Active Reconnaissance and Exploitation

Raphael Karger & Mike Antoniades 9/24/2020

Housekeeping

- UB Lockdown Interest Form - https://forms.gle/XPibHTvH4N2wMv6f7
- CPTC Interest Form - https://forms.gle/oAj22SsBUK48P1FF8

Summary

1. Services
   a. Service Definition and Example
   b. Detection
   c. Enumeration
2. Exploitation
   a. Exploit Definition and Example
   b. Exploitation using Metasploit
3. King of the Hill Activity!

Services

“a network service is an application running at the network application layer and above, that provides data storage, manipulation, presentation, communication or other capabilities”

- Common Services and associated Ports:
  - File Transfer Protocol (FTP) - 20, 21 (TCP)
  - Secure Shell (SSH) - 22 (TCP and UDP)
  - Domain Name System (DNS) - 53 (TCP and UDP)
  - HyperText Transfer Protocol (HTTP) - 80 (TCP)
  - HTTP with Secure Sockets Layer (SSL) - 443 (TCP and UDP)
  - Remote Desktop Protocol (RDP) - 3389 (TCP and UDP)
- Service and Port listing - https://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers

Service Pentesting Methodology

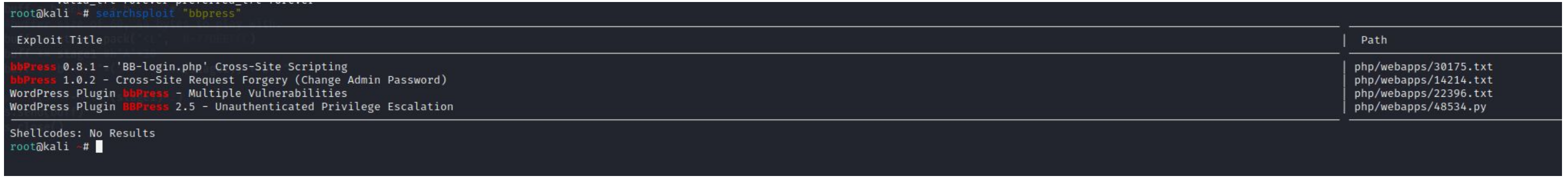
- Identifying running services and associated versions
- Identifying possible exploits
- Utilizing service-specific tools
- Utilizing textbook techniques per service
- Resources:
    - Service Identification - https://book.hacktricks.xyz/pentesting/pentesting-network
    - Techniques per service - eg. https://book.hacktricks.xyz/pentesting/pentesting-telnet
    - Exploit Database - https://www.exploit-db.com/
    - Google dorks

Identifying Services with Nmap

- Network Map (NMAP) is a free and open-source network scanner
- $ nmap -sV -n 192.168.3.18 --min-rate 5000
  - -sV : Enable Service Detection
  - -Pn : Skip host discovery
  - -n : No DNS resolution
  - --min-rate : Send packets faster than NUMBER per second

