PAPER C331

NETWORK AND WEB SECURITY

Tuesday 12 May 2020, 11:00
Duration: 120 minutes
NO post-processing time
Answer THREE questions

While this time-limited remote assessment has not been designed to be open book, in the present circumstances it is being run as an open-book examination. We have worked hard to create exams that assesses synthesis of knowledge rather than factual recall. Thus, access to the internet, notes or other sources of factual information in the time provided will not be helpful and may well limit your time to successfully synthesise the answers required.
Where individual questions rely more on factual recall and may therefore be less discriminatory in an open book context, we may compare the performance on these questions to similar style questions in previous years and we may scale or ignore the marks associated with such questions or parts of the questions. In all examinations we will analyse exam performance against previous performance and against data from previous years and use an evidence-based approach to maintain a fair and robust examination. As with all exams, the best strategy is to read the question carefully and answer as fully as possible, taking account of the time and number of marks available.

Paper contains 4 questions

General instructions

- All your answers should be submitted electronically by accessing the website `https://co331.doc.ic.ac.uk` using a standard web browser (Chrome or Firefox are recommended). Log in to the website using your *college username* and *college password*.

- Remember to save your answers periodically, and especially before navigating to a different page or closing the browser. We strongly advise not to rely on submitting answers during the last 2 minutes of the exam.

- You are advised to read the exam questions in the following pages directly on Answerbook, because **several links are relative to Answerbook and will not be accessible from this pdf file**.

- Only your browser is necessary to complete the practical parts of the exam. Other tools you may want to use are your code editor and standard command line utilities.

- Although due to the open-book nature of the exam you are allowed to consult reference material, doing so is not deemed necessary and may cost you valuable time.

Warning: attempts to abuse `https://co331.doc.ic.ac.uk` or Answerbook itself will be considered serious violations and may lead to disciplinary action.

1 Advanced Persistent Threats (APTs)

a APTs are highly-skilled adversaries who employ well-trained and well-resourced cyber security personnel to target specific organizations with objectives such as espionage, data exfiltration and damaging critical infrastructure.

i) *Spear (targeted) Phishing* and *DNS Hijacking* are two common techniques used by APTs for the initial compromise of a target network. Describe both techniques and compare their advantages and disadvantages in this specific context.

b After the initial compromise, an APT gains a foothold on the target network and proceeds with the exploitation phase, which may happen over a long period of time. Stealth is crucial to avoid detection during this phase.

i) Compromised hosts mostly use DNS queries to find Command and Control (C2) servers dynamically. Briefly discuss what kind of domain names an APT should choose in order to avoid detection by the security defences of the target network and to ensure that the domain will remain available for an extended period of time. File domains.txt contains a list of fully qualified domain names (FQDNs) visited by hosts of a network compromised by an APT. Most items in the list were legitimate, except for 15 which were APT FQDNs. Report 5 of the APT FQDNs.

ii) The ascii-formatted file capture.txt contains APT activity on a local network. Report the IP and port of the compromised host running a hidden service. Briefly describe how the service was hidden, providing any technical information you deem relevant.

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

2 Passive web application security assessment

a You are currently using Answerbook to submit your answers for the 331 Network and Web Security exam. This web application was developed here at DOC specifically for this exam, with security in mind. Yet, *security is a process* and constant review is necessary.

i) Answerbook was originally designed to be served only to the lab machines of students present in the DOC lab. Based on this scenario, perform a threat analysis of Answerbook from the point of view of the lecturer running the exam. Report 2 relevant and non-trivial STRIDE threats. For each threat, declare the STRIDE category, and briefly describe the attacker objective and what technique could be realistically used to achieve it.

ii) Because of Covid-19, this year the 331 exam is running over the Internet. Report 2 additional STRIDE threats for Answerbook specifically relevant to this new scenario. For each threat, declare the STRIDE category, and briefly describe the attacker objective and what technique could be realistically used to achieve it.

b You are now tasked with performing a passive security assessment of Answerbook, based only on observing the HTTP requests and responses that you can see in your browser as part of a normal interaction with Answerbook. (For this part you do not need to, and should not, tamper with requests, submit fake data, use external tools besides your browser.)

i) Does Answerbook appear to defend against CSRF attacks? Briefly justify your answer.

ii) Discuss the use (or lack of use) that Answerbook makes of 2 HTTP headers, from the security point of view. Prioritise headers where you can say something insightful rather than prioritising them by popularity.

iii) Some students of 331 are renowned for their advanced cross-site scripting (XSS) skills. Discuss how the structure of the question web pages, and their Content Security Policy (CSP), could be changed to harden Answerbook against XSS attacks able to bypass the server-side filters which, rest assured, are in place. Your solution must preserve the existing functionality of the web application and cannot introduce the use of `<iframe>` elements.

The two parts carry equal marks.

3 Server side security

a Web server logs are an important source of information to detect attempted and ongoing attacks on web applications. Each log entry is on a separate line, and reports information about an HTTP request, including timestamp, requested URL, HTTP status code, response body size, referer URL, User-Agent string.

i) Name 2 attacks against the server side of a web application that can be detected by looking at individual entries in web server logs containing the information mentioned above, and describe how the attacks can be detected.

ii) The file web-server-log.txt shows real (anonymized) access logs from the DOC home pages web server. Report the log entries that show an attacker attempting to discover or exploit a vulnerability. (Points will be subtracted for any legitimate entry reported.)

b i) Describe and compare two independent ways to prevent SQL injection against a database exposed on the server side of a web application.

ii) The function `prepareCondition` in the PHP library file pdo-mysql-cond.php contains a SQL injection vulnerability. Paste below the vulnerable line, provide a replacement line that fixes the vulnerability and provide a Proof Of Concept exploit, in the form of a PHP value such that the code `$x = <your value>; $db->prepareCondition('y', $x);` returns a query where you can inject SQL code.

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

4 **Dangerous browsing**

a Consider a home network where a router R is connected to the internet via a commercial ISP, which assigns to the router the public IP address 178.79.130.100. The router connects 178.79.130.100 via NAT to a LAN on the range 192.168.1.0/24. It also acts as the base station for an unencrypted WiFi network that provides access to the LAN. The home is a flatshare with several users who connect to the WiFi with various devices in order to gain access to the internet.

i) How is it possible for the router to know what network response received at 178.79.130.100 should be sent to what host on the LAN? Provide a simplified example.

ii) Can any flatmate see the content of the HTTP websites browsed by other flatmates? Justify your answer.

iii) Describe a scenario where any flatmate can find out what HTTPS websites another flatmate is browsing, and one where it is not possible.

iv) Describe a scenario where a website attacker controlling a site visited by a security-conscious flatmate using a fully-patched browser can still spoof HTTP websites to the other flatmates, and propose 2 countermeasures.

b Visit the malicious website https://nah.fun in your browser (no harm will come of it).

i) The site sets 3 cookies in your browser. Identify which one of these is a first-party tracking cookie, and report its *value* below.

ii) Analyse the script `evil.js` loaded by nah.fun, report the flag you discover. Briefly describe what kind of attack the script was attempting.

iii) Report another flag that you find by analysing more in depth the behaviour of nah.fun. (You only need your browser, no external tools.)

The two parts carry equal marks.