ECE 458/750: Computer Security Final			Marks obtained ↓
Date: August 17, 2026,	Total questions: **17**	Total points: **71**	
ID:	Name:		Time: 2.5 hours

Instructions

No aids allowed. All you are allowed is a pen and pencil.

Use space provided. Answer the questions in the spaces provided. If you run out of room for an answer extra pages are provided at the end of the test booklet starting on page 17. They are clearly marked as EXTRA ANSWER SPACE. Please state in the original answer space if the extra pages are being used so that the grader knows to look there.

Point value in right-hand margin. The number of points each question is worth is listed in the right hand margin. The number of points and the space provided are roughly indicative of how long of an answer is expected.

Pencils and pens allowed. Both pens and pencils are allowed. Pencil marks need to be clearly present or erased. If it is unclear if a mark is or is not present then it is up to the discretion of the grader and this point cannot be contested later.

Fill in or circle multiple choice answers. Multiple choice and multi answer questions will have boxes or circles next to the answer options. You may fill these in, clearly mark them, or circle the whole answer. It needs to be clear which answer option(s) have been selected.

Figures provided. Some content has been provided from the lecture slides. This content appears as figures, and is directly referenced by the question were we expect that you will need the figure information. For example: "The rules on Figure 1 may be helpful in this question."

Grad only questions. The last question is only for ECE750 students. It is very clearly marked as grad only. Undergraduates taking ECE458 do not need to complete this question, and any answers they provide will be ignored when assigning final grades.

General Security Questions

1. A malicious actor launches a ransomware attack which encrypts all the files on a system while ensuring that only the malicious actor has the private key. Which CIAAA principle is undermined when a user is unable to open a file? Name the principle and provide at most one sentence of justification. (2)

2. Imagine that you are playing a YouTube video and an advertisement comes up. You do not want to watch the advertisement. How might you use the URL below to avoid the advertisement? (2)
   This is a real older attack that has now been fixed by YouTube and therefore no longer works.

   https://www.youtube.com/watch?v=GZniJBygnX8&t=133s

3. Which of the following access control structures we learned about best approximates how Linux manages access control of files? (2)

   ◯ Access Control Directory
   ◯ Access Control Matrix
   ◯ Access Control Triples
   ◯ Access Control Lists

4. A software vendor discovers a buffer overflow vulnerability in its web server and assigns it the identifier CVE-2026-12345. (2)

   What does this CVE identifier represent?

   ◯ A category of programming mistakes that can occur in many applications
   ◯ A specific publicly documented vulnerability in a particular product
   ◯ A security patch released by the vendor
   ◯ A security risk score assigned to the vulnerability
   ◯ An identifier of the software bill of materials (SBOM)

Public/private key cryptography

5. Alice and Bob decide to use the third party chat app *ChatApp* to communicate which is developed and run by Eve. *ChatApp* uses a central server where it stores all messages. Because they do not fully trust *ChatApp*, they decide to use the Linux GPG program to securely do public/private key encryption and decryption of messages. They then copy/paste the encrypted messages in/out of *ChatApp*. Alice and Bob only ever communicate over *ChatApp* and do not independently verify or sign their keys in advance. (6)

   Imagine that the following scenario occurred where Eve was successfully using her control over *ChatApp* to perform a Man-in-the-Middle attack on Alice and Bob's communication.

   - Alice and Bob attempt to exchange public keys using ChatApp. Eve intercepts both requests and sends her own public key to each user while pretending to be the other person.
   - Alice and Bob then begin using GPG and *ChatApp* send and encrypt/decrypt messages. Both can successfully encrypt and decrypt messages and neither notices anything unusual. Eve can read all messages exchanged between them.
   - Eve is able to read all messages sent between Alice and Bob.

   In the following table, place a mark (✓or ■) in each box corresponding to a key (row) that the person (column) possesses at the end of the attack described above. Assume that no keys were exchanged except through ChatApp in the scenario described above.

