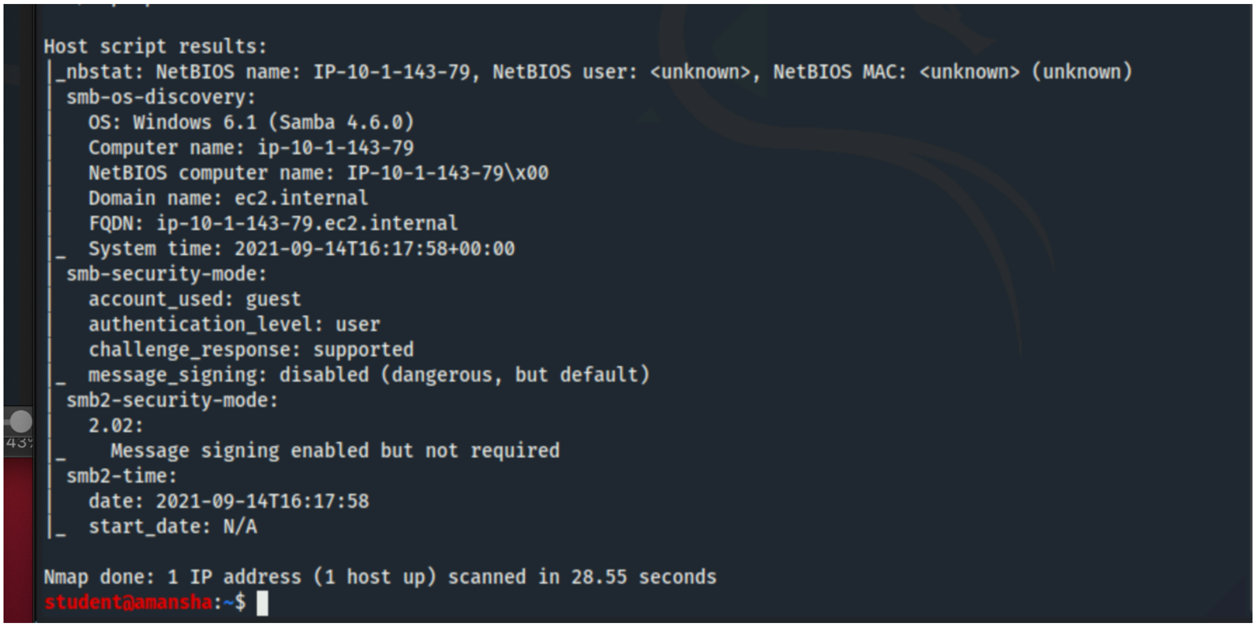
Amir Mansha
Lab 2-3 Vulnerabilities Scanning
CYSE 425
Fall 2021

Task 2: Use nmap scripts to scan for vulnerabilities

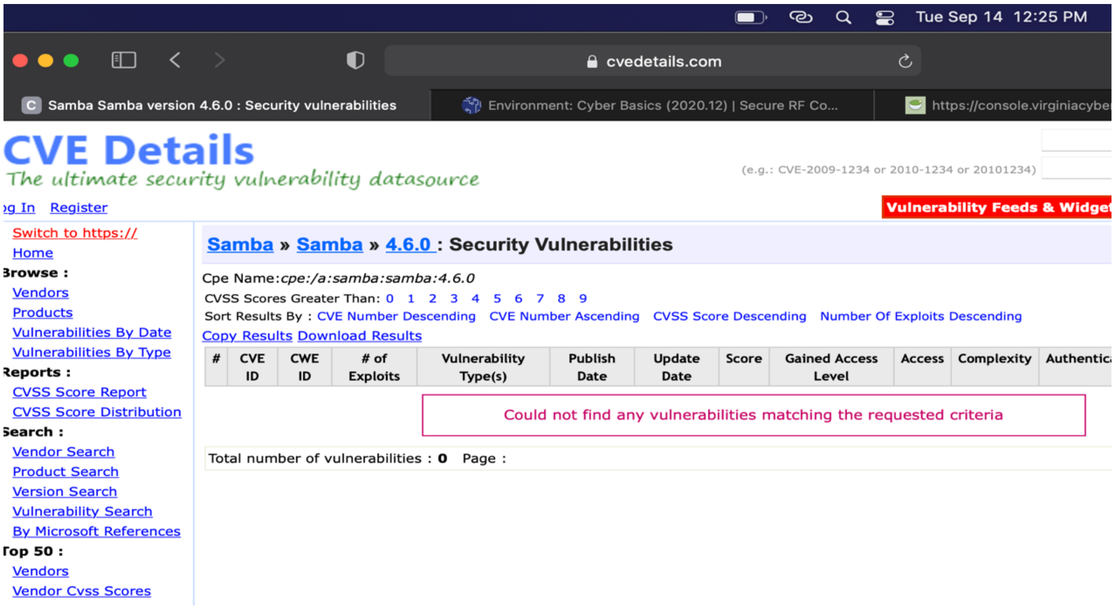
Using terminal, I ran the nmap command to scan for any vulnerabilities and saved the data to "nmap_scripts" using the tee command.



```
Host script results:
|_nbstat: NetBIOS name: IP-10-1-143-79, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
| smb-os-discovery:
|   OS: Windows 6.1 (Samba 4.6.0)
|   Computer name: ip-10-1-143-79
|   NetBIOS computer name: IP-10-1-143-79\x00
|   Domain name: ec2.internal
|   FQDN: ip-10-1-143-79.ec2.internal
|_  System time: 2021-09-14T16:17:58+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
| smb2-time:
|   date: 2021-09-14T16:17:58
|_  start_date: N/A

Nmap done: 1 IP address (1 host up) scanned in 28.55 seconds
student@amansha:~$
```

I then searched the Samba Version 4.6.0 online becuase that was the result from the smb-os-discovery script. Howver, just like the previous lab, it showed no vulnerabilities.



