Lab 9

Metasploit

Estimated time to complete: 30 Min

WHAT YOU WILL LEARN

You will learn how to use metasploit to find vulnerable devices and attack them.

Understanding metasploit can keep you ahead of the game whether you are on the CyberSecoffense or defense.

WHY IT'S IMPORTANT

Metasploit is used by whitehat and blackhat hackers to systematically probe and find exploits in networks and servers.

Metasploit also tells you the type of vulnerability your target equipment has, helping you to easily attack it or patch it.

SKILLS GAINED

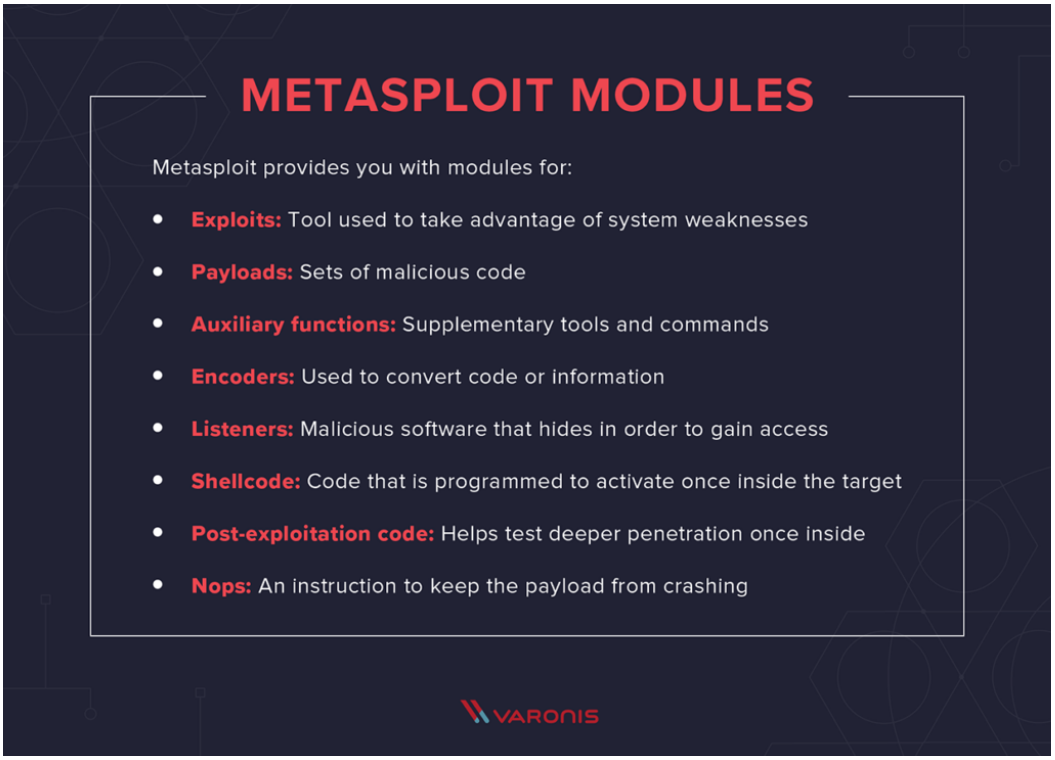
- Network scanning
- Penetration testing
- Service hardening

REQUIRED HARDWARE

- Raspberry Pi

WHAT IS METASPLOIT

Metasploit is a powerful tool that can be used to systematically probe for vulnerabilities on networks and servers. Metasploit contains over 1600 exploits on over 25 platforms including Linux, Windows, Android, Cisco and more. Once you find a vulnerable device, metasploit contains over 500 payloads that include a large variety of hacks and exploits. When combined with a powerful networking scanning tool like nmap, this might just be one of the most powerful tools in a hackers arsenal.



METASPLOIT MODULES

Metasploit provides you with modules for:

- **Exploits:** Tool used to take advantage of system weaknesses
- **Payloads:** Sets of malicious code
- **Auxiliary functions:** Supplementary tools and commands
- **Encoders:** Used to convert code or information
- **Listeners:** Malicious software that hides in order to gain access
- **Shellcode:** Code that is programmed to activate once inside the target
- **Post-exploitation code:** Helps test deeper penetration once inside
- **Nops:** An instruction to keep the payload from crashing

