UNIVERSITY OF LONDON

BSc EXAMINATION 2024

For Internal Students of
Royal Holloway

DO NOT TURN OVER UNTIL TOLD TO BEGIN

IY2840: Computer and Network Security
IY2840R: Computer and Network Security – for
FIRSTSIT/RESIT CANDIDATES

Time Allowed: **TWO hours**

Please answer **ALL** questions

Calculators are not permitted

1. TRUE/FALSE QUESTIONS

State which of the following statements are **TRUE** and which are **FALSE**, making sure that in each case you provide a brief justification for your answer (no marks will be awarded for answers that are not justified).

(i) Data and programs are separated in memory. [2 marks]

(ii) ARP prevents man-in-the-middle attacks. [2 marks]

(iii) DNS by itself provides strong integrity guarantees. [2 marks]

(iv) Security policies should be written in legal language to be as secure as possible. [2 marks]

(v) Reflected cross-site scripting attacks are based on a vulnerability of the database system used by the web application. [2 marks]

(vi) UNIX user groups never have the same ID number as the user's UID. [2 marks]

(vii) SYN cookies can have the secure flag and are then not sent in plain. [2 marks]

(viii) MULTICS inspired fundamental concepts of modern operating system access control. [2 marks]

(ix) Commercial computers in the 1970s came with no security controls. [2 marks]

(x) Unprivileged processes can modify the UNIX system clock. [2 marks]

(xi) The first computers were programmed in decimal. [2 marks]

(xii) Javascript can be embedded in HTML in several tags. Give **two** examples of such HTML tags. [3 marks]

2. NETWORK SECURITY

(a) What do the following acronyms stand for in the context of networking?

i. DNS
ii. TCP
iii. ARP
iv. ICMP
v. MAC [5 marks]

(b) Explain the steps involved when a client uses DNS to find the IP address of a particular domain. You may use a diagram if this helps. [10 marks]

(c) How does a DNS resolver authenticate replies from authoritative name servers, and how does this help the attacker with their attack? [3 marks]

(d) Explain the steps when a client uses ARP to find the MAC address of a particular host [3 marks]

(e) How do hosts authenticate ARP replies from authoritative name servers, and how could this help an attacker with an attack? Provide examples. [4 marks]

3. SYSTEM SECURITY

(a) What do the following acronyms stand for in the context of system security.

i. TOP
ii. GDB
iii. NOP
iv. RGID
v. EUID [5 marks]

(b) Consider the following C code fragment, which is vulnerable to a memory corruption attack:

```
int main(int argc, char **argv){
  char lbuf[64];
  if (argc > 1)
    strcpy(lbuf, argv[1]);
  return(0);
}
```

Explain why the above code is exploitable on x86-32 architecture. Is it possible to execute arbitrary code, such as spawning a shell? Explain how you would exploit it (high-level steps). [5 marks]

(c) Consider the following modified excerpt from `/etc/users` from a Linux system.

```
root:x:?:?:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
acooper:x:1299:1320:IT,A-1-24,x867:/home/IT/acooper:/bin/bash
bmorse:x:1321:1342:IT,A-1-26,x5309:/home/IT/bmorse:/bin/bash
cbrown:x:1352:1380:IT,C-5-12,x606:/home/IT/cbrown:/bin/bash
dprince:x:1444:1480:IT,B-4-55,x0842:/home/IT/dprince:/bin/bash
```

i. What value should be in place of ? in the first line. [1 marks]
ii. What is the purpose of the `x` in the second field of all entries? [1 marks]
iii. What does the value 1444 correspond to in the last entry? [1 marks]
iv. What does the value 1480 correspond to in the last entry? [1 marks]
v. Provide the value of the GECOS field for any of the last 4 entries. [1 marks]

(d) Explain what a reference monitor is and what it does. Your answer should include any properties it must fulfil and any possible configurations it may take. [10 marks]

4. WEB SECURITY

(a) What do the following acronyms stand for in the context of web security.

i. SOP
ii. DOM
iii. TLS
iv. CSRF
v. XML [5 marks]

(b) Cross-Site Scripting (XSS) is a widespread problem affecting a number of web services.

i. State the main vulnerability that leads to XSS attacks. [2 marks]
ii. Briefly describe the *general principle* of XSS attacks. Which security policy is both evaded and exploited in such attacks. [8 marks]

(c) SQL injection is an example of a Web Application exploit.

i. Give a brief description (at most three sentences) of this attack and explain why it can succeed. [6 marks]
ii. An online shopping site takes an email address as input to `$EMAIL` and constructs an SQL query as follows:

```
$query = "SELECT * FROM members WHERE email='$EMAIL'";
```

What would a malicious user enter as their `email` address in order to get the database to delete all entries from table `foo` (assuming the table exists)? (No need to explain the answer.) [4 marks]

END