IT-SECURITY PRACTITIONER

Sample Exam

SECO INSTITUTE

Sample exam IT-Security Practitioner

SECO-Institute provides the official Cyber Security & Governance courseware to accredited training centres where students are trained by accredited instructors. Students can take their exams at an accredited exam centre or directly at the SECO-Institute. Attending an official certification course is not a prerequisite for taking an exam. Upon successful completion of a certification exam (with a passing score of 60%), students can claim their certification titles at the SECO-Institute, whereupon they will receive a title and a digital badge.

This document provides a sample exam for you to familiarise yourself with the topic areas of the current Information Security Practitioner examination. We strongly recommend you to test your knowledge before taking the actual assessment. The results of this test do not count towards your certification assessment.

Examination type

Computer-based

- 10 Multiple choice: 3 points per question
- 5 Open questions: 8 points per question
- 1 Case study: 30 points per case

Time allotted for examination

120 minutes

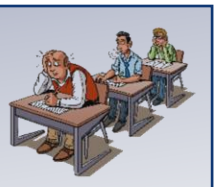
Examination details

- Pass mark: 60% (out of 100)
- Open book/notes: no
- Electronic equipment permitted: no
- The Rules and Regulations for SECO-Institute examinations apply to this exam.

This sample exam consists of:

- 10 Open questions
- 1 Case study

Questions

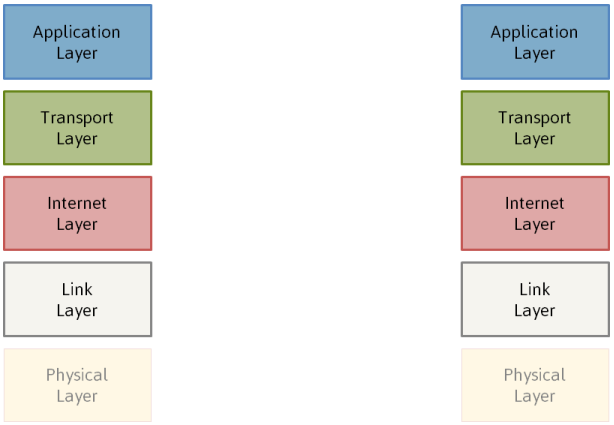


Question 1

Let's imagine that passwords are kept in a file on an arbitrary system.
What measures could be taken to preserve confidentiality as well as integrity of those passwords?

Question 2

a) On how many layers does a stateless firewall operate when it filters the network traffic between the left and right application on separate systems in the figure to the right? Name those layers.
b) At which layers does filtering based on IP addresses and port numbers take place?
c) If Application-layer content has been encrypted, would it still be possible to filter out packets with particular IP addresses?
d) Does it make any sense for a stateless firewall to filter traffic on the Physical Layer? Why or why not?



Question 3

Suppose the organization Booking.com asks you to test their site on the presence of vulnerabilities and before that asks you to sign a responsible disclosure contract, what does that mean and what possible agreements could be made in that type of contract?

Question 4

Suppose the Security Operations Center of your company gets an alert, a message that a core server of the enterprise resource planning process has been compromised and certain important files have been encrypted. The message states that a ransom must be paid in order to decrypt the files again. What possible actions should be taken if you mark this event as an incident?

Hint: the ENISA model should be taken as reference when you answer this question.

Question 5

a) Explain the differences between a network-based IDS and an IPS.
b) Where in a Defense-in-Depth network architecture would you place these systems?

Suppose your architecture/design is built up using three zones: Outer, Inner, and Restricted.

c) Where would you place a core database server in this architecture/design?
d) How would you protect this server against a DDoS attack?

Question 6

Look at the SNORT rule at the right.

```
reject icmp any any -> $HOME_NET any
(msg:"ICMP test detected"; GID:1; sid:10000001; rev:001;
classtype:icmp-event;)
```

What can you tell about this rule regarding:

– direction of traffic?
– protocol?
– port number(s)?

Question 7

a) What does it mean when they say Unix access control is assigned in a “discretionary” manner?
b) How is that implemented in Linux? Give an example of the protection of a file and a directory.
c) In what way differs SELinux from that manner?

Question 8

a) Why, when, and how should you patch your business-critical servers when a vulnerability has been published and afterwards a patch for it has been released by the software vendor?
b) Why is it important to develop a patch policy for your organization?