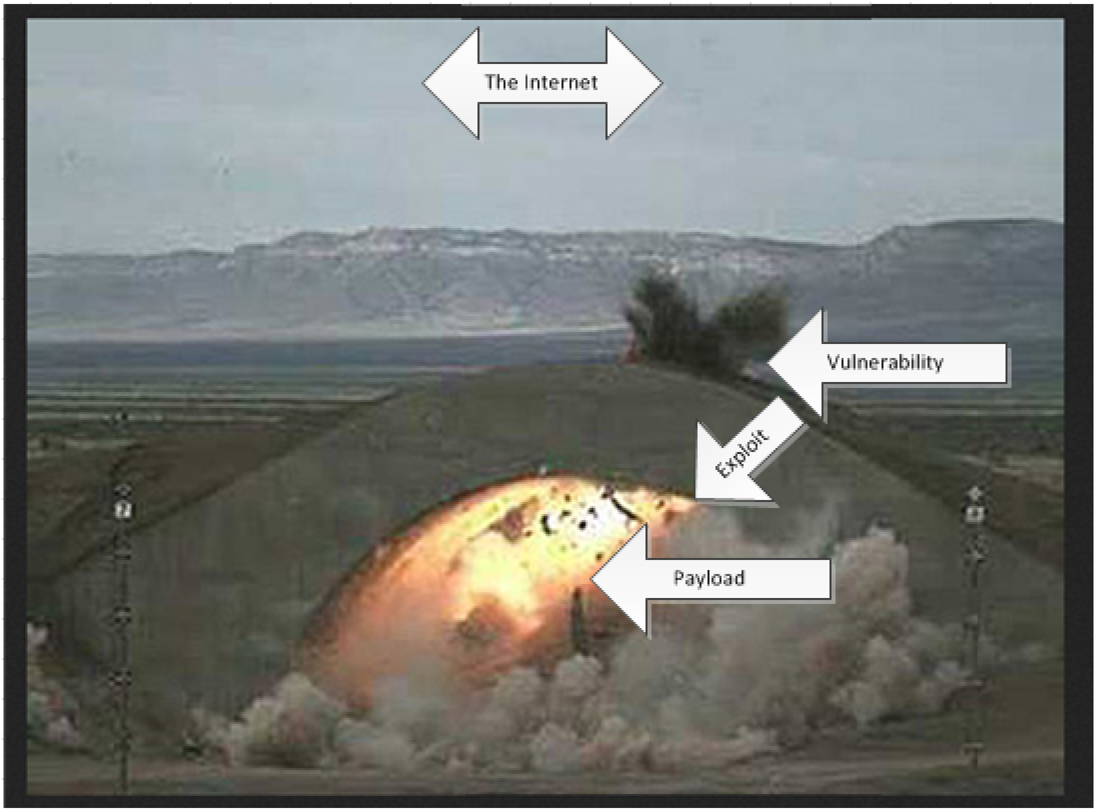
VARONIS

METASPLOIT FRAMEWORK VS PRO

Metasploit is available in two different editions: Framework and Pro. Framework is a free edition with a basic command-line interface and manual exploitation. The Pro edition is recommended for IT security teams and penetration testing as it has a multitude of advanced features for automation and infiltration such as smart exploitation, dynamic payloads, penetration testing reports, and many more. A comprehensive list of features can be found here: https://www.rapid7.com/products/metasploit/download/editions/.

EXPLOITS VS PAYLOADS

When learning metasploit, you will hear the terms vulnerability, exploit, and payload, it's important to know the difference. A **vulnerability** is a mistake in configuration or a fault in a technology that makes it exposed to attack, it's like a hole in the defenses of a network or system. How you decide to attack this vulnerability is the **exploit**, this can also be seen as the delivery system for the payload, common exploits may allow you to pop a shell or run your payload code where you normally wouldn't be able to. The **payload** is the piece of code that is actually doing damage, these can be things such as a rootkit, keylogger, trojans, RATs or reverse shells.



COMMON VULNERABILITIES AND EXPOSURES

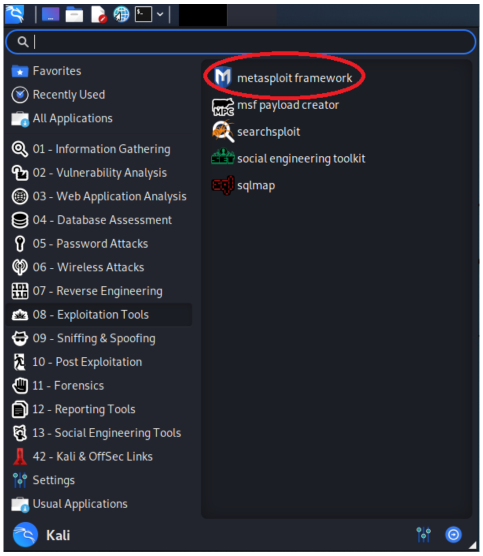
Common Vulnerabilities and Exposures, or CVE, is a long list of publicly known security threats and issues. This list is maintained by The Mitre Corporation and is sponsored by the US National Cyber Security Division of the US Department of Homeland Security. A vulnerability is a software coding error that allows hackers to directly access a system or network. An exposure is a software coding or configuration error that allows a hacker to indirectly access a system or network. CVE was designed to have a standardized way to identify vulnerabilities and exposures through the use of a CVE ID, allowing people to quickly reference the issue and find information about it.

