IMPERIAL COLLEGE OF SCIENCE, TECHNOLOGY AND MEDICINE

EXAMINATIONS 2016

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 (Specialist)
MRes in High Performance Embedded and Distributed Systems
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 23 March 2016, 10:00
Duration: 120 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.

- 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.

- The username and password for `pentest-vm` are respectively `exam` and `exam`. If needed, you can gain root access via `sudo`.

- 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 `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.

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

1 Botnets and JavaScript

One of the goals of malware authors is to compromise user machines and recruit them into a botnet. You work for a threat analysis firm and a client has just reported a suspicious email that may contain botnet-related malware. You are tasked with analysing this threat and producing a report.

a In your report, you are asked to provide background information about malware and botnets to the client's Chief Technology Officer, who is not a security expert.

i) Briefly describe these 3 different kinds of malware: worm, adware, drive-by download. Which kind is more likely to be part of a botnet campaign?

ii) List 3 different ways that a botmaster can profit economically from running a botnet.

iii) Take the viewpoint of a botnet operator, and write down indented bulletpoints for an attack tree with root: "*Recruit a new machine for the Botnet*". Your answer should contain at least 2 levels and 6 nodes (excluding the root). The attack tree need not be exhaustive. Use bulletpoint marker '+' for necessary steps and '-' for sufficient steps.

b The reported email states that the recipient has won a large sum of money, and needs to click on this link to claim it: `cashprize.lottery.com.zxy.ru`.

i) Analyse the attack to find out what vulnerability it is trying to exploit: if you are on the right trail, you will discover a clearly marked flag that you need to report. (Hint: Burp may be a useful tool for this question.)

ii) Briefly describe what kind of vulnerability you think the attacker is trying to exploit. Suggest a mitigation for this vulnerability.

iii) Based on your analysis of the attack in part (b.i) above, and possibly on further analysis of the attack, trick the botmaster into thinking that the attack has succeeded, and obtain a flag from the botmaster.

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

2 SQL Injection and Passwords

BorkBork, a telecoms company, is blaming the loss of customer data on negligence by their customer relationship manager Alice, because the data was stored on a file in her account `crm`. You are hired by Alice to prove that her account could easily have been hacked by a malicious outsider. The company lets you run a gray-box penetration testing exercise on their network (on IP range `10.39.26.64-95`).

a You are told that there is a database server somewhere on the company network, which you need to identify.

i) In the lectures we have defined the *Malicious web user*, the *Malware attacker* and the *Active network attacker*. Briefly describe their capabilities and compare their attacking power.

ii) Survey BorkBork's network to identify the database server. Report the IP and port where the database server is listening, the brand of database server software and its approximate version. The database server is also used by a web application hosted on `cms.borkbork.co.uk`. Report the Linux distribution (and version) of the host, and the brand (and version) of its web server software.

b You are told the database server contains a table with (salted) hashes of passwords. You want to demonstrate that a web attacker could have stolen Alice's password hash from the database.

i) Identify a SQL Injection vulnerability in `cms.borkbork.co.uk/login.php` that allows you to log in as user `root` with PIN `9110`, and report the flag displayed in the welcome page of the `root` user. (Hint: you may find it helpful to look at the HTTP request.)

ii) After logging in, identify a new SQL Injection vulnerability, and report the password hash of the user with employee ID `1`. Briefly explain your attack, and suggest how it could be prevented. (You can use credentials `guest` and `p4ssword` with PIN `1234` to log in, if needed).

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

The two parts carry, respectively, 40% and 60% of the marks.

3 PHP and Post-exploitation

The owner of `hack.it` hired you to run a black-box penetration testing exercise against two web servers on their network: `hack.it` and `tools.hack.it`.

a As part of your professional approach to penetration testing, you structure your activity following the Penetration Testing Execution Standard (PTES) methodology.

i) Describe some of the main objectives of the PTES phases *Intelligence gathering*, *Vulnerability analysis*, and *Post-exploitation*, when the testing target is a web application.

ii) As part of your vulnerability analysis you find that one of the two web applications 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 The developer of the `tools.hack.it` website has the bad habit of editing the file `index.php` directly on the web server, so his text editor saves a backup which is accessible at `tools.hack.it/index.php~`.

i) Review the code in `index.php~` to find vulnerabilities: one may still apply to `tools.hack.it`! Report 2 different lines of code that contain vulnerabilities, and suggest fixes for them.

ii) Exploit `tools.hack.it` and report the flag in `/var/www/private/E-FLAG.txt`.

iii) Access the file `/home/backups/PE-FLAG.txt` on `hack.it` and report the flag it contains. Briefly describe the process you followed. (Hint: you need to succeed with (b.ii) first.)

The two parts carry, respectively, 40% and 60% of the marks.

4 **Client-side Security and Sessions**

You work for the cybercrime unit of a law enforcement organisation, and are tasked with discovering the accomplices of notorious cybercriminal Charlie. A tip revealed that Charlie has an account on `grumblr.com`, where he has added his accomplices as friends. Unfortunately, `grumblr.com` is run from a country with weak rule of law and does not respond to your organisation's requests for data disclosure. You need to launch a targeted attack on the criminal.

a To begin with, you review your options.

i) Identify a *Spoofing*, a *Tampering* and an *Information disclosure* threat that can be leveraged to violate the privacy of an online social network user. Indicate to what architectural component (or communication channel) of the social network each threat applies, and suggest a mitigation.

ii) A common attack vector against web applications is XSS. Briefly describe *DOM-based*, *Reflected* and *Stored* XSS attacks, and compare how they can be deployed.

b The tip also revealed that Charlie regularly visits both `grumblr.com` and `petflix.com`, and may click on any link on either site.

i) Find and exploit 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.

ii) You are now looking for a CSRF attack on `grumblr.com`. Provide a malicious link that, when clicked by Charlie, causes `grumblr.com` to reveal the email of his accomplice Shady. (Assume that Charlie 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.

iii) `petflix.com` has been DDoSed by a botnet, so your malicious link cannot be clicked by Charlie after all. Find a JavaScript injection attack against `grumblr.com`. Describe where the vulnerability is, and suggest a fix. Provide the exploit code to display Charlie's session cookie in an alert box, and explain how you are able to deploy the exploit code.

The two parts carry, respectively, 40% and 60% of the marks.