

Scanning & Enumeration

Installing Kioptrix Level 1 or Installing Vulnerable VM

Steps: perform attack on kioptrix machine.

>> Search on google: kioptrix level 1(www.vulnhub.com) is great resource

<https://www.vulnhub.com/entry/kioptrix-level-1-1,22/>

>> We can download and open virtual machine again,

>> Select the download "**fileKioptrix Level 1**" Run it

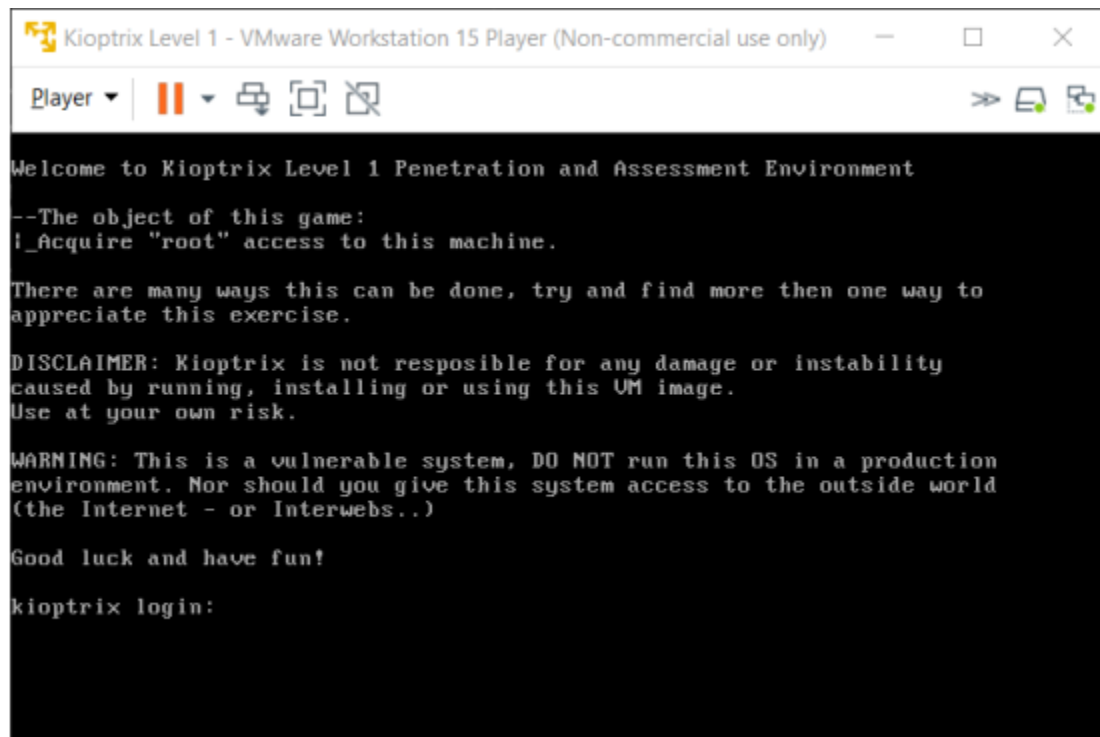
>> Select edit the virtual machine setting > go to network adapter setting, and choose NAT

>> select the RAM and increase the ram size,

Open FILEKIOPTIX LEVEL 1, select the file Virtual machine configuration file, and open with Notepad.

>> search Bridged and change to NAT and save the file.

>> Now open virtual machine and run the file



```

Kioptrix Level 1 - VMware Workstation 15 Player (Non-commercial use only)
Player | [Pause] [Full Screen] [Close]
Welcome to Kioptrix Level 1 Penetration and Assessment Environment
--The object of this game:
l_Acquire "root" access to this machine.

There are many ways this can be done, try and find more then one way to
appreciate this exercise.

DISCLAIMER: Kioptrix is not resposible for any damage or instability
caused by running, installing or using this VM image.
Use at your own risk.

WARNING: This is a vulnerable system, DO NOT run this OS in a production
environment. Nor should you give this system access to the outside world
(the Internet - or Interwebs..)

Good luck and have fun!

kioptrix login:
```

>> minimize this machine because we can attack this machine with our virtual machine.

We can also download the oscp to vulnhub boxes

>> Search on google **OSCP VULNHUB BOXES**

<https://www.abatchy.com/2017/02/oscp-like-vulnhub-vm>

Scanning with NMap 2019

1st method to find machines. (**netdiscover**)

Now our kioptrix is running and we are going to do active scanning,

>> Open kali terminal

>> We are going to open tool called "**net discover**"

>> Type "**ifconfig**"

>> copy ip address and type command

>> **netdiscover -r 127.0.0.0/24** (-r means Arp protocol)

>> **netdiscover -r 192.168.182.0/24** (this will open results, how many machines are running currently.)

>> We will going to attack on 192.168.182.129

```
Currently scanning: Finished! | Screen View: Unique Hosts
4 Captured ARP Req/Rep packets, from 4 hosts. Total size: 240
-----
IP           At MAC Address      Count  Len  MAC Vendor / Hostname
-----
192.168.182.1 00:50:56:c0:00:08    1     60  VMware, Inc.
192.168.182.2 00:50:56:e0:af:27    1     60  VMware, Inc.
192.168.182.129 00:0c:29:54:b6:56    1     60  VMware, Inc.
192.168.182.254 00:50:56:e5:c2:ed    1     60  VMware, Inc.
```

```
kali@kali: ~
Currently scanning: Finished! | Screen View: Unique Hosts
12 Captured ARP Req/Rep packets, from 3 hosts. Total size: 720
-----
IP           At MAC Address      Count  Len  MAC Vendor / Hostname
-----
192.168.182.2 00:50:56:e0:af:27    9    540  VMware, Inc.
192.168.182.129 00:0c:29:54:b6:56    2    120  VMware, Inc.
192.168.182.254 00:50:56:e8:39:23    1     60  VMware, Inc.

root@kali:/home/kali# netdiscover -r 127.0.0.0/24
```

>> We know the TCP handshake (we will going to find open port and make connection)

>>stelhthscanning -Ss (means it's undetectable, now days other scans are detectable)

>>SYN SYNACK ACK RST (this will just check connection like open port but it cannot connect or establish connection that means technically stealthy, We are not going to make connection but this is how we can find the port iss open)

>>**nmap -T4 -p- -A** (we want to connect the ip)

>> **-T4** (is the speed to connect ip, between T1 (slow) to T5 (fast), by default we use T4 not that fast and slow)

>> **-p-** (is the port, which the scan will find the open port during the entire scan) if we not use the port, this will by default scan 1000 common port. Total ports are 65534 port.

If we do scan like **-p 443, 80, 53** then it will use for specific port to scan.

>> **-A** means (all of them), I want you to tell me everything Version information, Operating system information.