BROWSING THE EXPLOITS

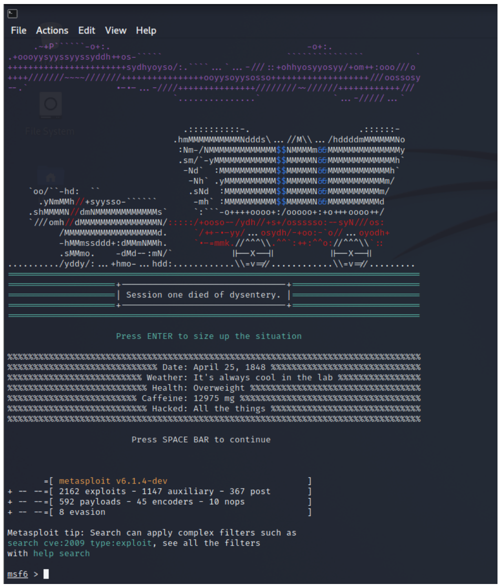
With over 1600 exploits, there's a lot to look at in metasploit. In this section we are going to look at all of the available common vulnerabilities and exposures and learn to navigate metasploit to find the right one.

STEP 1: STARTING METASPLOIT

Open metasploit by clicking: Start Button -> "08 - Exploitation Tools" -> metasploit framework



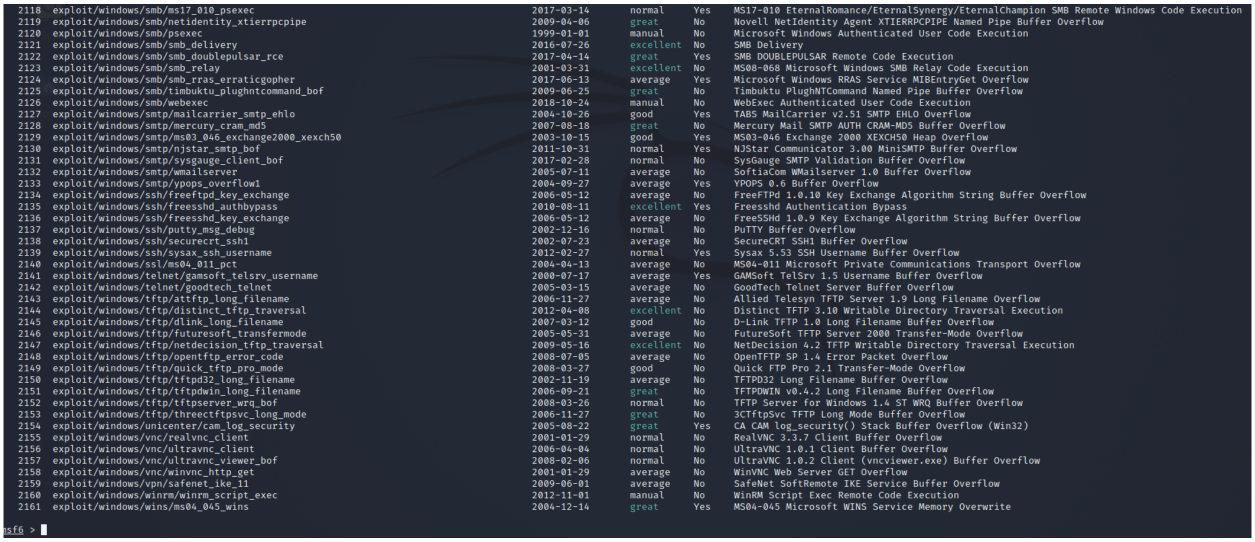
Type in your password "*Pentesttheworld1!*" and hit enter in order to let the framework start



```
| Session one died of dysentery. |

Press ENTER to size up the situation

%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%% Date: April 25, 1848 %%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%%%% Weather: It's always cool in the lab %%%%%%%%%%%%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%%%%% Health: Overweight %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%%% Caffeine: 12975 mg %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%%%%% Hacked: All the things %%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%

                       Press SPACE BAR to continue



       =[ metasploit v6.1.4-dev                           ]
+ -- --=[ 2162 exploits - 1147 auxiliary - 367 post       ]
+ -- --=[ 592 payloads - 45 encoders - 10 nops            ]
+ -- --=[ 8 evasion                                       ]

Metasploit tip: Search can apply complex filters such as
search cve:2009 type:exploit, see all the filters
with help search

msf6 >
```