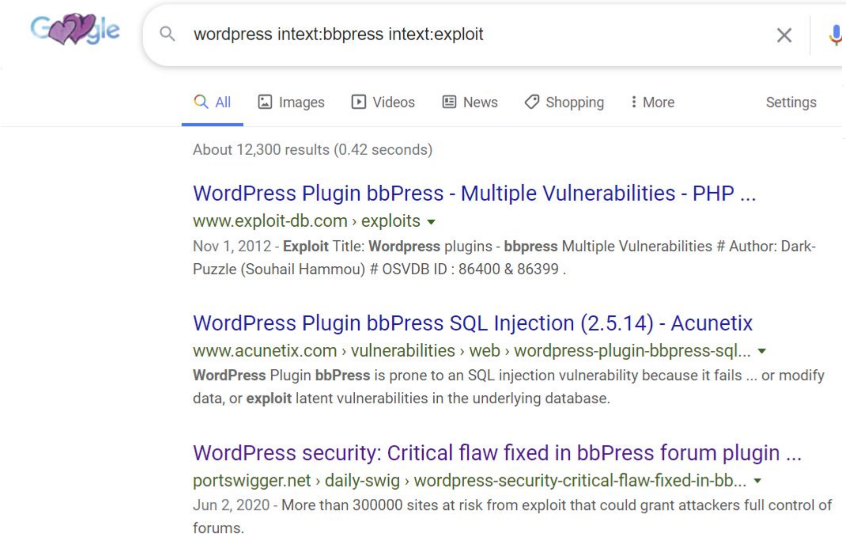
Locating an Exploit - searchsploit

- $ searchsploit “product name”
- Results are located in “/usr/share/exploitdb/exploits” example “/usr/share/exploitdb/exploits/php/webapps/48534.py”



```
root@kali ~# searchsploit "bbpress"
-----------------------------------------------------------------------------  ------------------------
 Exploit Title                                                                |  Path
-----------------------------------------------------------------------------  ------------------------
bbPress 0.8.1 - 'BB-login.php' Cross-Site Scripting                           | php/webapps/30175.txt
bbPress 1.0.2 - Cross-Site Request Forgery (Change Admin Password)            | php/webapps/14214.txt
WordPress Plugin bbPress - Multiple Vulnerabilities                           | php/webapps/22396.txt
WordPress Plugin BBPress 2.5 - Unauthenticated Privilege Escalation           | php/webapps/48534.py
-----------------------------------------------------------------------------  ------------------------
Shellcodes: No Results
root@kali ~# 
```

Locating an Exploit - google



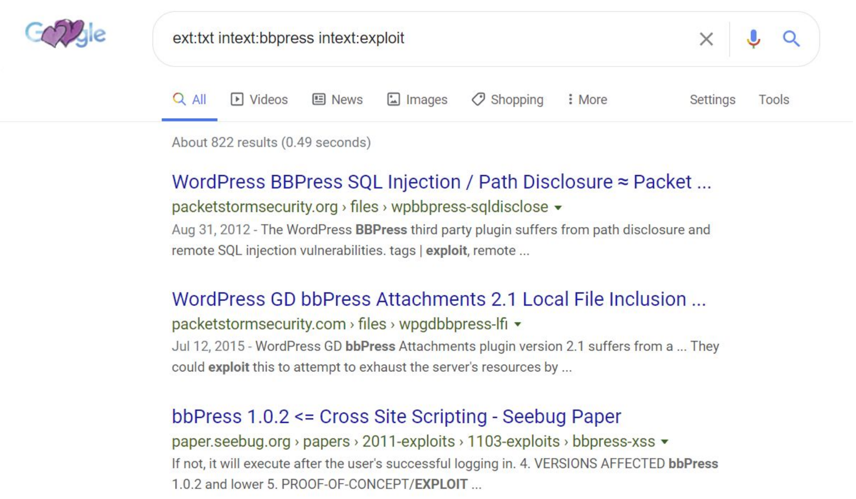
wordpress intext:bbpress intext:exploit

About 12,300 results (0.42 seconds)

WordPress Plugin bbPress - Multiple Vulnerabilities - PHP ...
www.exploit-db.com › exploits
Nov 1, 2012 - **Exploit** Title: **Wordpress** plugins - **bbpress** Multiple Vulnerabilities # Author: Dark-Puzzle (Souhail Hammou) # OSVDB ID : 86400 & 86399 .

WordPress Plugin bbPress SQL Injection (2.5.14) - Acunetix
www.acunetix.com › vulnerabilities › web › wordpress-plugin-bbpress-sql...
WordPress Plugin **bbPress** is prone to an SQL injection vulnerability because it fails ... or modify data, or **exploit** latent vulnerabilities in the underlying database.

WordPress security: Critical flaw fixed in bbPress forum plugin ...
portswigger.net › daily-swig › wordpress-security-critical-flaw-fixed-in-bb...
Jun 2, 2020 - More than 300000 sites at risk from exploit that could grant attackers full control of forums.



ext:txt intext:bbpress intext:exploit

About 822 results (0.49 seconds)

WordPress BBPress SQL Injection / Path Disclosure ≈ Packet ...
packetstormsecurity.org › files › wpbbpress-sqldisclose
Aug 31, 2012 - The WordPress **BBPress** third party plugin suffers from path disclosure and remote SQL injection vulnerabilities. tags | **exploit**, remote ...

WordPress GD bbPress Attachments 2.1 Local File Inclusion ...
packetstormsecurity.com › files › wpgdbbpress-lfi
Jul 12, 2015 - WordPress GD **bbPress** Attachments plugin version 2.1 suffers from a ... They could **exploit** this to attempt to exhaust the server's resources by ...

