**VulnHub – Thales Walkthrough**

* There are 2 flags to find: **user.txt** & **root.txt**

1. First you must discover the devices on the network. The device we are looking for is the 192.168.56.106. Achieved by running ‘sudo netdiscover -i eth1 192.168.56.0/24’.

A screenshot of a computer screen

Description automatically generated

1. A screen shot of a computer

   Description automatically generatedSecondly, using nmap to discover the open ports (if any). In this case there was two discovered, one for SSH(22) and http-proxy (8080).

* Port 8080 is used for web servers, which means it could be word-press or qdpm.

1. A computer screen shot of numbers

   Description automatically generatedTo determine the possible web api/framework I will use Nikto to check.

* Running this will use the default port 80, which will produce no results since we need to look for 8080. To fix, use ‘-port 8080’ and run again.
* This now shows Tom-cat which is a web-server environment.

A screenshot of a computer program

Description automatically generated

1. A screenshot of a computer

   Description automatically generatedLoading the webpage.

* The version of Apache Tomcat is 9.0.52. A quick google search states that this version has possible XXS.

1. Checking with search-sploit shows no exploits found.

A screen shot of a computer code

Description automatically generated

1. A screenshot of a computer

   Description automatically generatedSearching through the possible different.

* Attempting to get into the manager html page directory prompts us with username and password.
* A screenshot of a computer

  Description automatically generatedUpon multiple failed attempts another page is prompted. It provides a possible username and password. I will try this because it may be a default password they didn’t change.

1. Since that didn’t work, I moved onto Metasploit, run ‘msfconsole -q’ in the root terminal.

* A screen shot of a computer

  Description automatically generatedThis is as recommended by online articles.
* The result is the username and password being cracked.
* USER: tomcat
* PASS: role1

A screenshot of a computer

Description automatically generated

* Successful login.

1. A screenshot of a computer program

   Description automatically generatedIn the same Metasploit console, type in the yellow highlighted text and exploit.
2. A screenshot of a computer

   Description automatically generatedNow in the server it is time to locate the user directory in /home.

A screenshot of a computer screen

Description automatically generated

* In the directory you see the two flags we are after. However the permissions for user.txt is going to require privilege escalation to view, since everything has been revoked.

1. Notes.txt displays a message and a directory to follow.
2. User.txt won’t open due to restrictions.
3. Since SSH is open we can look at the ‘.ssh’ file to see if there is a private key that has been stored. In this case we can see the file ‘id\_rsa’ which is storing the private key.

A screenshot of a computer program

Description automatically generated

1. Now we need to use john the ripper to find the password.

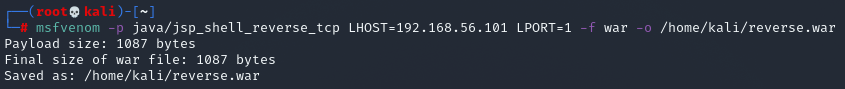
* A close up of a computer code

  Description automatically generatedwe need to use this version for ssh.
* Running the above command outputs a file that contains the hash of the key.
* This can now be ran through john the ripper and a wordlist passed.



* A screenshot of a computer program

  Description automatically generatedFinally the password is found and revealed to be ‘vodka06’.

1. It is now time to craft a WAR payload so we can netcat for connecting to the system.

* This will allow us to use netcat to create a connection and remotely execute commands on behalf of Thales. Upload the file to the dashboard of tomcat while you are in the ‘manager/html’. Run ‘nc -nlvp 1’ to connect and start exploiting.



1. Create interactive shell. Enter command ‘python3 -c ‘import pty; pty.spawn(“/bin/bash”)’ ’.

// I never got passed this bit because I had an error where my tomcat would not allow me to import my own WAR payload file.

1. You visit the “backup.sh” file and since it is writeable and readable you can modify to give you root privileges to view that files content ‘user.txt’, which reveals the flag.