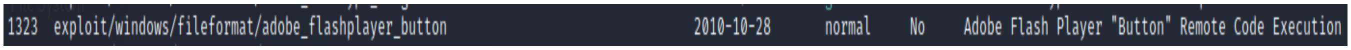
STEP 2: EXPLOITS AND PAYLOADS GALORE

Even though we are using the free version of metasploit, we still have access to a significant amount of exploits and payloads. You can look at the amount available to you on the start splash screen. In order to view all the exploits, we just need to type *"show all* ***exploits****"* and hit enter. You should see a screen similar to the one below:



```
2118  exploit/windows/smb/ms17_010_psexec                               2017-03-14       normal     Yes    MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Code Execution
2119  exploit/windows/smb/netidentity_xtierrpcpipe                      2009-04-06       great      No     Novell NetIdentity Agent XTIERRPCPIPE Named Pipe Buffer Overflow
2120  exploit/windows/smb/psexec                                        1999-01-01       manual     No     Microsoft Windows Authenticated User Code Execution
2121  exploit/windows/smb/smb_delivery                                  2016-07-26       excellent  No     SMB Delivery
2122  exploit/windows/smb/smb_doublepulsar_rce                          2017-04-14       great      Yes    SMB DOUBLEPULSAR Remote Code Execution
2123  exploit/windows/smb/smb_relay                                     2001-03-31       excellent  No     MS08-068 Microsoft Windows SMB Relay Code Execution
2124  exploit/windows/smb/smb_rras_erraticgopher                        2017-06-13       average    Yes    Microsoft Windows RRAS Service MIBEntryGet Overflow
2125  exploit/windows/smb/timbuktu_plughntcommand_bof                   2009-06-25       great      No     Timbuktu PlughNTCommand Named Pipe Buffer Overflow
2126  exploit/windows/smb/webexec                                       2018-10-24       manual     No     WebExec Authenticated User Code Execution
2127  exploit/windows/smtp/mailcarrier_smtp_ehlo                        2004-10-26       good       Yes    TABS MailCarrier v2.51 SMTP EHLO Overflow
2128  exploit/windows/smtp/mercury_cram_md5                             2007-08-18       great      No     Mercury Mail SMTP AUTH CRAM-MD5 Buffer Overflow
2129  exploit/windows/smtp/ms03_046_exchange2000_xexch50                2003-10-15       good       Yes    MS03-046 Exchange 2000 XEXCH50 Heap Overflow
2130  exploit/windows/smtp/njstar_smtp_bof                              2011-10-31       normal     Yes    NJStar Communicator 3.00 MiniSMTP Buffer Overflow
2131  exploit/windows/smtp/sysgauge_client_bof                          2017-02-28       normal     No     SysGauge SMTP Validation Buffer Overflow
2132  exploit/windows/smtp/wmailserver                                  2005-07-11       average    No     SoftiaCom WMailserver 1.0 Buffer Overflow
2133  exploit/windows/smtp/ypops_overflow1                              2004-09-27       average    Yes    YPOPS 0.6 Buffer Overflow
2134  exploit/windows/ssh/freeftpd_key_exchange                         2006-05-12       average    No     FreeFTPd 1.0.10 Key Exchange Algorithm String Buffer Overflow
2135  exploit/windows/ssh/freesshd_authbypass                           2010-08-11       excellent  Yes    Freesshd Authentication Bypass
2136  exploit/windows/ssh/freesshd_key_exchange                         2006-05-12       average    No     FreeSSHd 1.0.9 Key Exchange Algorithm String Buffer Overflow
2137  exploit/windows/ssh/putty_msg_debug                               2002-12-16       normal     No     PuTTY Buffer Overflow
2138  exploit/windows/ssh/securecrt_ssh1                                2002-07-23       average    No     SecureCRT SSH1 Buffer Overflow
2139  exploit/windows/ssh/sysax_ssh_username                            2012-02-27       normal     Yes    Sysax 5.53 SSH Username Buffer Overflow
2140  exploit/windows/ssl/ms04_011_pct                                  2004-04-13       average    No     MS04-011 Microsoft Private Communications Transport Overflow
2141  exploit/windows/telnet/gamsoft_telsrv_username                    2000-07-17       average    Yes    GAMSoft TelSrv 1.5 Username Buffer Overflow
2142  exploit/windows/telnet/goodtech_telnet                            2005-03-15       average    No     GoodTech Telnet Server Buffer Overflow
2143  exploit/windows/tftp/attftp_long_filename                         2006-11-27       average    No     Allied Telesyn TFTP Server 1.9 Long Filename Overflow
2144  exploit/windows/tftp/distinct_tftp_traversal                      2012-04-08       excellent  No     Distinct TFTP 3.10 Writable Directory Traversal Execution
2145  exploit/windows/tftp/dlink_long_filename                          2007-03-12       good       No     D-Link TFTP 1.0 Long Filename Buffer Overflow
2146  exploit/windows/tftp/futuresoft_transfermode                      2005-05-31       average    No     FutureSoft TFTP Server 2000 Transfer-Mode Overflow
2147  exploit/windows/tftp/netdecision_tftp_traversal                   2009-05-16       excellent  No     NetDecision 4.2 TFTP Writable Directory Traversal Execution
2148  exploit/windows/tftp/opentftp_error_code                          2008-07-05       average    No     OpenTFTP SP 1.4 Error Packet Overflow
2149  exploit/windows/tftp/quick_tftp_pro_mode                          2008-03-27       good       No     Quick FTP Pro 2.1 Transfer-Mode Overflow
2150  exploit/windows/tftp/tftpd32_long_filename                        2002-11-19       average    No     TFTPD32 Long Filename Buffer Overflow
2151  exploit/windows/tftp/tftpdwin_long_filename                       2006-09-21       great      No     TFTPDWIN v0.4.2 Long Filename Buffer Overflow
2152  exploit/windows/tftp/tftpserver_wrq_bof                           2008-03-26       normal     No     TFTP Server for Windows 1.4 ST WRQ Buffer Overflow
2153  exploit/windows/tftp/threectftpsvc_long_mode                      2006-11-27       great      No     3CTftpSvc TFTP Long Mode Buffer Overflow
2154  exploit/windows/unicenter/cam_log_security                        2005-08-22       great      Yes    CA CAM log_security() Stack Buffer Overflow (Win32)
2155  exploit/windows/vnc/realvnc_client                                2001-01-29       normal     No     RealVNC 3.3.7 Client Buffer Overflow
2156  exploit/windows/vnc/ultravnc_client                               2006-04-04       normal     No     UltraVNC 1.0.1 Client Buffer Overflow
2157  exploit/windows/vnc/ultravnc_viewer_bof                           2008-02-06       normal     No     UltraVNC 1.0.2 Client (vncviewer.exe) Buffer Overflow
2158  exploit/windows/vnc/winvnc_http_get                               2001-01-29       average    No     WinVNC Web Server GET Overflow
2159  exploit/windows/vpn/safenet_ike_11                                2009-06-01       average    No     SafeNet SoftRemote IKE Service Buffer Overflow
2160  exploit/windows/winrm/winrm_script_exec                           2012-11-01       manual     No     WinRM Script Exec Remote Code Execution
2161  exploit/windows/wins/ms04_045_wins                                2004-12-14       great      Yes    MS04-045 Microsoft WINS Service Memory Overwrite

msf6 >
```