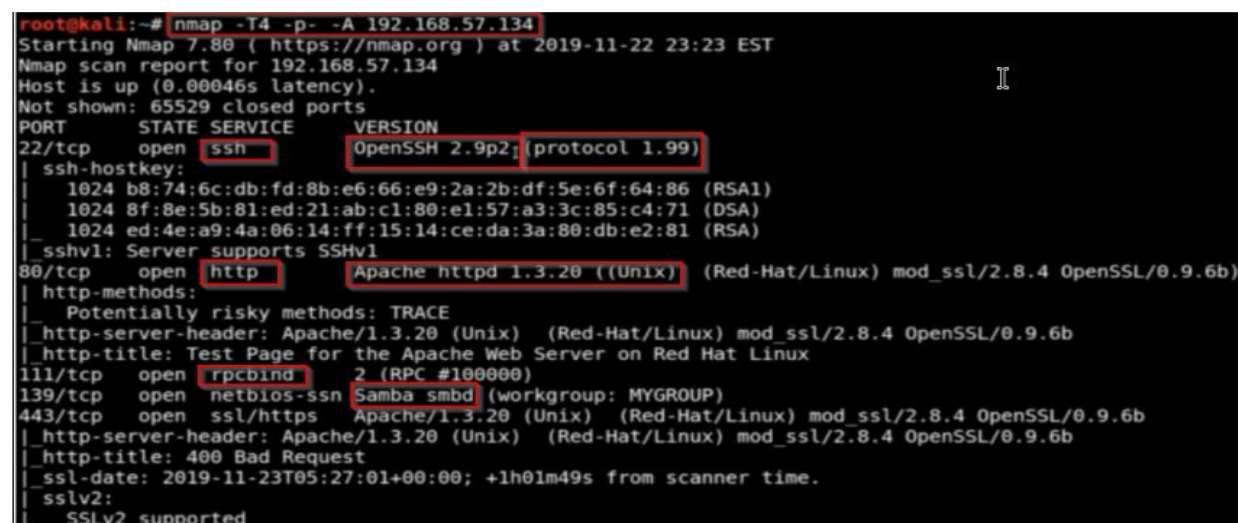
>> **-sU** means UDP scan it will scan all the port with UDP scan.

We have to check commands.

>> **nmap --help** & Man pages are good as well.



>> **nmap -T4 -p- -A 192.168.57.134** # every port running different services and version



```

root@kali:/home/kali# nmap -T4 -p- -A 192.168.182.129
Starting Nmap 7.80 ( https://nmap.org ) at 2020-03-24 07:07 EDT
Stats: 0:00:06 elapsed; 0 hosts completed (0 up), 1 undergoing ARP Ping Scan
Parallel DNS resolution of 1 host. Timing: About 0.00% done
Nmap scan report for 192.168.182.129
Host is up (0.00083s latency).
Not shown: 65529 closed ports
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 2.9p2 (protocol 1.99)
|_ ssh-hostkey:
|_ 1024 b8:74:6c:db:fd:8b:e6:66:e9:2a:2b:df:5e:6f:64:86 (RSA1)
|_ 1024 8f:8e:5b:81:ed:21:ab:c1:80:e1:57:a3:3c:85:c4:71 (DSA)
|_ 1024 ed:4e:a9:4a:06:14:ff:15:14:ce:da:3a:80:db:e2:81 (RSA)
|_ sshv1: Server supports SSHv1
80/tcp    open  http         Apache httpd 1.3.20 ((Unix) (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b)
|_ http-methods:
|_ Potentially risky methods: TRACE
|_ http-server-header: Apache/1.3.20 (Unix) (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
|_ http-title: Test Page for the Apache Web Server on Red Hat Linux
111/tcp   open  rpcbind      2 (RPC #100000)
139/tcp   open  netbios-ssn  Samba smbd (workgroup: XMYGROUP)
443/tcp   open  ssl/https    Apache/1.3.20 (Unix) (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
|_ http-server-header: Apache/1.3.20 (Unix) (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
|_ http-title: 400 Bad Request
|_ ssl-date: 2020-03-24T12:11:16+00:00; +1h01m51s from scanner time.
|_ sslv2:
|_ SSLv2 supported
|_ ciphers:

```

>> **nmap -sU -T4 -p 192.168.57.134**

```

root@kali:~# nmap -sU -T4 -p 192.168.57.134

```

That means we can also do scanning with -sU, but this with UDP scan.

2nd way to find machine (**arp**)

>> open the terminal

>> **arp-scan -l** & netdiscover both are the same. (Gives list of machine connected with our network)

netdiscover -r 192.168.86.0/24

nmap -T4 -p- -A 192.168.86.130

Open the kioptrix machine

Name: **john**

Password is: **TwoCows2**

After login we can also do the

>> ping 8.8.8.8

Enumerating HTTPHTTPS - Part 1

In this, we find the **OPEN PORTS** and **OUTDATED versions**,

We can see the port 22 Ssh,

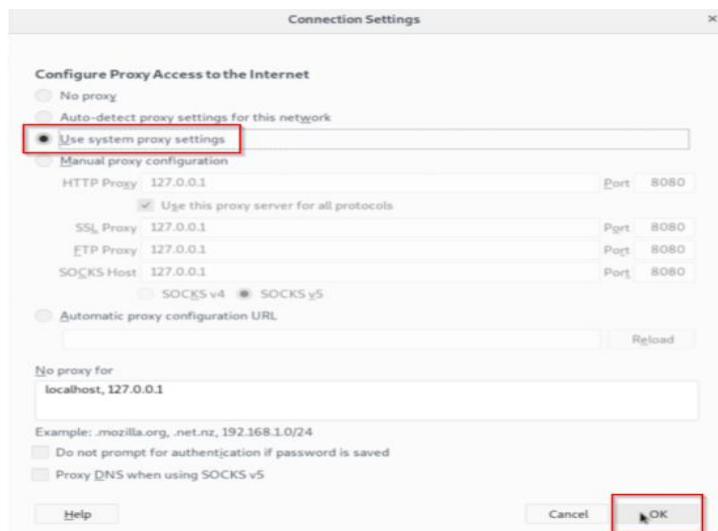
>> We can use brute force attack, default credential on root toor on it.

```
root@kali:/home/kali# nmap -T4 -p- -A 192.168.182.129
Starting Nmap 7.80 ( https://nmap.org ) at 2020-03-24 07:07 EDT
Stats: 0:00:06 elapsed; 0 hosts completed (0 up), 1 undergoing ARP Ping Scan
Parallel DNS resolution of 1 host. Timing: About 0.00% done
Nmap scan report for 192.168.182.129
Host is up (0.00083s latency).
Not shown: 65529 closed ports
PORT      STATE SERVICE        VERSION
22/tcp    open  ssh            OpenSSH 2.9p2 (protocol 1.99)
|_ ssh-hostkey:
|_ 1024 b8:74:6c:db:fd:8b:e6:66:e9:2a:2b:df:5e:6f:64:86 (RSA1)
|_ 1024 8f:8e:5b:81:ed:21:ab:c1:80:e1:57:a3:3c:85:c4:71 (DSA)
|_ 1024 ed:4e:a9:4a:06:14:ff:15:14:ce:da:3a:80:db:e2:81 (RSA)
|_ _sshv1: Server supports SSHv1
80/tcp    open  http           Apache httpd 1.3.20 ((Unix)) (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
|_ http-methods:
|_ _ Potentially risky methods: TRACE
|_ _http-server-header: Apache/1.3.20 (Unix) (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
|_ _http-title: Test Page for the Apache Web Server on Red Hat Linux
111/tcp   open  rpcbind        2 (RPC #100000)
139/tcp   open  netbios-ssn    Samba smbd (workgroup: XMYGROUP)
443/tcp   open  ssl/https      Apache/1.3.20 (Unix) (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
|_ _http-server-header: Apache/1.3.20 (Unix) (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
|_ _http-title: 400 Bad Request
|_ _ssl-date: 2020-03-24T12:11:16+00:00; +1h01m51s from scanner time.
|_ _sslv2:
|_ _ SSLv2 supported
```

If you see any website in browser just go through once.

