readme.md

Pentest 21 - NAS - 121 - 10.14.1.121

Scanning and Enumerating

Nmap

```
# Nmap 7.94 scan initiated Sun Sep  3 18:47:33 2023 as: nmap -vv --reason -Pn -T4 -s
Increasing send delay for 10.14.1.121 from 0 to 5 due to 219 out of 547 dropped prob
Increasing send delay for 10.14.1.121 from 5 to 10 due to 11 out of 27 dropped probe
Nmap scan report for 10.14.1.121
Host is up, received user-set (0.22s latency).
Scanned at 2023-09-03 18:47:33 EDT for 45s
Not shown: 997 closed tcp ports (reset)
PORT     STATE SERVICE REASON         VERSION
21/tcp   open  ftp     syn-ack ttl 63 ProFTPD 1.3.5b
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
80/tcp   open  http    syn-ack ttl 63 lighttpd 1.4.39
|_http-server-header: lighttpd/1.4.39
|_http-favicon: Unknown favicon MD5: B88C0EEDC72D3BF4E86C2AA0A6BA6F7B
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
| http-title: nas.local -
|_Requested resource was login.php
8080/tcp open  http    syn-ack ttl 63 lighttpd
|_http-server-header: webserv
| http-methods:
|_  Supported Methods: OPTIONS GET HEAD POST
|_http-title: Index of /
Device type: storage-misc|general purpose|firewall
Running (JUST GUESSING): FreeBSD 10.X|7.X|9.X|8.X|6.X (99%), IronPort AsyncOS 7.X (8
OS CPE: cpe:/a:nas4free:nas4free cpe:/o:freebsd:freebsd:10.2 cpe:/o:freebsd:freebsd:
Aggressive OS guesses: NAS4Free (FreeBSD 10.2-RELEASE) (99%), FreeBSD 7.0-RELEASE (9
No exact OS matches for host (If you know what OS is running on it, see https://nmap
TCP/IP fingerprint:
OS:SCAN(V=7.94%E=4%D=9/3%OT=21%CT=1%CU=42489%PV=Y%DS=2%DC=I%G=Y%TM=64F50D32
OS:%P=x86_64-pc-linux-gnu)SEQ(SP=102%GCD=1%ISR=106%II=I%TS=22)SEQ(SP=103%GC
OS:D=1%ISR=108%II=I%TS=21)SEQ(SP=103%GCD=1%ISR=109%II=I%TS=21)SEQ(SP=105%GC
OS:D=1%ISR=10C%II=I%TS=21)SEQ(SP=106%GCD=1%ISR=10E%II=I%TS=21)OPS(O1=M5B4NW
OS:9ST11%O2=M578NW9ST11%O3=M280NW9NNT11%O4=M5B4NW9ST11%O5=M218NW9ST11%O6=M1
```

```
OS:09ST11)WIN(W1=FFFF%W2=FFFF%W3=FFFF%W4=FFFF%W5=FFFF%W6=FFFF)ECN(R=Y%DF=N%
OS:T=40%W=FFFF%O=M5B4NW9SLL%CC=N%Q=)T1(R=Y%DF=N%T=40%S=O%A=S+%F=AS%RD=0%Q=)
OS:T2(R=N)T3(R=N)T4(R=N)T5(R=Y%DF=N%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=
OS:N)T7(R=N)U1(R=Y%DF=N%T=40%IPL=38%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)
OS:IE(R=Y%DFI=S%T=40%CD=S)

Uptime guess: 0.000 days (since Sun Sep  3 18:48:08 2023)
Network Distance: 2 hops
TCP Sequence Prediction: Difficulty=259 (Good luck!)
IP ID Sequence Generation: Busy server or unknown class
Service Info: OS: Unix

TRACEROUTE
HOP RTT       ADDRESS
1   218.46 ms 10.14.1.121

Read data files from: /usr/bin/../share/nmap
OS and Service detection performed. Please report any incorrect results at https://n
# Nmap done at Sun Sep  3 18:48:18 2023 -- 1 IP address (1 host up) scanned in 45.63
```