Question 9

We visit the website of a financial institution. Explain what you see here:

(TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384, 256-bits sleutels, TLS 1.2)

a) Which asymmetric encryption algorithm is used and for what purpose?
b) Which symmetric algorithm is used with what key length?
c) For what reason could hashing possibly be used by the website?

Question 10

a) For what reasons would you develop a classification model for your company?
b) Could an RBAC model be of any use in relation to this classification model?

Case: Incident Response

Scenario

You are an incident response investigator of Utopia CERT. Your team is part of NREN, the research and academic network in Utopia – a well-known ISP for universities, and academic medical centres.

Being the eldest and most familiar CERT of Utopia your team is often asked to investigate incidents that take place within Utopia. You have a good relationship with other ISPs in Utopia and national CERTs abroad.

Assignment

- Analyze the following alert, and describe the situation. What activities do you believe were going on?
- Classify the incident and assign a priority (-1- high, -2- middle, -3- low). Point out the reasons why you assign this classification and priority.
- How would you mitigate the consequences of these activities?

----------Extra information----------

10/8 are networks within Utopia.

10.187/16 are networks of Utopia NREN (your organization)

.ut is Utopia's top-level domain.

----------Classification----------

* ABUSIVE CONTENT: SPAM, Harassment, Child/Sexual/Violence

* MALICIOUS CODE: Virus / Worm/ Trojan, Spyware, Dialer

* INFORMATION GATHERING: Scanning, Sniffing, Social Engineering

* INTRUSION ATTEMPTS: Exploit known vulnerabilities, Login Attempts, New Attack Signatures

* INTRUSIONS: (un)Privileged Account Compromize, Application Commpromize

* AVAILABILTIY: (D)DoS, Sabotage

* INFORMATION SECURITY: Unauthorized Access to information, -Modification of Information

* FRAUD: Unauthorized use of resources, Copyright abuse, Masquerading

* OTHER: All Other incidents, new types of incidents

----------Alert----------

Return-Path: <system@atreides.system.ut>

X-Spam-Checker-Version: SpamAssassin 3.1.3 (2006-06-01) on fingon2.net.ut

X-Spam-Level:

X-Spam-Status: No, score=-1.5 required=4.9 tests=BAYES_00,HOT_NASTY,

NO_REAL_NAME autolearn=no version=3.1.3

X-Original-To: cert@fingon2.net.ut

Delivered-To: cert@fingon2.net.ut

Received: from boromir.net.ut (boromir.net.ut [10.187.245.66])

by fingon2.net.ut (Postfix) with ESMTP id B24F8B801F

for <cert@fingon2.net.ut>; Tue, 13 May 2012 07:10:14 +0200 (CEST)

Received: from boromix.net.ut (boromix.net.ut [10.187.245.33])

by boromir.net.ut with ESMTP id m4D5ADmH018658

for <cert@boromir.net.ut>; Tue, 13 May 2012 07:10:13 +0200 (CEST)

Received: from atreides.system.ut ([10.187.5.131])

by boromix.net.ut/massMailer with ESMTP id m4D5AD8l028910

for <cert@cert.ut>; Tue, 13 May 2012 07:10:13 +0200

Received: by atreides.system.ut (Postfix, from userid 98)

id 101F73D4039; Tue, 13 May 2012 07:10:11 +0200 (CEST)

To: cert@cert.ut

Subject: Incident 10.187.21.203

From: ir@system.ut

X-Priority: 4 (Low)

Mime-Version: 1.0

Content-Type: text/plain; charset=utf-8

Content-Transfer-Encoding: 7bit

X-Mailer: Php/Mail

Message-Id: <20120513051012.101F73D4039@atreides.system.ut>

Date: Tue, 13 May 2012 07:10:11 +0200 (CEST)

Status: RO

Content-Length: 4702

Lines: 89

10.187.21.203

Scanning activity was observed

from: 2012-05-12 07:12:43

until: 2012-05-12 17:29:31

scanned ports:

