

Scanning & Enumeration

Installing Kroptrix Level 1 or Installing Vulnerable VM

Steps: perform attack on kroptrix machine.

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

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

>> We can download and open virtual machine again,

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

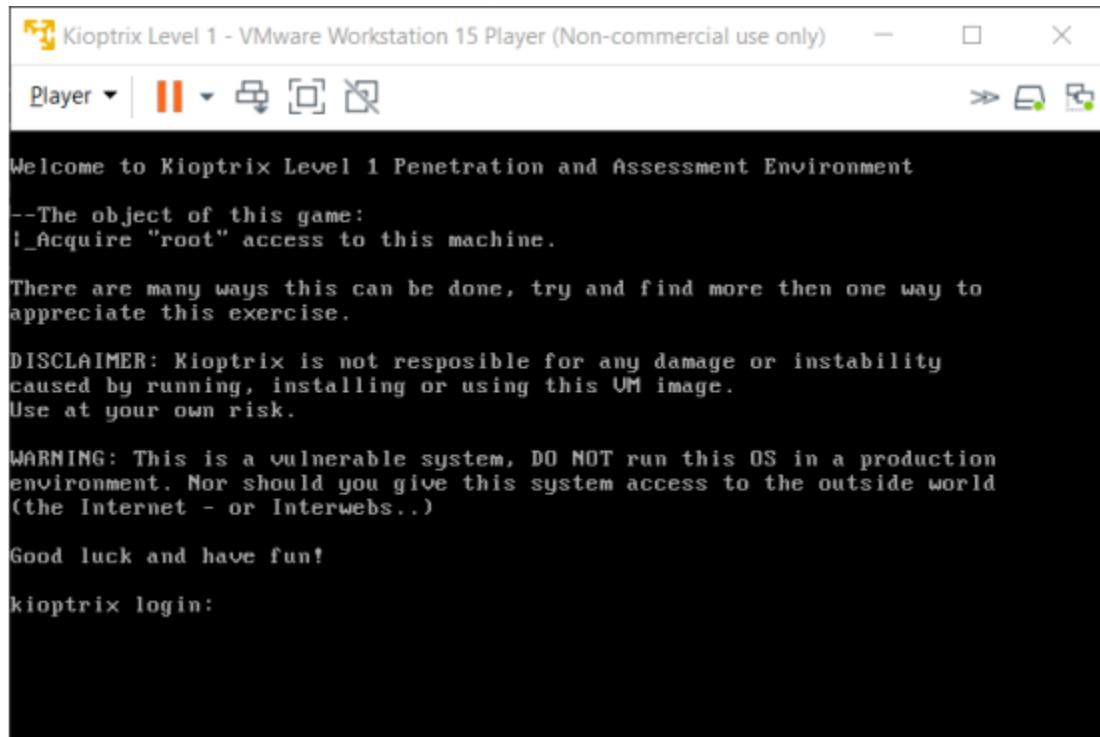
>> Select edit the virtual machine setting > go to network adapter setting, and choose NAT

>> select the RAM and increase the ram size,

Open FILEKROPTIX 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



>> 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-vms>

Scanning with NMap 2019

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

Now our kroptrix 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: ~ | 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 | are a member of the gene
```

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

```
root@kali:~# nmap --help
```

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

```
root@kali:~# nmap -T4 -p- -A 192.168.57.134
Starting Nmap 7.80 ( https://nmap.org ) at 2019-11-22 23:23 EST
Nmap scan report for 192.168.57.134
Host is up (0.00046s 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 (RSA)
|   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: MYGROUP)
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: 2019-11-23T05:27:01+00:00; +1h01m49s from scanner time.
|_sslv2:
|_ SSLv2 supported
```