OS Type: `Linux 2.6.36 (98%)`

Port	Service	Protocol	Version
21	FTP	TCP	vsftpd 3.0.2
22	SSH	TCP	OpenSSH 7.4 (protocol 2.0)
80	HTTP	TCP	Apache httpd 2.4.6 ((CentOS) PHP/7.4.30)
8080	HTTP	TCP	Apache httpd 2.4.6 ((CentOS) PHP/7.4.30)

Notable items:

Nikto

```
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          10.14.1.121
+ Target Hostname:    10.14.1.121
+ Target Port:        80
+ Start Time:         2023-09-03 18:48:19 (GMT-4)
---------------------------------------------------------------------------
+ Server: lighttpd/1.4.39
+ /: Retrieved x-powered-by header: PHP/7.0.8.
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://devel
```

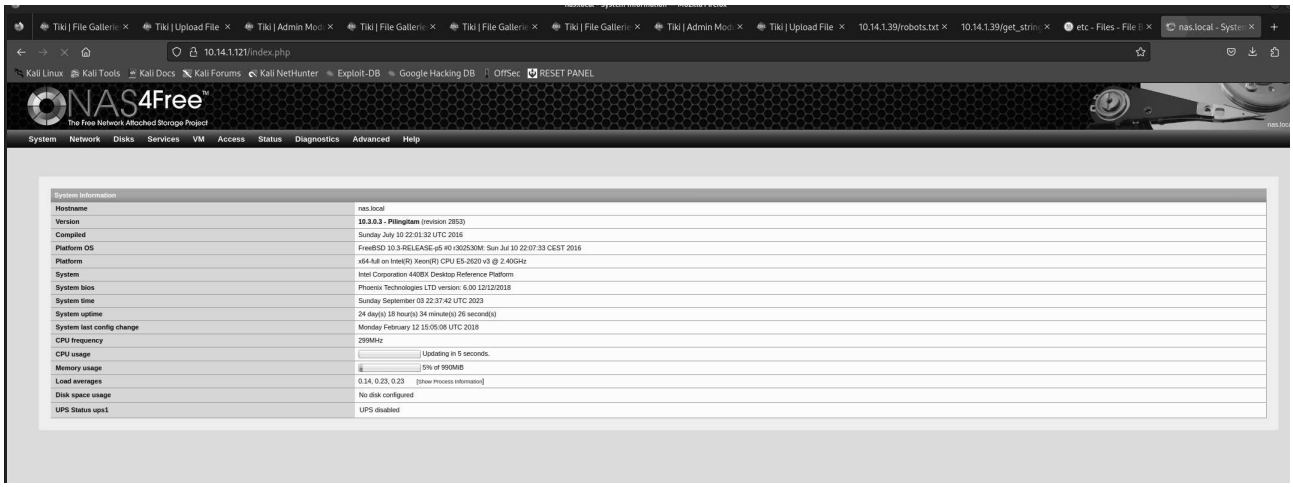
```
+ /: The X-Content-Type-Options header is not set. This could allow the user agent t
+ /: Cookie PHPSESSID created without the httponly flag. See: https://developer.mozi
+ Root page / redirects to: login.php
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ /favicon.ico: identifies this app/server as: NAS4Free 9.0. See: https://en.wikiped
+ OPTIONS: Allowed HTTP Methods: OPTIONS, GET, HEAD, POST .
