Kioptrix level 1

**Executive Summary**

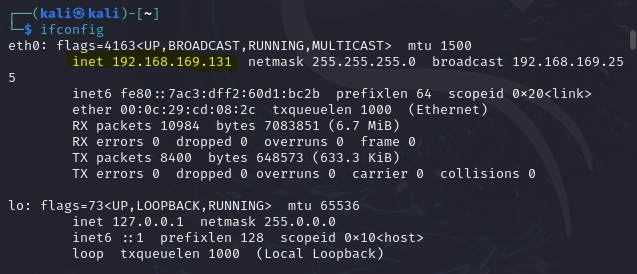
* Kioptrix is a vulnerable machine which we have no access to its user name or password
* We successfully open a shell to the target machine
* We recommend upgrade the apache to the latest version

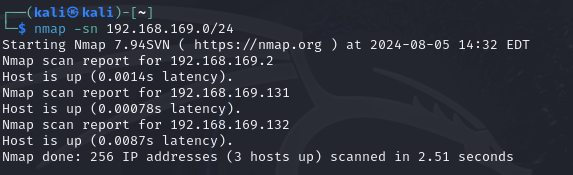
**Scope and Objectives**

* Systems and networks tested: the test was on the local network (local IP)
* Goals of the penetration test: open a shell to the target machine

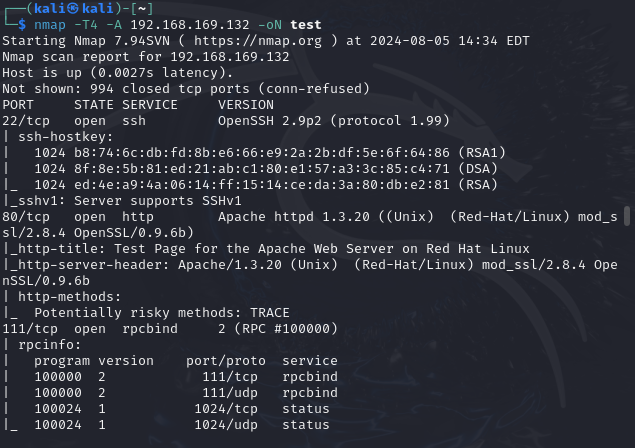
**Methodology**

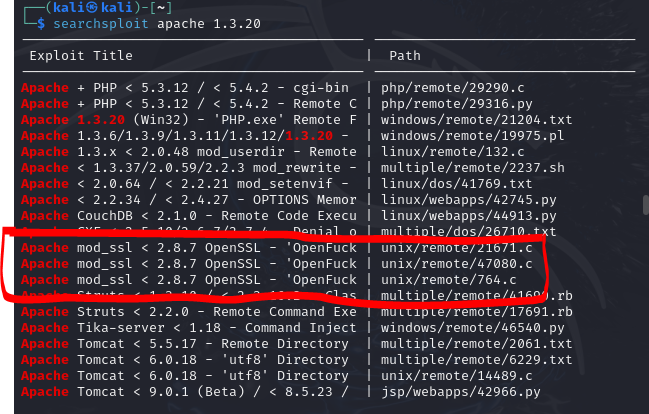
* First we use Ifconfig to know my IP



* Then we use Nmap –sn 192.168.169.0/24 or Nmap –sn 192.168.169.1-254 to scan the local network searching for the machine IP the 1st ip is for vmware and 2nd is my ip and the 3rd is the target machine
* Run a combination of command that gather more info and OS used with the default script and use timing template T4 which means make it fast as there is no firewall and save the output in a file called test

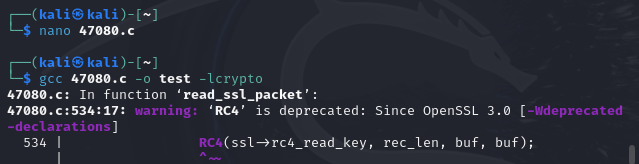
Nmap –T4 –A 192.168.169.132 –oN test



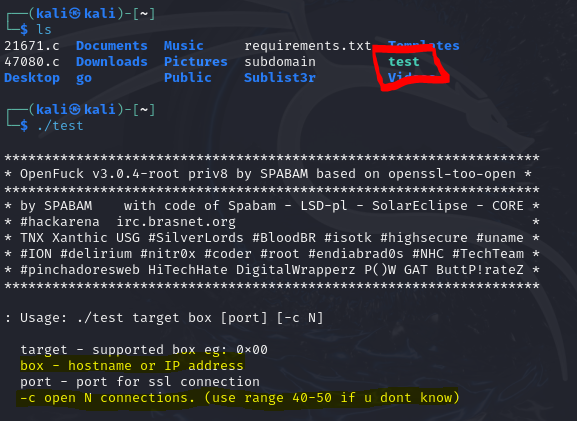
* After deep scan we found the target use apache 1.3.20 so Search for a code to exploit it in exploit-DB or Rapid 7 in her we use Searchsploit which is the API for exploit-DB and search for code to exploit apache 1.3.20 if the results is few try delete number from the version
* We then mirror the selected code in the current directory to use it

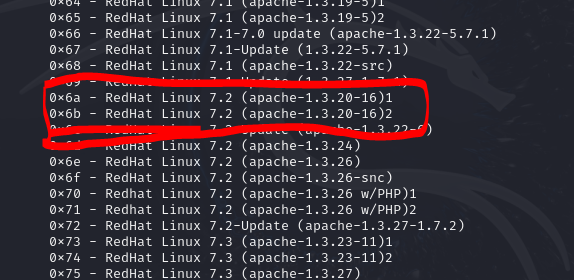


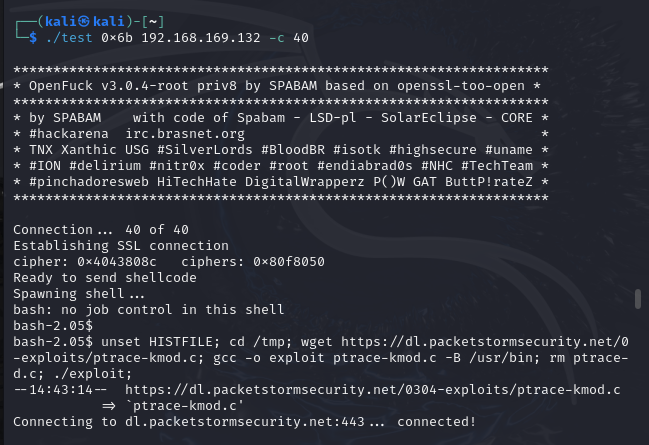
* Open the code and read the instruction then build it to get the exe file



* Run the code to see the parameters it takes



* It takes target which can choose one from the list, box as host name, port is optional and –c as number of connections recommended 40 to 50
* We choose redhat linux as the target run on this OS and choose the version of apache
* we run the code and it may hang so try again



**Findings**

1. **Vulnerability 1**
   * Description: Can open a shell in the target machine
   * Severity: high
   * Potential impact: high
   * Recommendations: update apache to the latest version

**Conclusion**

* Kioptrix is a vulnerable machine which we have no access to its user name or password
* We successfully open a shell to the target machine
* We recommend upgrade the apache to the latest version