University of Glasgow

Tuesday 10 May 2022
09:30-11:30 BST
Duration: 2 hours
Additional time: 30 minutes
Timed exam – fixed start time

DEGREES OF MSci, MEng, BEng, BSc, MA and MA (Social Sciences)

Cyber Security Fundamentals H
COMPSCI 4062

(Answer All 3 Questions)

This examination paper is an open book, online assessment and is worth a total of 60 marks.

1. You are working as a police officer and are conducting an investigation into a cyber-crime.

(a) One of the pieces of evidence gathered is a notepad which you are going through. On the last page there is a note that stands out as it does not make any sense. You start thinking that it might be referring to ciphers and decide to attempt to break them. (In order for you to get full marks you will need to demonstrate the whole procedure and mention which ciphers are being used).

[15 marks]

7 marks for every correct conversion and 1 mark for clear explanation and answer to the questions posed.

Note: 1^{st}: 2 → (to the right)

2^{nd}: pass (keywd) → SGMNYCWEVT

(b) On a different page of the notepad you find the following: DB Password = ASECRETMESSAGE. You try ASECRETMESSAGE as a password, but it does not work. There is a chance this is a clue to derive the password through substitution of characters. Please state at least 3 different passwords deriving from this information and in comparison, with password setup guidelines discussed in the course defend the level of strength that these passwords you think provide. Your answer should not exceed 250 words.

[5 marks]

2 marks for the list of three potential passwords and 3 marks for discussing different factors that affect the strength of a password alongside with a comparison to your findings.

[Total: 20 marks]

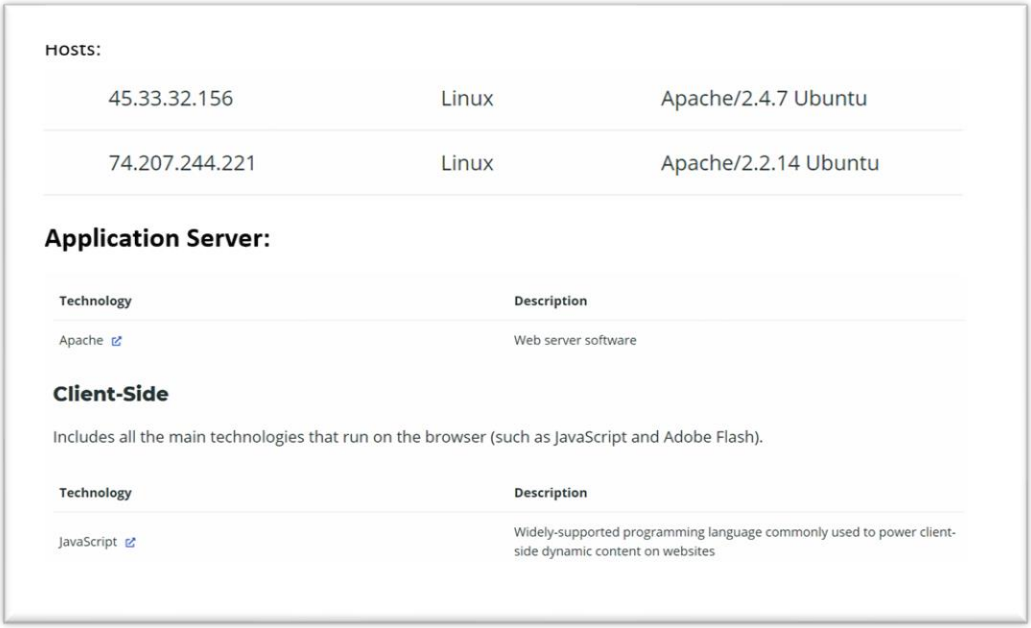
2. A company is concerned about the level of information they have available online.

(a) Is there any type of penetration testing that can be considered realistically possible with a duration of 2 weeks? Your answer should not exceed 200 words.

[3 marks]

(b) From Figure 1 & 2 (next page) can you extract at least three pieces per figure of vital information and explain how an attacker might use them in a malicious way (3 pieces of information for each image; 6 in total)? Your answer should not exceed 700 words.

[12 marks]



Hosts:

45.33.32.156	Linux	Apache/2.4.7 Ubuntu
74.207.244.221	Linux	Apache/2.2.14 Ubuntu

Application Server:

Technology	Description
Apache	Web server software

Client-Side

Includes all the main technologies that run on the browser (such as JavaScript and Adobe Flash).