```
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:
|     ESS
```

>> 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 k10ptrix 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 finds the **OPEN PORTS** and **OUTDATED versions**,

We can see the port 22 Ssh,

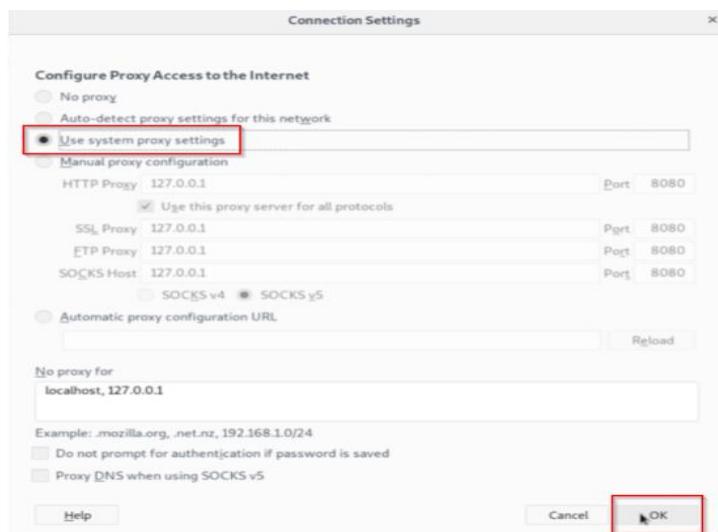
>> We can use brute force attack, default credential on root toor on it.

```
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:b8: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
SSLv2 supported
```

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

>> go to Mozilla Firefox,

>> go to preferences, and follow this image

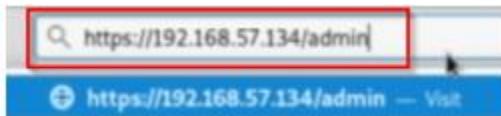


>> Copy ip address 192.168.57.134 and paste on browser **http://192.168.182.129** and
https://192.168.182.129 # this will open this page

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.

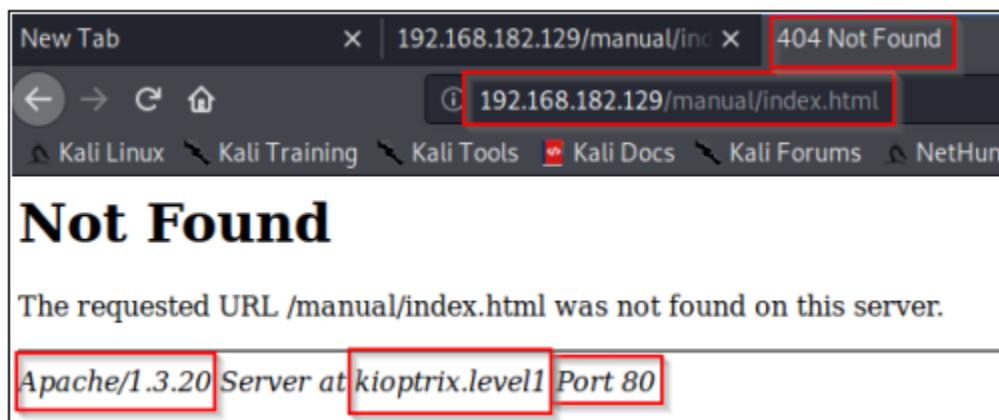
1- Are there other directory behind this? (See the image)



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

A screenshot of a Firefox browser window. The title bar says 'Test Page for the Apache Web Server'. The main content area displays the 'Test Page' for Apache, which includes sections for administrators and general public, and mentions Red Hat Linux documentation and a Red Hat logo.

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 = kioptix_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.>)

>> niklo -h <http://192.168.182.129>

```
root@kali:/home/kali# nikto -h http://192.168.182.129
- Nikto v2.1.6
[+] 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)  If you are the administrator of this website

+ 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-2002-0882, 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