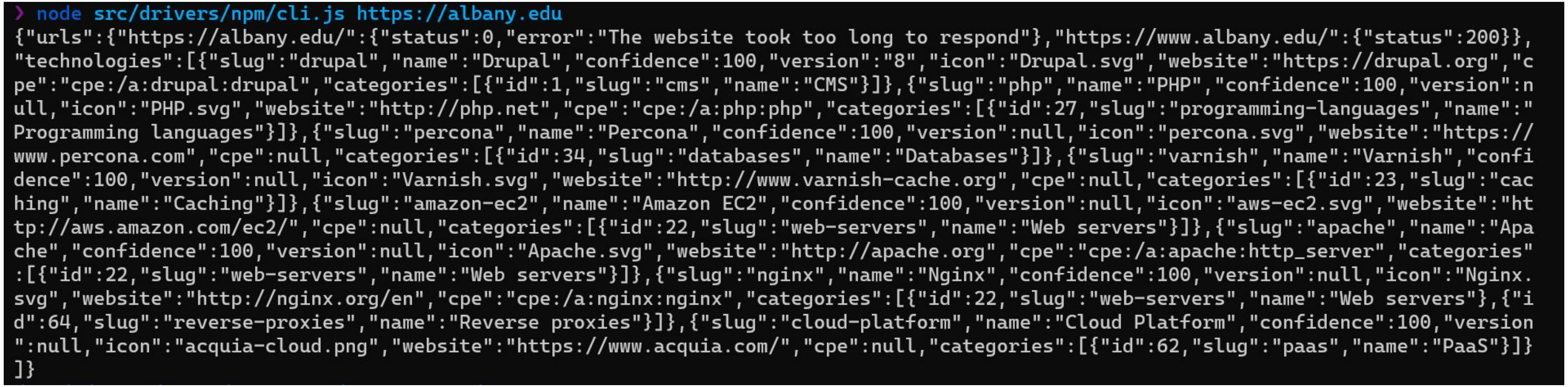
bbPress 1.0.2 <= Cross Site Scripting - Seebug Paper
paper.seebug.org › papers › 2011-exploits › 1103-exploits › bbpress-xss
If not, it will execute after the user's successful logging in. 4. VERSIONS AFFECTED **bbPress** 1.0.2 and lower 5. PROOF-OF-CONCEPT/**EXPLOIT** ...

Web Reconnaissance - Finding Directories

- $ gobuster dir --url http://10.10.10.171/ -w /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt
  - --url : Specify URL
  - -w : path to wordlist
  - Dir : specify directory search
- Wordlists - https://github.com/danielmiessler/SecLists

Web Reconnaissance - Framework Identification

- Wappalyzer - https://github.com/AliasIO/wappalyzer
- Does not come by default with kali

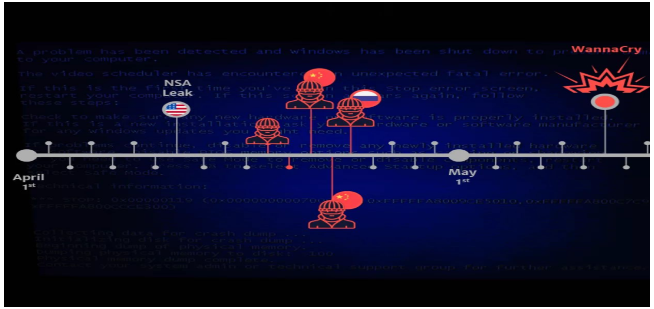


```
❯ node src/drivers/npm/cli.js https://albany.edu
{"urls":{"https://albany.edu/":{"status":0,"error":"The website took too long to respond"},"https://www.albany.edu/":{"status":200}},
"technologies":[{"slug":"drupal","name":"Drupal","confidence":100,"version":"8","icon":"Drupal.svg","website":"https://drupal.org","c
pe":"cpe:/a:drupal:drupal","categories":[{"id":1,"slug":"cms","name":"CMS"}]},{"slug":"php","name":"PHP","confidence":100,"version":n
ull,"icon":"PHP.svg","website":"http://php.net","cpe":"cpe:/a:php:php","categories":[{"id":27,"slug":"programming-languages","name":"
Programming languages"}]},{"slug":"percona","name":"Percona","confidence":100,"version":null,"icon":"percona.svg","website":"https://
www.percona.com","cpe":null,"categories":[{"id":34,"slug":"databases","name":"Databases"}]},{"slug":"varnish","name":"Varnish","confi
dence":100,"version":null,"icon":"Varnish.svg","website":"http://www.varnish-cache.org","cpe":null,"categories":[{"id":23,"slug":"cac
hing","name":"Caching"}]},{"slug":"amazon-ec2","name":"Amazon EC2","confidence":100,"version":null,"icon":"aws-ec2.svg","website":"ht
tp://aws.amazon.com/ec2/","cpe":null,"categories":[{"id":22,"slug":"web-servers","name":"Web servers"}]},{"slug":"apache","name":"Apa
che","confidence":100,"version":null,"icon":"Apache.svg","website":"http://apache.org","cpe":"cpe:/a:apache:http_server","categories"
:[{"id":22,"slug":"web-servers","name":"Web servers"}]},{"slug":"nginx","name":"Nginx","confidence":100,"version":null,"icon":"Nginx.
svg","website":"http://nginx.org/en","cpe":"cpe:/a:nginx:nginx","categories":[{"id":22,"slug":"web-servers","name":"Web servers"},{"i
d":64,"slug":"reverse-proxies","name":"Reverse proxies"}]},{"slug":"cloud-platform","name":"Cloud Platform","confidence":100,"version
":null,"icon":"acquia-cloud.png","website":"https://www.acquia.com/","cpe":null,"categories":[{"id":62,"slug":"paas","name":"PaaS"}]}
]}
```

