



Ethical hacking

Summer

Training

ASSIGNMENT

NAME – SANKET KUMAR SINGH

TRAINING ROLL – 219

MACHINE -
StickOS

TECHNOLOGY– VirtualBox

Introduction about stickOS:

StickOS® BASIC is an entirely MCU-resident patented interactive programming environment, which includes an easy-to-use editor, transparent line-by-line compiler, interactive debugger, performance profiler, and flash filesystem, all running entirely within the MCU and controlled thru an interactive command-line user interface

Additionally, when coupled with an optional Freescale MC13201 2.4GHz ZigFlea™ Wireless Transceiver, the MCU may be remotely controlled by another MCU, via a telnet/rlogin-like interface, eliminating the need for a direct connection to the host computer altogether. Also, BASIC programs may trivially remotely access variables on other MCUs, enabling the use of “remote pin variables” or other forms of inter-MCU communication

Introduction about VIRTUALBOX:



Oracle VM VirtualBox (formerly Sun VirtualBox, Sun xVM VirtualBox and InnoTek VirtualBox) is a hosted hypervisor for x86 virtualization developed by Oracle Corporation. VirtualBox was originally created by InnoTek Systemberatung GmbH, which was acquired by Sun Microsystems in 2008, which was in turn acquired by Oracle in 2010.

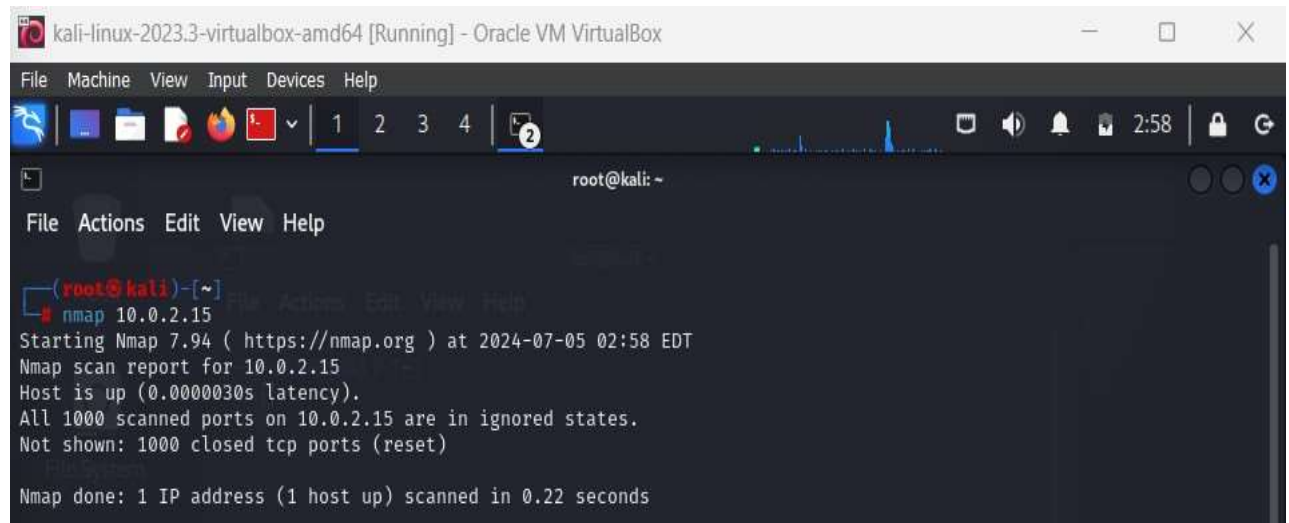
STEP 01:

At first we have to find IP address:



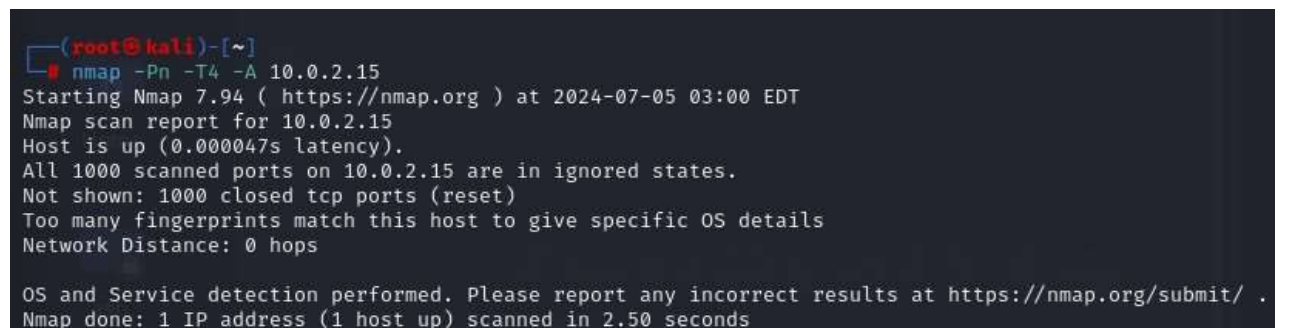
STEP 02:

After finding IP address, we have to scan port numbers



```
kali-linux-2023.3-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4 5
root@kali: ~
File Actions Edit View Help
(root@kali)~# nmap 10.0.2.15
Starting Nmap 7.94 ( https://nmap.org ) at 2024-07-05 02:58 EDT
Nmap scan report for 10.0.2.15
Host is up (0.0000030s latency).
All 1000 scanned ports on 10.0.2.15 are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Nmap done: 1 IP address (1 host up) scanned in 0.22 seconds
```

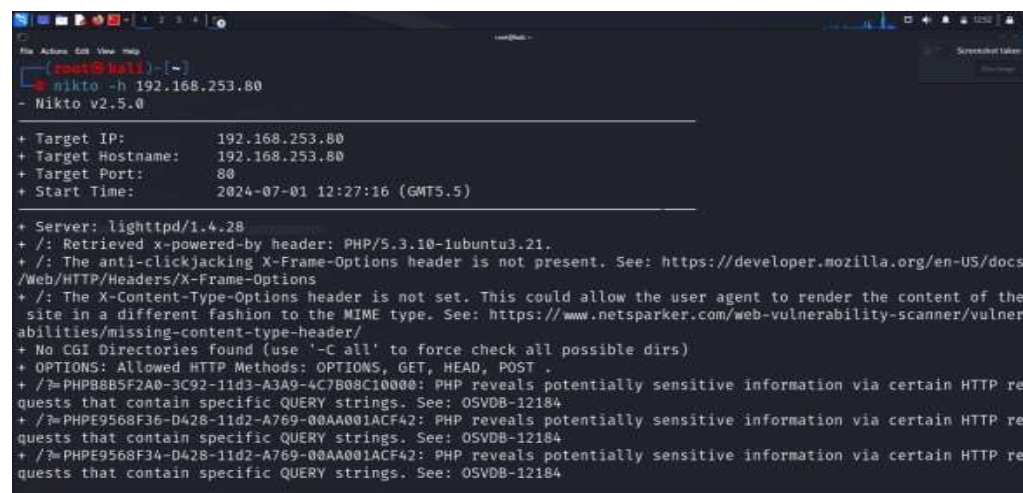


```
(root@kali)~# nmap -Pn -T4 -A 10.0.2.15
Starting Nmap 7.94 ( https://nmap.org ) at 2024-07-05 03:00 EDT
Nmap scan report for 10.0.2.15
Host is up (0.000047s latency).
All 1000 scanned ports on 10.0.2.15 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
Too many fingerprints match this host to give specific OS details
Network Distance: 0 hops

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 2.50 seconds
```

The results shows that 2 ports are open. One is SSH and the second one is HTTP means a website should be running.

Now i ran Nikto to check for any vulnerabilities and found nothing.