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	Authentic

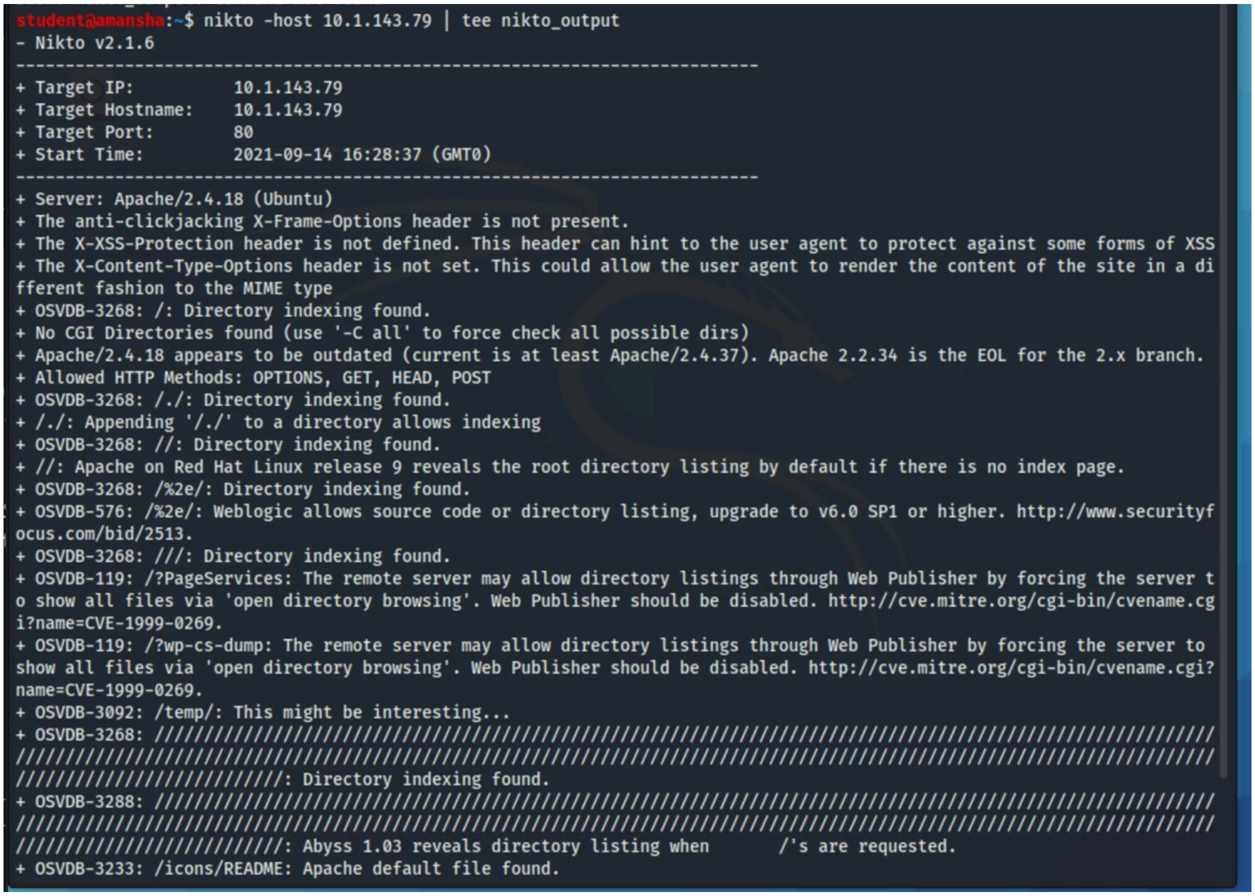
Could not find any vulnerabilities matching the requested criteria

Total number of vulnerabilities : **0** Page :

Amir Mansha
Lab 2-3 Vulnerabilities Scanning
CYSE 425
Fall 2021

Task 3: Use Nikto to scan for vulnerabilities

I used the Nikoto command to scan and find any vulnerabilities. Over all my output for this command was different then the example shown.



```
student@amansha:~$ nikto -host 10.1.143.79 | tee nikto_output
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          10.1.143.79
+ Target Hostname:    10.1.143.79
+ Target Port:        80
+ Start Time:         2021-09-14 16:28:37 (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 di
fferent 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.securityf
ocus.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 t
o show all files via 'open directory browsing'. Web Publisher should be disabled. http://cve.mitre.org/cgi-bin/cvename.cg
i?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.
```