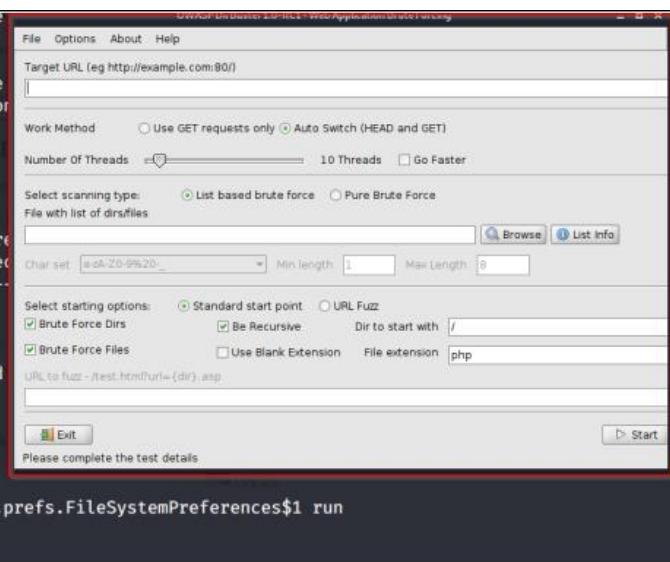
>> irb

>> Gobuster

Open kali terminal run below command

>> **dirbuster&**

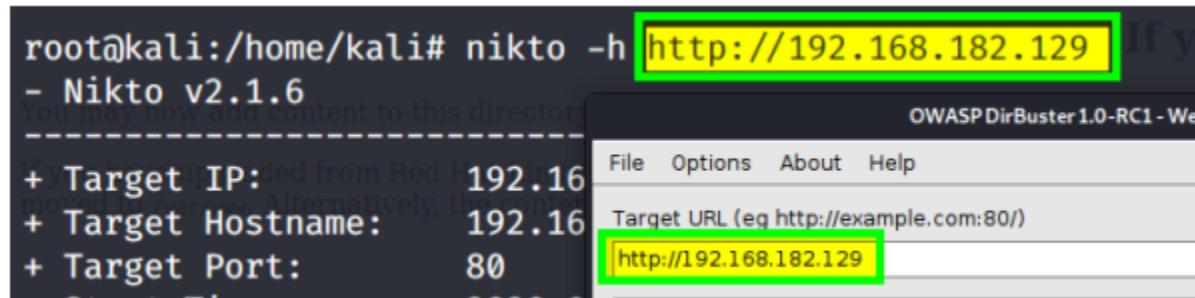
(this will open up tool Dirbuster)



```
mod_ssl/2.8.4 - mod_ssl 2.8.7 and lower are VULNERABLE
name=CVE-2002-0082, OSVDB-756.
Allowed HTTP Methods: GET, HEAD, OPTIONS, TRACE
OSVDB-877: HTTP TRACE method is active, suggesting the
OSVDB-682: /usage/: Webalizer may be installed. Version
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 re
End Time: 2020-03-23 06:28:22 (GMT-4) (53 sec)

1 host(s) tested
oot@kali:/home/kali# durbuster&
1] 5541
oot@kali:/home/kali# bash: durbuster: command not found
C
1]+ Exit 127 durbuster
oot@kali:/home/kali# sudo su
oot@kali:/home/kali# dirbuster&
1] 5547
oot@kali:/home/kali# Mar 24, 2020 2:44:04 AM java.util.prefs.FileSystemPreferences$1 run
NFO: Created user preferences directory.
Starting OWASP DirBuster 1.0-RC1
```

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



```
root@kali:/home/kali# nikto -h http://192.168.182.129
- Nikto v2.1.6
You may now add content to this directory
-----
+ Target IP: 192.168.182.129
+ Target Hostname: 192.168.182.129
+ Target Port: 80
```

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

OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing

File Options About Help

Target URL (eg http://example.com:80/)
http://192.168.182.129:80/

Work Method Use GET requests only Auto Switch (HEAD and GET)

Number Of Threads 10 Threads 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)

Select scanning type: List based brute force Pure Brute Force

File with list of dirs/files

(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

OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing

File Options About Help

http://192.168.182.129:80/

Scan Information | Results - List View: Dirs: 8 Files: 17 | Results - Tree View | Errors: 0 |

Directory Structure	Response Code	Response Size
/	200	3267
└ test.php	200	323
└ cgi-bin	403	231
└ icons	200	204
└ manual	200	204
└ doc	403	231
└ usage	200	4687
└ mrtg	200	18036

Current speed: 419 requests/sec (Select and right click for more options)

Average speed: (T) 929, (C) 774 requests/sec

Parse Queue Size: 0 Current number of running threads: 200

Total Requests: 104134/1577772

Time To Finish: 00:31:43

Starting dir/file list based brute forcing /icons/recentsearches/

>> 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.

Burp Suite Community Edition v2.1.0.7

Burp Project Intruder Repeater Window Help

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project

Intercept HTTP history WebSockets history Options

Request to https://safebrowsing.googleapis.com:443 [172.217.166.74]

Forward Drop Intercept is on Action

Raw Params Headers Hex

```
GET /v4/threatListUpdates:fetch?<key>=AIZaSyD3uzXks34szqkSWhKoFZypVPgdDbT3MDEwARDLoggaAhgGg2znDCICIAoARonCAEQAhobCgOIARAGGAEiAzAwMTABEPiVBxocGAar9SLfIgIgAigBGicIAxACGhAhhGqlhovyICIAoARo1CAKQAhOZCgOICRAGGAEiAzAwMTABEBkaAhgGsaJs9yICIAioAQ== HTTP/1.1
Host: safebrowsing.googleapis.com
User-Agent: Mozilla/5.0 (X11; Linux x86_64;
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
<HTTP-Method-Override: POST
Connection: close
Pragma: no-cache
Cache-Control: no-cache
```