TCP/445 206 packets

TCP/139 71 packets

TCP/135 58 packets

UDP/137 9 packets

Overall packets: 344

Examples of abusive traffic

2012-05-12 18:03:02: 10.187.21.203 -> xxx.xxx.188.167 TCP/445

2012-05-12 18:02:58: 10.187.21.203 -> xxx.xxx.188.167 TCP/445

2012-05-12 18:02:55: 10.187.21.203 -> xxx.xxx.188.167 TCP/445

2012-05-12 18:02:34: 10.187.21.203 -> xxx.xxx.188.141 TCP/445

2012-05-12 18:02:27: 10.187.21.203 -> xxx.xxx.188.141 TCP/445

2012-05-12 18:02:24: 10.187.21.203 -> xxx.xxx.188.141 TCP/445

2012-05-12 18:02:20: 10.187.21.203 -> xxx.xxx.188.141 TCP/445

2012-05-12 18:02:03: 10.187.21.203 -> xxx.xxx.190.30 TCP/445

2012-05-12 18:01:32: 10.187.21.203 -> xxx.xxx.190.30 TCP/445

2012-05-12 18:01:31: 10.187.21.203 -> xxx.xxx.190.30 TCP/445

2012-05-12 18:01:13: 10.187.21.203 -> xxx.xxx.188.148 TCP/445

2012-05-12 18:01:10: 10.187.21.203 -> xxx.xxx.188.148 TCP/445

2012-05-12 18:01:07: 10.187.21.203 -> xxx.xxx.188.148 TCP/445

2012-05-12 17:40:04: 10.187.21.203 -> xxx.xxx.118.27 TCP/445

2012-05-12 17:39:08: 10.187.21.203 -> xxx.xxx.119.8 TCP/445

2012-05-12 17:37:51: 10.187.21.203 -> xxx.xxx.118.10 TCP/445

2012-05-12 17:30:02: 10.187.21.203 -> xxx.xxx.119.15 TCP/445

2012-05-12 17:28:12: 10.187.21.203 -> xxx.xxx.118.18 TCP/445

2012-05-12 17:26:53: 10.187.21.203 -> xxx.xxx.118.28 TCP/445

2012-05-12 17:18:13: 10.187.21.203 -> xxx.xxx.119.16 TCP/445

2012-05-12 18:03:02: 10.187.21.203 -> xxx.xxx.188.167 TCP/139

2012-05-12 18:02:58: 10.187.21.203 -> xxx.xxx.188.167 TCP/139

2012-05-12 18:02:34: 10.187.21.203 -> xxx.xxx.188.141 TCP/139

2012-05-12 18:02:27: 10.187.21.203 -> xxx.xxx.188.141 TCP/139

2012-05-12 18:02:24: 10.187.21.203 -> xxx.xxx.188.141 TCP/139

2012-05-12 18:02:03: 10.187.21.203 -> xxx.xxx.190.30 TCP/139

2012-05-12 18:01:32: 10.187.21.203 -> xxx.xxx.190.30 TCP/139

2012-05-12 18:01:13: 10.187.21.203 -> xxx.xxx.188.148 TCP/139

2012-05-12 18:01:10: 10.187.21.203 -> xxx.xxx.188.148 TCP/139

2012-05-12 15:54:20: 10.187.21.203 -> xxx.xxx.190.27 TCP/139

2012-05-12 15:53:49: 10.187.21.203 -> xxx.xxx.190.27 TCP/139

2012-05-12 15:24:10: 10.187.21.203 -> xxx.xxx.190.28 TCP/139

2012-05-12 15:23:39: 10.187.21.203 -> xxx.xxx.190.28 TCP/139

2012-05-12 15:19:10: 10.187.21.203 -> xxx.xxx.190.27 TCP/139

2012-05-12 15:18:39: 10.187.21.203 -> xxx.xxx.190.27 TCP/139

2012-05-12 14:56:10: 10.187.21.203 -> xxx.xxx.190.30 TCP/139

2012-05-12 14:55:39: 10.187.21.203 -> xxx.xxx.190.30 TCP/139

2012-05-12 14:39:39: 10.187.21.203 -> xxx.xxx.190.30 TCP/139

2012-05-12 14:39:08: 10.187.21.203 -> xxx.xxx.190.30 TCP/139

2012-05-12 14:24:53: 10.187.21.203 -> xxx.xxx.190.27 TCP/139

2012-05-12 18:03:25: 10.187.21.203 -> xxx.xxx.188.188 TCP/135

2012-05-12 18:02:55: 10.187.21.203 -> xxx.xxx.188.167 TCP/135

2012-05-12 18:02:21: 10.187.21.203 -> xxx.xxx.188.141 TCP/135

2012-05-12 18:01:31: 10.187.21.203 -> xxx.xxx.190.30 TCP/135

2012-05-12 18:01:07: 10.187.21.203 -> xxx.xxx.188.148 TCP/135

2012-05-12 17:34:57: 10.187.21.203 -> xxx.xxx.188.129 TCP/135

2012-05-12 17:19:43: 10.187.21.203 -> xxx.xxx.188.156 TCP/135

2012-05-12 16:37:44: 10.187.21.203 -> xxx.xxx.188.156 TCP/135

2012-05-12 16:01:43: 10.187.21.203 -> xxx.xxx.188.159 TCP/135

2012-05-12 15:53:48: 10.187.21.203 -> xxx.xxx.190.27 TCP/135

2012-05-12 15:23:38: 10.187.21.203 -> xxx.xxx.190.28 TCP/135

2012-05-12 15:18:38: 10.187.21.203 -> xxx.xxx.190.27 TCP/135

2012-05-12 15:02:07: 10.187.21.203 -> xxx.xxx.188.154 TCP/135

2012-05-12 14:55:37: 10.187.21.203 -> xxx.xxx.190.30 TCP/135

2012-05-12 14:39:07: 10.187.21.203 -> xxx.xxx.190.30 TCP/135

2012-05-12 14:30:21: 10.187.21.203 -> xxx.xxx.188.158 TCP/135

2012-05-12 14:24:21: 10.187.21.203 -> xxx.xxx.190.27 TCP/135

2012-05-12 14:12:57: 10.187.21.203 -> xxx.xxx.188.131 TCP/135

