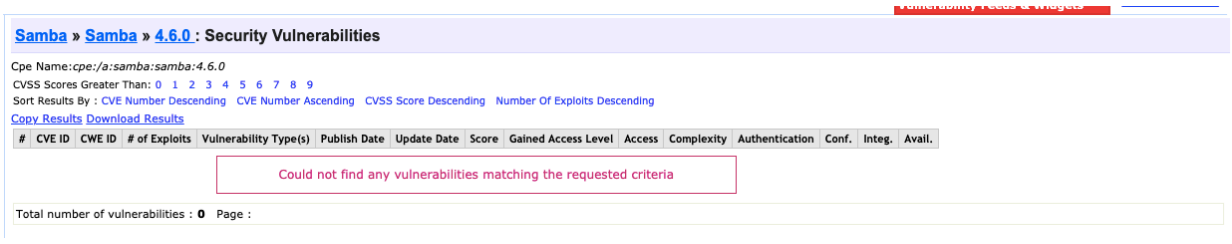
Roozah Khan
Laboratory Exercise 2-3 – Vulnerability Scanning Lab Exercise

Task 2: Use nmap scripts to scan for vulnerabilities

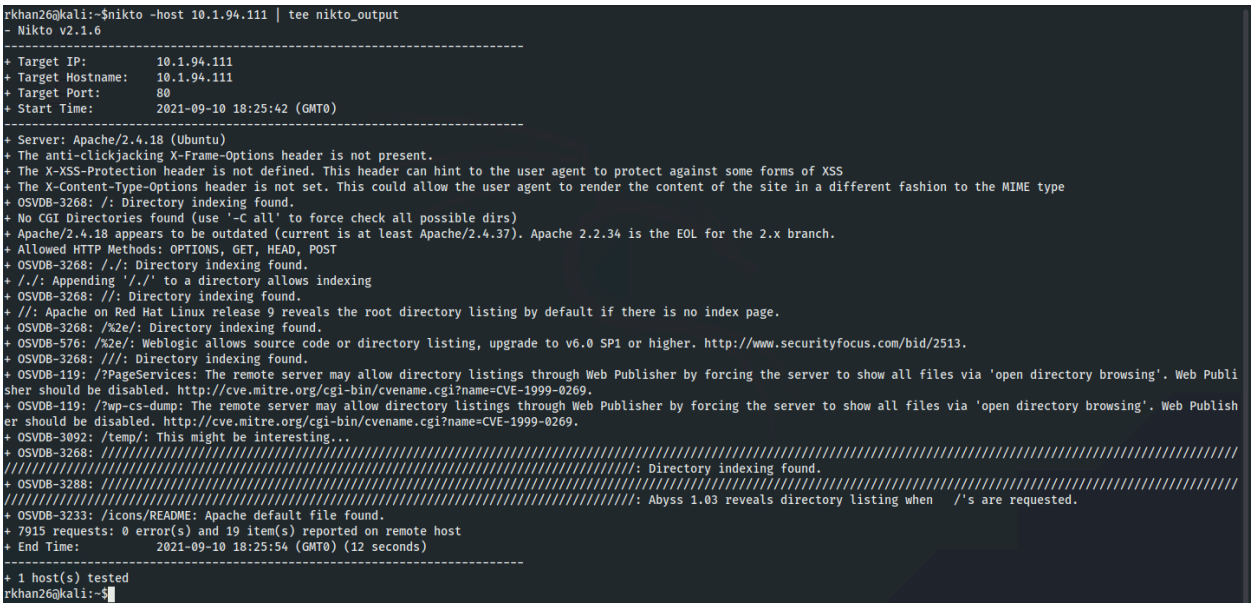
```
rkhan26@kali:~$nmap -sC 10.1.94.111 | tee nmap_scripts
Starting Nmap 7.80 ( https://nmap.org ) at 2021-09-10 17:00 UTC
Nmap scan report for ip-10-1-94-111.ec2.internal (10.1.94.111)
Host is up (0.0049s latency).
Not shown: 996 closed ports
PORT    STATE SERVICE
22/tcp  open  ssh
| ssh-hostkey:
|   2048 7b:54:1d:66:96:5e:c4:2b:64:1e:74:fe:bb:4b:1d:00 (RSA)
|   256 c6:5c:72:d4:be:b1:b2:bc:57:e8:e3:cf:a5:55:84:df (ECDSA)
|_  256 7f:ea:cd:5e:70:6a:72:3f:73:8f:ca:71:46:3e:ad:68 (ED25519)
80/tcp  open  http
| http-ls: Volume /
| SIZE  TIME              FILENAME
| 208   2017-06-09 13:27  hello.html
| 1.2K  2017-06-09 13:23  recipe
| -     2017-06-09 12:35  temp/
|_
|_http-title: Index of /
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds

Host script results:
|_nbstat: NetBIOS name: IP-10-1-94-111, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
| smb-os-discovery:
|   OS: Windows 6.1 (Samba 4.6.0)
|   Computer name: ip-10-1-94-111
|   NetBIOS computer name: IP-10-1-94-111\x00
|   Domain name: ec2.internal
|   FQDN: ip-10-1-94-111.ec2.internal
|_  System time: 2021-09-10T17:00:03+00:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-security-mode:
|   2.02:
|_    Message signing enabled but not required
```

I used the nmap command to scan for vulnerabilities and saved the output in the nmap_script file and used the tee command to print the output on the screen. The smb-os-discovery script has the same Samba version like it did in the Enumeration Lab.



I searched for the same Samba version 4.6.0 as it showed in the output and found there is nothing on the CVE website about any vulnerabilities associated with the SMB version.

Task 3: Use Nikto to scan for vulnerabilities



I used the nikto command to scan webserver vulnerabilities using the target IP address.