Understanding this output may seem a little difficult, but it’s pretty simple and helps us understand how searching works in metasploit. For example, take the exploit pictured here.:



```
1323  exploit/windows/fileformat/adobe_flashplayer_button                  2010-10-28      normal     No     Adobe Flash Player "Button" Remote Code Execution
```

Reading from left to right:

1323: This is the # of the exploit, this helps to keep track of an exploit but will only be unique to the search that we do.

exploit/windows/fileformat/adboe_flashplayer_button: This is the name of the exploit, this will not change between searches and can easily identify the exploit at a later time.

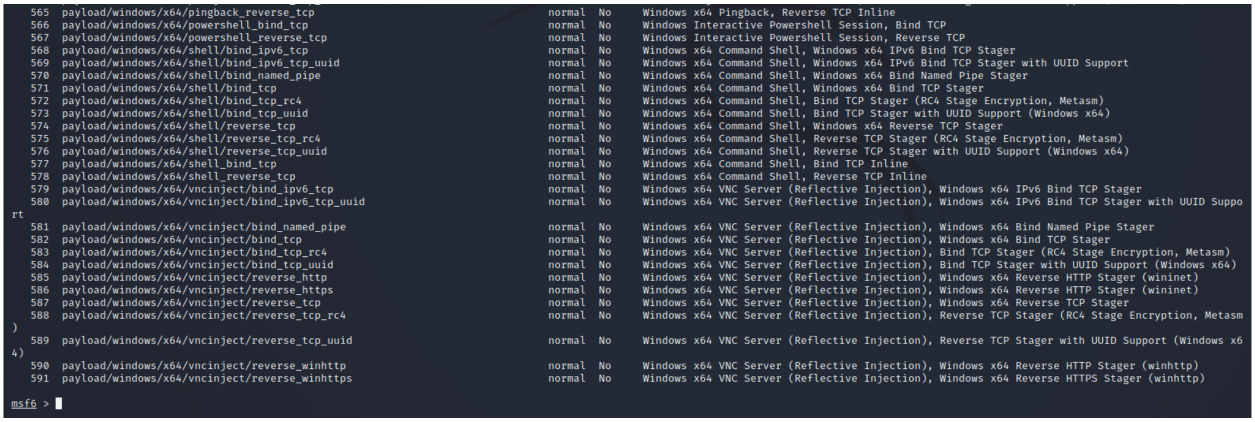
2010-10-28: This tells us what day the exploit was disclosed to the public.

normal: Normal defines the rank of the exploit. In this case, normal means that the exploit works but may need a specific version of the software and may have trouble auto detecting the service it is attacking

No: This tells us if the exploit is able to automatically “check” for the service on a target machine

Adobe Flash Player "Button" Remote Code Execution: This is the description of the exploit itself and can give users a quick glance as to what the code does.