2012-05-12 13:51:02: 10.187.21.203 -> xxx.xxx.188.182 TCP/135

2012-05-12 13:33:54: 10.187.21.203 -> xxx.xxx.188.155 TCP/135

2012-05-12 17:29:31: 10.187.21.203 -> xxx.xxx.188.167 UDP/137

2012-05-12 14:42:41: 10.187.21.203 -> xxx.xxx.188.152 UDP/137

2012-05-12 12:47:42: 10.187.21.203 -> xxx.xxx.188.143 UDP/137

2012-05-12 12:27:10: 10.187.21.203 -> xxx.xxx.188.137 UDP/137

2012-05-12 12:14:24: 10.187.21.203 -> xxx.xxx.188.145 UDP/137

2012-05-12 12:02:30: 10.187.21.203 -> xxx.xxx.190.28 UDP/137

2012-05-12 11:48:00: 10.187.21.203 -> xxx.xxx.188.169 UDP/137

2012-05-12 11:16:40: 10.187.21.203 -> xxx.xxx.188.188 UDP/137

2012-05-12 09:51:51: 10.187.21.203 -> xxx.xxx.188.185 UDP/137

–----------End----------

Answers

Question 1 (8 points)

Confidentiality must be preserved by assigning privileges to the files where passwords – or hashed passwords – are stored. Security labels may also be attached to those files to prevent unauthorized disclosure. The same counts for databases or registries, where passwords are stored in tables.

Integrity is preserved by hashing the password files or columns in the mentioned tables. Individual passwords are often stored as hashes instead of the original string values.

Optional: Salting is done to make it harder to crack passwords out of the hash values. Each individual password is concatenated with a random value, belonging to that particular password, before the hash is calculated and stored into the password file or database. The salt values must also be stored along with the password hashes. Advantage: Identical passwords will have different hash values.

Question 2 (7 points)

a) A stateless firewall consists of four layers, from bottom up: Physical, Link, Internet, and Transport.
b) The filtering takes place at the Internet and the Transport layer. It compares IP addresses, protocol numbers, and TCP or UDP port numbers with a set of predefined rules to filter them.
c) Because a stateless fire wall does not examine the contents of application messages, this content may be encrypted. The headers of IP packets and TCP or UDP segments are not touched by this encryption.
d) Filtering the physical layer makes no sense because this layer only transmits bits. Content is not relevant.

Question 3 (8 points)

From the lesson: Responsible disclosure is a tool for organizations and incident reporters to facilitate responsible reporting and handling of vulnerabilities in information systems, software and other ICT products. Incident reporters must hold off on publication until the organization has been able to remedy the problem. The public prosecutor has its own responsibility to press charges on incident reporters.

A responsible disclosure contract might contain the following:

– Declaring to hold proprietary or private information in strict confidence
– Never to make use of proprietary information for own purposes
– Not to copy proprietary information nor reverse engineer it from innocent info
– Immediately inform the disclosing party of any important information or vulnerability found
– The agreement shall be governed by the laws of the jurisdiction in the country where the (headquarters of the) disclosing party is located

Example of a standard agreement: http://www.ipwatchdog.com/tradesecret/standard-confidentiality-agreement/

Question 4 (8 points)

The relevance of the incident has already been determined, otherwise it would not have been declared an incident. Then the identification and classification process will be started, followed by a triage, in which the impact and development over time will be determined. Thereafter the person to resolve the incident will assigned. An incident "ticket" will be opened, and the resolver will be given the task to analyze, solve, report, and finally archive the incident.

