UPM	**Computer Security**	Date: November 4th, 2024
Midterm Exam (Network Security, Software Analysis)		
Name: YANG ZHAOPU		*Duration: 2 hours*

Problem 1 (Network Security) — 20 Points

1,1/10

(1.1) Scanning and DoS (10 Points)

(a) (2 points) A security researcher has identified the IP address of a command-and-control (C&C) server and wants to gather information about the botnet controlled through this server. By reverse-engineering a malware sample that connects to the C&C server, the researcher finds out that the communication happens through the following ports: 110, 143, 587.

0,6/2

1. For each probe sent on one of these ports, the researcher observes a different behavior:
   (a) from port 110 the server replied with a "ACK" packet;
   (b) from port 143 there was no response from the server;
   (c) from port 587 the server replied with an "ICMP port unreachable"

   Could you infer which transport protocol (i.e., TCP or UDP) did the researcher use in each probe?

TCP

+0,3

2. Could the server be behind a firewall? Motivate your answer.

Yes. From the ports the communication happens.

+0,3

(b) (2 points) What is IP spoofing? Name one attack type, which is not SYN flooding, and that typically uses IP spoofing.

0/2

Using lots of IP request to cost the server's ability, preventing it connect with the true user.

X

DDos

DDos

(c) (2 points) In presence of SYN flooding that uses spoofing, what would be consequence of using publicly accessible and reachable hosts? Can SYN flooding be used to target a UDP-based protocol? Motivate your answers.

0,5/2

Can't connect correctly.

NO. Because UDP don't need SYN.

+0,5

(d) (2 points) What is a DoS attack? Excluding the bandwidth, name two resources that an attacker can target in a DoS attack. What is the difference among a DoS and a DDoS attack?

0/2

server, ~~connector~~ router.

X

(e) (2 points) Define what are, and how are estimated, the Bandwidth Amplification Factor (BAF) and the Packet Amplification Factor (PAF) in a reflector amplification attack.

0/2

X

An attacker uses a reflector amplification attack on two protocols X and Y. On X, the value of PAF is 7, while on Y the value of BAF is 20. Which protocol is responsible for sending a higher volume of traffic (i.e., bytes) to the victim? Motivate your answer.

X

TCP.

(1.2) HTTPS (10 points) 0.25/10

(a) (2 points) What are the capabilities of a network attacker? Give an example of an entity that could act as a network attacker motivating why.

DNS Attacker.

It may let you go to the wrong IP.

0

Can inject, chop, modify packets, e.g., ISP

(b) (1 point) What are the TLS versions currently considered secure? Name one benefit of the latest TLS version.

1.3 and 1.2

+ 0.25

More protocols are ~~poor~~ provided.

Less

(c) (2 points) What entities appear in the *Subject* and in the *Issuer* field of a valid SSL leaf certificate for a website?

0 /

(d) (2 points) Which packet in the TLS handshake carries the SNI extension? What is the SNI extension used for?

The ~~second~~ first.

To ensure the secret ~~of the two~~ between the client and the server.

6

No, To enable multiple domains on same IP and to select correct certificate chain

(e) (3 points) Name three checks that a HTTPS client needs to perform on the certificate chain received from the server.

Header

CROS

Agent

Token

Host

Expiration

Revocation

Correct domain

...

0

Problem 2 (Software Security) — 20 Points

(2.1) Which of the following are memory safety vulnerabilities? Choose True or False for each entry (2 points, 0.25 each) 1.75/2

1. Buffer overflow: TRUE / FALSE ✓
2. Integer underflow: TRUE / FALSE ✓
3. Use-after-Free vulnerability: TRUE / FALSE ✓
4. Weak Credentials: TRUE / FALSE ✓
5. Time of Check Time of Use (TOCTOU): TRUE / FALSE ✓
6. XSS: TRUE / FALSE ✗
7. Out-of-bounds write: TRUE / FALSE ✓
8. Path Traversal: TRUE / FALSE ✓

(2.2) What is full disclosure? Please explain (2 Points) 0

~~The memory is able to be accessed by other.~~

When you access the part of the memory, you may get wrong result.

It is reused by not only one variable.

(2.2) What is the CVSS score? Please briefly explain (2 Points) 0

A score to compare the security of a software.

~~It uses many different~~

It stands from many differents points to assess the software, giving them correct weight.

(2.2) Vulnerable code (4 Points)

```
<?php
$ip_address = $_GET[ 'ip' ];
$cmd = exec( "ping $ip_address" );
....
?>
```

Given the above PHP code snippet describe the vulnerability and show how an attacker can exploit it.

The attacker can modify the "ip_address" which the program gets.

Explain pros and cons of using black lists vs white lists when trying to prevent injection attacks.

Using black list may let some attacks be ignored, ~~There are still~~ It is still dangerous.

Using white list can prevent all attacks at most of situation.

(2.2) Sessions and Cookies (4 Points)

1. Briefly explain what Cross-Site Request Forgery is.

   It stores the information of the usual users, as a certification to the website.

2. Is it enough to always resort to HTTPS when using ~~cooking~~ cookies to protect users from CSRF attacks? Why?

   No. The attacker can get cookies by some bad methods. At the same time, they can just request to skip the web ~~operate~~ operation.

(2.3) Taint analysis (6 points)

Consider the following code with taint analysis, and answer the following questions.

```
01. x = Source();
02. y = 0;
03. while(x > 1) {
04.   y = x + 1;
05.   x = x - 1;
06. }
07. if(x>=2) {
08.   z = y;
09.   Sink(z);
10. }
```

1. Would static taint analysis raise a warning? If so, at what line(s)? Mark tainted variables at each line of the analysis.

   Yes.

   03 07

   when the loop end, $X <= 1$,

   The condition is always wrong.

   X.

2. Would static taint analysis report any false positives?

0/1

No.

3. Would dynamic taint analysis raise a warning? If so, under which conditions and at what line(s)? Mark tainted variables at each line of the analysis.

0/1

Yes. When $x=1$ or $x<1$.

4. Briefly explain the advantages/disadvantages of static and dynamic analysis using this example.

0.5/2

	advantages	disadvantages
static :	simply, directly	~~many~~ can't catch all warning
dynamic :	whole,	complex