Now that we understand the basic formatting of metasploit, we can also view all of the payloads available on the free version using the command *"show all **payloads**"*



```
   565  payload/windows/x64/pingback_reverse_tcp                normal  No     Windows x64 Pingback, Reverse TCP Inline
   566  payload/windows/x64/powershell_bind_tcp                 normal  No     Windows Interactive Powershell Session, Bind TCP
   567  payload/windows/x64/powershell_reverse_tcp              normal  No     Windows Interactive Powershell Session, Reverse TCP
   568  payload/windows/x64/shell/bind_ipv6_tcp                 normal  No     Windows x64 Command Shell, Windows x64 IPv6 Bind TCP Stager
   569  payload/windows/x64/shell/bind_ipv6_tcp_uuid            normal  No     Windows x64 Command Shell, Windows x64 IPv6 Bind TCP Stager with UUID Support
   570  payload/windows/x64/shell/bind_named_pipe               normal  No     Windows x64 Command Shell, Windows x64 Bind Named Pipe Stager
   571  payload/windows/x64/shell/bind_tcp                      normal  No     Windows x64 Command Shell, Windows x64 Bind TCP Stager
   572  payload/windows/x64/shell/bind_tcp_rc4                  normal  No     Windows x64 Command Shell, Bind TCP Stager (RC4 Stage Encryption, Metasm)
   573  payload/windows/x64/shell/bind_tcp_uuid                 normal  No     Windows x64 Command Shell, Bind TCP Stager with UUID Support (Windows x64)
   574  payload/windows/x64/shell/reverse_tcp                   normal  No     Windows x64 Command Shell, Windows x64 Reverse TCP Stager
   575  payload/windows/x64/shell/reverse_tcp_rc4               normal  No     Windows x64 Command Shell, Reverse TCP Stager (RC4 Stage Encryption, Metasm)
   576  payload/windows/x64/shell/reverse_tcp_uuid              normal  No     Windows x64 Command Shell, Reverse TCP Stager with UUID Support (Windows x64)
   577  payload/windows/x64/shell_bind_tcp                      normal  No     Windows x64 Command Shell, Bind TCP Inline
   578  payload/windows/x64/shell_reverse_tcp                   normal  No     Windows x64 Command Shell, Reverse TCP Inline
   579  payload/windows/x64/vncinject/bind_ipv6_tcp             normal  No     Windows x64 VNC Server (Reflective Injection), Windows x64 IPv6 Bind TCP Stager
   580  payload/windows/x64/vncinject/bind_ipv6_tcp_uuid        normal  No     Windows x64 VNC Server (Reflective Injection), Windows x64 IPv6 Bind TCP Stager with UUID Suppo
rt
   581  payload/windows/x64/vncinject/bind_named_pipe           normal  No     Windows x64 VNC Server (Reflective Injection), Windows x64 Bind Named Pipe Stager
   582  payload/windows/x64/vncinject/bind_tcp                  normal  No     Windows x64 VNC Server (Reflective Injection), Windows x64 Bind TCP Stager
   583  payload/windows/x64/vncinject/bind_tcp_rc4              normal  No     Windows x64 VNC Server (Reflective Injection), Bind TCP Stager (RC4 Stage Encryption, Metasm)
   584  payload/windows/x64/vncinject/bind_tcp_uuid             normal  No     Windows x64 VNC Server (Reflective Injection), Bind TCP Stager with UUID Support (Windows x64)
   585  payload/windows/x64/vncinject/reverse_http              normal  No     Windows x64 VNC Server (Reflective Injection), Windows x64 Reverse HTTP Stager (wininet)
   586  payload/windows/x64/vncinject/reverse_https             normal  No     Windows x64 VNC Server (Reflective Injection), Windows x64 Reverse HTTP Stager (wininet)
   587  payload/windows/x64/vncinject/reverse_tcp               normal  No     Windows x64 VNC Server (Reflective Injection), Windows x64 Reverse TCP Stager
   588  payload/windows/x64/vncinject/reverse_tcp_rc4           normal  No     Windows x64 VNC Server (Reflective Injection), Reverse TCP Stager (RC4 Stage Encryption, Metasm
)
   589  payload/windows/x64/vncinject/reverse_tcp_uuid          normal  No     Windows x64 VNC Server (Reflective Injection), Reverse TCP Stager with UUID Support (Windows x6
4)
   590  payload/windows/x64/vncinject/reverse_winhttp           normal  No     Windows x64 VNC Server (Reflective Injection), Windows x64 Reverse HTTP Stager (winhttp)
   591  payload/windows/x64/vncinject/reverse_winhttps          normal  No     Windows x64 VNC Server (Reflective Injection), Windows x64 Reverse HTTPS Stager (winhttp)

msf6 > █
```

Take a few minutes and look at some of the payloads available and see if any of them could run on a device you own.

