**Hackthebox Nibbles**

Session 10.10.10.75

I opened my terminal and ran my recon for the server

Nmap -T4 -p- -A 10.10.10.75

Starting Nmap 7.70 ( https://nmap.org ) at 2020-11-10 21:59 EST

Stats: 0:08:21 elapsed; 0 hosts completed (1 up), 1 undergoing Traceroute

Traceroute Timing: About 32.26% done; ETC: 22:08 (0:00:00 remaining)

Nmap scan report for 10.10.10.75

Host is up (0.11s latency).

Not shown: 65533 closed ports

PORT STATE SERVICE VERSION

22/tcp open ssh OpenSSH 7.2p2 Ubuntu 4ubuntu2.2 (Ubuntu Linux; protocol 2.0)

| ssh-hostkey:

| 2048 c4:f8:ad:e8:f8:04:77:de:cf:15:0d:63:0a:18:7e:49 (RSA)

| 256 22:8f:b1:97:bf:0f:17:08:fc:7e:2c:8f:e9:77:3a:48 (ECDSA)

|\_ 256 e6:ac:27:a3:b5:a9:f1:12:3c:34:a5:5d:5b:eb:3d:e9 (ED25519)

80/tcp open http Apache httpd 2.4.18 ((Ubuntu))

|\_http-server-header: Apache/2.4.18 (Ubuntu)

|\_http-title: Site doesn't have a title (text/html).

No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).

TCP/IP fingerprint:

OS:SCAN(V=7.70%E=4%D=11/10%OT=22%CT=1%CU=38470%PV=Y%DS=2%DC=T%G=Y%TM=5FAB55

OS:9A%P=x86\_64-pc-linux-gnu)SEQ(SP=FD%GCD=1%ISR=103%TI=Z%CI=I%II=I%TS=8)OPS

OS:(O1=M54DST11NW7%O2=M54DST11NW7%O3=M54DNNT11NW7%O4=M54DST11NW7%O5=M54DST1

OS:1NW7%O6=M54DST11)WIN(W1=7120%W2=7120%W3=7120%W4=7120%W5=7120%W6=7120)ECN

OS:(R=Y%DF=Y%T=40%W=7210%O=M54DNNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O%A=S+%F=A

OS:S%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T5(R

OS:=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F

OS:=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y%DF=N%

OS:T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=40%CD

OS:=S)

Network Distance: 2 hops

Service Info: OS: Linux; CPE: cpe:/o:linux:linux\_kernel

TRACEROUTE (using port 8080/tcp)

HOP RTT ADDRESS

1 114.69 ms 10.10.14.1

2 113.63 ms 10.10.10.75

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .

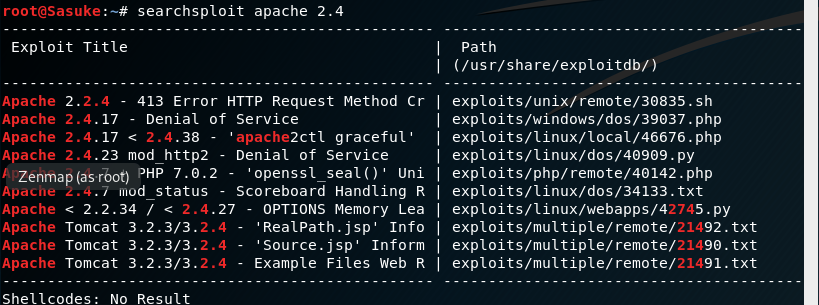
Nmap done: 1 IP address (1 host up) scanned in 505.19 seconds

I got to 10.10.10.75

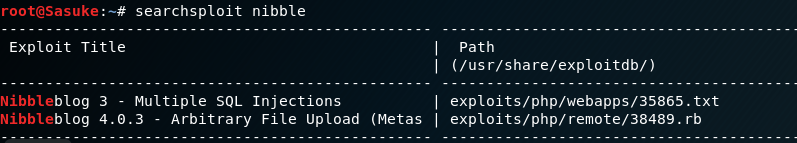
I right click the page source and it gives me a directory in the notes