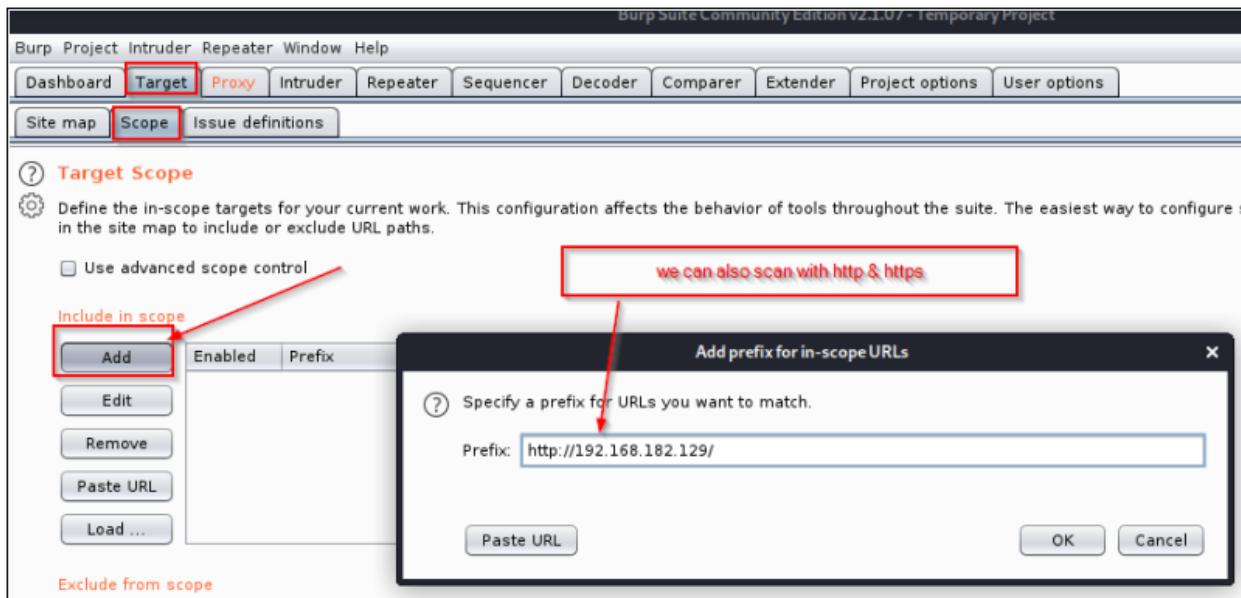
Scan [Pro version only]
 Send to Intruder Ctrl+I
Send to Repeater Ctrl+R
 Send to Sequencer
 Send to Comparer
 Send to Decoder
 Request in browser ▶

