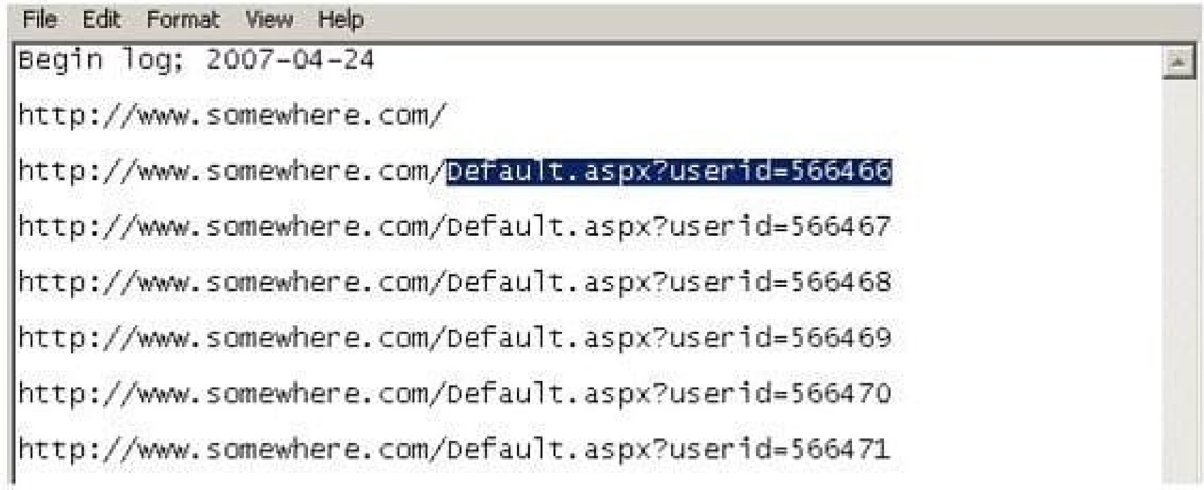
EC0-349$^{\text{Q\&As}}$

Computer Hacking Forensic Investigator

Pass EC-COUNCIL EC0-349 Exam with 100% Guarantee

QUESTION 1

Using Internet logging software to investigate a case of malicious use of computers, the investigator comes across some entries that appear odd.



```
Begin log; 2007-04-24
http://www.somewhere.com/
http://www.somewhere.com/Default.aspx?userid=566466
http://www.somewhere.com/Default.aspx?userid=566467
http://www.somewhere.com/Default.aspx?userid=566468
http://www.somewhere.com/Default.aspx?userid=566469
http://www.somewhere.com/Default.aspx?userid=566470
http://www.somewhere.com/Default.aspx?userid=566471
```

From the log, the investigator can see where the person in question went on the Internet. From the log, it appears that the user was manually typing in different user ID numbers. What technique this user was trying?

A. Parameter tampering

B. Cross site scripting

C. SQL injection

D. Cookie Poisoning

Correct Answer: A

QUESTION 2

John and Hillary works at the same department in the company. John wants to find out Hillary\\'s network password so he can take a look at her documents on the file server. He enables Lophtcrack program to sniffing mode. John sends Hillary an email with a link to Error! Reference source not found. What information will he be able to gather from this?

A. Hillary network username and password hash

B. The SID of Hillary network account

C. The SAM file from Hillary computer

D. The network shares that Hillary has permissions

Correct Answer: A

QUESTION 3

You just passed your ECSA exam and are about to start your first consulting job running security audits for a financial institution in Los Angeles. The IT manager of the company you will be working for tries to see if you remember your ECSA class. He asks about the methodology you will be using to test the company\\'s network. How would you answer?

A. Microsoft Methodology

B. Google Methodology

C. IBM Methodology

D. LPT Methodology

Correct Answer: D

QUESTION 4

What method of computer forensics will allow you to trace all ever-established user accounts on a Windows 2000 sever the course of its lifetime?

A. forensic duplication of hard drive

B. analysis of volatile data

C. comparison of MD5 checksums

D. review of SIDs in the Registry

Correct Answer: C

QUESTION 5

You are working as Computer Forensics investigator and are called by the owner of an accounting firm to investigate possible computer abuse by one of the firm\\'s employees. You meet with the owner of the firm and discover that the company has never published a policy stating that they reserve the right to inspect their computing assets at will. What do you do?

A. Inform the owner that conducting an investigation without a policy is not a problem because the company is privately owned

B. Inform the owner that conducting an investigation without a policy is a violation of the 4th amendment

C. Inform the owner that conducting an investigation without a policy is a violation of the employee\\'s expectation of privacy

D. Inform the owner that conducting an investigation without a policy is not a problem because a policy is only necessary for government agencies

Correct Answer: C