/nibbleblog/

I opened the terminal and ran:

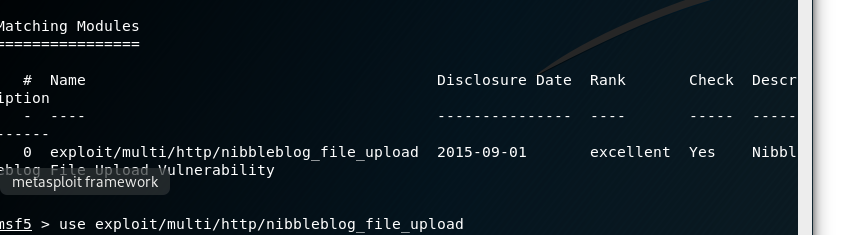


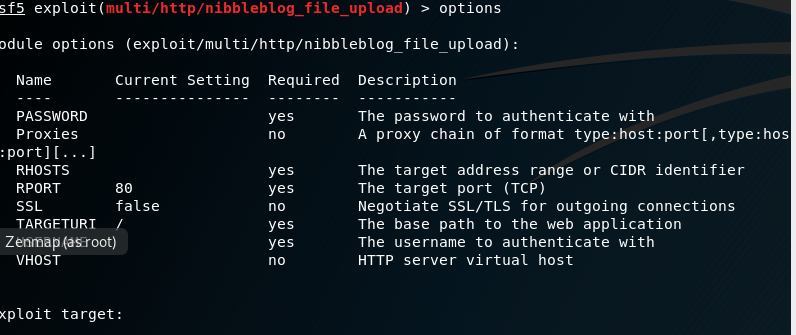
I didn’t really find much so then I searched searchsploit nibble



I boot up msfconsole

I search nibble





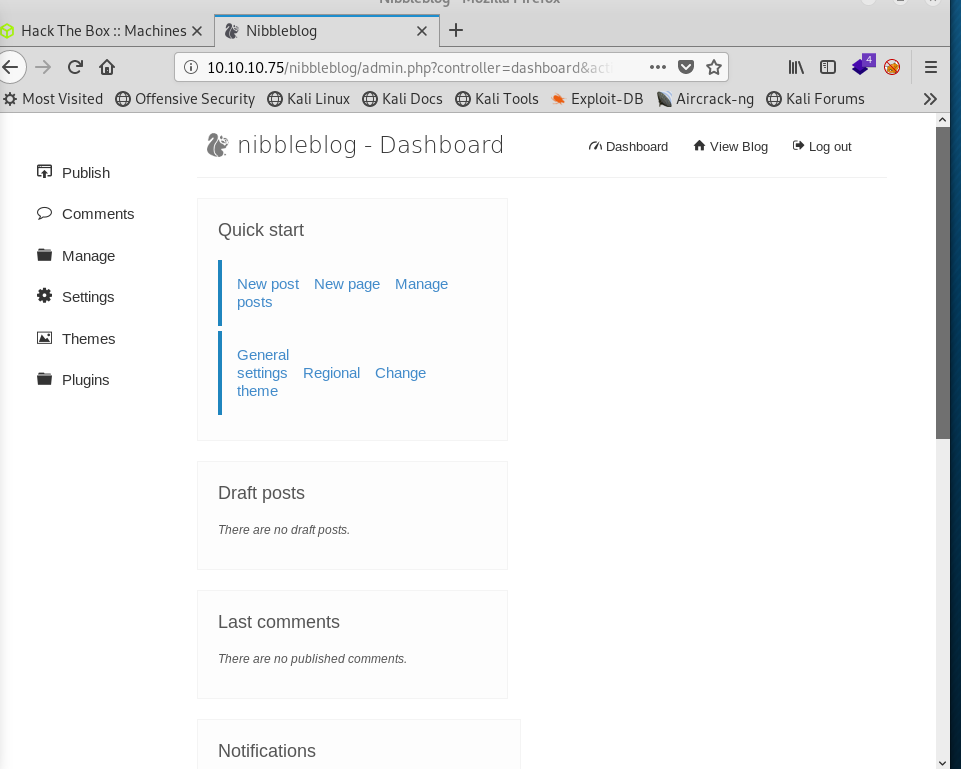
It shows in the description Authenticate, so we need credentials/log in page

