Scanning and Enumeration

Installing Kioptrix

Note: I ran PimpMyKali with the `N - New VM` option on my Kali machine. Enabled the root user and logged in as root.

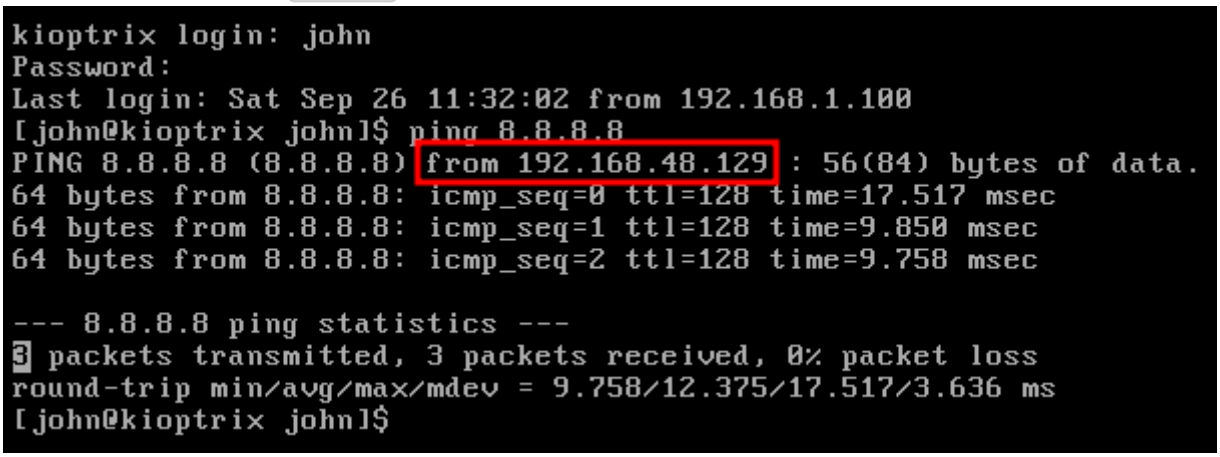
Kioptrix Download from TCM-Sec
The original was from Vulnhub but it was last updated in 2010, so the one on TCM-Sec website is updated a little to help.

I imported the file with VMWare as that is my preferred software.
Modify the settings of Kioptrix to have the Network Adapter on NAT.

Scanning with NMap

Ping

First, we need to find the IP address of the Kioptrix machine. We can "cheat" and log in with the username `john` and the password `TwoCows2`, then find the IP with the command `ping 8.8.8.8` and grab the IP from the "`from X`"



Arp Scan

You can use `arp-scan -l` to also find the IP.

```
┌──(root㉿kali)-[~]
└─# arp-scan -l
Interface: eth0, type: EN10MB, MAC: 00:0c:29:a5:61:5d, IPv4: 192.168.48.128
Starting arp-scan 1.10.0 with 256 hosts (https://github.com/royhills/arp-scan)
192.168.48.1    00:50:56:c0:00:08       VMware, Inc.
192.168.48.2    00:50:56:f8:5e:02       VMware, Inc.
192.168.48.129  00:0c:29:28:eb:5a       VMware, Inc.
192.168.48.254  00:50:56:ee:0f:d6       VMware, Inc.

4 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.10.0: 256 hosts scanned in 2.036 seconds (125.74 hosts/sec). 4 responded

┌──(root㉿kali)-[~]
└─#
```

Net Discover

You can use `netdiscover -r (subnet range)` to also find the IP. Eg. `netdiscover -r 192.168.49.0/24`
Running `ifconfig` or `ip a` to find your machines IP to find the subnet you're on and grabbing the first 2 octets.

```
 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
 -----------------------------------------------------------------------------
 192.168.48.1    00:50:56:c0:00:08      1      60  VMware, Inc.
 192.168.48.2    00:50:56:f8:5e:02      1      60  VMware, Inc.
 192.168.48.129  00:0c:29:28:eb:5a      1      60  VMware, Inc.
 192.168.48.254  00:50:56:ee:0f:d6      1      60  VMware, Inc.
```

My Kioptrix machine is: 192.168.48.129

Scanning with NMap

`-sS` - Steal scanning, not so stealthy anymore. It send a SYN packet, once we get the SYNACK, they send a RST(reset) packet dropping the connection.
`nmap -T4 -p- -A 192.168.48.129` - This changes the speed of nmap with `-T4`, the defult of the timing argument is 3, we're going to 4, `-p-` will scan all ports, `-A` scans for OS, version number of services running, script scanning, AND traceroute.
More on understanding NMap here.

