

Lab 2 Response Outline

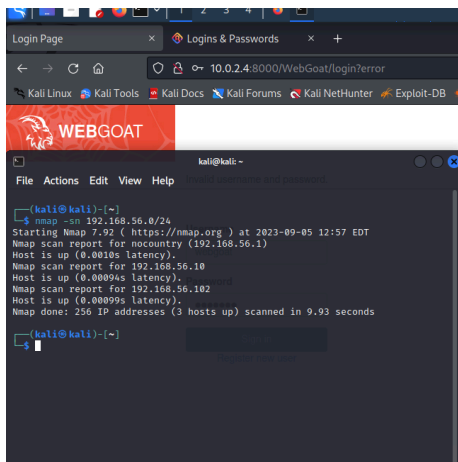
Lab 2: Penetration Testing: Reconnaissance

Test 1: Active Machines in the LAN

Summary of test experience:

A very first approach to getting to know about any system is to do a quick survey on how many machines are active in the entire network system. Tools such as Nmap, Netstat are widely used to scan a system and to find in-depth information about the system. Here, I, being an attacker, used nmap to find the active machines on 192.168.56.0/24 which is the entire network of the system. This means there could be at max 254 machines up as the subnet mask is 255.255.255.0, eight bits are dedicated for the hosts, the first address is for network and the last one for broadcasting. Nmap basically sends packets to each possible IP and analyzes the responses to discover the active machines and services

Screenshot of test results:



Provide a brief explanation of the results (1–2 sentences) answering the question: How does the image demonstrate that you completed the test?

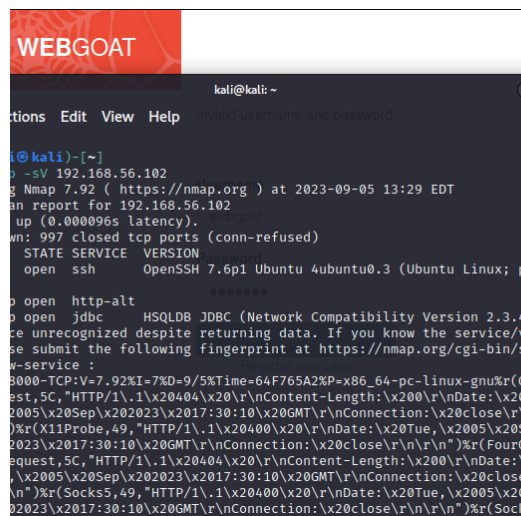
From the above image, we can see that 3 hosts are up: 192.168.56.1, 192.168.56.10 which is OpenWrt's website IP, and 192.168.56.102 which is the WebGoat server's IP.

Test 2: Open Ports on the Web Server

Summary of test experience:

Now it's time for gathering more information about the Web Server like open ports, services and their version using the nmap tool again. We can use this information to find CVEs and exploit the service if any services are in the older version.

Screenshot of test results:



```
kali@kali: ~  
File Edit View Help  
kali@kali:~  
$ nmap -sV 192.168.56.102  
Nmap 7.92 ( https://nmap.org ) at 2023-09-05 13:29 EDT  
Scan report for 192.168.56.102  
Up (0.000096s latency).  
Host is up (0.000096s latency).  
Not open: 997 closed tcp ports (conn-refused)  
STATE SERVICE VERSION  
open  ssh      OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; c  
open  http-alt  
open  jdbc      HSQLDB JDBC (Network Compatibility Version 2.3.4  
Unrecognized despite returning data. If you know the service/  
Please submit the following fingerprint at https://nmap.org/cgi-bin/s  
w-service :  
3000-TCP:V=7.92%I=7%D=9/5%Time=64F765A2%P=x86_64-pc-linux-gnu%r(0  
est,5C,"HTTP/1.1"x20404"x20\r\nContent-Length:x200\r\nDate:x20  
2005\x20Sep\x202023\x2017:30:10\x20GMT\r\nConnection:x20close\r  
)%r(X11Probe,49,"HTTP/1.1"x20400"x20\r\nDate:x20Tue,x2005\x20S  
2023\x2017:30:10\x20GMT\r\nConnection:x20close\r\n\r\n")%r(Four  
request,5C,"HTTP/1.1"x20404"x20\r\nContent-Length:x200\r\nDate:x  
2005\x20Sep\x202023\x2017:30:10\x20GMT\r\nConnection:x20close  
)\r\n)%r(Socks5,49,"HTTP/1.1"x20400"x20\r\nDate:x20Tue,x2005\x20  
2023\x2017:30:10\x20GMT\r\nConnection:x20close\r\n\r\n")%r(Sock
```

Provide a brief explanation of the results (1–2 sentences) answering the question: How does the image demonstrate that you completed the test?

The most interesting part we can infer from the above image is that the server's tcp port 22 is open and it's used for ssh service via OpenSSH version 7.6 which is not the latest version and might be exploitable.

Test 3: Active Web Pages Provided by the Web Server VM

Summary of test experience:

This test requires you to run a brute force test based on a dictionary to find the pages the Web server provides. I used two tools here: dirbuster and gobuster. I tried both small and medium dictionary wordlists of dirbuster. However, in those two tools' attacks, the server didn't show any WebGoat/login page which is mentioned in the documentation of this test.

Screenshot of test results:

Type	Found	Response	Size
Dir	/WebGoat/	302	214
Dir	/WebGoat/plugins/	200	336
Dir	/WebGoat/css/	200	336
Dir	/WebGoat/js/	200	336
Dir	/WebGoat/css/img/	200	336
Dir	/WebGoat/plugins/bootstrap/	200	336
Dir	/WebGoat/plugins/bootstrap/css/	200	336
Dir	/WebGoat/plugins/bootstrap/js/	200	336
Dir	/WebGoat/plugins/bootstrap/fonts/	200	336
Dir	/WebGoat/js/libs/	200	336
Dir	/WebGoat/js/backbone/	200	336
Dir	/WebGoat/js/instructor/	200	336
Dir	/WebGoat/js/jquery/	200	336

```
kali@kali: ~/gobuster
new Help
gobuster]
http://192.168.56.102:8000/ -w ~/Desktop/directory-list-lowercase-2.3-small.txt
[...]
```

Provide a brief explanation of the results (1–2 sentences) answering the question: How does the image demonstrate that you completed the test?

We can see from the left image that after I ran dirbuster on the server with 200 threads, I found 13 directories and 0 files. It took 3 hours and more. And from the right image, it's seen that gobuster can only find 1 active directory. In my estimation, gobuster doesn't perform a recursive brute force test.