Technology	Description
JavaScript	Widely-supported programming language commonly used to power client-side dynamic content on websites

Figure 1: "Example a"

IN	AAAA	2600:3c01::f03c:91ff:fe18:bb2f
IN	A	45.33.32.156
IN	AAAA	2600:3c01::f03c:91ff:fe98:ff4e
IN	TXT	v=spf1 a mx ptr ip4:45.33.49.119 ip4:173.255.243.189 ip4:192.81.131.254 ip6:2600:3c01::f03c:91ff:fe98:ff4e ip6:2600:3c01::f03c:91ff:fe70:d085 include:_spf.google.com ~all
IN	MX	preference: 10 exchange: aspmx2.googlemail.com
IN	MX	preference: 5 exchange: alt2.aspmx.l.google.com
IN	MX	preference: 10 exchange: aspmx3.googlemail.com

Figure 2: "Example b"

(c) Can you mention some of the tools that could produce similar results as figure 1 & 2 (seen in previous question)? Your answer should not exceed 150 words.

[2 marks]

(d) Figure 3 (below) shows an output from a different tool. Describe how this output differs from that shown in figure 1 & 2 (figures seen in question 2b). Your answer should not exceed 200 words.

[3 marks]

```
Host is up (0.17s latency).
Not shown: 498 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.10 (Ubuntu Linux; protocol 2.0)
80/tcp open  http    Apache httpd 2.4.7 ((Ubuntu))
Aggressive OS guesses: Linux 3.13 or 4.2 (96%), Linux 3.10 - 4.8 (95%), Linux 3.2 - 4.8 (93%), Linux 3.13 (92%), Linux 4.4 (92%), Asus RT-AC66U WAP (92%),
Linux 3.10 (92%), Linux 3.11 - 3.12 (92%), Linux 3.18 (92%), Linux 3.2 (92%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 18 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Figure 3: "Scan example"

(e) If an attacker had all this information, how could they use it for exploitation? Please describe two scenarios. Your answer should not exceed 250 words

[5 marks]

[Total: 25 marks]

3. **(a)** Looking at the screenshot available below (figure 4) please investigate, extract and explain 6 pieces of information.

[10 marks]

233	6.660398	10.1.1.101	10.1.1.1	TCP	54 3197 → 80 [ACK] Seq=623 Ack=2511 Win=65535 Len=0
234	6.736387	10.1.1.101	10.1.1.1	TCP	62 3198 → 80 [SYN] Seq=0 Win=0 Len=0 MSS=1460 SACK_PERM=1
235	6.736831	10.1.1.1	10.1.1.101	TCP	62 80 → 3198 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM=1
236	6.736873	10.1.1.101	10.1.1.1	TCP	54 3198 → 80 [ACK] Seq=1 Ack=1 Win=65535 Len=0
237	6.738548	10.1.1.101	10.1.1.1	TCP	62 3199 → 80 [SYN] Seq=0 Win=0 Len=0 MSS=1460 SACK_PERM=1
238	6.738992	10.1.1.1	10.1.1.101	TCP	62 80 → 3199 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM=1
239	6.739035	10.1.1.101	10.1.1.1	TCP	54 3199 → 80 [ACK] Seq=1 Ack=1 Win=65535 Len=0
240	6.762743	10.1.1.101	10.1.1.1	HTTP	686 GET /Websidan/2004-07-SeaWorld/320/DSC07858.JPG HTTP/1.1
241	6.763698	10.1.1.101	10.1.1.1	HTTP	686 GET /Websidan/2004-07-SeaWorld/320/DSC07859.JPG HTTP/1.1
242	6.763884	10.1.1.101	10.1.1.1	TCP	54 3197 → 80 [FIN, ACK] Seq=623 Ack=2511 Win=65535 Len=0
243	6.764522	10.1.1.1	10.1.1.101	TCP	60 80 → 3198 [ACK] Seq=1 Ack=633 Win=6952 Len=0
244	6.765075	10.1.1.1	10.1.1.101	TCP	60 80 → 3199 [ACK] Seq=1 Ack=633 Win=6952 Len=0