Key ↓	Alice	Bob	Eve
Alice's Public Key	☐	☐	☐
Alice's Private Key	☐	☐	☐
Bob's Public Key	☐	☐	☐
Bob's Private Key	☐	☐	☐
Eve's Public Key	☐	☐	☐
Eve's Private Key	☐	☐	☐

6. The attack in question 5 works because both Alice and Bob are making an inaccurate assumption. What inaccurate assumption are they making? (2)

7. A legitimate company named Acme contracts with a root-level Certificate Authority (CA) to obtain a new certificate. The root CA generates a new key pair and sends both keys back for Acme to install. (3)

   The above described scenario is a very bad way to do security, it breaks a key assumption in cryptography.

   What attack becomes possible if Certificate Authorities worked this way?

Networking

8. In the Networking module we discussed an attack done by Archive.today against a blogger (`gyrovague.com`) who wrote something the Archive.today site owner did not like. Archive.today is a website that was heavily used by Wikipedia at the time to reference paywalled citations. To accomplish the attack, Archive.today inserted the following code into the Archive.today website:

```
setInterval(function() {
  fetch("https://gyrovague.com/?s=" +
    Math.random().toString(36).substring(2, 3 + Math.random() * 8), {
      referrerPolicy: "no-referrer",
      mode: "no-cors"
    });
  }, 300);
```

   (a) Name the type of attack Archive.today is doing. (1)

   (b) Explain what happens when a visitor loads the Archive.today webpage. Describe how the JavaScript affects the visitor's browser, what requests are generated, and how those requests may affect `gyrovague.com`. (5)

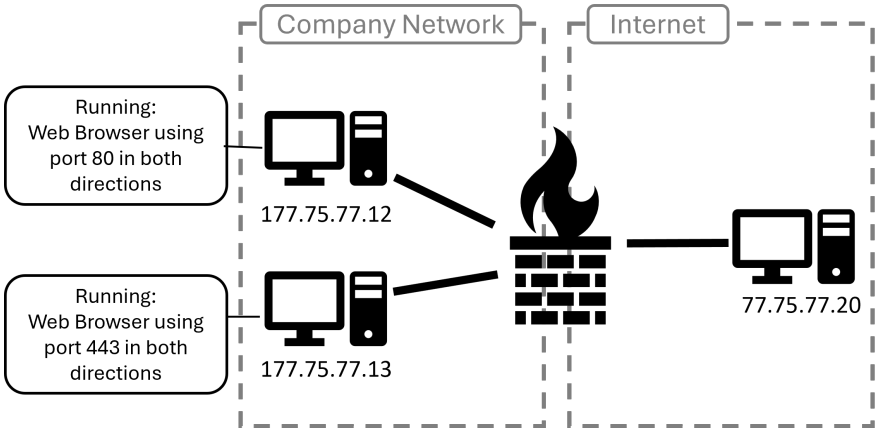

Figure 1: Network setup depicted similarly to the BlueTeam game.

Firewalls

9. Using the network diagram in Figure 1, determine what the firewall rules should be and fill in the tables below. This question is heavily based on the assigned game BlueTeam. Similar to that game, you should create a least-privilege setup that will allow the depicted computers to function. (6)

   Fill in only the parts of the table you need, leave unused rows blank.

INPUT Rules

Rule #	Policy (Reject)	Port	IP Address
1			
2			
3			

OUTPUT Rules

Rule #	Policy (Reject)	Port	IP Address
1			
2			
3			

10. Why are both INPUT and OUTPUT rules needed in the scenario in Figure 1? (2)

Spectre

11. Spectre is an example of a side-channel attack. What is the side channel used by Spectre? (2)

12. Which of the following statements about the Spectre attack is **true**? (2)

- ◯ Spectre allows an attacker process to directly read arbitrary memory belonging to another process using a normal memory load instruction.
- ◯ Spectre tricks a victim process into performing a buffer overread on behalf of the attacker and then uses a side channel to infer the leaked data.
- ◯ Spectre exploits a flaw in TLS certificate validation to impersonate websites.
- ◯ Spectre requires physical access to the victim's device in order to extract secrets from memory.