>> go to Mozilla Firefox,

>> go to preferences, and follow this image

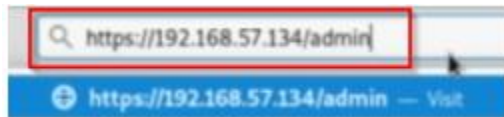


>> Copy ip address 192.168.57.134 and paste on browser **http://192.168.182.129** and **https://192.168.182.129** # this will open this page

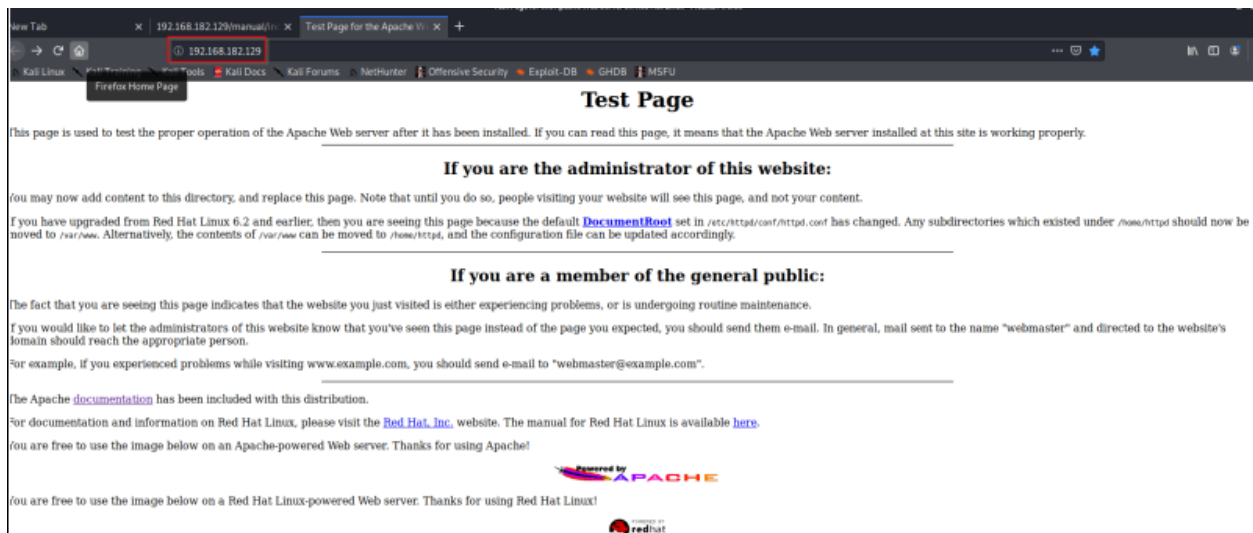
This page is default-automated page, and show architecture running behind scan (This page we cannot attack) but give client running little bit off hygiene.4

#what if client running default webpage: it will bring 2 question.

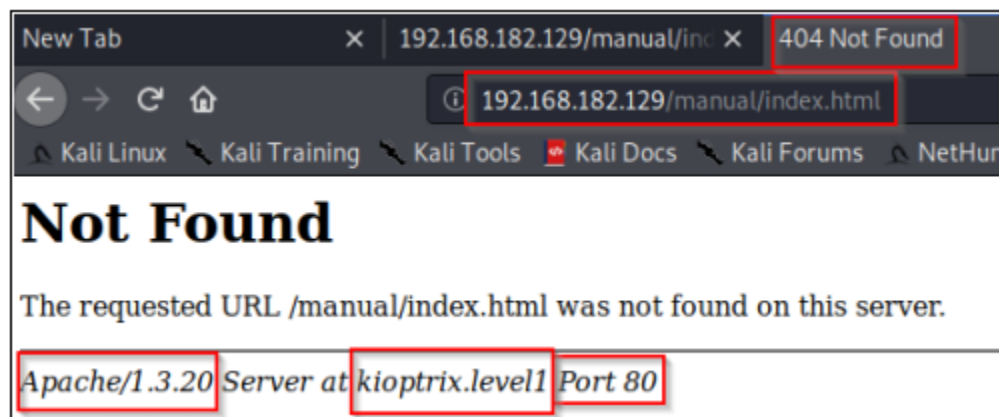
1- Are there other directory behind this? (See the image)



2- Left website hosting and open behind port 443 and put this default webpage out there.



3 - If we click on somewhere & see like below image is Information Disclosure



1st we can get information about

Server information = apache 1.3.20 server,

Host information = kioptrix_level 1

Port information = 443

We can make note and sent to client for information.

2nd **VULNERABILITY SCANNING** (inside we can use this)

Open kali terminal & type Nikto is scanner // practice against the CTF, Vulnhub, hackthebox do vulnerability scanning on website,

Issue is if website is running good security, it may auto block Nikto scans, (like good firewall)

-h means host (http://192.168.)

>> **nikto -h <http://192.168.182.129>**

```
root@kali: /home/kali# nikto -h http://192.168.182.129
- Nikto v2.1.6

----- Test Page -----
+ Target IP: 192.168.182.129
+ Target Hostname: 192.168.182.129
+ Target Port: 80
+ Start Time: 2020-03-23 06:27:29 (GMT-4)
+ Server: Apache/1.3.20 (Unix) (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
+ Server may leak inodes via ETags, header found with file /, inode: 34821, size: 2890, mtime: Wed Sep 5 23:12:46 2001
+ 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
+ Apache/1.3.20 appears to be outdated (current is at least Apache/2.4.37). Apache 2.2.34 is the EOL for the 2.x branch.
+ OpenSSL/0.9.6b appears to be outdated (current is at least 1.1.1). OpenSSL 1.0.0o and 0.9.8zc are also current.
+ mod_ssl/2.8.4 appears to be outdated (current is at least 2.8.31) (may depend on server version)
+ OSVDB-27487: Apache is vulnerable to XSS via the Expect header
+ OSVDB-838: Apache/1.3.20 - Apache 1.x up 1.2.34 are vulnerable to a remote DoS and possible code execution. CAN-2002-0392.
+ OSVDB-4552: Apache/1.3.20 - Apache 1.3 below 1.3.27 are vulnerable to a local buffer overflow which allows attackers to kill any process on the system. CAN-2002-0839.
+ OSVDB-2733: Apache/1.3.20 - Apache 1.3 below 1.3.29 are vulnerable to overflows in mod_rewrite and mod_cgi. CAN-2003-0542.
+ mod_ssl/2.8.4 - mod_ssl 2.8.7 and lower are vulnerable to a remote buffer overflow which may allow a remote shell. http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2002-0082, OSVDB-756.
+ Allowed HTTP Methods: GET, HEAD, OPTIONS, TRACE
+ OSVDB-877: HTTP TRACE method is active, suggesting the host is vulnerable to XST
+ OSVDB-682: /usage/: Webalizer may be installed. Versions lower than 2.01-09 vulnerable to Cross Site Scripting (XSS).
+ OSVDB-3268: /manual/: Directory indexing found.
+ OSVDB-3092: /manual/: Web server manual found.
+ OSVDB-3268: /icons/: Directory indexing found.
+ OSVDB-3233: /icons/README: Apache default file found.
+ OSVDB-3092: /test.php: This might be interesting...
+ 8724 requests: 0 error(s) and 20 item(s) reported on remote host
```

We have found lot of vulnerability here, like outdated

>> This is also we found

--->> mod_ssl/2.8.4 - mod_ssl 2.8.7 and lower are vulnerable to a remote buffer overflow, which may allow a remote shell. <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2002-0082>, OSVDB-756. <<---

Enumerating HTTPHTTPS - Part 2

There are 3 tools:

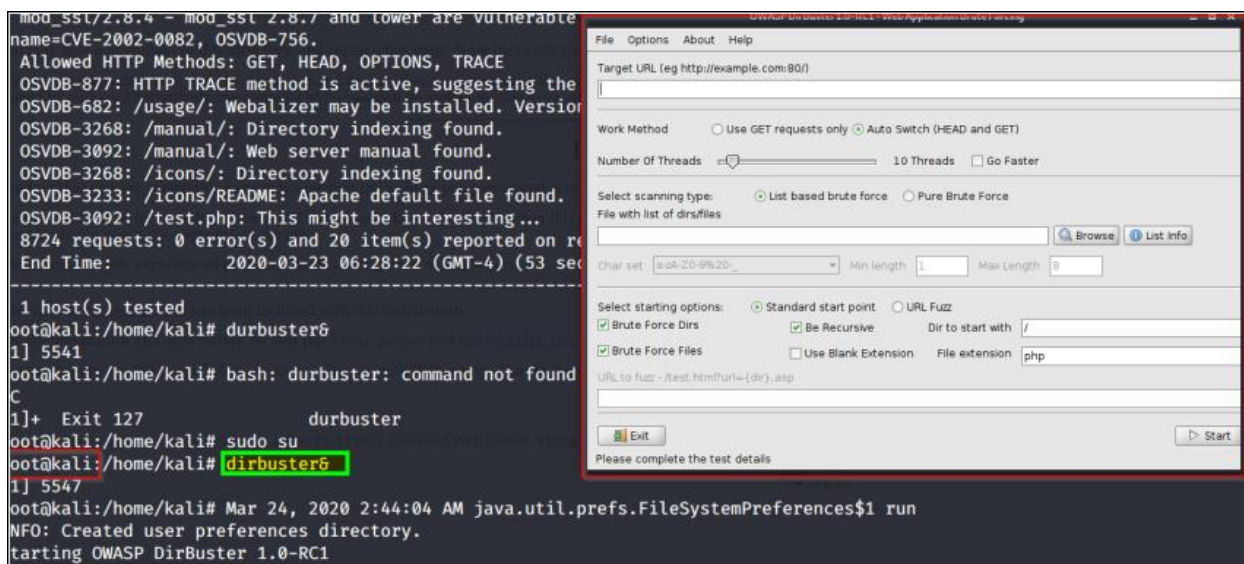
>> Dirbuster

>> irb

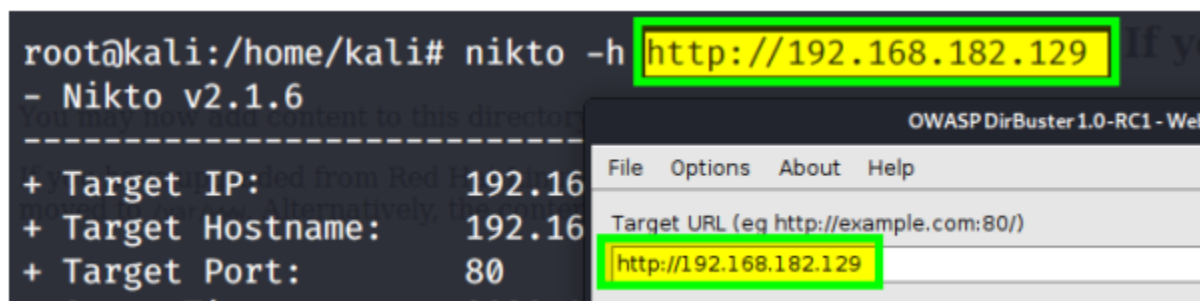
>> Gobuster

Open kali terminal run below command

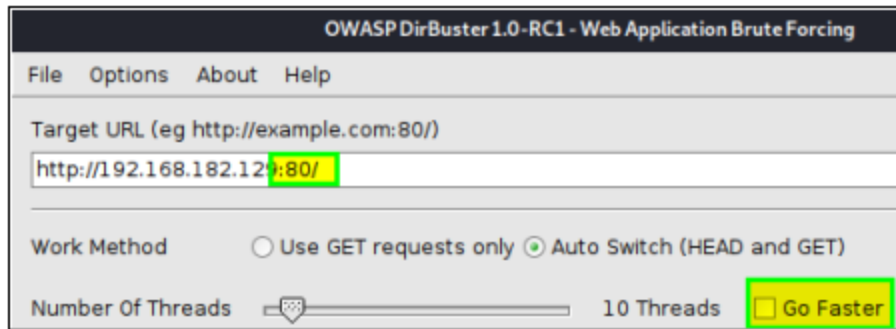
>> **dirbuster&** (this will open up tool Dirbuster)



>> copy the "nikto -h http://192.168.182.129" copy this ip address and paste in the dirbuster application

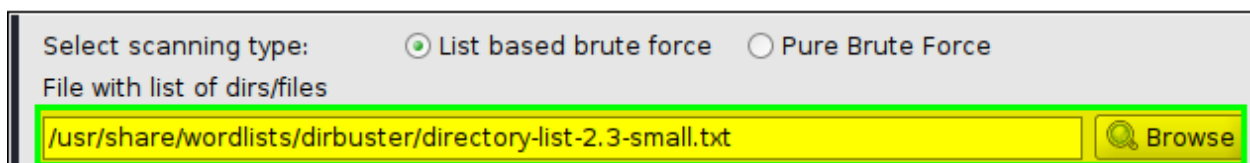


>> And add port: 80/ at the end select check box go faster



>> Browse to this directory /usr/share/wordlist/dirbuster/directory-list-2.3-small.txt

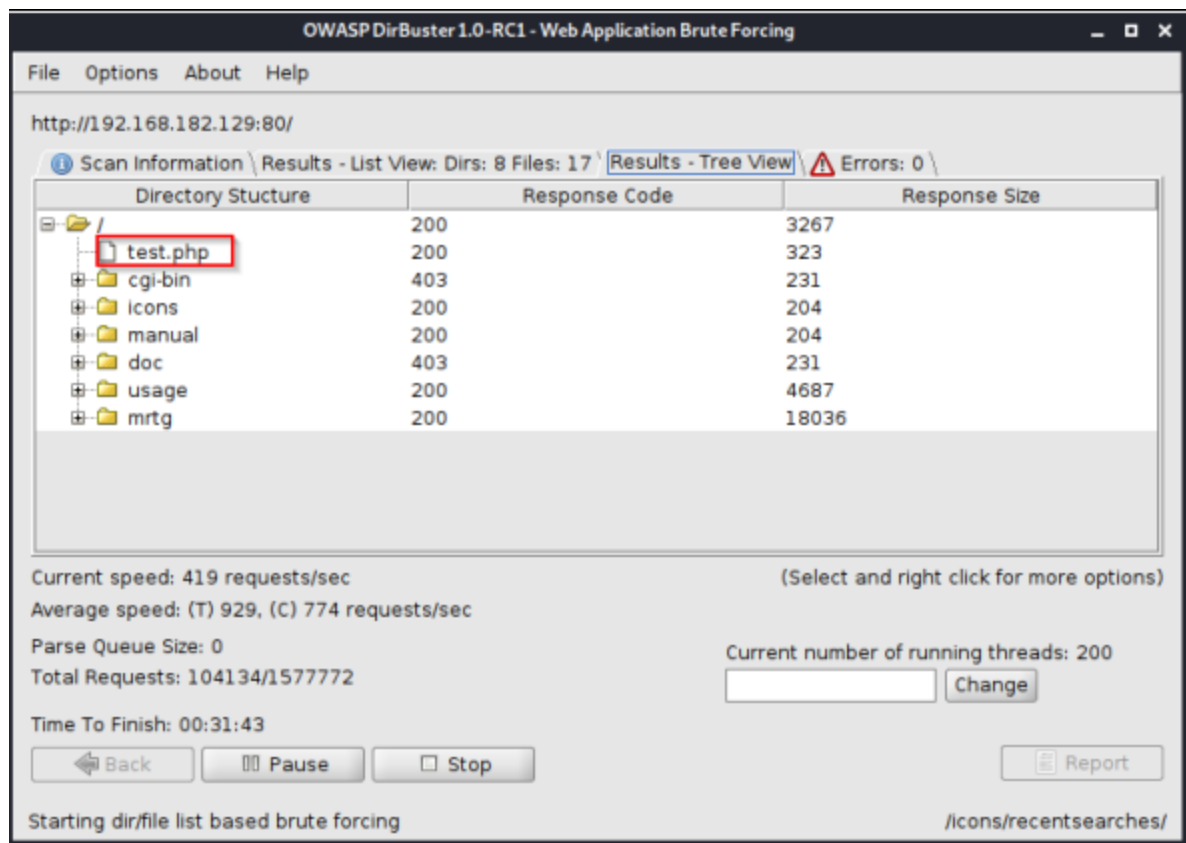
(Why we are selecting this because it's starting, if we not finding anything to small then we move up to medium.txt)