245	6.765205	10.1.1.1	10.1.1.101	TCP	60 80 → 3197 [ACK] Seq=2511 Ack=624 Win=6842 Len=0
246	6.767765	10.1.1.1	10.1.1.101	TCP	1514 80 → 3198 [ACK] Seq=1 Ack=633 Win=6952 Len=1460 [TCP segment of a reassembled PDU]
247	6.768985	10.1.1.1	10.1.1.101	TCP	1514 80 → 3198 [ACK] Seq=1461 Ack=633 Win=6952 Len=1460 [TCP segment of a reassembled PDU]
248	6.769047	10.1.1.101	10.1.1.1	TCP	54 3198 → 80 [ACK] Seq=633 Ack=2921 Win=65535 Len=0
249	6.770912	10.1.1.1	10.1.1.101	TCP	1514 80 → 3199 [ACK] Seq=1 Ack=633 Win=6952 Len=1460 [TCP segment of a reassembled PDU]
250	6.772157	10.1.1.1	10.1.1.101	TCP	1514 80 → 3198 [ACK] Seq=2921 Ack=633 Win=6952 Len=1460 [TCP segment of a reassembled PDU]
251	6.772230	10.1.1.101	10.1.1.1	TCP	54 3198 → 80 [ACK] Seq=633 Ack=4381 Win=65535 Len=0
252	6.773438	10.1.1.1	10.1.1.101	TCP	1514 80 → 3198 [ACK] Seq=4381 Ack=633 Win=6952 Len=1460 [TCP segment of a reassembled PDU]
253	6.774746	10.1.1.1	10.1.1.101	TCP	1514 80 → 3198 [ACK] Seq=5841 Ack=633 Win=6952 Len=1460 [TCP segment of a reassembled PDU]
254	6.774808	10.1.1.101	10.1.1.1	TCP	54 3198 → 80 [ACK] Seq=633 Ack=7301 Win=65535 Len=0
255	6.776006	10.1.1.1	10.1.1.101	TCP	1514 80 → 3199 [ACK] Seq=1461 Ack=633 Win=6952 Len=1460 [TCP segment of a reassembled PDU]
256	6.776087	10.1.1.101	10.1.1.1	TCP	54 3199 → 80 [ACK] Seq=633 Ack=2921 Win=65535 Len=0
257	6.777288	10.1.1.1	10.1.1.101	TCP	1514 80 → 3198 [ACK] Seq=7301 Ack=633 Win=6952 Len=1460 [TCP segment of a reassembled PDU]
258	6.777374	10.1.1.101	10.1.1.1	TCP	54 3198 → 80 [ACK] Seq=633 Ack=8761 Win=65535 Len=0
259	6.777805	10.1.1.1	10.1.1.101	HTTP	542 HTTP/1.1 200 OK (JPEG JFIF image)
260	6.777871	10.1.1.101	10.1.1.1	TCP	54 3198 → 80 [ACK] Seq=633 Ack=9250 Win=65047 Len=0
261	6.779883	10.1.1.1	10.1.1.101	TCP	1514 80 → 3199 [ACK] Seq=2921 Ack=633 Win=6952 Len=1460 [TCP segment of a reassembled PDU]
262	6.779941	10.1.1.101	10.1.1.1	TCP	54 3199 → 80 [ACK] Seq=633 Ack=4381 Win=65535 Len=0
263	6.781133	10.1.1.1	10.1.1.101	TCP	1514 80 → 3199 [ACK] Seq=4381 Ack=633 Win=6952 Len=1460 [TCP segment of a reassembled PDU]
264	6.782447	10.1.1.1	10.1.1.101	TCP	1514 80 → 3199 [ACK] Seq=5841 Ack=633 Win=6952 Len=1460 [TCP segment of a reassembled PDU]
265	6.782500	10.1.1.101	10.1.1.1	TCP	54 3199 → 80 [ACK] Seq=633 Ack=7301 Win=65535 Len=0
266	6.783706	10.1.1.1	10.1.1.101	TCP	1514 80 → 3199 [ACK] Seq=7301 Ack=633 Win=6952 Len=1460 [TCP segment of a reassembled PDU]
267	6.783798	10.1.1.101	10.1.1.1	TCP	54 3199 → 80 [ACK] Seq=633 Ack=8761 Win=65535 Len=0
268	6.785011	10.1.1.1	10.1.1.101	TCP	1514 80 → 3199 [ACK] Seq=8761 Ack=633 Win=6952 Len=1460 [TCP segment of a reassembled PDU]
269	6.785744	10.1.1.1	10.1.1.101	HTTP	824 HTTP/1.1 200 OK (JPEG JFIF image)
270	6.785825	10.1.1.101	10.1.1.1	TCP	54 3199 → 80 [ACK] Seq=633 Ack=10992 Win=65535 Len=0

Figure 4: "From wireshark.org"

(b) Can you describe two potential attacks scenarios based on the above information (that you have gathered from question 3 (a)) including explanation on how these scenarios can be employed? Your answer should not exceed 250 words

[5 marks]

[Total: 15 marks]