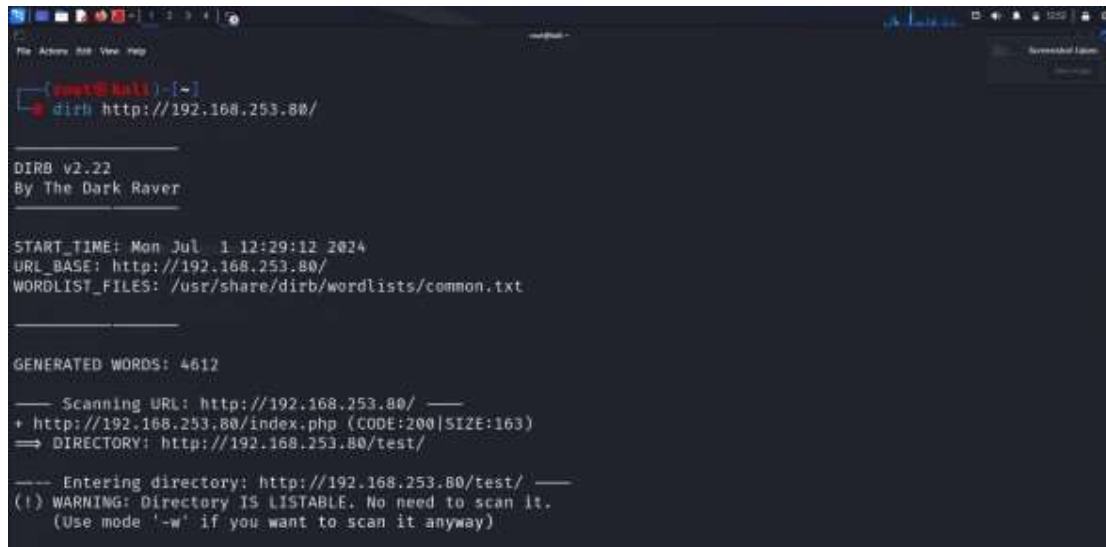


```
(root@kali)~# nikto -h 192.168.253.80
- Nikto v2.5.0

+ Target IP: 192.168.253.80
+ Target Hostname: 192.168.253.80
+ Target Port: 80
+ Start Time: 2024-07-01 12:27:16 (GMT5.5)

+ Server: lighttpd/1.4.28
+ /: Retrieved x-powered-by header: PHP/5.3.10-1ubuntu3.21.
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: 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. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ OPTIONS: Allowed HTTP Methods: OPTIONS, GET, HEAD, POST .
+ /?PHPBB85F2A0-3C92-11d3-A3A9-4C7B08C10000: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See: OSVDB-12184
+ /?PHP9568F36-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See: OSVDB-12184
+ /?PHP9568F34-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See: OSVDB-12184
```

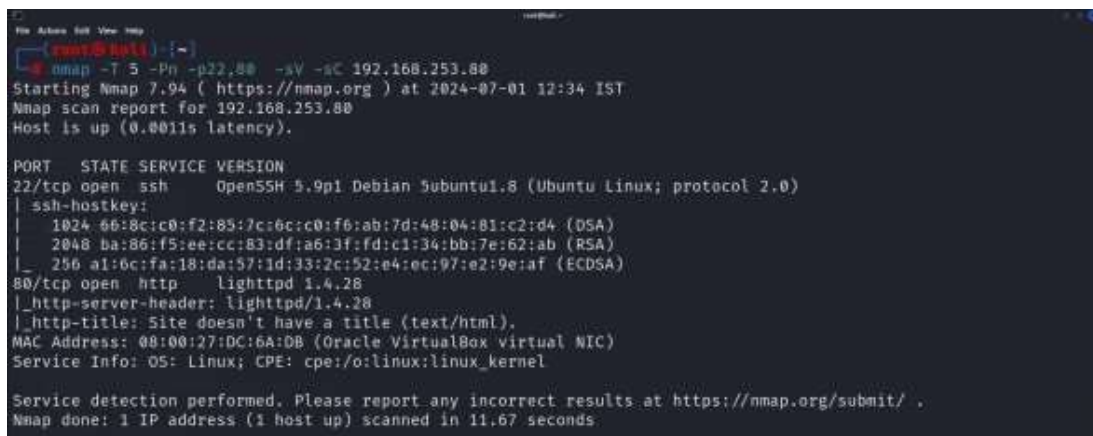
Let's try running dirb to look for hidden directories.



```
{root@kali} ~  
# dirb http://192.168.253.80/  
  
DIRB v2.22  
By The Dark Raver  
  
START_TIME: Mon Jul 1 12:29:12 2024  
URL_BASE: http://192.168.253.80/  
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt  
  
GENERATED WORDS: 4612  
  
--- Scanning URL: http://192.168.253.80/ ---  
+ http://192.168.253.80/index.php (CODE:200|SIZE:163)  
=> DIRECTORY: http://192.168.253.80/test/  
  
--- Entering directory: http://192.168.253.80/test/ ---  
(!) WARNING: Directory IS LISTABLE. No need to scan it.  
      (Use mode '-w' if you want to scan it anyway)
```