(We are going to web directory and using this wordlists because it has 100s and 1000s of well-known directories like admin, cgi-bin, etc.)

Click the - Run the scan,

>> We can also open the scan files and

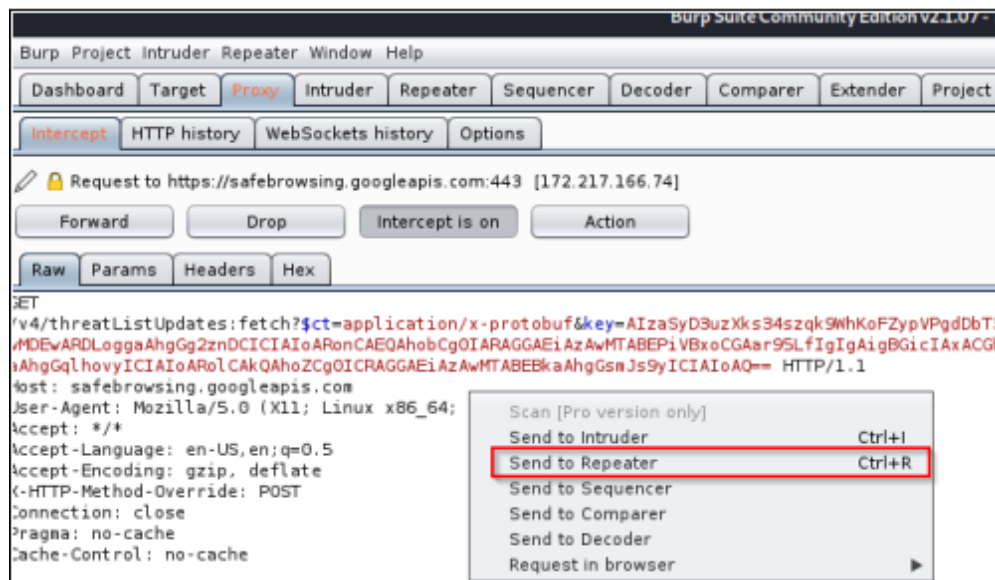


>> Now change the preference in manual proxy setting & open BurpSuite

>> Reload this page http://192.168.182.129/ and open BurpSuite

>> Do right click and sent this to Repeater

>> Go to repeater tab and Perform modifications with Request message like POST and click on sent button to check the request messages.

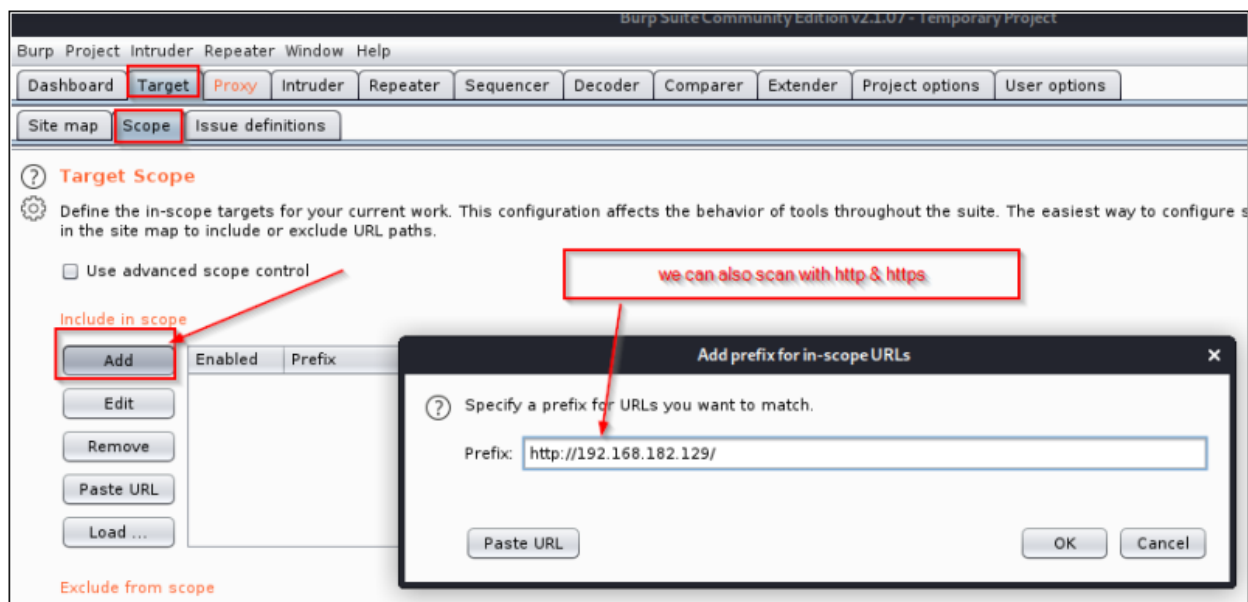


>> If we not miss anything then Open proxy tab and click forward. (This will be blank after click forward)