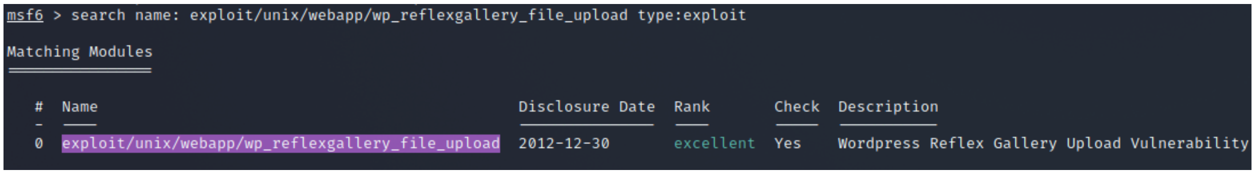
STEP 3: SEARCHING FOR SPECIFICS

While having all these exploits and payloads at the tip of your fingers is great, sometimes we want to get info on a specific exploit. In order to do this all we need to do is modify our search command. The layout of the command is

search name:[Exploit Name] type:[Exploit/Payload] platform:[Windows/Linux/Mac/Etc]

Using this, we can start looking for new vulnerabilities. Recently, we found out that a hacker used a wordpress upload exploit to run bad code on our servers. We think the name of the exploit is **exploit/unix/webapp/wp_reflexgallery_file_upload.** We can search for the exploit using the command below

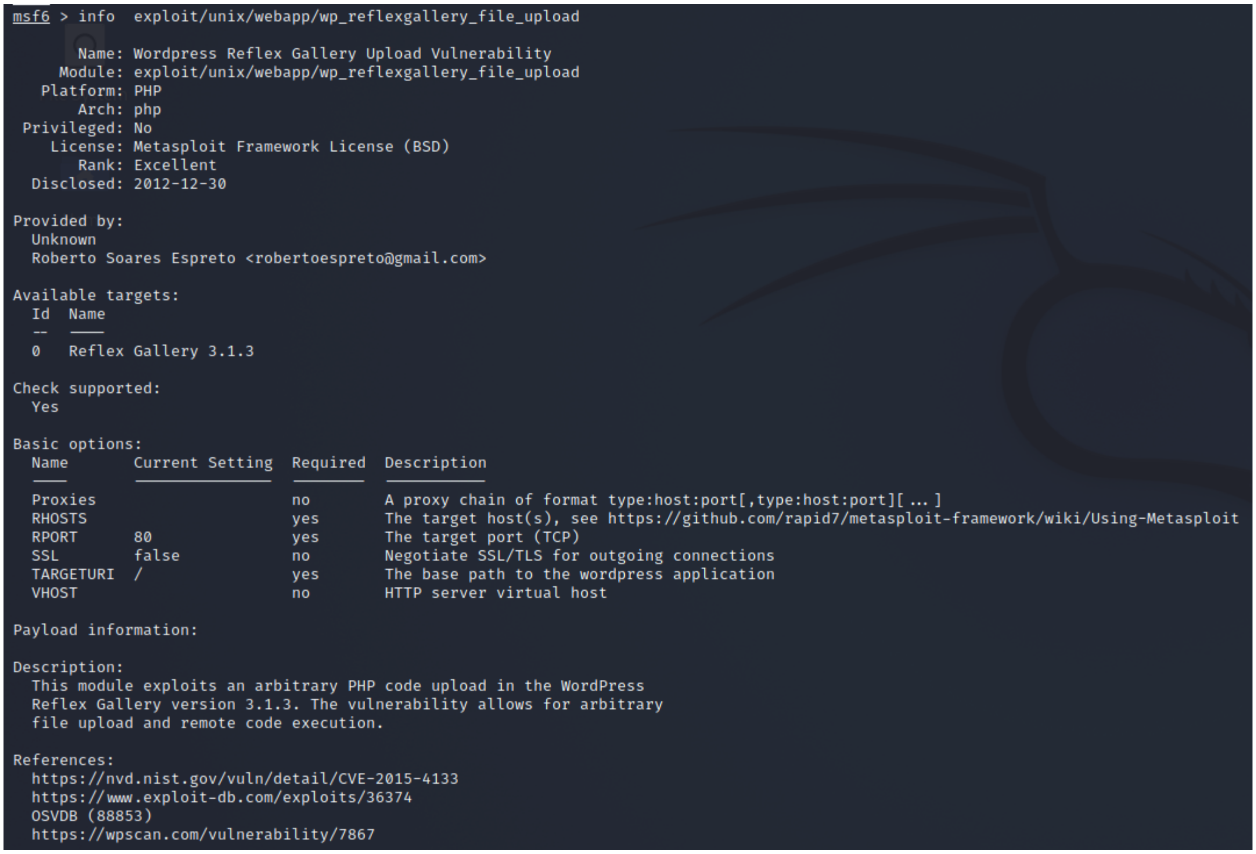
"search name: exploit/unix/webapp/wp_reflexgallery_file_upload type:exploit"



```
msf6 > search name: exploit/unix/webapp/wp_reflexgallery_file_upload type:exploit

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

   #  Name                                              Disclosure Date  Rank       Check  Description
   -  ----                                              ---------------  ----       -----  -----------
   0  exploit/unix/webapp/wp_reflexgallery_file_upload  2012-12-30       excellent  Yes    Wordpress Reflex Gallery Upload Vulnerability
```