Website

Figure 2 shows a section of the server-side code of a website.

The code is written in PHP, you may assume the following:

- variables start with a `$`
- `.` means string concatenation
- `isset()` returns TRUE if the variable has a value, FALSE otherwise
- `echo()` prints a string on the resulting website
- Comments start with a `//` and can be read as accurate general descriptions of the code (obviously code is more precise).

```php
// Global session management variables
// (in reality these would be in a database or file)
$SESSION_TABLE = [];        // Maps session_id to user data
$NEXT_SESSION_ID = 1;       // Session ID counter

// --- Session Setup Logic ---

// Check if there is a sid in the GET string
if (isset($_GET['sid'])) {
    // Sanitize sid and ensure it is an integer
    $sid = intval($_GET['sid']);

    // Check if the sid is a real session ID
    if (is_valid_session($sid)) {
        // Existing valid session
        $current_session = $SESSION_TABLE[$sid];
        echo "Welcome back! Your session ID is: " . $sid;
    } else {
        // Invalid session ID provided
        echo "Invalid session ID!";
        exit();
    }

} else {
    // No session ID provided - create a new one
    $sid = $NEXT_SESSION_ID;
    $NEXT_SESSION_ID++;

    // Create new session record indexed at position $sid
    $SESSION_TABLE[$sid] = ["created" => time()];

    echo "New session created. Your session ID is: " . $sid;
}
```

Figure 2: Snippet of server code. This code has a security flaw. You may treat the comments as accurate descriptions of the code's intent. You may also ask course staff about function meanings.

13. The code in Figure 2 has a flaw (whiteboard-level design issue). Explain how an attacker could exploit the session management design shown in Figure 2. (6)

14. Describe two ways in which the code in Figure 2 could be made more secure. We recommend using the line numbers to be precise about what would need to be changed. (4)

(a) First improvement

(b) Second improvement

Cross-Site Scripting

15. A website uses cookies to keep users logged in. But an attacker discovers a Cross-Site Scripting (XSS) vulnerability on the site.

    (a) Briefly describe what Cross-Site Scripting (XSS) using JavaScript is. (2)

    (b) The attacker puts JavaScript into their XSS attack. Where is that JavaScript meant to be executed? (2)

    (c) How could the attacker use JavaScript to take over another user's account? (4)

(d) State one server-side defense against XSS. (2)

Memory

16. Consider the following program.

```
void function(char *str) {
    int authenticated = 0;
    char buffer[16];
    strcpy(buffer, str);
}

int main() {
    char input[128] = "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA";

    function(input);
    return 0;
}
```

Similar to Assignment 3, assume that the program is compiled as a Set-UID root program and that stack protection and address space randomization has been disabled.

(a) Identify the vulnerability. (2)

(b) Explain why an attacker would want to overwrite the return address. (2)

(c) Draw a stack diagram for `function` showing the locations of: (3)

- buffer[16],
- authenticated,
- return address.

Indicate the order in which memory locations are overwritten.

Grad Students Only (ECE750)

Only graduate students completing ECE750 need to answer the questions in this section. We will ignore answers by ECE458 students when assigning final grades.

17. In the graduate-only assignment you watched a video by Kamara in which he describes the Vula system used by the ANC. The Vula system was intentionally designed to operate asynchronously.

    (a) The system is purposely asynchronous. What security advantage exists to making it asynchronous? (3)

    (b) The encryption scheme used words copied from books as seed values in a pseudo random number generator. In the authentication part of the class we learned about passwords and the general advice to not write a password down. (4)

    Explain why using words from books for encryption safe but writing a password down is unsafe?

Extra Answer Space

If you need extra space to give an answer, please state in the original answer space that you will be using the extra pages and continue or write your answer here. If you choose to use the extra space as scratch paper, please write "scratch" so that graders know to ignore anything you have written. You may also tear off an extra space page and use it for scratch paper.

EXTRA ANSWER SPACE

EXTRA ANSWER SPACE