WIll be using `-sS` and `-sU` for a majority of this course.

Heath likes to use `-sU` to scan for UDP and removes the `-A` and does `-p`. UDP scans take a long time so the `-p` will scan the top 1000 ports.

Scan Results:

```
nmap -T4 -p- -A 192.168.48.129
Starting Nmap 7.94 ( https://nmap.org ) at 2023-08-31 05:36 EDT
Nmap scan report for 192.168.48.129
Host is up (0.00055s latency).
Not shown: 65529 closed tcp ports (reset)
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-title: Test Page for the Apache Web Server on Red Hat Linux
|_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
|_ssl-date: 2023-08-31T09:37:03+00:00; +4s from scanner time.
| sslv2:
|   SSLv2 supported
|   ciphers:
|     SSL2_RC4_64_WITH_MD5
|     SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|     SSL2_DES_64_CBC_WITH_MD5
|     SSL2_DES_192_EDE3_CBC_WITH_MD5
|     SSL2_RC4_128_EXPORT40_WITH_MD5
|     SSL2_RC4_128_WITH_MD5
|_    SSL2_RC2_128_CBC_WITH_MD5
|_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/stateOrPr
ovinceName=SomeState/countryName=--
| Not valid before: 2009-09-26T09:32:06
|_Not valid after:  2010-09-26T09:32:06
32768/tcp open  status      1 (RPC #100024)
MAC Address: 00:0C:29:28:EB:5A (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:
|_nbstat: NetBIOS name: KIOPTRIX, NetBIOS user: <unknown>, NetBIOS MAC:
<unknown> (unknown)
|_smb2-time: Protocol negotiation failed (SMB2)
|_clock-skew: 3s

TRACEROUTE
HOP RTT     ADDRESS
1   0.55 ms 192.168.48.129

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 21.61 seconds
```

We note important things like:

- Port 20 - ssh - OpenSSH 2.9p2
- Port 80 - http - Apache httpd 1.3.20
- Port 139 - netbios-ssn - Samba smbd
- Port 443 - ssl/https - Apache/1.3.20

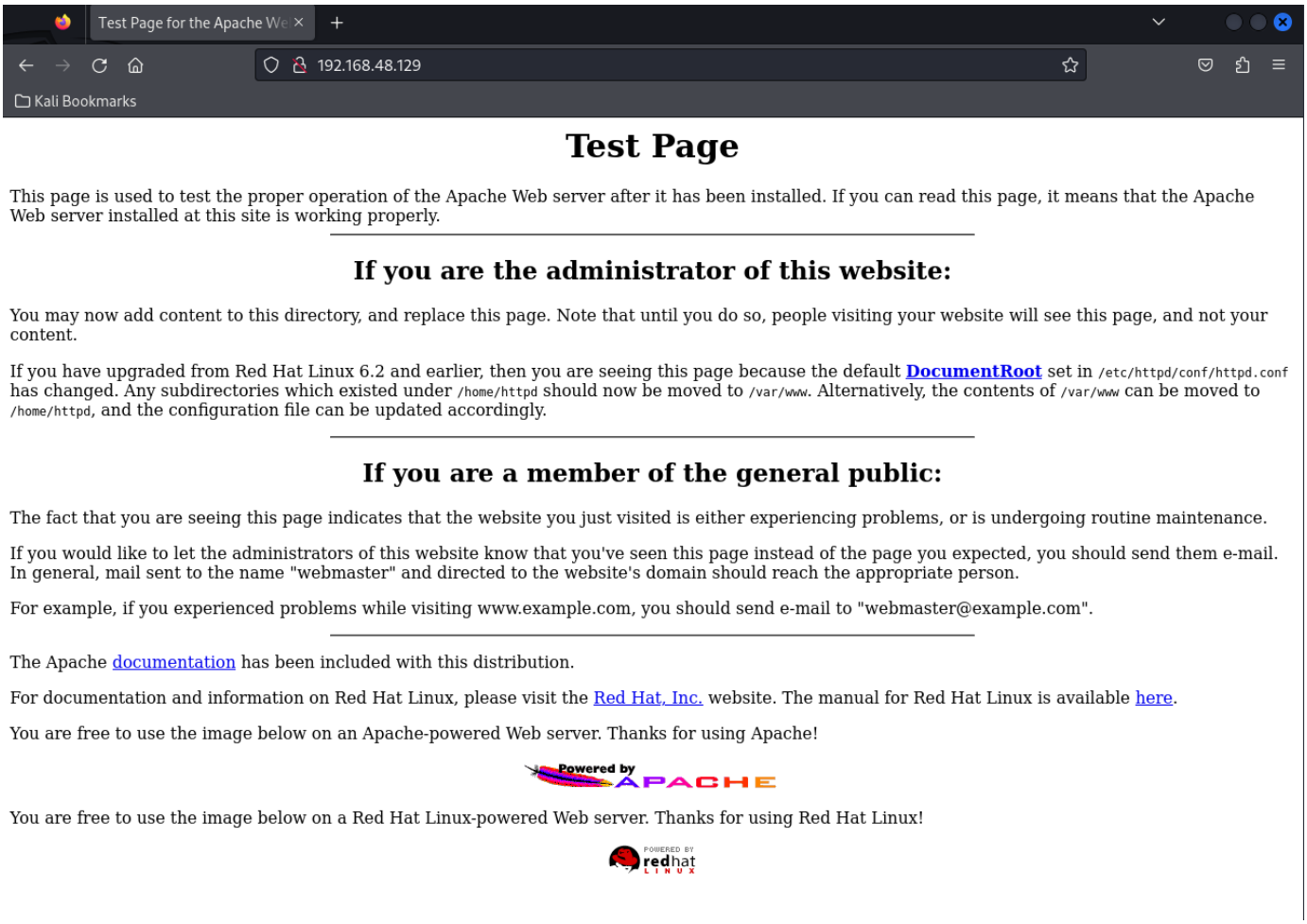
We want to see port 80 and 443, and port 139/445 for SMB. These are great to see because these are pretty common with exploits.