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

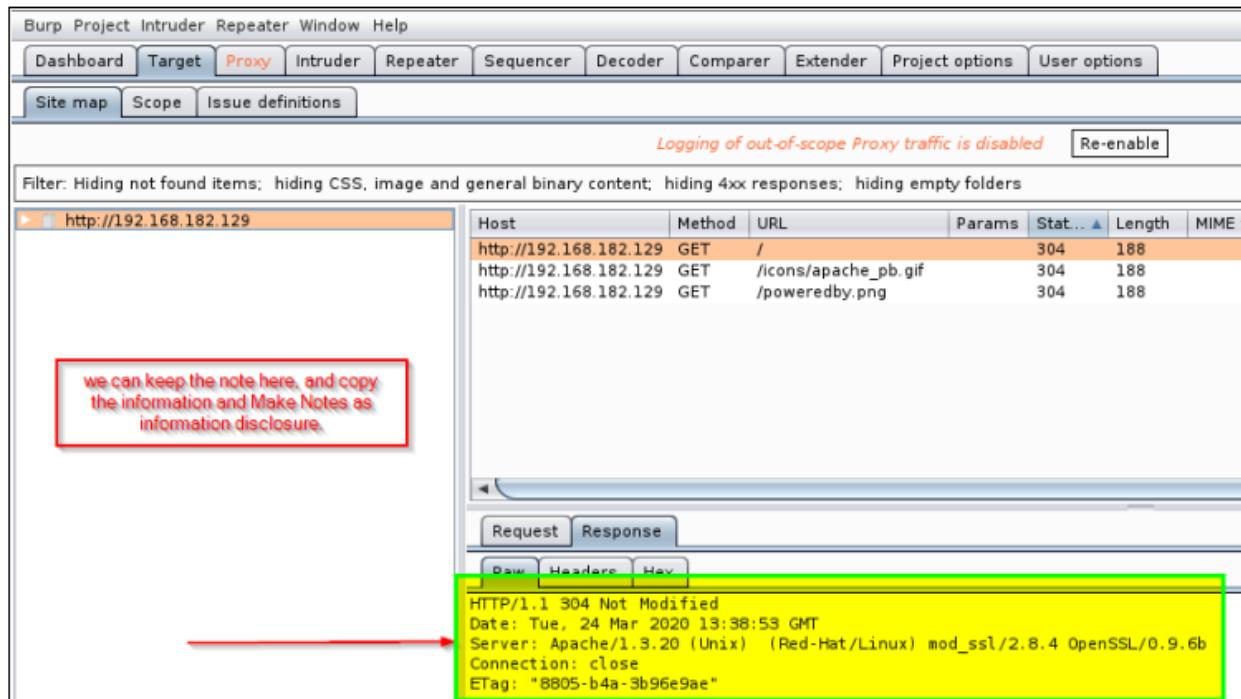
>> We can also copy the ip address **http://192.168.182.129/** we can see the target **http://192.168.182.129/**

>> 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 ans 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: 34821
+ 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

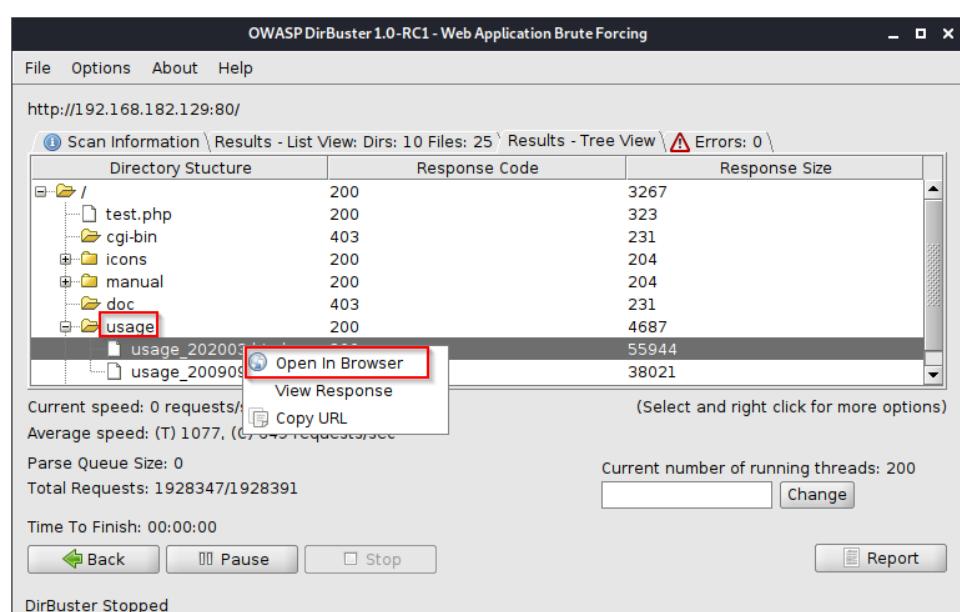
Response code 300 is redirect

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

Usage Statistics for kali.level1
Make sure intercept turn off

Summary Period: March 2020
Generated 24-Mar-2020 05:55 EST

Burp Suite Community Edition v2.1.07 - Temporary Project

Intercept is off

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.

192.168.182.129/usage/usage_202003.html

Make copy this URL and Webalizer version 2.01 as note

Top 1 of 1 Total Cou

#	Hits	Files	KBytes			
1	598998	100.00%	223	100.00%	3373	100.00%

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.