Now we can see that is is real, we can find more information about the exploit using the command:

“info exploit/unix/webapp/wp_reflexgallery_file_upload”



```
msf6 > info  exploit/unix/webapp/wp_reflexgallery_file_upload

       Name: Wordpress Reflex Gallery Upload Vulnerability
     Module: exploit/unix/webapp/wp_reflexgallery_file_upload
   Platform: PHP
       Arch: php
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2012-12-30

Provided by:
  Unknown
  Roberto Soares Espreto <robertoespreto@gmail.com>

Available targets:
  Id  Name
  --  ----
  0   Reflex Gallery 3.1.3

Check supported:
  Yes

Basic options:
  Name       Current Setting  Required  Description
  ----       ---------------  --------  -----------
  Proxies                     no        A proxy chain of format type:host:port[,type:host:port][...]
  RHOSTS                      yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
  RPORT      80               yes       The target port (TCP)
  SSL        false            no        Negotiate SSL/TLS for outgoing connections
  TARGETURI  /                yes       The base path to the wordpress application
  VHOST                       no        HTTP server virtual host

Payload information:

Description:
  This module exploits an arbitrary PHP code upload in the WordPress
  Reflex Gallery version 3.1.3. The vulnerability allows for arbitrary
  file upload and remote code execution.

References:
  https://nvd.nist.gov/vuln/detail/CVE-2015-4133
  https://www.exploit-db.com/exploits/36374
  OSVDB (88853)
  https://wpscan.com/vulnerability/7867
```

Now we can see how it works, links to find more info at the bottom, and a description of all it’s operations. From here, we can figure out how it did the exploit, and what services we should look at to stop it from happening again!

METASPLOIT CERTIFICATIONS

Metasploit has an online certification program called the Metasploit Pro Specialist Certification where you can become a certified pen-tester. The passing score is an 80 percent, the exam is online and open book which takes about 2 hours. It costs about $195 and you can print your certification once you’ve passed. There is also a metasploit training course that is directed toward those who do not have much cybersecurity or pen-testing experience and should teach you everything you need to know to pass the exam, though it is very expensive, at around $2000 per student. The course will teach how to use metasploit pro, network scanning, exploitation techniques, web app testing, social engineering and reporting.

EXERCISES:

1: Tracing back the steps:

Uh, oh. Your boss just got hacked! He's really mad and wants to figure out what he did wrong to get hacked! One of the cybersecurity team members told him, his phone got hacked at home. They suspect his Netgear R7000 has malicious code running on it. Go check out the exploit "***exploit/linux/http/netgear_r7000_cgibin_exec***" and search the description to find what firmware version is affected by this.

2: Determine the vulnerability

Your firewall recently pick up two exploits running on the network. It seems one was blocked and the other one got through your security. Now all the Apple computers in the office talk whenever we highlight TEXT option. Look at these two exploits and determine which one got through so we can figure out how to stop it

post/osx/admin/say OR ***exploit/android/browser/samsung_knox_smdm_url***

REVIEW

1: What is an exploit?

A) A hole in the defenses of a network

B) How you deliver a payload

C) The code that does damage

D) A way to defend a hack

2: What is a CVE?

A) A metasploit version number

B) Common vulnerability environment

C) An index number for a certain known vulnerability

D) A mid 90s Honda

3: About how many vulnerabilities are available in metasploit?

A) 1600

B) 500

C) 150

D) 5000

4: What is **not** a feature in metasploit pro?

A) Smart exploitation

B) Dynamic payloads

C) Pen-testing reporting

D) AI brute forcing

5: Who is in charge of the CVE list?

A) Amazon Web Services

B) Mitre Corporation

C) Acme Corporation

D) US Department of Homeland Security

6: What is not an example of a payload?

A) A rootkit

B) A trojan

C) An open port

D) A keylogger

Answers: 1:B 2:C 3:A 4:D 5:B 6:C