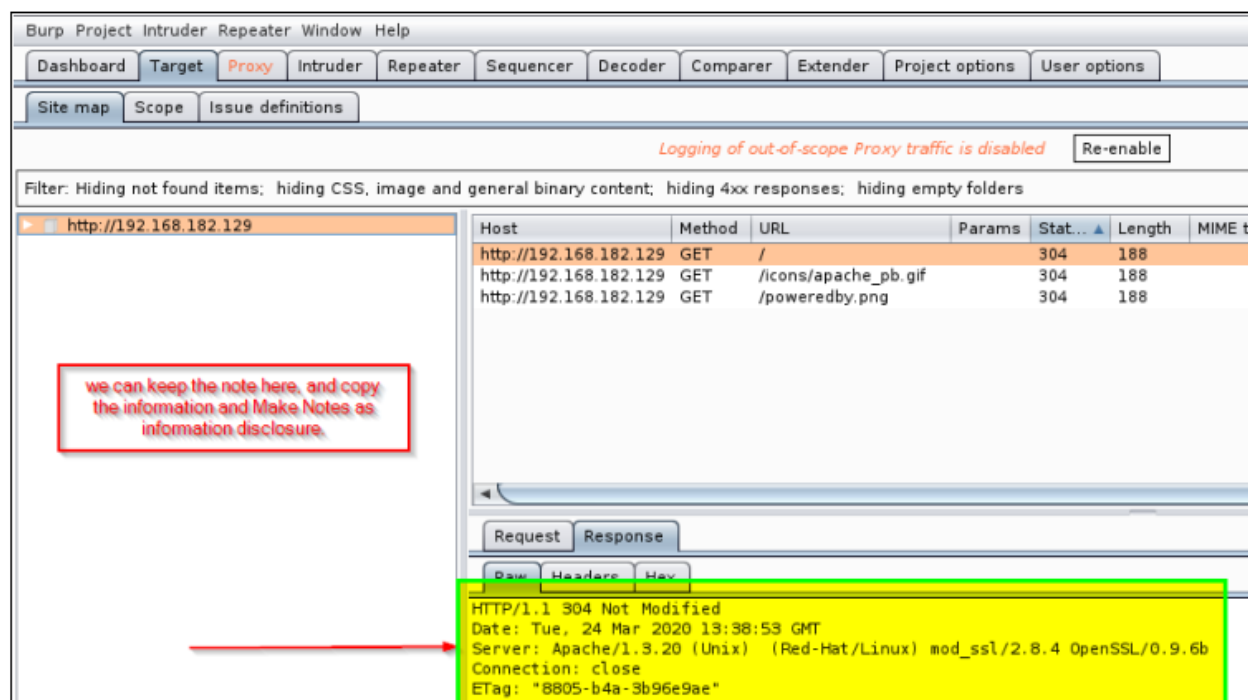
>> We can also copy the ip address **http://192.168.182.129/** we can see the target **http://192.168.182.129/**

>> We can also add here and scan with http, https, and ip address press ""YES"".

It does the limit to search item in scope.



>> Back to target tab and click response tab to check Information Disclosure: "we can keep the note here, and copy the information and Make Notes as information disclosure."



>> Compare it with Nikto scan; apache and open ssl information is same

```
root@kali:/home/kali# nikto -h http://192.168.182.129
- Nikto v2.1.6
-----
+ Target IP: 192.168.182.129
+ Target Hostname: 192.168.182.129
+ Target Port: 80
+ Start Time: 2020-03-24 07:17:14 (GMT-4)
-----
+ Server: Apache/1.3.20 (Unix) (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
+ Server may leak inodes via ETags, header found with file /, inode: 34821, size
+ The anti-clickjacking X-Frame-Options header is not present.
```

Now back to dirbuster& application which is running,

Concept is to check the active directory and response code with it

Directory and response code

Response code 200 normal

Response code 400 some error

Response code 404 page is not found

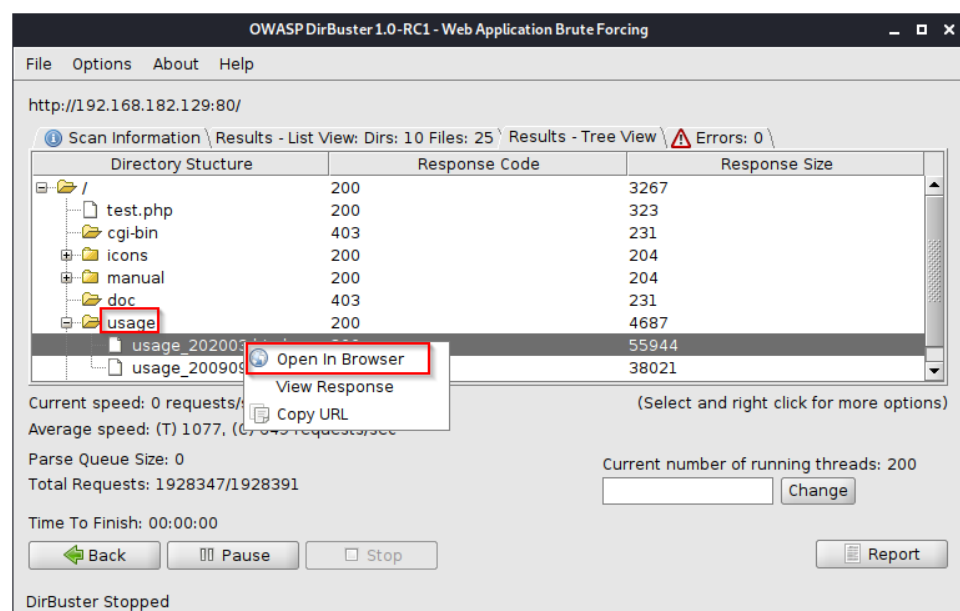
Response code 300 is redirect

Response code 500 server error

>> Open NON-IMP files: cgi-bin, icons, manual, doc,

>> Open IMP files: usage and open this files in browser. (This page will no load until intercept will turn off)

>> Turn off intercept an and page will load automatically.



>> Web page loaded after intercept turn off

The screenshot shows a web browser with the address bar at `192.168.182.129/usage/usage_202003.html`. The page title is "Usage Statistics for kioptrix.level1". A red box highlights the address bar. Another red box highlights a button that says "Make sure intercept turn off". A Burp Suite window is overlaid on the page, showing the "Intercept is off" button highlighted with a red box. The Burp Suite window also shows a "Monthly Statistics for March 2020" table.

Monthly Statistics for March 2020	
Total Hits	598998
Total Files	223
Total Pages	300617
Total Visits	45
Total KBytes	3373
Total Unique Sites	1
Total Unique URLs	39
Total Unique Referrers	8

>> copy this highlighted item and add to notes.

The screenshot shows a web browser with the address bar at `192.168.182.129/usage/usage_202003.html`. The page title is "Usage Statistics for kioptrix.level1 - March 2020". A red box highlights the address bar. Another red box highlights a text box that says "Make copy this URL and Webalizer version 2.01 as note". The page also shows a "Top 1 of 1 Total Count" table.

#	Hits	Files	KBytes
1	598998	223	3373

Generated by **Webalizer Version 2.01**

>> opening the dirbuster will help to get directory and check every directory finds important information about the scan reports.

>> Metasploit console run:

Open terminal and type command

```
>> msfconsole
```

```
#this will run Metasploit framework in terminal
```

other tools like msfvenom use later.

[illegible]

>> msfconsole (Metasploit) does lot many thing for us

- 1st exploits
- 2nd Auxiliary means scanning and enumerations (port scanning, information gathering)
- 3rd post (if we had shell in machine we can do something in post)
- 4th payloads it's used in tool called msfvenom used to create own shell

open terminal and type below command

```
>>search smb
```

This will show list of modules with what service running on

Example: Module: auxiliary, Service: admin

```
msf5 > search smb
```

Matching Modules

#	Name	Disclosure Date	Rank	Check	Description
0	auxiliary/admin/mssql/mssql_enum_domain_accounts		normal	No	Microsoft SQL Server SUSER_
1	auxiliary/admin/mssql/mssql_enum_domain_accounts_sql		normal	No	Microsoft SQL Server SQLi S
2	auxiliary/admin/mssql/mssql_ntlm_stealer		normal	No	Microsoft SQL Server NTLM S
3	auxiliary/admin/mssql/mssql_ntlm_stealer_sql		normal	No	Microsoft SQL Server SQLi N
4	auxiliary/admin/oracle/ora_ntlm_stealer	2009-04-07	normal	No	Oracle SMB Relay Code Execu
5	auxiliary/admin/smb/check_dir_file		normal	No	SMB Scanner Check File/Dire
6	auxiliary/admin/smb/delete_file		normal	No	SMB File Delete Utility
7	auxiliary/admin/smb/download_file		normal	No	SMB File Download Utility
8	auxiliary/admin/smb/list_directory		normal	No	SMB Directory Listing Utili
9	auxiliary/admin/smb/ms17_010_command	2017-03-14	normal	No	MS17-010 EternalRomance/Ete
10	auxiliary/admin/smb/psexec_command		normal	No	Microsoft Windows Authentic

>> We have to remember two things either number or either address

Example: number: 60

Example: auxiliary/scanner/smb/smb_version

>> command:

>> **use 60** (we can use the either one item which is preferable)

>> **use auxiliary/scanner/smb/smb_version** and paste enter. (This will load the module and we can access the file what ever available inside it.)

