SECURITY F2017

Systems Architecture and Security, Examination set, June 9, 2017.

What to answer

1. MSc students (class code KSSECUR1KU) must answer all questions.
2. BSc students (class code BSSECUR1KU) must answer all questions EXCEPT those titled MSC-ONLY-1 through MSC-ONLY-8.

What to hand in

You submit electronically, via LearnIT:

1. A plain-text file `answers.txt` with your answers to multiple choice questions, one line per answer: the question identifier, a colon, and the answer digit (format example below). You can submit only one answer for each question; multiple answers will be awarded zero points.
2. A pdf file `discussion.pdf` containing the answers to discussion questions D1 and D2. It may contain text and figures in any form.

If there are technical or logistical problems with submitting in this way, please turn to available personnel in order to find a backup solution. Feel free to submit a .zip archive containing the above two files.

How to answer

Example multiple choice question:

> **Question 9-7**
>
> This is the question text. It is followed by the possible answers:
>
> 1. The first possible answer.
> 2. The second possible answer.
> 3. The third possible answer.
> 4. The fourth possible answer.

Example answer. You choose "The third possible answer":

```
9-7:3
```

Permissible aids

This examination is A11: Written, on-premise, with access to all aids and internet.

Questions begin on the next page.

Multiple-choice Questions

Your answers to the multiple choice questions counts 60% towards the final grade.

Security principles

Question 1-0

Saltzer and Schroeder's "economy of mechanism" principle is also known as the principle of

1. Open design
2. Simplicity
3. Minimum exposure
4. Usability

Question 1-1

The IT-department of Naive Corp Ltd. is experiencing performance issues with the main database. In an attempt to rectify these issues, they disable all logging features of the database, including failed authentication attempts. This approach violates the principle of

1. Generating secrets
2. Minimum exposure
3. No single point of failure
4. Traceability

Question 1-2

To avoid brute-force attempts on Naive Corp computer logins, IT imposes an artifical 120 second delay between the user entering his password and the subsequent login. Users, as a consequence, tend to not log out, instead sharing accounts. This policy is a violation of the principle of

1. Least privilege
2. Minimum Trust and maximum trustworthiness
3. Generating secrets
4. Usability

Question 1-3

In the event the central authorisation server of Naive Corp is unreachable, employee laptops revert to allowing password-less logins. This is an example of violation of the principle of:

1. No single point of failure
2. Secure, fail-safe defaults
3. Open design
4. Complete mediation

Question 1-4

For historical reasons, Naive Corp is running its invoicing database and web-server in the same VM. This is a violation of the principle of:

1. Compartmentalization
2. Traceability
3. Secure, fail-safe defaults
4. Simplicity

Question 1-5

The receptionist of Naive Corp needs access to everyone's calendar. The IT department was

not sure how to achieve this, and so just made the receptionist an Administrator on the Outlook server. This is a violation of the principle of:

1. No single point of failure
2. Traceability
3. Least privilege
4. Secure, fail-safe defaults

Question 1-6

The Naive Corp webserver is also running proftpd 1.3.1. No-one is using it, but no-one remembers why it is there, so no one dares remove it. This is a violation of the principle of:

1. Minimum exposure
2. Secure, fail-safe defaults
3. Traceability
4. Complete mediation

Question 1-7

The Naive Corp login service---the one imposing the 120 second delay---is actually running off Mike from IT's laptop. This is a violation of the principle of:

1. Open design
2. Usability
3. No single point of failure
4. Generating secrets

Question 1-8

The disk on Mike's laptop is not encrypted, so the user database on the laptop is available to whomever has physical access to it. This is a violation of the principle of:

1. Usability
2. No single point of failure
3. Minimum exposure
4. Complete mediation

Question 1-9

The IT-department of Naive Corp. Ltd. has implemented their own session-key encryption scheme for use in cookies. The scheme simply applies ROT13 to sequential session-ids, but Naive Corp IT maintains this is secure "since no-one but us no that it works that way". This security mechanism violates the principle of

1. Open design
2. Compartmentalisation
3. Usability
4. Least privilege

Computer Networks

Question MSC-ONLY-1

What is the 8th byte (byte 7, the start-of-frame delimiter) of an ethernet packet?