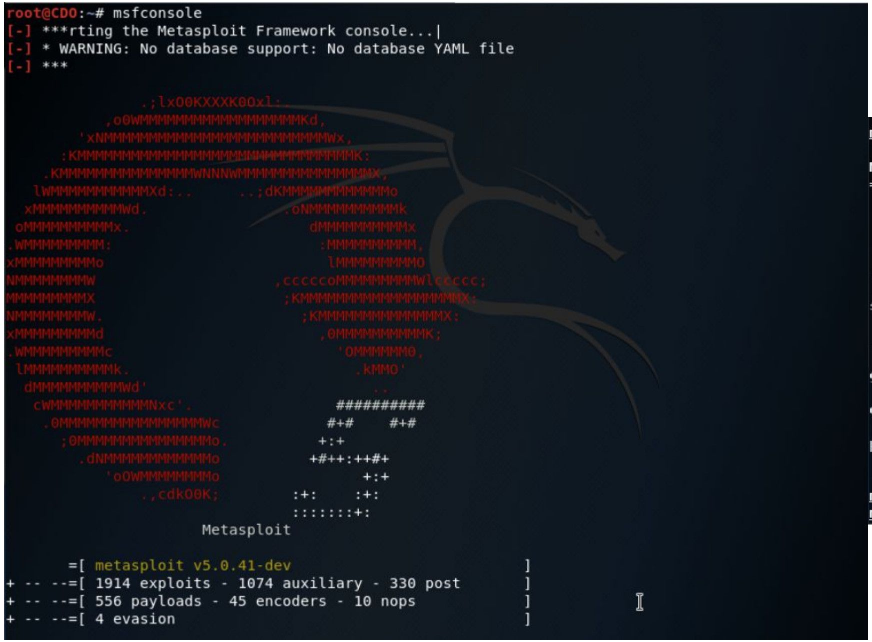
What is an Exploit?

“a piece of software, a chunk of data, or a sequence of commands that takes advantage of a bug or vulnerability to cause unintended or unanticipated behavior”

- In industry; a bug that enables an actor to perform unintended behaviour in software that results in an advantage
- For our purposes; a way of gaining access to a system
- Well known exploits include, Eternal Blue, Dirty Cow, and Shellshock