I search 10.10.10.75/nibbleblog/admin.php

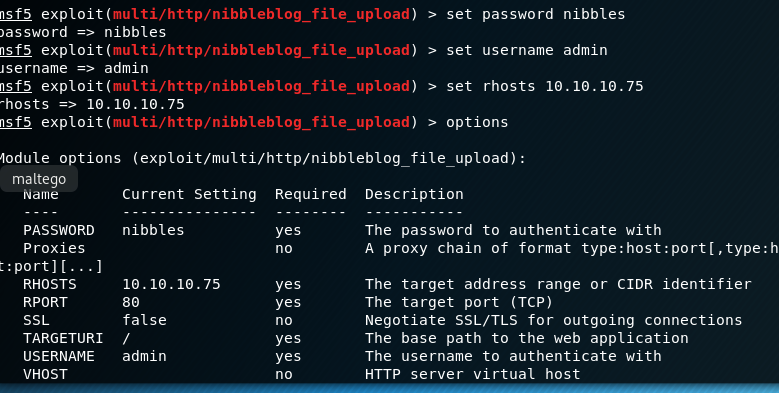
Given the title of the nibbleblog page,

The title is nibbles

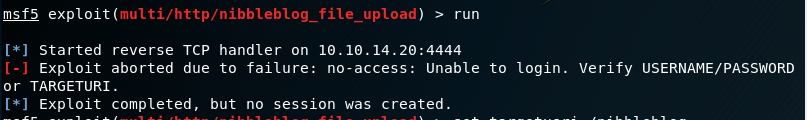
So I try some passwords like nibbles and username admin and it worked! I am in



I go back to metaspolit to set the payload correctly



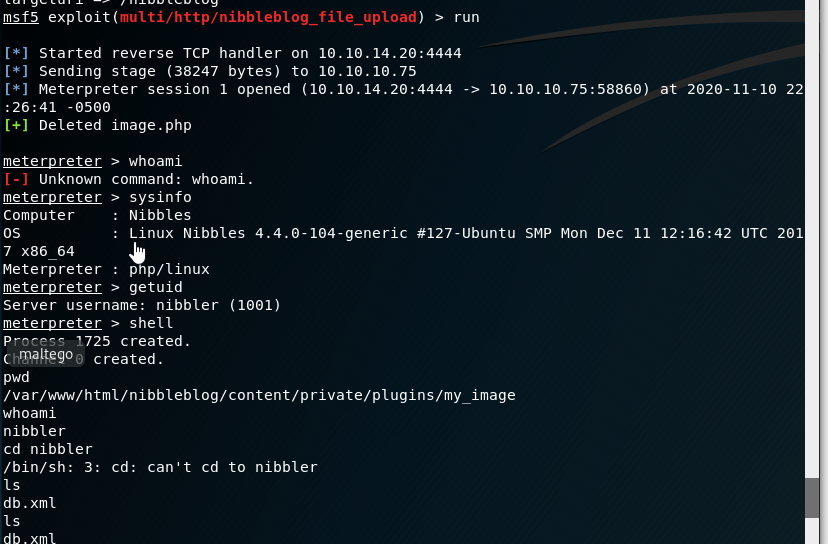
I am ready for my exploit



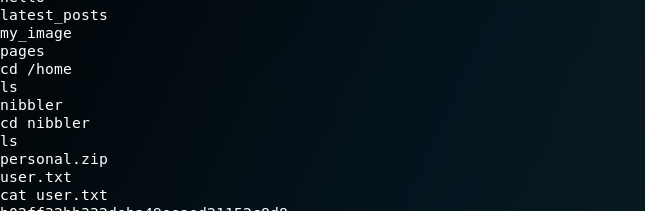
It failed,

I forgot to add the directory nibbleblog





Success! I am in



It eventually leads me to the Flag below