

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_script
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.

[Samba](#) » [Samba](#) » [4.6.0](#) : Security Vulnerabilities

Cpe Name: cpe:/a:samba:samba:4.6.0

CVSS Scores Greater Than: [0](#) [1](#) [2](#) [3](#) [4](#) [5](#) [6](#) [7](#) [8](#) [9](#)

Sort Results By : [CVE Number Descending](#) [CVE Number Ascending](#) [CVSS Score Descending](#) [Number Of Exploits Descending](#)

[Copy Results](#) [Download Results](#)

#	CVE ID	CWE ID	# of Exploits	Vulnerability Type(s)	Publish Date	Update Date	Score	Gained Access Level	Access	Complexity	Authentication	Conf.	Integ.	Avail.
Could not find any vulnerabilities matching the requested criteria														

Total number of vulnerabilities : 0 Page :

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

```
rkhan26@kali:~$ nikto -host 10.1.94.111 | tee nikto_output
- Nikto v2.1.6
-----
+ Target IP:      10.1.94.111
+ Target Hostname: 10.1.94.111
+ Target Port:    80
+ Start Time:     2021-09-10 18:25:42 (GMT0)
-----
+ Server: Apache/2.4.18 (Ubuntu)
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
+ OSVDB-3268: /: Directory indexing found.
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Apache/2.4.18 appears to be outdated (current is at least Apache/2.4.37). Apache 2.2.34 is the EOL for the 2.x branch.
+ Allowed HTTP Methods: OPTIONS, GET, HEAD, POST
+ OSVDB-3268: /.: Directory indexing found.
+ /.: Appending './' to a directory allows indexing
+ OSVDB-3268: //: Directory indexing found.
+ //: Apache on Red Hat Linux release 9 reveals the root directory listing by default if there is no index page.
+ OSVDB-3268: /%2e/: Directory indexing found.
+ OSVDB-576: /%2e/: Weblogic allows source code or directory listing, upgrade to v6.0 SP1 or higher. http://www.securityfocus.com/bid/2513.
+ OSVDB-3268: ///: Directory indexing found.
+ OSVDB-119: /?PageServices: The remote server may allow directory listings through Web Publisher by forcing the server to show all files via 'open directory browsing'. Web Publisher should be disabled. http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0269.
+ OSVDB-119: /?wp-cs-dump: The remote server may allow directory listings through Web Publisher by forcing the server to show all files via 'open directory browsing'. Web Publisher should be disabled. http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0269.
+ OSVDB-3092: /temp/: This might be interesting...
+ OSVDB-3268: ////////////////////////////////////////: Directory indexing found.
+ OSVDB-3288: ////////////////////////////////////////: Abyss 1.03 reveals directory listing when /'s are requested.
+ OSVDB-3233: /icons/README: Apache default file found.
+ 7915 requests: 0 error(s) and 19 item(s) reported on remote host
+ End Time:      2021-09-10 18:25:54 (GMT0) (12 seconds)
-----
+ 1 host(s) tested
rkhan26@kali:~$
```

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