100% Money Back Guarantee

Vendor:EC-COUNCIL

Exam Code:312-49

Exam Name:ECCouncil Computer Hacking Forensic Investigator (V9)

Version: Demo

QUESTION 1

What information do you need to recover when searching a victim\\'s computer for a crime committed with specific e-mail message?

A. Internet service provider information

B. E-mail header

C. Username and password

D. Firewall log

Correct Answer: B

QUESTION 2

Which of the following options will help users to enable or disable the last access time on a system running Windows 10 OS?

A. wmic service

B. Reg.exe

C. fsutil

D. Devcon

Correct Answer: C

QUESTION 3

Buffer overflow vulnerability of a web application occurs when it fails to guard its buffer properly and allows writing beyond its maximum size. Thus, it overwrites the_____. There are multiple forms of buffer overflow, including a Heap Buffer Overflow and a Format String Attack.

A. Adjacent memory locations

B. Adjacent bit blocks

C. Adjacent buffer locations

D. Adjacent string locations

Correct Answer: A

QUESTION 4

When using Windows acquisitions tools to acquire digital evidence, it is important to use a well-tested hardware write-

blocking device to:

A. Automate Collection from image files

B. Avoiding copying data from the boot partition

C. Acquire data from host-protected area on a disk

D. Prevent Contamination to the evidence drive

Correct Answer: D

QUESTION 5

You are working in the security Department of law firm. One of the attorneys asks you about the topic of sending fake email because he has a client who has been charged with doing just that. His client alleges that he is innocent and that there is no way for a fake email to actually be sent. You inform the attorney that his client is mistaken and that fake email is possibility and that you can prove it. You return to your desk and craft a fake email to the attorney that appears to come from his boss. What port do you send the email to on the company SMTP server?

A. 10

B. 25

C. 110

D. 135

Correct Answer: B

QUESTION 6

What header field in the TCP/IP protocol stack involves the hacker exploit known as the Ping of Death?

A. ICMP header field

B. TCP header field

C. IP header field

D. UDP header field

Correct Answer: B

QUESTION 7

What happens when a file is deleted by a Microsoft operating system using the FAT file system?

A. only the reference to the file is removed from the FAT

B. the file is erased and cannot be recovered

C. a copy of the file is stored and the original file is erased

D. the file is erased but can be recovered

Correct Answer: A

QUESTION 8

The use of warning banners helps a company avoid litigation by overcoming an employee assumed _____. When connecting to the company\\'s intranet, network or Virtual Private Network(VPN) and will allow the company\\'s investigators to monitor, search and retrieve information stored within the network.

A. Right to work

B. Right of free speech

C. Right to Internet Access

D. Right of Privacy

Correct Answer: D

QUESTION 9

Pagefile.sys is a virtual memory file used to expand the physical memory of a computer. Select the registry path for the page file:

A. HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management

B. HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\System Management

C. HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Device Management

D. HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management\PrefetchParameters

Correct Answer: A

QUESTION 10

When using an iPod and the host computer is running Windows, what file system will be used?

A. iPod+

B. HFS

C. FAT16

D. FAT32

Correct Answer: D

QUESTION 11

Which of the following processes is part of the dynamic malware analysis?

A. Process Monitoring

B. Malware disassembly

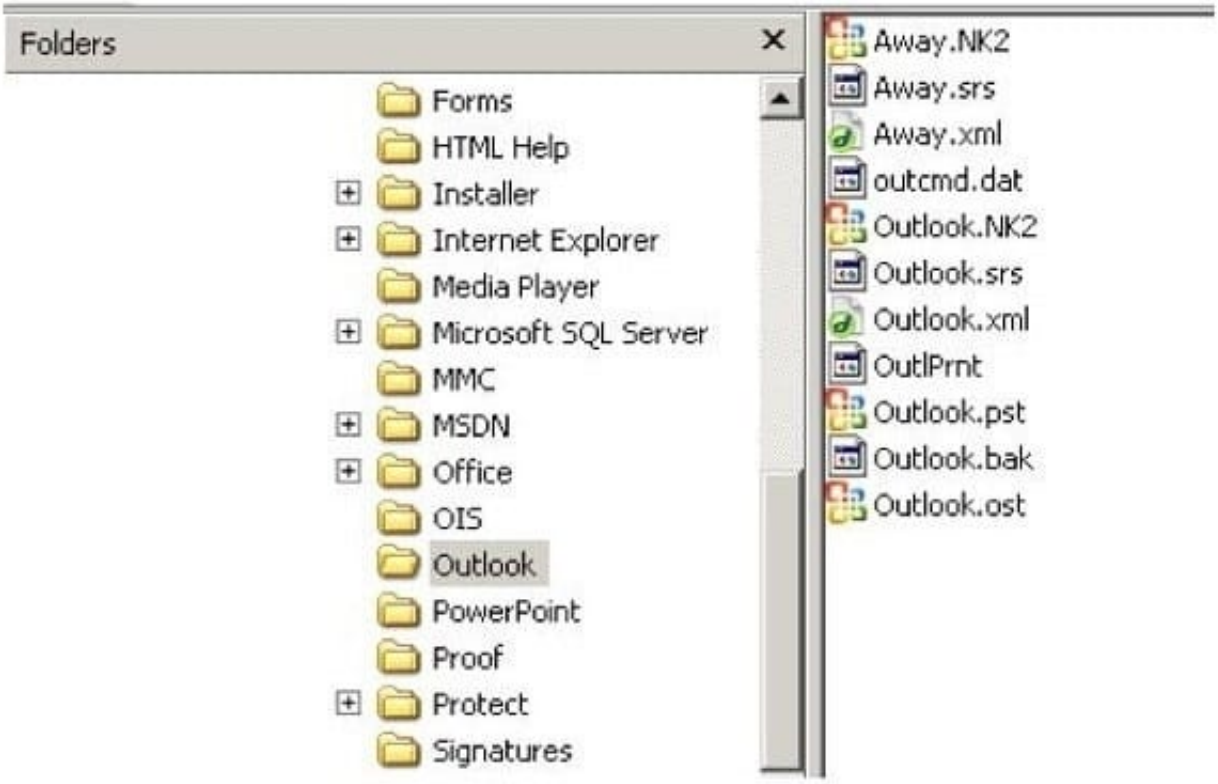
C. Searching for the strings

D. File fingerprinting

Correct Answer: A

QUESTION 12

In the following directory listing,



Which file should be used to restore archived email messages for someone using Microsoft Outlook?

A. Outlook bak

B. Outlook ost

C. Outlook NK2

D. Outlook pst

Correct Answer: D