IMPERIAL COLLEGE OF SCIENCE, TECHNOLOGY AND MEDICINE

EXAMINATIONS 2017

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

Thursday 23 March 2017, 10:00
Duration: 180 minutes

Answer THREE questions

Paper contains 4 questions
Calculators not required

General instructions

- Log-in on the Linux computer in front of you using your college 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 Linux environment. All other access to the network is intentionally blocked.
- In order to answer the practical questions below, you need to start VirtualBox and then start the virtual machines `pentest-vm` and `question-vm` that you will find pre-installed. All the websites and services described in the questions are available on the VirtualBox internal network.
- The username and password for `pentest-vm` are respectively `exam` and `exam`. You are not given root access on `pentest-vm` because it is not needed for the exam. Intentionally, you are not given username and password for `question-vm`.

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 the snapshot, any changes you made to the VMs 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.

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 **Server compromise and PHP analysis**

The owner of `bobthehack.er` and `tools.bobthehack.er` hired you to run a black-box penetration testing exercise against their network (on IP range `10.39.26.32-63`).

a i) Survey their network to identify hosts and TCP services. Report the IPs, open ports and corresponding services that you discover. Where applicable, also report brand and versions of operating systems and server software.

ii) As part of your vulnerability analysis you find that `bobthehack.er` has a *path traversal* vulnerability. Exploit the vulnerability and find a file named `PT-FLAG.txt` and report the flag it contains. Briefly describe your strategy for discovering the vulnerability.

b As part of your intelligence gathering activity on `tools.bobthehack.er`, you also found a backup version of the source code for `index.php` accessible 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 `index.php`. Exploit it in order to retrieve the flag in `/var/www/private/E-FLAG.txt`.

iii) Once you have gained access to `tools.bobthehack.er` by solving (b.ii), explore its file system in order to find information on how to gain access to `bobthehack.er` as well. Gain access, and report the flag contained in `/home/bob/PE-FLAG.txt` on `bobthehack.er` to prove it. Briefly describe the process you followed.

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

2 **Targeted cross-site attacks**

You have been recently hired as a security engineer for the social network `grumblr.com`. The incident response team flagged a number of suspicious activities on the social network, and you are tasked to investigate. You suspect that they may be the result of sloppy handling of sessions and third party content.

a i) Identify a *Spoofing*, a *Tampering* and an *Information disclosure* threat to a web application that hosts both user content (such as status updates and comments) and third-party content (such as JavaScript libraries and web advertisements). Suggest a mitigation for each threat.

ii) Briefly describe *Stored*, *Resident*, and *Self-XSS* attacks, and compare how they can be deployed.

b You now want to demonstrate to your supervisor (Trent) that the current design of `grumblr.com` is open to cross-site attacks: Cross-Site Request Forgery (CSRF) and JavaScript injection.

i) Find a CSRF attack on `grumblr.com`. Provide a malicious link that, when clicked by Trent, causes `grumblr.com` to reveal the email address of his friend Victor. (Assume that Trent is always logged-in on `grumblr.com`.) Briefly describe the idea behind your attack and suggest how `grumblr.com` could be fixed to prevent this attack.

ii) You need some way to deploy the CSRF link crafted at step (b.i). Since `grumblr.com` users are known to regularly visit `petflix.com`, you want to find a stored XSS vulnerability on the comments form of `petflix.com` that lets you add a malicious link on the web page, so that other visitors will be able to see it and click on it. As the answer, provide a comment that, when posted via the form, automatically displays a JavaScript alert with the message "XSS!" whenever `petflix.com` is visited.

iii) Now identify a JavaScript injection attack against `grumblr.com`. Describe where the vulnerability is, and suggest a fix. Provide the exploit code to display Trent's session cookie in an alert box, and explain how you are able to deploy the exploit code. (Hint: who can control what sponsored post gets displayed?)

The two parts carry equal marks.

3 **Authentication and SQL Injection**

Login data from the corporate database of BorkBork, a telecoms company, has been detected on the Dark Web. Now BorkBork is hiring you to perform a gray-box pentesting exercise to survey the weaknesses of their database authentication system.

a i) Describe some of the main objectives of the PTES phases *Passive intelligence gathering*, *Active intelligence gathering* and *Exploitation*, when the testing target is a web-based database.

ii) Compare *online* and *offline dictionary attacks* against password-based authentication, and discuss 2 countermeasures for each.

b You are told the database server at `db.borkbork.co.uk` contains a table with (salted) hashes of passwords, and you are given some of the stolen login data, available at `http://db.borkbork.co.uk/pentest/data.txt`.

i) Identify a SQL Injection vulnerability in `http://db.borkbork.co.uk/login.php` that allows you to log in as user `root`, and report the flag displayed in the welcome page. (Hint: you may find it helpful to look at the HTTP request.)

ii) After logging in (as `root`, or as any other user), identify a new SQL Injection vulnerability that lets you steal the password hash of the user with employee ID `1`. Briefly explain your attack, and suggest how it could be prevented.

iii) You may have noticed that usernames are also stored as (salted) hashes in this database. Find the password hash for the database administrator, whose username is `dba`. Briefly describe the steps you've taken.

The two parts carry equal marks.

4 **Web-based malware and JavaScript analysis**

You work for a security startup that offers a service which collects potentially malicious URLs from any web user willing to contribute. The malicious URLs are used to compile blacklists of web pages that should be blocked by a browser extension, available to the startup customers.

a i) Briefly describe these three different kinds of web-based attacks that normally involve tricking users: *phishing, click-jacking, drive-by download*. For each, provide a typical example of what may confuse the victim, and of what the attacker gains from the attack.

ii) How could an author of web-based malware abuse the service for reporting malicious URLs described above? Describe three attacks against a naive implementation of the service, and discuss a mitigation for each attack.

b Your startup implements a system to automatically classify the web pages pointed to by reported URLs. Yet, for some reason the URL `http://www.lloyd5bank.com/login.asp` fails to be classified automatically. You are tasked to analyse it in your pentesting environment.

i) Analyse the web page and identify what kind of attack it is trying to deploy: if you are on the right trail, you will discover a clearly marked flag that you need to report. (Hint: Burp is a useful tool for this question.)

ii) Briefly describe what kind of vulnerability you think the attacker is trying to exploit, and whether or not the attack has been successful. Suggest a mitigation for this vulnerability.

iii) Continuing your analysis of the attack in part (b.i) above, find a way to send a message to the attacker that will signal that the attack has succeeded (if you manage, you will obtain a flag from the attacker in response).

The two parts carry equal marks.