replay Attack

ANSWER: B C E

QUESTION NO: 14

You visit a website to retrieve the listing of a company's staff members. But you can not find it on the website. You know the listing was certainly present one year before. How can you retrieve information from the outdated website?

A. Through Google searching cached files

B. Through Archive.org

C. Download the website and crawl it

D. Visit customers' and prtners' websites

ANSWER: B

QUESTION NO: 15

One of your junior administrator is concerned with Windows LM hashes and password cracking. In your discussion with them, which of the following are true statements that you would point out?

Select the best answers.

A. John the Ripper can be used to crack a variety of passwords, but one limitation is that the output doesn't show if the password is upper or lower case.

B. BY using NTLMV1, you have implemented an effective countermeasure to password cracking.

C. SYSKEY is an effective countermeasure.

D. If a Windows LM password is 7 characters or less, the hash will be passed with the following characters, in HEX-0011223344556677889.

E. Enforcing Windows complex passwords is an effective countermeasure.

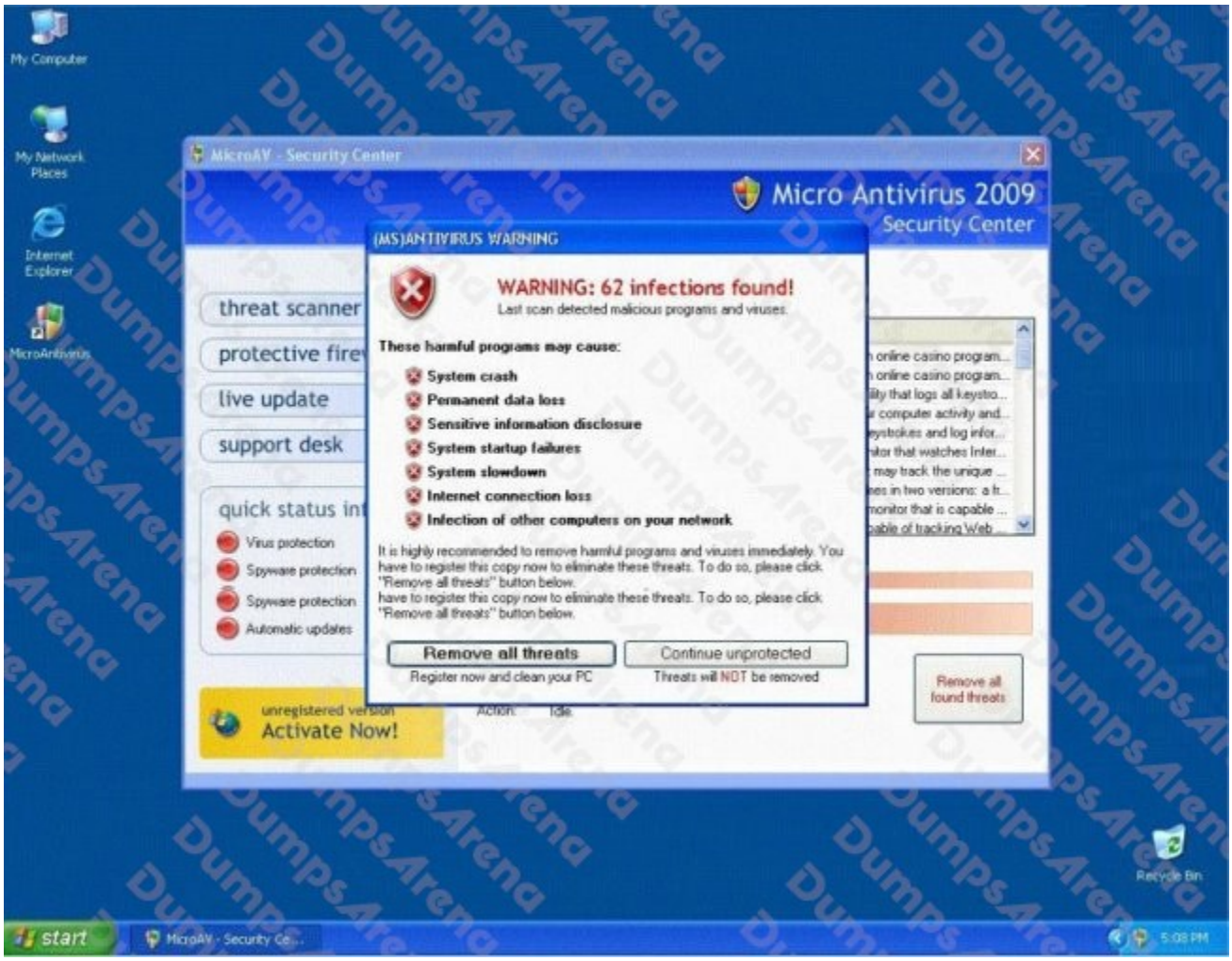
ANSWER: A C E

QUESTION NO: 16

Fake Anti-Virus, is one of the most frequently encountered and persistent threats on the web. This malware uses social engineering to lure users into infected websites with a technique called Search Engine Optimization.

Once the Fake AV is downloaded into the user's computer, the software will scare them into believing their system is infected with threats that do not really exist, and then push users to purchase services to clean up the non-existent threats.

The Fake AntiVirus will continue to send these annoying and intrusive alerts until a payment is made.



What is the risk of installing Fake AntiVirus?

A. Victim's Operating System versions, services running and applications installed will be published on Blogs and Forums

B. Victim's personally identifiable information such as billing address and credit card details, may be extracted and exploited by the attacker

C. Once infected, the computer will be unable to boot and the Trojan will attempt to format the hard disk

D. Denial of Service attack will be launched against the infected computer crashing other machines on the connected network

ANSWER: B

QUESTION NO: 17

A tester is attempting to capture and analyze the traffic on a given network and realizes that the network has several switches. What could be used to successfully sniff the traffic on this switched network? (Choose three.)

A. ARP spoofing

B. MAC duplication

C. MAC flooding

D. SYN flood

E. Reverse smurf attack

F. ARP broadcasting

ANSWER: A B C

QUESTION NO: 18

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: 19

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: 20

Which of the following are valid types of rootkits? (Choose three.)

A. Hypervisor level

B. Network level

C. Kernel level

D. Application level

E. Physical level

F. Data access level

ANSWER: A C D