IMPERIAL COLLEGE OF SCIENCE, TECHNOLOGY AND MEDICINE

EXAMINATIONS 2019

BEng Honours Degree in Computing Part III
BEng Honours Degree in Electronic and Information Engineering Part III
MEng Honours Degree in Electronic and Information Engineering Part III
MEng Honours Degree in Electronic and Information Engineering Part IV
MEng Honours Degree in Mathematics and Computer Science 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

Friday 22nd March 2019, 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`. Despite that, Netcat has permission to listen on port numbers below 1024, and Wireshark will have access to a promiscuous mode interface.

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 Web Fingerprinting and Tracking

a Modern web applications routinely use fingerprinting and tracking techniques to collect information about users and their devices.

i) Describe the main goals of web fingerprinting and tracking. Explain the relationship between the two techniques.

ii) Describe 2 fingerprinting features that can be collected by a web server. Describe 2 fingerprinting features that can be collected by JavaScript on the client side. Briefly compare strengths and weaknesses of client- and server-side fingerprinting.

b Social networks are among the main users of fingerprinting and tracking techniques.

i) Identify the strategy used by Grumblr to fingerprint its users. Report the fingerprint that it assigns by default to your current browser on visiting `grumblr.com`. Find a way to trick Grumblr into assigning a different fingerprint to the same browser. Report this spoofed fingerprint. Briefly describe the process you followed.

ii) A web advertisement which is displayed both on `grumblr.com` and on `bobthehack.er` is actually served from `pentest-vm`. Find where the ad code resides on `pentest-vm`, and report the flag present in that same directory. Modify the ad code to let you track users of both sites. Your goal is to identify a black hat hacker who is expected to visit Grumblr sometime after visiting BobTheHacker. Report the flag hidden in the Grumblr page for that user. Briefly describe the process you followed. (Note: an automated browser process visits the sites above on behalf of different users, approximately once a minute.)

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

2 Protecting web applications

a In order to protect web applications we need to be familiar with defensive and offensive practices.

i) Briefly describe 4 HTTP headers that were designed to improve the security of web applications.

ii) Describe the following attacks against web-based authentication, and the conditions necessary to launch them: *offline dictionary attack*, *online dictionary attack*, *attack against passwordless authentication*.

b i) Inspect the client side of BorkBork. Recommend 4 security improvements.

ii) From dark net chatter you infer that the home page of `petflix.com` has been compromised, and under certain conditions it performs an attack against BorkBork using the browser of a visiting user. Find a way to trigger the attack, analyse the attack, and report the 3 flags you find during this process. Briefly describe the process you followed.

The two parts carry equal marks.

3 Penetration testing and SQLi

a BorkBork has engaged your firm to perform black-box penetration testing of their web applications. They are particularly concerned about attacks coming form malicious web users, rather than MITM, eavesdroppers or insiders.

i) Describe what kind of *passive intelligence gathering* and *active intelligence gathering* against a web application a pentester can perform using only a web browser.

ii) As part of the threat analysis for BorkBork, report two realistic and non-trivial threats exploitable by a web attacker, against a web site that uses a database on the intranet to handle personal data. Also report the relevant STRIDE categories for each of these threats.

b i) Gather information about BorkBork using active and passive techniques. Report the name and surname of the DB administrator, 3 leaked `username:password` pairs of BorkBork employees, two addresses of hidden BorkBork pages. (Hint: you may also want to look at Petflix and Grumblr)

ii) Identify and exploit SQL injection vulnerabilities on `hr.borkbork.co.uk` to log in, and to steal the DB administrator password hash and salt. Report the flag you encounter on successful login and the DB administrator credentials. Briefly describe the process you followed. (Hint: you can take shortcuts if you compete part (3.b.i) first.)

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

4 **Delivering Network Attacks**

a i) Describe the DNS hijacking attack, and in particular: what does an attacker need to do in order to deliver the attack, what is the goal of the attack, and propose a specific countermeasure.

ii) Describe the SSL stripping attack, and in particular: what does an attacker need to do in order to deliver the attack, what is the goal of the attack, and propose a specific countermeasure.

b i) Scan the network of BobTheHacker (IP range `10.39.26.128-159`) and report IPs and ports of its DNS server and web server.

ii) Report 2 lines of code from `http://tools.bobthehack.er/bad-idea/sources/index.php` containing vulnerabilities, and propose fixes.

iii) Ransomware botnet processes access `http://c2.pw` almost every minute, asking for encryption keys. Exploit BobTheHacker to become a man-in-the-middle between the bots and `c2.pw`. Report the 2 flags you find while doing so. Use your MITM position to intercept a bot communication and obtain the key that the command-and-control server sends back to the bot. Report it as a flag. Briefly describe the process you followed. (Hints: Solve all the preceding parts of Question 4 first. Sniff the network with Wireshark to understand the bot's behaviour.)

The two parts carry equal marks.