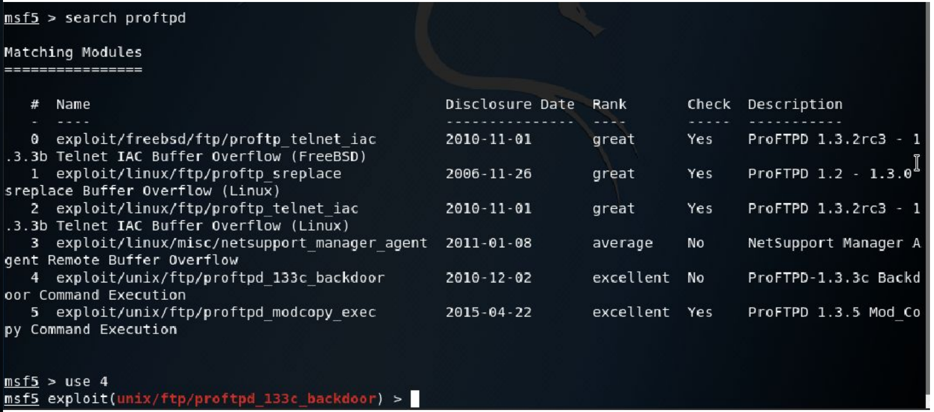
Using an exploit - Metasploit



```
root@CDO:~# msfconsole
[-] ***rting the Metasploit Framework console...|
[-] * WARNING: No database support: No database YAML file
[-] ***

               .;lxO0KXXXK0Oxl:.
           ,o0WMMMMMMMMMMMMMMMMMMKd,
        'xNMMMMMMMMMMMMMMMMMMMMMMMMMWx,
      :KMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMK:
    .KMMMMMMMMMMMMMMMWNNNWMMMMMMMMMMMMMMMX,
   lWMMMMMMMMMMMXd:..     ..;dKMMMMMMMMMMMMo
  xMMMMMMMMMMWd.               .oNMMMMMMMMMMk
 oMMMMMMMMMMx.                    dMMMMMMMMMMx
.WMMMMMMMMM:                       :MMMMMMMMMM,
xMMMMMMMMMo                         lMMMMMMMMMO
NMMMMMMMMW                    ,cccccoMMMMMMMMMWlccccc;
MMMMMMMMMX                     ;KMMMMMMMMMMMMMMMMMMX:
NMMMMMMMMW.                      ;KMMMMMMMMMMMMMMX:
xMMMMMMMMMd                        ,0MMMMMMMMMMK;
.WMMMMMMMMMc                         'OMMMMMM0,
 lMMMMMMMMMMk.                         .kMMO'
  dMMMMMMMMMMWd'                         ..
   cWMMMMMMMMMMMNxc'.                ##########
    .0MMMMMMMMMMMMMMMMWc            #+#    #+#
      ;0MMMMMMMMMMMMMMMo.          +:+
        .dNMMMMMMMMMMMMo          +#++:++#+
           'oOWMMMMMMMMo                +:+
               .,cdkO0K;        :+:    :+:
                                :::::::+:
                      Metasploit

       =[ metasploit v5.0.41-dev                          ]
+ -- --=[ 1914 exploits - 1074 auxiliary - 330 post       ]
+ -- --=[ 556 payloads - 45 encoders - 10 nops            ]
+ -- --=[ 4 evasion                                       ]
```