1. 10101010
2. 10111010
3. 10101110
4. 10101011

Question MSC-ONLY-2

An 8-way switch has the following internal switching table:

```
LINK MAC
1    ff:78:ad:00:fe:01
2    01:00:5e:00:00:fb
```

An ethernet frame where bytes 8-20 are as follows arrives on Link 3:

```
01005e0000fb0021f7c2aa00
```

What should the switch do with the packet?

1. Nothing
2. Forward the packet on Link 1
3. Forward the packet on Link 2
4. Forward the packet on all links but Link 3

Question MSC-ONLY-3

How should the switch in the preceding question update its switching table?

1. Do not update the switching table
2. Add an entry for Link 3, MAC 00:21:f7:c2:aa:00.
3. Remove the entry for Link 1
4. Remove the entry for Link 2

Question MSC-ONLY-4

This is the contents of my routing table:

```
Destination        Gateway            Flags         Refs      Use   Netif Expire
default            10.28.6.1          UGSc            52        0     en0
10.28.6.1/32       link#4             UCS              1        0     en0
192.168.1.1/24     link#3             UCS              5        0     en1
172.18.1.1/16      link#5             UCS              5        0     en2
172.19.10.1/30     link#6             UCS              7        0     en3
```

On what network interface should a packet for 172.18.23.19 go?

1. en0
2. en1
3. en2
4. en3

Question MSC-ONLY-5

The Address Resolution Protocol is used for

1. Dynamically obtaining an IP address
2. Dynamically obtaining a DNS address
3. Discovering IP/MAC associations
4. Discovering IP/DNS associations

Question MSC-ONLY-6

Complete the three-way handshake:

```
A -> B : SYN seq(7)
B -> A : SYN ACK(8) seq(89)
```

1. `A -> B : ACK(90) seq(8)`
2. `A -> B : ACK(8) seq(90)`
3. `A -> B : ACK(9) seq(89)`
4. `A -> B : ACK(89) seq(9)`

Question MSC-ONLY-7

Here is a trace of a recursive DNS lookup for www.google.com:

```
> dig www.google.com A +trace

; <<>> DiG 9.8.3-P1 <<>> www.google.com A +trace
;; global options: +cmd
.                       334020  IN      NS      c.root-servers.net.
.                       334020  IN      NS      h.root-servers.net.
...
;; Received 496 bytes from 130.226.142.2#53(130.226.142.2) in 38 ms

com.                    172800  IN      NS      a.gtld-servers.net.
com.                    172800  IN      NS      b.gtld-servers.net.
...
;; Received 492 bytes from 192.203.230.10#53(192.203.230.10) in 65 ms

google.com.             172800  IN      NS      ns2.google.com.
google.com.             172800  IN      NS      ns1.google.com.
...
;; Received 168 bytes from 192.42.93.30#53(192.42.93.30) in 23 ms

www.google.com.         300     IN      A       216.58.209.132
;; Received 48 bytes from 216.239.36.10#53(216.239.36.10) in 79 ms
```

Which of the following nameservers is in the above trace responsible for the dot-com domain?

1. c.root-servers.net
2. b.gtld-servers.net
3. ns2.google.com
4. 216.58.209.132

Question MSC-ONLY-8

In the protocol stack model:

1. Headers of lower layers are payload of higher layers
2. Headers of higher layers are payload of lower layers
3. Payload of lower layers are headers of higher layers
4. Payload of higher layers are headers of lower layers

Network Security

Question 3-1

An 8-way switch has the following internal switching table:

```
LINK MAC
1    ff:78:ad:00:fe:01
2    01:00:5e:00:00:fb
```

An adversary who wishes to eavesdrop on `01:00:5e:00:00:fb` via a MAC flooding attack would:

1. Repeatedly send packets with source MAC `01:00:5e:00:00:fb` to the switch
2. Repeatedly send packets with target MAC `01:00:5e:00:00:fb` to the switch
3. Repeatedly send packets with random source MAC to the switch
4. Repeatedly send packets with random target MAC to the switch

Question 3-2

An adversary with MAC `ff:78:ad:00:fe:01/IP 10.122.19.9` who wishes to eavesdrop on MAC `01:00:5e:00:00:fb/IP 10.122.19.8` using an ARP Spoofing attack would broadcast ARP packets:

1. `10.122.19.8 IS-AT 01:00:5e:00:00:fb`
2. `10.122.19.8 IS-AT ff:78:ad:00:fe:01`
3. `10.122.19.9 IS-AT 01:00:5e:00:00:fb`
4. `10.122.19.9 IS-AT ff:78:ad:00:fe:01`

Question 3-3

Tasked with breaking in to Naive Corp, I begin by port scanning their webserver. Unfortunately, my own IT department denied me root access on the machine I'm using for the scan, so nmap cannot craft custom TCP packets. Which scan is still available to me?

1. SYN
2. ACK
3. CONNECT
4. Maimon

Question 3-4

I use nmap to scan the Naive Corp webserver. This is what I find:

```
Not shown: 65531 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
443/tcp   open  ssl/http
8022/tcp  open  unknown
```

How would we proceed with an attack?

1. Re-scan with settings to open closed ports
2. Re-scan with settings to find version numbers
3. Apply metasploit to port 80
4. Apply metasploit to port 8022

Question 3-5

The Naive Corp sysadmin notices my scans. Scrambling to harden his system, he runs `sudo lsof -i | grep LISTEN` on the Linux box serving as the Naive Corp webserver. He sees the following:

```
sshd      1623      ssh   08u  IPv4   7269      0t0  TCP *:ssh (LISTEN)
proftpd   8028      ftp   20u  IPv4   4824      0t0  TCP *:8022 (LISTEN)
nginx     8029      ftp   20u  IPv4   4825      0t0  TCP *:http (LISTEN)
nginx     8030      ftp   23u  IPv4   4898      0t0  TCP *:https (LISTEN)
```

What should he do?

1. Consider filtering ports 08u and 20u
2. Consider filtering ports 20u and 23u
3. Consider filtering ports 22 and 8022
4. Consider filtering ports 80 and 443

Question 3-6

It turns out the ftp process is there to accept new content from the Naive Corp marketing department, including user/password combinations for the CRM system running inside the webserver. Using FTP this way is

1. Appropriate
2. Inappropriate because FTP transfers are vulnerable to eavesdropping
3. Inappropriate because FTP remote administration allows public-key only logins
4. Inappropriate because FTP domain name resolution is often used in DDOS attacks

Authentication & Access Control

Question 4-0

The Naive Corp sysadmin looks at `/var/log/auth.log` of his webserver and sees this:

```
May 15 07:24:27 ncws sshd[27405]: Invalid user user from 195.3.144.213
May 15 07:24:27 ncws sshd[27405]: Invalid user adm from 195.3.144.213
```

```
May 15 07:24:27 ncws sshd[27405]: Invalid user webadm from 195.3.144.213
May 15 07:24:27 ncws sshd[27405]: Invalid user a from 195.3.144.213
```

This goes on for literally thousands of lines, the only variation being the timestamp and the word immediately after "Invalid user". This is indicative of

1. A brute-force attempt on the nginx webserver process
2. A brute-force attack on the ssh remote administration server process
3. A brute-force attempt on the login daemon
4. A brute-force attempt on the system portscanner

Question 4-1

Which of these has to do with "Authentication"?

1. cron
2. nginx
3. login
4. ACL

Question 4-2

Which of these has to do with "Access control"?

1. cron
2. nginx
3. login
4. ACL

Question 4-3

Which of these has to do with "Authorization"?

