SECO

INSTITUTE

IT SECURITY EXPERT

INFORMATION SECURITY

IT-SECURITY

DATA PROTECTION

ETHICAL HACKING

SECURE SOFTWARE

BUSINESS CONTINUITY

CRISIS MANAGEMENT

SECURITY OPERATIONS CENTER (SOC) ANALYST

Sample Exam Questions

Introduction

This document contains 4 questions (and answers) that help you familiarise yourself with the structure and topic areas of the SECO-Institute's IT Security Expert-SOC Analyst certification exam.

To download our Complete Sample Exam, create a free study account at https://members.seco-institute.org

We recommend you to take the Complete Sample Exam before registering for the certification exam.

The results of the Sample Exam do not count towards your examination score.

Certification exam

You can book your exam with an accredited training partner or directly with the SECO-Institute.

To book an exam with the SECO-Institute go to: https://www.seco-institute.org/how-to-book-your-exam-schedule-an-exam/

Passing the certification exam and earning a SECO-Institute IT Security Expert-SOC Analyst certificate demonstrates your ability to work as a competent Tier 1/Tier 2 SOC Analyst.

Exam format

- Part 1: Lab exercise completed in class on Day 5
- Part 2: Computer-based written exam
    - 10 multiple-choice questions
    - 6 open-ended questions
- Time allowed: 120 minutes
- Closed-book exam
- Pass mark: 60% of the total marks

Questions

Question 1

What type of log format is this and where does it come from?

```
***:0|Incapsula|SIEMintegration|1|1|Normal|0| sourceServiceName=site123.abcd.info siteid=1509732 suid=50005477 requestClientApplication=Mozilla/5.0 (Windows NT 6.1; WOW64; rv:40.0) Gecko/20100101 Firefox/40.0 deviceFacility=mia ccode=IL
```

A. This is a W3C extended log format produced by Microsoft Internet Information Server
B. This is a CEF (Common Event Format) produced by Microsoft Internet Information Server
C. This is a W3C extended log format produced by Firefox 69.0
D. This is a CEF (Common Event Format) produced by Firefox 40.0

Question 2

There is a technique that allows an attacker to authenticate as a user without having access to the user's cleartext password. The technique consists of capturing valid password hashes through Credential Access and leveraging them to authenticate to the systems the account has access to. What is this technique called?

A. Pass the Authentication
B. Pass the Ticket
C. Pass the Kerberos
D. Pass the Hash

Question 3

What does this Splunk query do?

```
sourcetype=windows EventCode=4625 OR EventCode=4624

 | bin _time span=5m as minute

 | rex "Security ID:\s*\w*\s*\w*\s*Account Name:\s*(?<username>.*)\s*Account Domain:"

 | stats count(Keywords) as Attempts,

 count(eval(match(Keywords,"Audit Failure"))) as Failed,

 count(eval(match(Keywords,"Audit Success"))) as Success by minute username

 | where Failed>=4

 | stats dc(username) as Total by minute

 | where Total>5
```

A. Checks for accounts having an account login failure of 4 or more & checks for the quantity of accounts that have failed by 5.

B. Displays login attempts within a 5-minute range.

C. Checks for accounts having an account login failure of 4624 or more & checks for the quantity of accounts that have failed by 4625.

D. Checks for accounts having an account login failure of 5 or more & checks for the quantity of accounts that have failed by 4.

Question 4

You are a security analyst at the Bicsma SOC. There is an incident concerning a high-profile user. You receive the following log from a junior analyst. What conclusion can you draw from the log?

```
Files Created:

C:\Users\<USER>\Documents\@Please_Read_Me@.txt

C:\Users\<USER>\AppData\Local\Temp\b.wnry


Connections:

173.194.192.99:443 (TCP)

74.125.124.113:443 (TCP)
```

Answer Key

Question 1 - Answer

The correct answer is **B**.

```
***:0|Incapsula|SIEMintegration|1|1|Normal|0| sourceServiceName=site123.abcd.info siteid=1509732 suid=50005477 requestClientApplication=Mozilla/5.0 (Windows NT 6.1; WOW64; rv:40.0) Gecko/20100101 Firefox/40.0 deviceFacility=mia ccode=IL
```

is a CEF (Common Event Format) produced by Microsoft Internet Information Server.

Question 2 - Answer

The correct answer is **D**. Pass the Hash is a technique that allows an attacker to authenticate as a user without having access to the user’s cleartext password. In this technique, valid password hashes for the account being used are captured using a Credential Access technique. Captured hashes are used with PtH to authenticate as that user. Once authenticated, PtH may be used to perform actions on local or remote systems.

Question 3 - Answer

The correct answer is **A**.

```
sourcetype=windows EventCode=4625 OR EventCode=4624
 | bin _time span=5m as minute
 | rex "Security ID:\s*\w*\s*\w*\s*Account Name:\s*(?<username>.*)\s*Account Domain:"
 | stats count(Keywords) as Attempts,
 count(eval(match(Keywords,"Audit Failure"))) as Failed,
 count(eval(match(Keywords,"Audit Success"))) as Success by minute username
 | where Failed>=4
 | stats dc(username) as Total by minute
 | where Total>5
```

checks for accounts having an account login failure of 4 or more & checks for the quantity of accounts that have failed by 5.

Question 4 - Answer

Files Created:

C:\Users\<USER>\Documents\@Please_Read_Me@.txt

C:\Users\<USER>\AppData\Local\Temp\b.wnry

Connections:

173.194.192.99:443 (TCP)

74.125.124.113:443 (TCP)

The conclusion you can draw from this log: The computer is infected with the WannaCry virus. https://www.virustotal.com/gui/file/ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa/behavior/SNDBOX

Although the SECO Institute has done everything to prevent irregularities in this document, errors may still occur. Therefore, any person who acts on the basis of the content of this document does so at his/her own risk and is aware of the fact that the SECO Institute cannot be held accountable for any possible damage ensuing from his/her actions.

The authors of this document have done their utmost to identify all possible rightful parties other than the SECO Institute. Should you be a rightful party,
or represent one, or know one, and be of the opinion that this document unjustly contains copyrighted material, please do not hesitate to contact the SECO Institute.