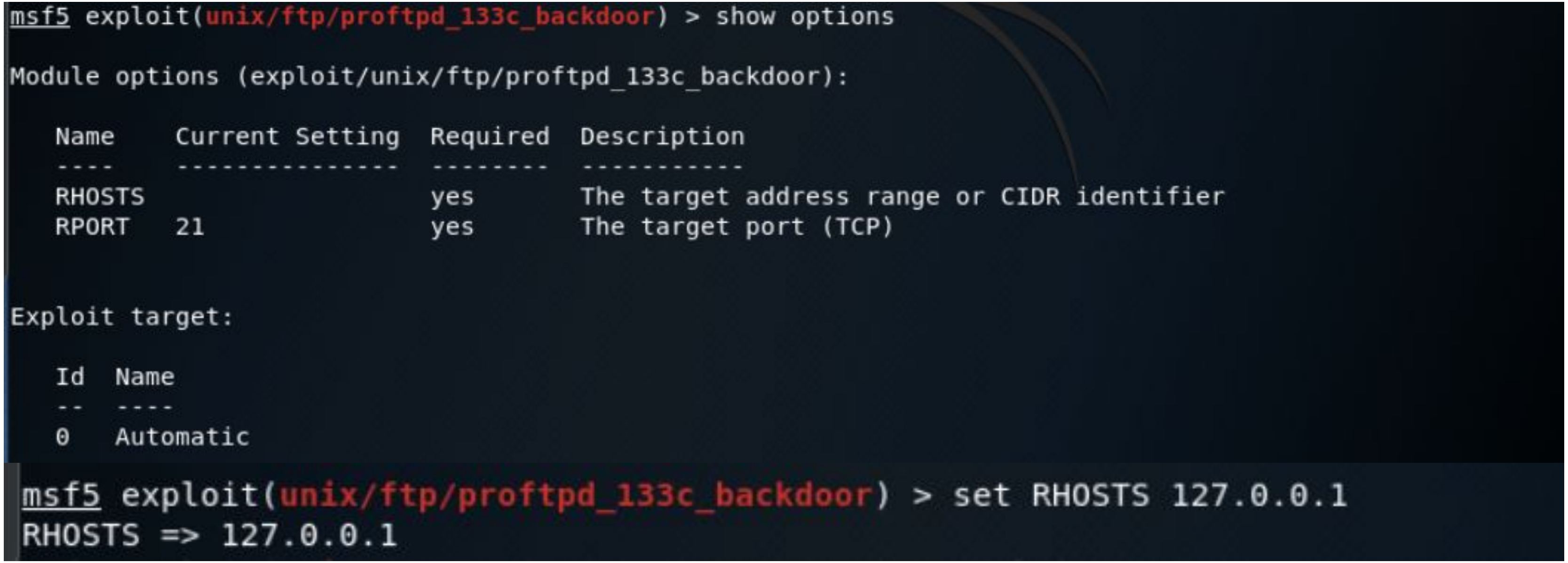
```
msf5 > search proftpd

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

   #  Name                                         Disclosure Date  Rank       Check  Description
   -  ----                                         ---------------  ----       -----  -----------
   0  exploit/freebsd/ftp/proftp_telnet_iac        2010-11-01       great      Yes    ProFTPD 1.3.2rc3 - 1
.3.3b Telnet IAC Buffer Overflow (FreeBSD)
   1  exploit/linux/ftp/proftp_sreplace            2006-11-26       great      Yes    ProFTPD 1.2 - 1.3.0
sreplace Buffer Overflow (Linux)
   2  exploit/linux/ftp/proftp_telnet_iac          2010-11-01       great      Yes    ProFTPD 1.3.2rc3 - 1
.3.3b Telnet IAC Buffer Overflow (Linux)
   3  exploit/linux/misc/netsupport_manager_agent  2011-01-08       average    No     NetSupport Manager A
gent Remote Buffer Overflow
   4  exploit/unix/ftp/proftpd_133c_backdoor       2010-12-02       excellent  No     ProFTPD-1.3.3c Backd
oor Command Execution
   5  exploit/unix/ftp/proftpd_modcopy_exec        2015-04-22       excellent  Yes    ProFTPD 1.3.5 Mod_Co
py Command Execution


msf5 > use 4
msf5 exploit(unix/ftp/proftpd_133c_backdoor) > 
```

Using an exploit - Metasploit



```
msf5 exploit(unix/ftp/proftpd_133c_backdoor) > show options

Module options (exploit/unix/ftp/proftpd_133c_backdoor):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS                   yes       The target address range or CIDR identifier
   RPORT   21               yes       The target port (TCP)


Exploit target:

   Id  Name
   --  ----
   0   Automatic
```

```
msf5 exploit(unix/ftp/proftpd_133c_backdoor) > set RHOSTS 127.0.0.1
RHOSTS => 127.0.0.1
```

Metasploit Resources / Guides

- https://www.offensive-security.com/metasploit-unleashed/exploits/
- https://www.exploit-db.com/docs/english/44040-the-easiest-metasploit-guide-you%E2%80%99ll-ever-read.pdf
- https://www.sans.org/security-resources/sec560/misc_tools_sheet_v1.pdf

Activity - King of the Hill

King of the Hill Beta

Be the first to hack into a machine, and then retain your presence by patching vulnerabilities to stop your foes from taking your position!

Attack then defend!

1. Connect to Globalprotect
2. Go to https://server.uacyber.org:8006
3. Log in using number given redteam(1 - 20):bb123#123
4. Set Authentication Realm to: Proxmox VE authentication server
5. Login with user: root password: bb123#123
   a. Each Box will have a file /root/name.txt place your name into the file and stop others from over writing it!
   b. If the file doesn't exist create it!
   c. Note this will require a basic knowledge of Bash (https://www.guru99.com/linux-commands-cheat-sheet.html)

Activity - King of the Hill

Server Name	IP
Server 1	192.168.3.18
Server 2	192.168.3.19
Server 3	192.168.3.20
Server 4	192.168.3.21
Server 5	192.168.3.22
Server 6	192.168.3.23

Basic Steps

1. Nmap to find services
    a. If its unknown Google it, everything is vulnerable!
2. Identify a vulnerability
3. Exploit
4. Change directory into /root/ and edit name.txt
5. Keep other attackers off!