1. /etc/papersize
2. /etc/shadow
3. /var/log/nginx/error.log
4. /var/log/syslog

Question 4-4

The file `~/.ssh/known_hosts` has the purpose of:

1. Allowing password-less remote logins by storing public keys of pre-authorised users
2. Allowing password-less remote logins by storing private keys of pre-authorised users
3. Detecting MITM attacks by pre-registering known public keys of remote servers
4. Detecting MITM attacks by pre-registering known private keys of remote servers

Question 4-5

Consider this partial output of `ls -l /etc/init.d` on linux.

```
-rwx----wx 1 root root  438 May 21  2015 lvm2
-rwxr-xr-x 1 root root 1392 Jun 12  2015 monoserver
lrwxrwxrwx 1 root root 2116 Jun 13  2015 mono-xsp4
-rwxr-xr-x 1 root root  696 Nov 10  2014 mountall-bootclean.sh
```

Based only on the permissions of these files, which one poses the larger security risk?

1. lvm2
2. monoserver
3. mono-xsp4
4. mountall-bootclean.sh

Question 4-6

Consider this partial output of `ls -l /usr/bin`.

```
-rwxr-sr-x 1 root   tty        27368 Aug  5  2015 wall
-rwxr-xr-x 1 root   root       48112 Jan  1  2015 whatis
-rwx------ 1 root   root       23648 Aug  5  2015 whereis
-rwsr-xr-x 1 root   root        1460 Mar 23  2015 wifi-status
```

Which of these files will execute with the privileges of root, no matter which user executes the file?

1. wall
2. whatis
3. whereis
4. wifi-status

Question 4-7

I wrote a script which has special functionality when run as root:

```
#! /bin/bash
SPECIAL=0
if [ "$ISROOT" = "root" -o "$UID" = "0"]; then
    echo "Special mode enabled for user 'root'"
    SPECIAL=1
fi
# ...
```

However, my script is insecure: users other than root may still have the script proceed with `SPECIAL` set to 1, because:

1. The adversary may perform a CSRF attack by setting UID to an appropriate cookie
2. The adversary may simply set the `SPECIAL` environment variable to 1
3. The adversary may simply set the `ISROOT` environment variable to "root"
4. The adversary may simply set the `UID` environment variable to "0"

Question 4-8

Running a server in a chroot jail is an attempt to adhere to the security principle of:

1. Simplicity
2. Compartmentalization
3. No single point of failure
4. Privacy

Question 4-9

Which password does the MD5 hash `6aecf77cb2f2b614c4f1cb6d655e3294` correspond to?

1. password
2. greatsecurity
3. itusecuritycourse
4. 23f7f375efa75dd6d106ef9eb2700655

Question 5-1

System-wide logging services can sometimes be configured to log to a remote logging service rather than to a local file. Why?

1. To prevent concurrency issues
2. To prevent eavesdropping
3. To prevent tampering
4. To prevent denial-of-service attacks

Question 5-2

Which of the following is incorrect?

1. A host-based IDS does not run on the monitored machine
2. A host-based IDS may use snapshots to detect break-ins
3. A network-based IDS runs on a dedicated host
4. A network-based IDS actively transmits messags

Question 5-3

Logging may itself pose vulnerabilities because

1. Log output may include user input, making logging services vulnerable to injection attacks
2. Log output may include user output, making logging services vulnerable to DDOS attacks
3. Log input may include adversary input, making logging services vulnerable to port scanning attacks
4. Log input may include adversary output, making logging services vulnerable to eavesdropping

Question 5-4

Naive Corp IT staff is suspecting a root kit is installed on the webserver. The sysadmin executes the following command:

```
root@webserver.naivecorp.com> find /dev -type f -o -type d
/dev
/dev/
/dev/net
...
```

Which, if any, is the suspicious line of output?

