FINAL

IMPERIAL COLLEGE OF SCIENCE, TECHNOLOGY AND MEDICINE

EXAMINATIONS 2018

BEng Honours Degree in Computing Part III
MEng Honours Degree in Electronic and Information Engineering Part IV
BEng Honours Degree in Mathematics and Computer Science Part III
MEng Honours Degree in Mathematics and Computer Science Part III
MEng Honours Degrees in Computing Part III
MSc in Advanced Computing
MSc in Computing Science
MSc in Computing Science (Specialist)
for Internal Students of the Imperial College of Science, Technology and Medicine

This paper is also taken for the relevant examinations for the Associateship of the City and Guilds of London Institute

PAPER C331

NETWORK AND WEB SECURITY

Wednesday 21 March 2018, 14:00
Duration: 180 minutes

Answer THREE questions

Paper contains 4 questions
Calculators not required

General instructions

- Log-in to the Linux computer in front of you using your college username as *both* username and password.
- All your answers should be submitted electronically by accessing the website `https://co331.doc.ic.ac.uk` using a standard web browser from the host Linux environment. All other access to the network is intentionally blocked. Log in to the website using your college username and college password.
- Start VirtualBox and then start the virtual machines `question-vm` and `pentest-vm` that you will find pre-installed. All the websites and services described in the questions are available on the VirtualBox internal network.
- Your username and password for `pentest-vm` are respectively `exam` and `exam`. Intentionally, you are not given a username and password for `question-vm`, and you are not given root access on `pentest-vm` (although Netcat has permission to listen on port numbers below 1024).

For your convenience

- Bidirectional copying and pasting is enabled between `pentest-vm` and the host Linux environment.
- We saved a snapshot of each VM in case you need to recover from a crash. If you revert to a snapshot, any changes you made to that VM will be lost.
- On `pentest-vm` you can find selected tools that you can use for the practical questions, and in the home directory you can find a folder `exam-docs` with some reference documentation.
- On your local Linux machine you can save temporary files that are periodically backed up by CSG. This is for your convenience only: such files will not be considered part of your exam submission.
- If your mouse pointer is accidentally captured by `question-vm` you can release it by pressing the right `Ctrl` key.

Warning: attempts to abuse `https://co331.doc.ic.ac.uk`, the college network, or anything else outside of the provided VirtualBox environment will be considered a serious violation and may lead to disciplinary action.

1 Network scanning and data exfiltration

The owner of `bobthehack.er` has been hacked, and suspects the presence of an APT on their system. He hired you to run a forensic analysis of their network.

a i) Survey their network on the IP range `10.39.26.128-159` in order to identify hosts and services. Report the IPs, open ports and identifying information of the services that you discover.

ii) At `http://bobthehack.er/captures/pk.pcap` you are provided with a network capture file that contains suspicious traffic. Use the information in the file to identify a hidden TCP service, contact the service and report the flag you obtain. Briefly describe the *port-knocking* technique to protect ports from scans.

b As part of your intelligence gathering activity, you found some exposed source code at `http://tools.bobthehack.er/index.php~`.

i) Review the code in `index.php~` to find vulnerabilities. Report two different lines of code that contain vulnerabilities, and suggest fixes for them.

ii) A vulnerability from `index.php~` has not been patched in `http://tools.bobthehack.er/index.php`. Exploit it in order to retrieve the flag in `/home/bob/private/FLAG.txt`. Briefly describe the steps you have taken. (Hint: you may find the `-u` parameter of `Netcat` useful.)

The two parts carry equal marks.

2 Hacking the hackers

A member of the notorious hacking group `RoflSec` has exploited `petflix.com`, which now shows an annoying popup "`Owned by RoflSec`" to all visitors. You belong to the rival gang `pwnzone`, and your task is to take coldhearted revenge.

a i) Describe and compare the pentesting activities of *Passive information gathering* and *Active information gathering*, as applicable to investigating a web application during a black-box pentesting exercise.

ii) Several principals can influence the behaviour of a web page: the user, the hosting domain, third-party domains, and browser extensions. Discuss a security or privacy threat against each of these principals, as may be posed by one (or more) of the others, and declare its STRIDE category.

b It is now time to take action: clean up `petflix.com` and retaliate on `grumblr.com`, the favourite hangout of the `RoflSec` crew.

i) Inspect the client-side code of `petflix.com`, and determine how `RoflSec` managed to install the annoying popup. Report what kind of vulnerability was exploited.

ii) Exploit the vulnerability you discovered in part (b.i) and substitute the attacker message with "`RoflSec sux0rz`". Report the exploit code you used to achieve this.

iii) Now you want to find a way to impersonate `babou` (the leader of `RoflSec`) on `grumblr.com`, his favourite social network. Every minute, a browser running on his behalf visits `grumblr.com` as part of a logged-in session. Find a way to exploit `grumblr.com` so that you can steal the session cookie of `babou`. Report the value of the cookie as a flag. Briefly describe the steps you have taken.

The two parts carry equal marks.

3 **Second-order injection**

Tired of being owned by hackers, BorkBork, a telecoms company, has joined HackerOne and is offering bug bounties for any non-DoS-like security issues discovered in their database and its web interface. You want to hone your hacking skills, and maybe earn some money while doing so, by looking for vulnerabilities in `hr.borkbork.co.uk`.

a i) Describe and propose a mitigation for these server-side vulnerabilities: *path traversal*, *remote file inclusion*, and *server-side request forgery*.

ii) Recommend actions to improve the security of web-based logins, in these circumstances: when a username is invalid; after a few failed attempts for the same username; upon successful login.

b Access to the database should be restricted to legitimate users, via the login page `http://hr.borkbork.co.uk/login.php`.

i) During your passive information gathering on the technical support blog of the contractor that developed the web interface for BorkBork, you found out that usernames and passwords for testing accounts used during development may be stored at `/var/www/private/logins.txt`. Exploit a path traversal vulnerability on `hr.borkbork.co.uk` to access that file. Report a flag that you find in that file. Briefly describe the steps you have taken.

ii) Log in to the web application using username `test2` and password `qwerty`, which you discovered in (b.i). Use SQL injection to steal the password hash of the database administrator (user `dba`). Report the password hash as a flag. Briefly explain your attack, and suggest how it could be prevented.

The two parts carry, respectively, 45% and 55% of the marks.

4 **Analysis of web-based malware**

A website controlled by the NSA has been defaced by hackers. CIA agent Stan Smith shared with you an anonymous tip that the website now hosts a targeted attack aiming to exploit a vulnerability present on the US President's laptop.

a i) Briefly compare the main pros and the cons of *full disclosure*, *responsible disclosure* and *non disclosure* of vulnerabilities. Provide also an example of the kind of agent that may prefer each of these practices.

ii) How could an author of web-based malware target only a small set of users? Describe an appropriate technique, its limitations, and discuss a mitigation.

b You are tasked to analyse the hacked website `http://tweets.nsa.org`, and trick the attackers into thinking that the President has been infected.

i) Identify the obfuscated client-side code that loads the attack, and report the flag you find in a comment there. (Hint: Burp is a useful tool for this question.)

ii) Trick the website into launching the attack at your browser, and report the flag you find in the actual attack code. Briefly describe the steps you have taken.

iii) Analyse the attack further until you find out how to send a message reporting that the President was infected. Spoof such a message. If you succeed, you will obtain a flag from the attacker in response: report this flag. Briefly describe the steps you have taken.

The two parts carry, respectively, 45% and 55% of the marks.