Question 5 (7 points)

a) An IDS is a security device that monitors and analyzes security-related events with the purpose of providing (near) real-time warnings; an IPS is an IDS that includes the capability of blocking sessions and preventing malicious activities that result in violating confidentiality, integrity, and availability.
b) In a defense-in-depth network architecture an IPS should be placed on the perimeter between two zones. An IDS should be place in a zone, connected to a switch, analyzing the traffic that passes the switch. For this purpose switches often have a Switch Port Analyzer (SPAN) attached to one of the interfaces.
c) A core database server should be placed in the restricted zone.
d) This server is protected by an IPS being able to drop all packets recognized as DDoS attack packets.

Question 6 (7 points)

Direction of traffic is from outside directed to the inner network. The protocol that is filtered is ICMP, probably a Ping activity. The packets containing ICMP messages are rejected. ICMP resides on the Internet Layer so no port numbers are filtered.

Question 7 (7 points)

a) Discretionary means that the owner may decide who or what subject may access an object, e.g., a file or directory.
b) This is implemented by assigning a value to each object consisting of 9 bits, divided into 3 parts, meaning "owner", "group", and "others". Each part of 3 bits have the meaning of "read", "write", and "execute" access.
c) SELinux is a security kernel module with enhanced capabilities for access control. It changes the discretionary principle into a mandatory system of controlling access for subjects to objects. The system may overrule decisions of object owners if it is contrary to the policy laid down in domain security rules.

Question 8 (7 points)

a) Patching is necessary for security reasons. Patches should not be applied before an extensive test has been done because business processes could be disrupted if patches lead to new problems. On the other hand, patching should also not be delayed too long because unpatched systems might be the target of malicious intruders.
b) The moment should be chosen very carefully and the balance between moments of testing and patching should be driven by policy. This policy defines the way of patch working and stimulates uniformity in that.

Question 9 (8 points)

a) Elliptic Curve combined with Diffie-Hellman is used as an asymmetric algorithm to exchange session keys for symmetric encryption of data. RSA is used to sign the certificate of the ABN-AMRO site.
b) Advanced Encryption Standard is used as a symmetric algorithm to encrypt the TLS 2.1 session between the browser and the web server. The key length for this is 256 bits.
c) Hashing is used to preserve the integrity of the certificate. The hash value is the value that is signed by the trusted third party, the certificate authority.

Question 10 (8 points)

a) Because not all information should be treated equally. Some information is more important, more sensitive, or more confidential than other information. It all has to do with the impact when losing it or when it is compromised. Because not all people in an organization perform the same role, it is therefore not appropriate that anyone can see, use or may change data without permission or oversight. Subjects should obtain clearance for objects to be able to access them in a specific way.
b) A Role Based Access Control system assigns roles to subjects. Each role is entitled to access objects of which a set of privileges are defined. Bringing it all together it is possible to implement "least privilege" as a policy, meaning that one should not be allowed to do more with an object than his role in the organization warrants. Standard measures will also help simplifying the implementation.

Case: Incident Response (25 points)

Possible solution

This is a report of an automatic monitoring system reporting a scanning from one of the hosts of one of your participants, concentrated round the listed UDP and TCP ports.

Station 10.187.21.203 performs scanning activities on several hosts in the 10-network on TCP ports 445 (206 packets), 139 (71 packets), 137 (9 packets) and 135 (58 packets). Further investigation must follow concerning the cause: user, intruder, or malware.

Classification:

INFORMATION GATHERING (vulnerability scanning?), just a port scan, no intrusion. It could also be a WORM (MALICIOUS SOFTWARE). The used/scanned ports (135, 137, 139, 445) could be the signature of a WORM, but it could also be a combination.

Priority:

Scanning is priority –2– (Middle), no direct danger, attention required.
If it were a WORM priority should be -1- (High).

Mitigation:

Contact management of 10.187.21.203 a.s.a.p.
If possible, start an investigation of the presence of intrusion and malware.
Also investigate vulnerability of targets!

Handle this incident according to the defined procedures:

- Relevance
- Identification
- Classification
- Triage
- Actions
  - Start ticket
  - Solve incident
  - Report incident
  - Archive incident

ITSP-Sample Exam-EN-v1.0