Port 22 is SSH hasn't been THAT bad but we can try Brute Forcing and or default credentials, but not a great way of RCE(Remote Code Execution). So not super common to attack SSH other than brute forcing. We want the low hanging fruits.

Enumerating HTTP and HTTPS

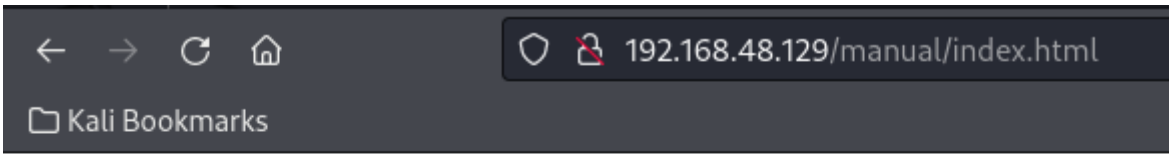
As the machine shows 80 and 443 for a webserver.

Simply browsing to the IP



This gives us information of the machine, such as that it's running RedHat linux, they are using apache, and they are running a default weboage like this. This means there coule be other web directories behind this. Maybe they left this open on accident and aren't running a website which means they may not have things updated or properly configured. Indicating they may have 'bad hygene' and other vulnerabilities.

If we try links, we can see a 404 page, but on this page, it confirms the version number of apache, and potentially the hostname.



Not Found

The requested URL /manual/index.html was not found on this server.

Apache/1.3.20 Server at 127.0.0.1 Port 80

Nikto

Nikto (Also link here) is an Open Source (GPL) web server scanner which performs comprehensive tests against web servers for multiple items.

Syntax: `nikto -h http://(ip)`


```
nikto -h http://192.168.48.129
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          192.168.48.129
+ Target Hostname:    192.168.48.129
+ Target Port:        80
+ Start Time:         2023-08-31 06:08:31 (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. 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-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ /: Apache is vulnerable to XSS via the Expect header. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-3918
+ 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.
+ mod_ssl/2.8.4 appears to be outdated (current is at least 2.9.6) (may depend on server version).
```

```
+ 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:           2023-08-31 06:08:53 (GMT-4) (22 seconds)
```

```
-----------------------------------------------------------------------------
+ 1 host(s) tested
```