1. `/dev`
2. `/dev/`
3. `/dev/net`
4. None of these lines are suspicious

Question 5-5

The webserver periodically executes the following script as root.

```
find /bin -xdev -type f -print0 | xargs -0 md5sum > /var/h
diff -l -u /etc/h /var/h || shutdown -h now
```

What does this script have to do with rootkit detection?

1. It halts the machine if it detects the `xdev` rootkit
2. It halts the machine if there are changes in the `md5sum` tool
3. It halts the machine if there are changes in the configuration of the webserver
4. It halts the machine if there are changes in files under `/bin`

Question 5-6

Naive Corp IT department maintains also a USB copy of the original installed image so they may find rootkits in their running servers by comparison. They do such a comparison and find the following differences. Which one is most likely to be due to an adversary?

1. `/var/log/nginx/backup.log.7.gz`: Only on production machine
2. `/etc/shadow`: Update time differ, contents, and last-access time differ
3. `/sbin/mount`: Last-access time differs
4. `/var/log/dmesg`: Update time and contents differ

Web Application Security

Question 6-1

Naive Corp hires you as a penetration tester, requesting a white-box audit. What is (typically) not necessary in a white-box audit?

1. Accessing webserver source code
2. Reading Naive Corp documentation
3. Port scanning
4. Reading Test reports

Question 6-2

The whitebox audit is suddenly cancelled, by orders from the CEO, so you do a blackbox audit instead. You try to figure out the version of the webserver. HTTP responses from it tends to look like this:

```
Date: Fri, 19 May 2017 12:06:31 GMT
Server: Microsoft-IIS/7.5
Cache-Control: no-cache, no-store
Pragma: no-cache
Content-Type: text/html; charset=utf-8
Expires: -1
X-AspNet-Version: 4.0.30319
X-Powered-By: ASP.NET
Content-Length: 104386
Set-Cookie: ASP.NET_SessionId=unm1fwyeqffjgtjzpbqntgvy; path=/; HttpOnly
Set-Cookie: cookieConsent=maybe; domain=.itu.dk; expires=Sun, 19-Nov-2017 13:06:32 GMT; path=/
```

Which of the following HTTP headers gives the best lead on the server version?

1. Server
2. Pragma
3. Set-Cookie
4. None of them

Question 6-3

You look at the pages served by the webserver. Apparently they are PHP. One of them has a "post a comment" form, with a list of previously posted comments below. You want to try a SQL injection. Pick input most likely to succeed as a SQL injection:

1. `AAAAAAAAAAAAAAAA\x90\x90\x90\x90\x4a\x8a\x65\x56\x00\x00\x76\xa5\xb5`
2. `'; SELECT * from USERS; --`
3. `<input onClick="console.log('pwned!')">`
4. `)>) [ "user": "admin", "login": "now" ]`

Question 6-4

Another page has an "upload file" facility, enabled by the following html fragment:

```
...
<form >
  <input type="file" name="file_name" >
  <input name="upload_path" value="/var/www/uploads" >
  <input name="XSCF_TOKEN" hidden value="d3b07384d113edec49eaa6238ad5ff00" >
  <input type="submit">
</form >
...
```

You try for a remote file upload vulnerability. Which form field should you modify?

1. `file_name`
2. `upload_path`
3. `XSCF_TOKEN`
4. `submit`

Question 6-5

Using the remote file upload exploit, you get remote command execution on the webserver. To impress the CIO who hired you, you decide to exfiltrate data from the database about a

suspicious collaboration with the so-called "JU University of Lolland-Falster". What should you do?

1. Disable the firewall
2. Replace queries in some PHP file with the ones you wish to execute
3. Brute force the database server
4. DDOS the IDS proxy

Question 6-6

The CIO is insufficiently impressed, wanting you to obtain root access to the server. Which of the following is your best option?