>> **info** (to check what are information available it)

>> **options** (to check the host which are available) later we LHOSTS (local host) is also available.

```
msf5 auxiliary(scanner/smb/smb_version) > options
```

Module options (auxiliary/scanner/smb/smb_version):

Name	Current Setting	Required	Description
RHOSTS		yes	The target address range or CIDR identifier
SMBDomain	.	no	The Windows domain to use for authentication
SMBPass		no	The password for the specified username
SMBUser		no	The username to authenticate as
THREADS	1	yes	The number of concurrent threads

Rhost is remote host. Is a victim we are attacking? Means we are import only 1 host,

Type command:

>> **set ROSTS 192.168.182.129**

>> **run**

```
msf5 auxiliary(scanner/smb/smb_version) > set RHOSTS 192.168.57.134
RHOSTS => 192.168.57.134
msf5 auxiliary(scanner/smb/smb_version) > run

[*] 192.168.57.134:139 - Host could not be identified: Unix (Samba 2.2.1a)
[*] 192.168.57.134:445 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

Rhost is we can run with ip and use run command to check samba, it will give Exact information about version. (Samba 2.2.1a) # We can make note and add to it

Open kali terminal and type command:

>> **smbclient** (ability to connect file share which is available out there. and access file anonymously. that gives important information which files available for us.)

>> **-l** (L) (that will list out all the file which is available for us.)

>> **smbclient -l \\192.168.182.129** and ENTER. (It will show list of sharenames we can check one by one. with ADMIN\$ and IPC\$.)

```
root@kali:~# smbclient -L \\192.168.57.134\\
Server does not support EXTENDED_SECURITY but 'client use spnego = yes' and 'client ntlmv2 auth = yes' is set
Anonymous login successful
Enter WORKGROUP\root's password: press Enter

  Sharename      Type            Comment
  -----
  IPC$           IPC             IPC Service (Samba Server)
  ADMIN$         IPC             IPC Service (Samba Server)
Reconnecting with SMB1 for workgroup listing.
Server does not support EXTENDED_SECURITY but 'client use spnego = yes' and 'client ntlmv2 auth = yes' is set
Anonymous login successful

  Server          Comment
  -----
  KIOPTRIX        Samba Server

  Workgroup       Master
  -----
  MYGROUP         KIOPTRIX
```

>> **smbclient \\192.168.182.129\\ADMIN\$** #this will not allow us to login.


```
root@kali:~# smbclient \\\\192.168.57.134\\ADMIN$
Server does not support EXTENDED_SECURITY but 'client use spnego = yes' and 'client ntlmv2 auth = yes' is set
Anonymous login successful
Enter WORKGROUP\\root's password: I
tree connect failed: NT STATUS_WRONG_PASSWORD
```

>> **smbclient \\\192.168.182.129\\IPC\$** (this will login us automatically and we check RUN commands like)

>> **help**

>> **ls**

```
root@kali:~# smbclient \\\\192.168.57.134\\IPC$
Server does not support EXTENDED_SECURITY but 'client use spnego = yes' and 'client ntlmv2 auth = yes' is set
Anonymous login successful
Enter WORKGROUP\\root's password:
Try "help" to get a list of possible commands.
smb: \> help
?          allinfo      altname      archive      backup
blocksize  cancel        case_sensitive cd            chmod
chown      close         del          deltreetree  dir
du         echo          exit         get          getfacl
geteas     hardlink     help        history      iosize
lcd        link         lock        lowercase    ls
l          mask         md          mget         mkdir
more       mput         newer       notify       open
posix      posix_encrypt posix_open   posix_mkdir  posix_rmdir
posix_unlink posix_whoami  print       prompt       put
pwd        q            queue       quit         readlink
rd         recurse     reget       rename       reput
rm         rmdir       showacl     setea        setmode
scopy      stat        symlink     tar          tarmode
timeout    translate   unlock      volume       vuid
wdel       logon       listconnect showconnect  tcon
tdis       tid         utimes      logoff       ..
!
smb: \> ls
```

Enumerating SSH

Open kali terminal and type the command.

>> **ssh 192.168.182.129** (this command to check specified IP address. but it say not found any matching key) (-c means cipher.)

```
root@kali:~# ssh 192.168.57.134
Unable to negotiate with 192.168.57.134 port 22: no matching key exchange method found. Their offer: diffie-hellman-group-exch
ange-sha1,diffie-hellman-group1-sha1
```

>> **ssh 192.168.182.129 -okexAlgorithms=+diffie-hellmen-group1-sha1** Note:
#this will come occasionally, it's not regular command. = after line is copied from above results.

(This is asking for cipher we can copy aes128-cbc)

```
root@kali:~# ssh 192.168.57.134 -oKexAlgorithms=+diffie-hellman-group1-sha1
Unable to negotiate with 192.168.57.134 port 22: no matching cipher found. Their offer: aes128-cbc,3des-cbc,blowfish-cbc,cast1
28-cbc,arcfour,aes192-cbc,aes256-cbc,rijndael128-cbc,rijndael192-cbc,rijndael256-cbc,rijndael-cbc@lysator.liu.se
```

>> **ssh 192.168.182.129 -okexAlgorithms=+diffie-hellmen-group1-sha1 -c aes128-cbc**
#this will provide the opportunity for connect.

```
root@kali:~# ssh 192.168.57.134 -oKexAlgorithms=+diffie-hellman-group1-sha1 -c aes128-cbc
The authenticity of host '192.168.57.134 (192.168.57.134)' can't be established.
RSA key fingerprint is SHA256:VDo/h/SG4A6H+WPH3LsQqw1jwjyseGYq9nLeRWPCY/A.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.57.134' (RSA) to the list of known hosts.
root@192.168.57.134's password:
```

(Why we use this?)

Sometimes banner is exposed and banner will say we're running SSH Version XYZ by this company or client, unfortunately there is no banner, we can see here

in between os SHA256: so that does not give any login information