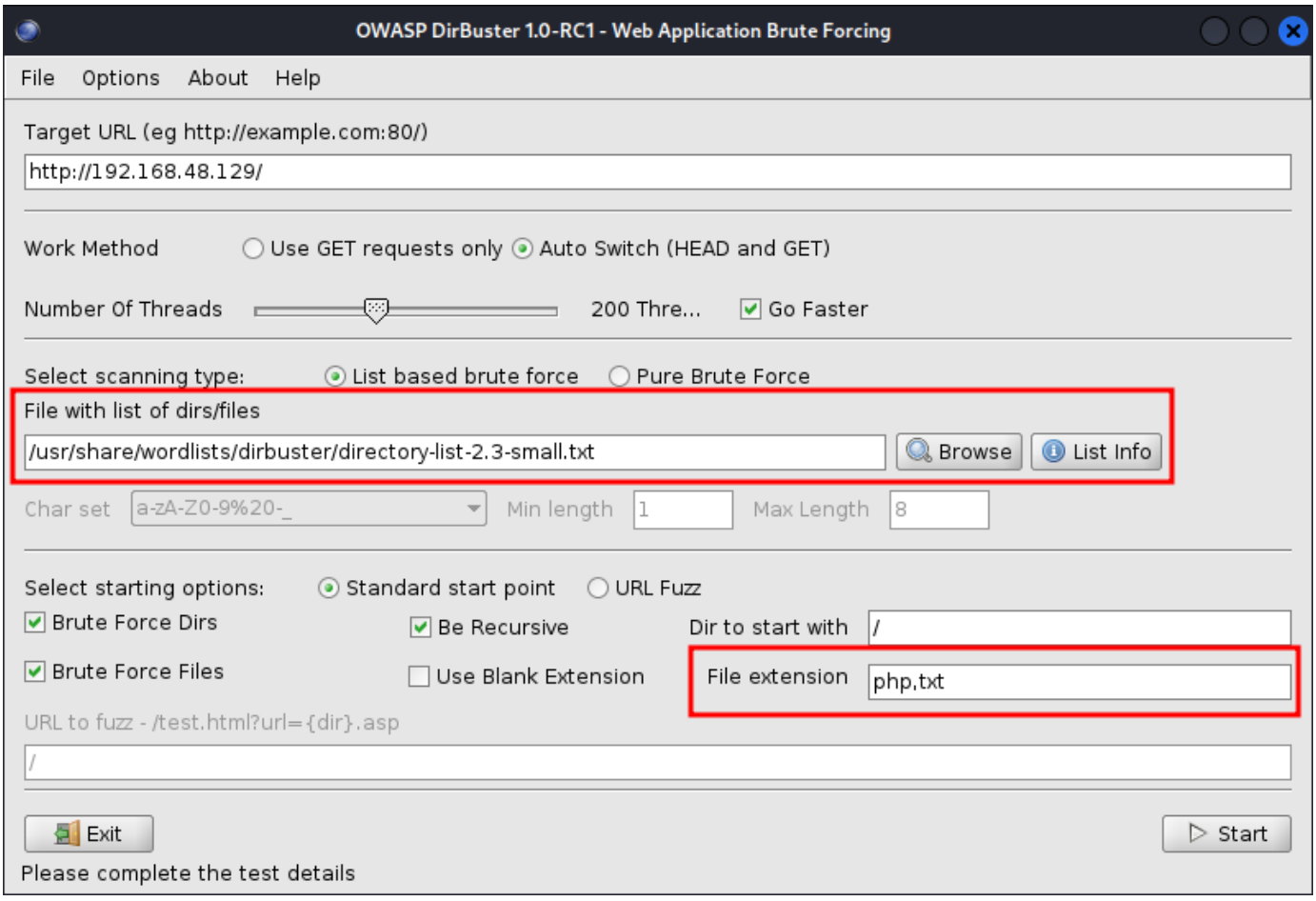
We want to see the potential vulnerabilities like "mod_ssl/2.8.4 - mod_ssl 2.8.7 and lower are vulnerable to a remote buffer overflow which may allow a remote shell."

Dirbuster, dirb and GoBuster

We are ging to use Dirbuster, dirb and GoBuster to potentially find more directories on their webhost. I have my personal notes on these tools here.

Dirbuster

Dirbuster is a GUI tool and a multi threaded java application designed to brute force directories and files names on web/application servers.
When running it be sure to specify a list of directories and/or file extentions depending on what software the server is running, like .asp or .aspcx. A good practice is to include .txt, .zip, etc but this can add more time.