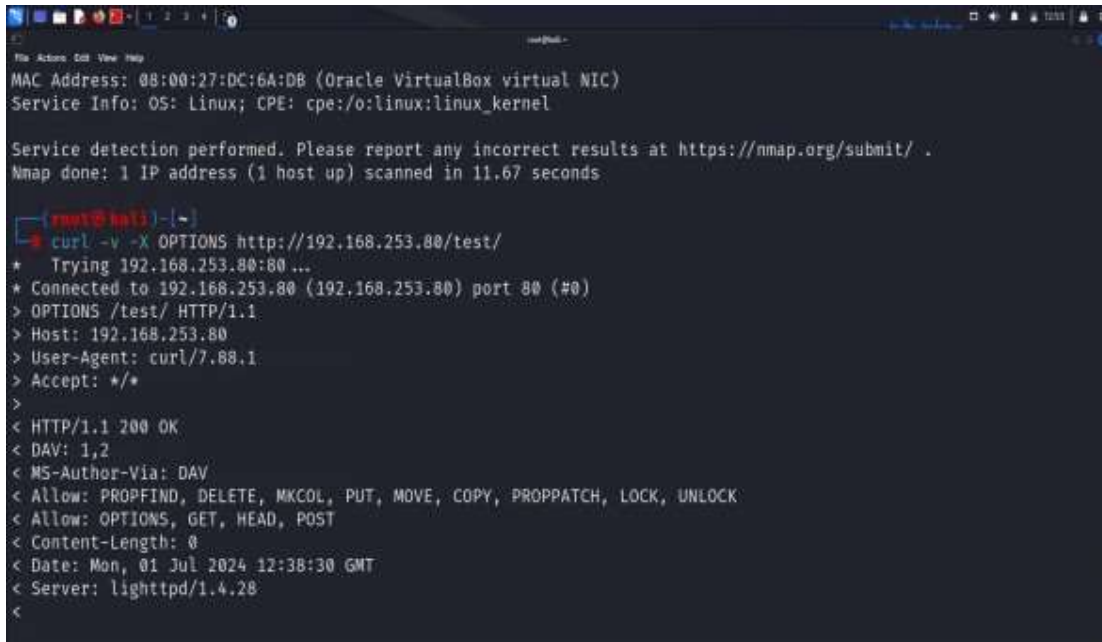
Yes we have found one “/test” directory

Let's see http method



```
{root@kali} ~  
# nmap -T 5 -Pn -p22,80 -sV -sC 192.168.253.80  
Starting Nmap 7.94 ( https://nmap.org ) at 2024-07-01 12:34 IST  
Nmap scan report for 192.168.253.80  
Host is up (0.0011s latency).  
  
PORT      STATE SERVICE VERSION  
22/tcp    open  ssh      OpenSSH 5.9p1 Debian 5ubuntu1.8 (Ubuntu Linux; protocol 2.0)  
|_ ssh-hostkey:  
|   1024 66:8c:c0:f2:85:7c:6c:c0:f6:ab:7d:48:04:81:c2:d4 (DSA)  
|   2048 ba:86:f5:ee:cc:83:df:a6:3f:fd:c1:34:bb:7e:62:ab (RSA)  
|_   256 a1:6c:fa:18:da:57:1d:33:2c:52:e4:ec:97:e2:9e:af (ECDSA)  
80/tcp    open  http      lighttpd 1.4.28  
|_ http-server-header: lighttpd/1.4.28  
|_ http-title: Site doesn't have a title (text/html).  
MAC Address: 08:00:27:DC:6A:DB (Oracle VirtualBox virtual NIC)  
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel  
  
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .  
Nmap done: 1 IP address (1 host up) scanned in 11.67 seconds
```

It's simply directory listing and nothing else. So far we have found nothing which can lead to the root access of SickOS .Here comes the CURL. Let's check whether we find any evil methods available



```
File Actions Edit View Help
MAC Address: 08:00:27:DC:6A:DB (Oracle VirtualBox virtual NIC)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.67 seconds

(root@kali) ~
$ curl -v -X OPTIONS http://192.168.253.80/test/
* Trying 192.168.253.80:80 ...
* Connected to 192.168.253.80 (192.168.253.80) port 80 (#0)
> OPTIONS /test/ HTTP/1.1
> Host: 192.168.253.80
> User-Agent: curl/7.88.1
> Accept: */*
>
< HTTP/1.1 200 OK
< DAV: 1,2
< MS-Author-Via: DAV
< Allow: PROPFIND, DELETE, MKCOL, PUT, MOVE, COPY, PROPPATCH, LOCK, UNLOCK
< Allow: OPTIONS, GET, HEAD, POST
< Content-Length: 0
< Date: Mon, 01 Jul 2024 12:38:30 GMT
< Server: lighttpd/1.4.28
<
```

CURL is a command-line tool used to transfer data to or from a server, using various protocols like HTTP, HTTPS, FTP, etc. Below is a brief guide to using cURL with different HTTP methods, along with examples of enumeration and escalation commands.