1. Look for pre-installed rootkits
2. Look in the CVE register for remote access vulnerabilites in /etc/unpxrst
3. Look for XSCF attack opportunities
4. Look for writable setuid scripts

Question 6-7

Using sequential plain-text session ids in HTTP Cookies violate the security principle of:

1. Single point of failure
2. Compartmentalisation
3. Generating secrets
4. Open design

Computer forensics

Question F-1

Why would we issue the following command in the context of computer forensics?

```
dd if=/dev/sdc of=/dev/sdd bs=64K
```

1. To make a verbatim copy of the disk `/dev/sdc` onto `/dev/sdd`
2. To make a verbatim copy of the disk `/dev/sdd` onto `/dev/sdc`
3. To make a verbatim copy of the first 65535 bytes of disk `sdc`
4. To make a verbatim copy of the last 65535 bytes of disk `sdd`

Question F-2

What is carving?

1. The process of searching for packet headers in a data stream
2. The process of searching for file headers in a data stream
3. The process of searching for RSA public keys in a data stream
4. The process of searching for DES shared keys in a data stream

Question F-3

What is file slack?

1. Disk space left unused because the sector size is not a multiple of a file's size
2. Bits inadverdently written to an adjacent sector due to rotational forces (a.k.a. "padding")
3. The part of the volume not included in the file system
4. Disk space left unused because a file's size is not a multiple of the sector size

Question F-4

What does the following line from `/etc/shadow` tells us that may be relevant in a forensic setting about the user `fantasticmrfox`?

```
fantasticmrfox:9$a9I.rU98mhFp78qgflo1vXAsWOz83gyjwUiz3Ner7H3Tpz9KpdivieheqF/89.:17198:0:99999:7:
```

1. The user last changed his passwords on August 19, 2007
2. The user chose a really strong password
3. The user last changed his passwords on February 21, 2017
4. The user chose a really weak password

Question F-5

The tool `exiftool` is relevant for computer forensics in that it can

1. Extract meta-data from compiled programs
2. Extract meta-data from on-the-wire traffic
3. Extract meta-data from images
4. Extract meta-data via MITM attacks

Question F-6

Why would the cache of a web-browser be relevant to computer forensics?

1. Cached objects always contains IP destinations and TTL information
2. Cached objects may overwrite deleted files
3. Cached objects are generally not of interest in computer forensics
4. Cached objects include pictures and web-pages visited by previous users of the machine in questions

Question F-7

Which of the following commands could, if repeated a sufficient number of times, succesfully counter subsequent forensics efforts?

1. `rm -rf /`
2. `delete C:\*`
3. `dd if=/dev/random of=/dev/sdb bs=256K`
4. None of the above

Discussion Questions

A hospital wants to introduce an automated medication-dispenser device to patients in treatment for pain. Traditionally, nurses dispense medication to patients on the patients requests, observing dosage and frequency limitations. The hospital wishes to leave this responsibility with a machine.

The dispenser is programmed by hospital nurses using an ipad, which connects to the dispenser through a wire, while at the same time retrieving data on dosage etc. from the central hospital database of patient records using the wireless network.

The patient operates the dispenser device by connecting to it via bluetooth; the patient can then request medication using an app on his iOS or Android device. The device will refuse to dispense medication above dosage or frequency as programmed by the nurse.

Question D1: Authentication

Your answer to this question counts 20% towards the final grade.

Design, using appropriate cryptographic primitives, an authentication scheme for the above system. Be sure to note (a) who has access to which keys, (b) what happens if a key is compromised, and (c) how keys a distributed/revoked.

Report your design as the answer to this question. Your answer is expected to consume ~1 page.

Hint: This question can be answered satisfactorily using either simple or advanced machinery from the course.

Question D2: Risk assessment

Your answer to this question counts 20% towards the final grade.

Write an abbreviated risk analysis for the medication dispenser system *including* your authentication scheme.

You may hypothesise details of the system and must stipulate yourself its security requirements. Be sure to cover System, Stakeholders, Assets, Vulnerabilities, Threats, and Risk. You may find Chapter 8 of the course book helpful.

Report your analysis as the answer to this question. Your answer is expected to consume ~1 page.

(End of questions.)

Fri May 4 09:38:16 CEST 2018