Nmap Room

TryHackMe - Nmap room

#1 Deploy machine

Nmap Quiz
Reference:
on your Kali, man nmap
web ref:
https://nmap.org/book/man.html

#2 ‘syn scan’
on man, go to port scan techniqueue
-sS is for TCP SYN Scan

#3 ‘UDP Scan’
-sU is for UDP scan

#4 ‘Operating system detection’
-O

#5 ‘service version detction’
-sV

#6 ‘verbosity flag’
-v

#7 ‘very verbose’
-vv

#8 ‘xml output’
go to the ‘output’ section of man.html ref
-oX

#9 ‘Insane’ Level
-A

#10 set timing to the Max
-T5

#11 scan specific port
-p

#12 scan every port
-p-

#13 inlcude script to run.
--script

#14 run all script
-script vuln

#15 don't want to ping the host
-Pn

Nmap Scanning
#1 syn scan. What will the command be without the IP address
nmap -sS

#2 How many ports do we find open under 1000?
2

```
kali@gui-kali:~$ sudo nmap -sS 10.10.247.51
[sudo] password for kali:
Starting Nmap 7.80 ( https://nmap.org ) at 2020-08-06 02:23 UTC
Nmap scan report for 10.10.247.51
Host is up (0.094s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
```

#3 communication protocol
tcp

#4 perform service version detection scan, what is the version running on port 22?

```
kali@gui-kali:~$ sudo nmap -sV -sS 10.10.247.51
Starting Nmap 7.80 ( https://nmap.org ) at 2020-08-06 02:29 UTC
Nmap scan report for 10.10.247.51
Host is up (0.086s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.10 (Ubuntu Linux; protocol 2.0)
80/tcp open  http    Apache httpd 2.4.7 ((Ubuntu))
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

SSH version: 6.6.1p1

#5 perform an agressive scan, what flag isn't set under the results for port 80

```
kali@gui-kali:~$ sudo nmap -A sS 10.10.247.51
Starting Nmap 7.80 ( https://nmap.org ) at 2020-08-06 02:31 UTC
Failed to resolve "sS".
Nmap scan report for 10.10.247.51
Host is up (0.081s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.10 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 32:0c:cb:66:98:6b:7a:84:57:08:39:25:9f:a8:0e:bb (DSA)
|   2048 94:2a:fc:6a:21:79:7a:8d:93:74:bf:b4:78:dd:eb:55 (RSA)
|   256 63:f1:f7:d9:5f:c5:3f:71:03:6e:07:27:d8:73:6a:d2 (ECDSA)
|_  256 83:22:87:c4:ac:f5:81:12:24:b8:48:cc:a7:d3:b9:f3 (ED25519)
80/tcp open  http    Apache httpd 2.4.7 ((Ubuntu))
| http-cookie-flags:
|   /:
|     PHPSESSID:
|_      httponly flag not set
| http-robots.txt: 1 disallowed entry
```

httponly flag is not set.

#6 perform a script scan of vulnerabilites associated with this box, what denial of service attack is this box susceptible to?

```
kali@gui-kali:~$ sudo nmap --script vuln -sS 10.10.247.51
Starting Nmap 7.80 ( https://nmap.org ) at 2020-08-06 02:35 UTC
```

.....

.....

```
PORT   STATE SERVICE
22/tcp open  ssh
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
80/tcp open  http
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
| http-cookie-flags:
|   /:
|     PHPSESSID:
|       httponly flag not set
|   /login.php:
|     PHPSESSID:
|_      httponly flag not set
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
| http-enum:
|   /login.php: Possible admin folder
|   /robots.txt: Robots file
|   /config/: Potentially interesting directory w/ listing on 'apache/2.4.7 (ubuntu)'
|   /docs/: Potentially interesting directory w/ listing on 'apache/2.4.7 (ubuntu)'
|_  /external/: Potentially interesting directory w/ listing on 'apache/2.4.7 (ubuntu)'
| http-slowloris-check:
|   VULNERABLE:
|   Slowloris DOS attack
|     State: LIKELY VULNERABLE
|     IDs:  CVE:CVE-2007-6750
|       Slowloris tries to keep many connections to the target web server open and hold
|       them open as long as possible.  It accomplishes this by opening connections to
|       the target web server and sending a partial request. By doing so, it starves
|       the http server's resources causing Denial Of Service.
|
```

Vulnerable to “Slowloris DOS attack", http-slowloris-check