Enumerating SMB-139 IMP

>> Metasploit console run:

Open terminal and type command

```
>> msfconsole #this will run Metasploit framework in terminal  
other tools like msfvenom use later.
```

>> 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

```
kali㉿kali ~ └─╼ kali㉿kali ~ └─╼ nsf5 > search smb  
Matching Modules  
=====  
# Name  
- ---  
0 auxiliary/admin/mssql/mssql_enum_domain_accounts  
SNAME Windows Domain Account Enumeration  
1 auxiliary/admin/mssql/mssql_enum_domain_accounts_sqli  
JSER_SNAME Windows Domain Account Enumeration  
2 auxiliary/admin/mssql_ntlm_stealer  
tealer  
3 auxiliary/admin/mssql_ntlm_stealer_sqli  
TLM Stealer  
4 auxiliary/admin/oracle/ora_ntlm_stealer  
tion  
5 auxiliary/admin/smb/check_dir_file  
ctory Utility  
6 auxiliary/admin/smb/delete_file  
7 auxiliary/admin/smb/download_file  
ty  
8 auxiliary/admin/smb/list_directory  
9 auxiliary/admin/smb/ms17_010_command  
nalSynergy/EternalChampion SMB Remote Windows Command Execution  
10 auxiliary/admin/smb/psexec_command  
ated Administration Utility  
  
This will show list of modules with what service name  
Example Module: netcat, Metasploit, ...  
  
Test Page  
http://127.0.0.1:8080/test.html  
If you are the administrator  
-----  
Disclosure Date Rank Check Description  
-----  
normal No Microsoft SQL Server SUSER_S  
normal No Microsoft SQL Server SQLi S  
normal No Microsoft SQL Server NTLM S  
normal No Microsoft SQL Server SQLi N  
2009-04-07 normal No Oracle SMB Relay Code Execu  
normal No SMB Scanner Check File/Dire  
normal No SMB File Delete Utility  
normal No SMB File Download Utility  
normal No SMB Directory Listing Utili  
2017-03-14 normal No MS17-010 EternalRomance/Ete
```

>> 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 RHOSTS 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  
?  
blocksize  
chown  
du  
geteas  
lcd  
l  
more  
posix  
posix_unlink  
pwd  
rd  
rm  
scopy  
timeout  
wdel  
tdis  
!  
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 a web page for the "Samba trans2open Overflow (Linux x86)" exploit. At the top, there's a dark blue header with the title in white. Below the header, there's a light gray navigation bar with a "Back to Search" button and a left arrow icon. The main content area has a white background. It features a section titled "Samba trans2open Overflow (Linux x86)". Underneath this, there's a table with two columns: "Disclosed" and "Created". The "Disclosed" column contains the date "04/07/2003", and the "Created" column contains the date "05/30/2018". Below the table, there's a "Description" section. The text in this section describes the exploit as targeting Samba versions 2.2.0 to 2.2.8, noting that it requires systems without the noexec stack option set. It also mentions that some older RedHat versions are not vulnerable due to IPC access restrictions. A red rectangular box highlights the word "x86" in the title and the word "noexec" in the description text.

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

Description

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

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 3.0.7 - 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 2.0.0 < 2.1.8 (OSX) - transOpen Overflow (Metasploit)	exploits/osx/remote/9924.rb
Samba 2.2.2 < 2.1.6 - 'nttrans' Remote Buffer Overflow (Metasploit) (1)	exploits/linux/remote/16321.rb
Samba 2.2.8 (BSD x86) - 'transOpen' Remote Overflow (Metasploit)	exploitsbsd_x86/remote/16880.rb
Samba 2.1.8 (Linux Kernel 2.6 / Debian / Mandrake) - Share Privilege Escalation	exploits/linux/local/23674.txt
Samba 2.1.8 (Linux x86) - 'transOpen' Remote Overflow (Metasploit)	exploits/linux_x86/remote/16861.rb
Samba 2.1.8 (OSX/PPC) - 'transOpen' Remote Overflow (Metasploit)	exploits/osx_ppc/remote/16876.rb
Samba 2.2.8 (Solaris SPARC) - 'transOpen' 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_transOpen' Remote Buffer Overflow (1)	exploits/unix/remote/22468.c
Samba 2.2.x - 'call_transOpen' Remote Buffer Overflow (2)	exploits/unix/remote/22469.c
Samba 2.2.x - 'call_transOpen' Remote Buffer Overflow (3)	exploits/unix/remote/22470.c
Samba 2.2.x - 'call_transOpen' 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) - 'lsas_io_trans_names' Heap Overflow (Metasploit)	exploits/linux/remote/16859.rb
Samba 3.0.24 (Solaris) - 'lsas_io_trans_names' Heap Overflow (Metasploit)	exploits/solaris/remote/16329.rb

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

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/21671.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