Results and Tree view are helpful. We can right click to open in browser.

Dirb

dirb is a CLI tool that is a Web Content Scanner. It looks for existing (and/or hidden) Web Objects.

Gobuster

Gobuster is a tool used to brute-force:

- URIs (directories and files) in web sites.
- DNS subdomains (with wildcard support).
- Virtual Host names on target web servers.
- Open Amazon S3 buckets
- Open Google Cloud buckets
- TFTP servers

Enumerating SMB

As this machine as SMB open on port 129. SMB is a file share. It's commonly used in work environments for file sharing between co-workers and departments.

So we want to find version information and make a connection to see if we can see any files.

Metasploit

Metasploit is a exploitation framework, but has SO much more to it.

At the momebt we are looking at scanning SMB. So that's under the auxilary. So using `search smb` will give us a lot of results when in `msfconsole` but we can find `auxilary/scanner/smb_version`.

Select it with `use #` or `use /path/`, run `info` or `options` to see what info is needed.

```
msf6 > use 0
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-metasploit/basics/using-metasploit.html
  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) >
```

```
msf6 auxiliary(scanner/smb/smb_version) > set rhosts 192.168.48.129
rhosts => 192.168.48.129
msf6 auxiliary(scanner/smb/smb_version) > options

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

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOSTS   192.168.48.129   yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   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) > run

[*] 192.168.48.129:139    - SMB Detected (versions:) (preferred dialect:) (signatures:optional)
[*] 192.168.48.129:139    -   Host could not be identified: Unix (Samba 2.2.1a)
[*] 192.168.48.129:       - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smb/smb_version) >
```

Wee see this is Samba 2.2.1a, which is very helpful.

SMBClient

Syntax: `smbclient -L \\(IP)\\`

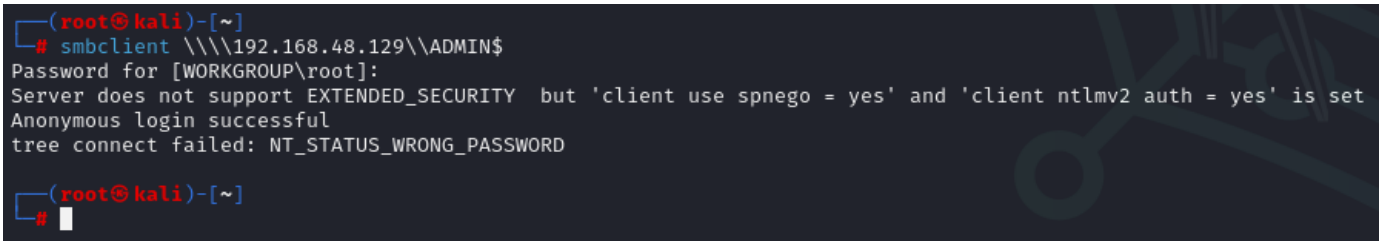
```
┌──(root㉿kali)-[~]
└─# smbclient -L \\192.168.48.129\\
Server does not support EXTENDED_SECURITY  but 'client use spnego = yes' and 'client ntlmv2 auth = yes' is set
Anonymous login successful
Password for [WORKGROUP\root]:

        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
```

Wee 2 shares of IPC and Admin. Lets try to log into the Admin share.



Enumerating SSH

From the scan we seen version `OpenSSH 2.9p2`.
We are going to attempt to log in.
`ssh user@ip`

We got nothing from this attempted login, BUT sometimes a banner will be exposed showing helpful information.

Researching Potential Vulnerabilities

Great places to look for potential vulnerabilities are:

- Google
- CVE Details
- ExploitDB
- SearchSploit. When using Searchsploit, be broad.

In our scan notes we have:

- Port 80/443 - Apache httpd 1.3.20 ((Unix) (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b)
-
    - 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. We see we can use OpenFuck and the Github from a Google search.
-
    - 404 Page
-
    - Server headers disclose version information
- Port 22 - OpenSSH 2.9p2 (protocol 1.99)
- Port 139 - SMB Samba 2.2.1a - This can potentiall use Trans2Open, or Samba 2.2.x - Remote Buffer Overflow, maybe Samba < 2.2.8 (Linux/BSD) - Remote Code Execution. Could anonymously connect to OPC with SMB client, but not Admin.