```
root@kali:~# ssh 192.168.57.134 -oKexAlgorithms=+diffie-hellman-group1-sha1 -c aes128-cbc
The authenticity of host '192.168.57.134 (192.168.57.134)' can't be established.
RSA key fingerprint is SHA256:VDo/h/SG4A6H+WPH3LsQqw1jwjyseGYq9nLeRWPCY/A.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.57.134' (RSA) to the list of known hosts.
root@192.168.57.134's password:
```

Researching Potential Vulnerabilities

>> identifies and researching potential vulnerabilities

>>80/443 - 192.168.182.129 - 10:59pm

Default webpage - apache - PHP

Information Disclosure - 404 page

Information Disclosure - server headers disclose version information

>>80/tcp open http Apache httpd 1-3.20(Unix) (Red-Hat/linux) mod_ssl/2.8.4
OpenSSL/0.9.6b) #We can used to research.

>>mod_ssl/2.8.4 - mod_ssl 2.8.7 and lower are vulnerable to remote buffer overflow,
which may allow a remote shell.

<http://cve.mitr.org/cgi-bin/cvename.cgi?name=CVE-2002-0082.OSVDB-756>

>>SMB

UNIX (Samba 2.2.1a)

>>Weblizer Version 2.01 - http://192.168.182.129/usage/usage_202003.html

80, 139, 443, 445 are easiest to me. Are the easiest way to get hack.

SSH

OpenSSH

Search on google: - mod_ssl/ 2.8.4 exploit

OPEN GITHUB link: <https://github.com/heltonWernik/OpenLuck>

Open exploit-db.com

80/443- Potentially vulnerable to Open Luck

<https://www.exploit-db.com/exploits/764> #this might be not working it is because it is outdated

<https://github.com/heltonWernik/OpenLuck> (Working)

Now search google: - Apache httpd 1.3.20 exploit

(If we want to check something like critical open this link check the score)

https://www.cvedetails.com/vulnerability-list/vendor_id-45/product_id-66/version_id-5146/Apache-Http-Server-1.3.20.html

Open SSL tied with Mod_ssl

Open google and search: samba 2.2.1a exploit

Open Rapid7: makes the Metasploit

139 - Potentially vulnerable to trans2open

<https://www.rapid7.com/db/modules/exploit/linux/samba/trans2open> in that we can use Module Options.

The screenshot shows the Metasploit module page for 'Samba trans2open Overflow (Linux x86)'. The page has a blue header with the title. Below the header is a 'Back to Search' link. The main content area contains a table with the following data:

Disclosed	Created
04/07/2003	05/30/2018

Below the table is a 'Description' section. The text in the description is as follows:

This exploits the buffer overflow found in Samba versions 2.2.0 to 2.2.8. This particular module is capable of exploiting the flaw on **x86 Linux** systems that do not have the noexec stack option set. NOTE: Some older versions of RedHat do not seem to be vulnerable since they apparently **do not allow anonymous access to IPC.**

this means we can access with password IPC to samba. Moreover, support 86 systems

2nd way is <https://www.exploit-db.com/exploits/7>

<https://www.exploit-db.com/exploits/10>

Suppose if no internet and no research capabilities then use command in terminal:

>> **searchsploit samba 2** (more accurate you are in searching the more worst it is.)

We can search via kali terminal we can get the information regarding versions

```
root@kali:/home/kali# searchsploit samba 2
```

Exploit Title	Path (/usr/share/exploitdb/)
Microsoft Windows XP/2003 - Samba Share Resource Exhaustion (Denial of Service)	exploits/windows/dos/148.sh
Samba 1.9.19 - 'Password' Remote Buffer Overflow	exploits/linux/remote/20308.c
Samba 2.0.7 - SWAT Logfile Permissions	exploits/linux/local/20341.sh
Samba 2.0.7 - SWAT Logging Failure	exploits/unix/remote/20340.c
Samba 2.0.7 - SWAT Symlink (1)	exploits/linux/local/20338.c
Samba 2.0.7 - SWAT Symlink (2)	exploits/linux/local/20339.sh
Samba 2.0.x - Insecure TMP File Symbolic Link	exploits/linux/local/20776.c
Samba 2.0.x/2.2 - Arbitrary File Creation	exploits/unix/remote/20968.txt
Samba 2.2.0 < 2.2.8 (OSX) - 'trans_open' Remote Buffer Overflow (Metasploit)	exploits/osx/remote/9974.rb
Samba 2.2.2 < 2.2.6 - 'nttrans' Remote Buffer Overflow (Metasploit) (1)	exploits/linux/remote/16311.rb
Samba 2.2.8 (BSD x86) - 'trans_open' Remote Overflow (Metasploit)	exploits/bsd_x86/remote/16880.rb
Samba 2.2.8 (Linux Kernel 2.6 / Debian / Mandrake) - Share Privilege Escalation	exploits/linux/local/23674.txt
Samba 2.2.8 (Linux x86) - 'trans_open' Remote Overflow (Metasploit)	exploits/linux_x86/remote/16861.rb
Samba 2.2.8 (OSX/PPC) - 'trans_open' Remote Overflow (Metasploit)	exploits/osx_ppc/remote/16876.rb
Samba 2.2.8 (Solaris SPARC) - 'trans_open' Remote Overflow (Metasploit)	exploits/solaris_sparc/remote/16330.rb
Samba 2.2.8 - Brute Force Method Remote Command Execution	exploits/linux/remote/55.c
Samba 2.2.x - 'call_trans_open' Remote Buffer Overflow (1)	exploits/unix/remote/22468.c
Samba 2.2.x - 'call_trans_open' Remote Buffer Overflow (2)	exploits/unix/remote/22469.c
Samba 2.2.x - 'call_trans_open' Remote Buffer Overflow (3)	exploits/unix/remote/22470.c
Samba 2.2.x - 'call_trans_open' Remote Buffer Overflow (4)	exploits/unix/remote/22471.txt
Samba 2.2.x - 'nttrans' Remote Overflow (Metasploit)	exploits/linux/remote/9936.rb
Samba 2.2.x - CIFS/9000 Server A.01.x Packet Assembling Buffer Overflow	exploits/unix/remote/22356.c
Samba 2.2.x - Remote Buffer Overflow	exploits/linux/remote/7.pl
Samba 3.0.20 < 3.0.25rc3 - 'Username' map script' Command Execution (Metasploit)	exploits/unix/remote/16310.rb
Samba 3.0.21 < 3.0.24 - LSA trans names Heap Overflow (Metasploit)	exploits/linux/remote/9950.rb
Samba 3.0.24 (Linux) - 'lsa_io_trans_names' Heap Overflow (Metasploit)	exploits/linux/remote/16859.rb
Samba 3.0.24 (Solaris) - 'lsa_io_trans_names' Heap Overflow (Metasploit)	exploits/solaris/remote/16319.rb

>> **searchsploit mod ssl 2** #we can check vulnerabilities and check each one of item we seen here.

```
root@kali:/home/kali# searchsploit mod ssl 2
```

Exploit Title	Path (/usr/share/exploitdb/)
Apache mod_ssl 2.0.x - Remote Denial of Service	exploits/linux/dos/24590.txt
Apache mod_ssl 2.8.x - Off-by-One HTAccess Buffer Overflow	exploits/multiple/dos/21575.txt
Apache mod_ssl < 2.8.7 OpenSSL - 'OpenFuck.c' Remote Buffer Overflow	exploits/unix/remote/71671.c
Apache mod_ssl < 2.8.7 OpenSSL - 'OpenFuckV2.c' Remote Buffer Overflow (1)	exploits/unix/remote/764.c
Apache mod_ssl < 2.8.7 OpenSSL - 'OpenFuckV2.c' Remote Buffer Overflow (2)	exploits/unix/remote/47080.c
Apache mod_ssl OpenSSL < 0.9.6d / < 0.9.7-beta2 - 'openssl-too-open.c' SSL2 KEY_ARG Overflow	exploits/unix/remote/40347.txt
DomainMOD 4.11.01 - 'ssl-provider-name' Cross-Site Scripting	exploits/php/webapps/46372.txt
Microsoft Edge Chakra - 'InterpreterStackFrame::ProcessLinkFailedAsmJsModule' Incorrect Usage of 'PushP	exploits/windows/dos/42470.html
Microsoft Edge Chakra - 'InterpreterStackFrame::ProcessLinkFailedAsmJsModule' Incorrectly Re-parses	exploits/windows/dos/42469.html

dos : denial of service,

remote : remote code execution

we can check exploits and check Unix, check remote also Apache mod ssl