+ /.htpasswd: Contains authorization information.
+ /xmlrpc.php: xmlrpc.php was found.
+ /login.php: Admin login page/section found.
+ 7729 requests: 0 error(s) and 9 item(s) reported on remote host
+ End Time:           2023-09-03 19:11:40 (GMT-4) (1401 seconds)
---------------------------------------------------------------------------
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          10.14.1.121
+ Target Hostname:    10.14.1.121
+ Target Port:        8080
+ Start Time:         2023-09-03 18:48:19 (GMT-4)
---------------------------------------------------------------------------
+ Server: webserv
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://devel
+ /: The X-Content-Type-Options header is not set. This could allow the user agent t
+ /: Directory indexing found.
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ .: Directory indexing found.
+ OPTIONS: Allowed HTTP Methods: OPTIONS, GET, HEAD, POST .
+ /./: Directory indexing found.
+ /./: Appending '/./' to a directory allows indexing.
+ //: Directory indexing found.
+ //: Apache on Red Hat Linux release 9 reveals the root directory listing by defaul
+ /%2e/: Directory indexing found.
+ /%2e/: Weblogic allows source code or directory listing, upgrade to v6.0 SP1 or hi
+ /%2f/: Directory indexing found.
+ /%2f/: Weblogic allows source code or directory listing, upgrade to v6.0 SP1 or hi
+ ///: Directory indexing found.
+ /?PageServices: The remote server may allow directory listings through Web Publish
+ /?wp-cs-dump: The remote server may allow directory listings through Web Publisher
+ ////////////////////////////////////////////////////////////////////////////////
+ ////////////////////////////////////////////////////////////////////////////////
+ /#wp-config.php#: #wp-config.php# file found. This file contains the credentials.
+ 7729 requests: 0 error(s) and 19 item(s) reported on remote host
+ End Time:           2023-09-03 19:11:14 (GMT-4) (1375 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

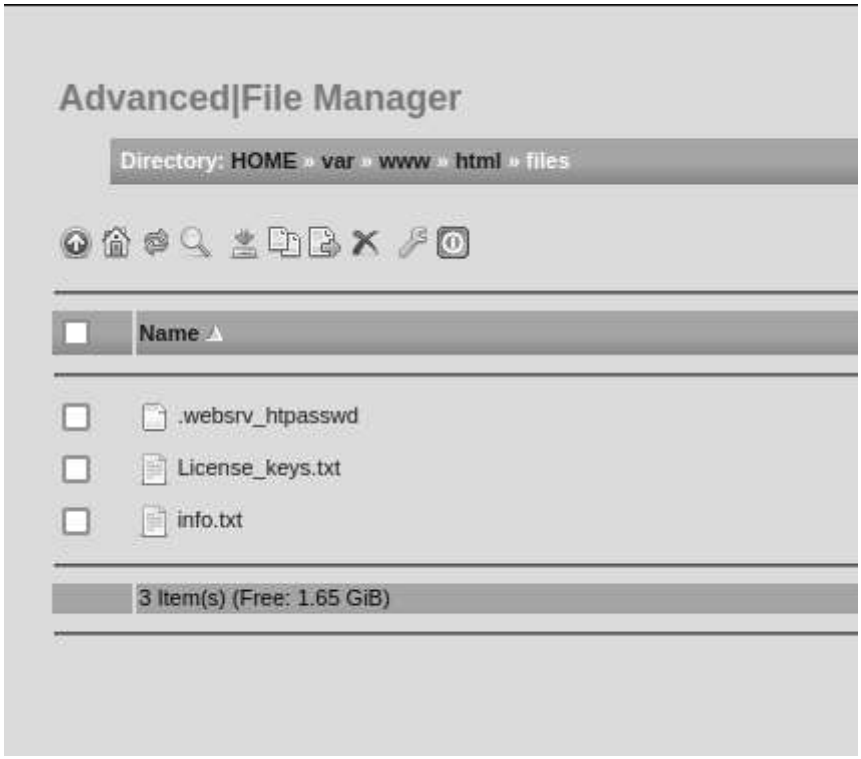
Exploitation

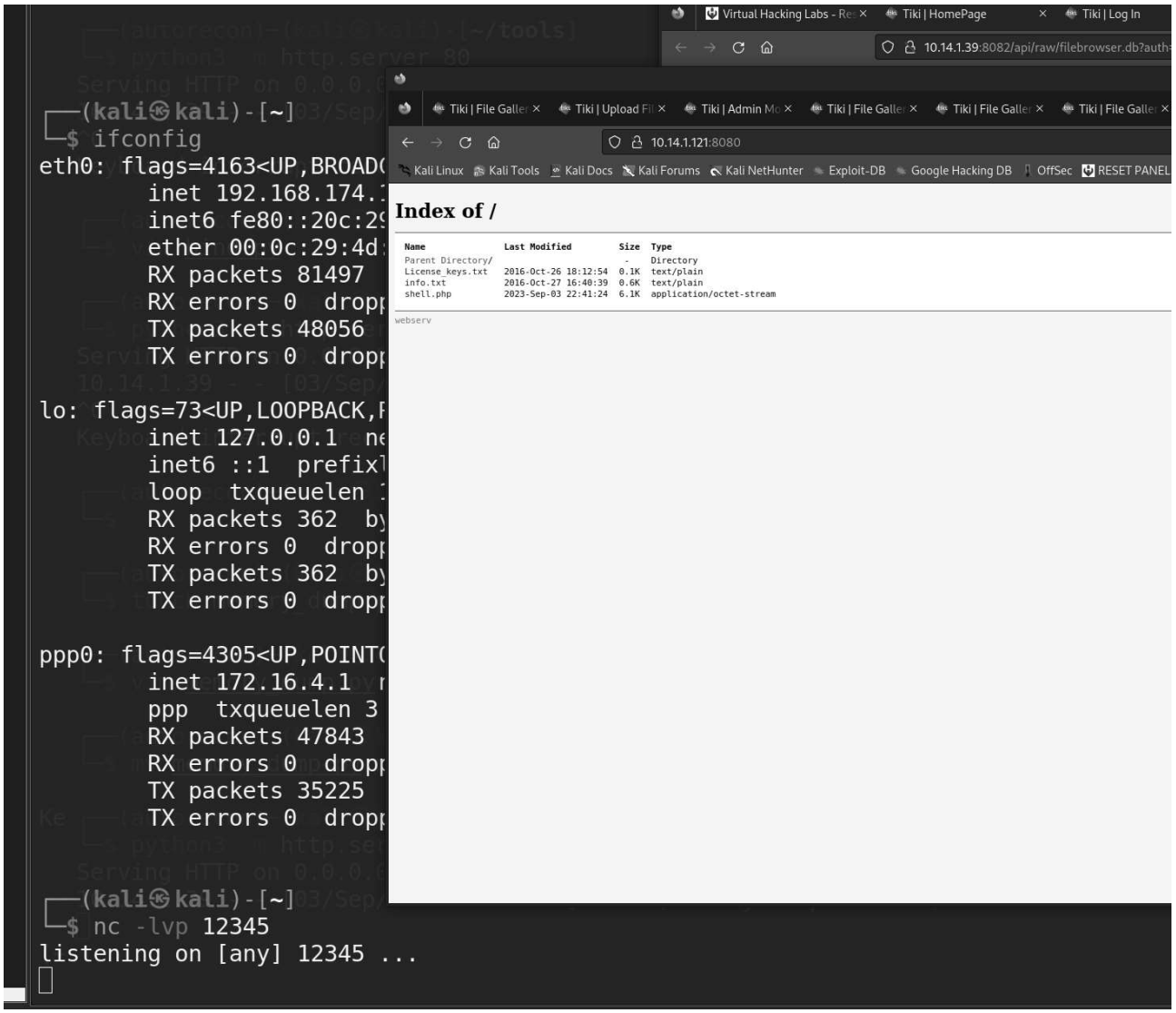
User	Pass
admin	nas4free123

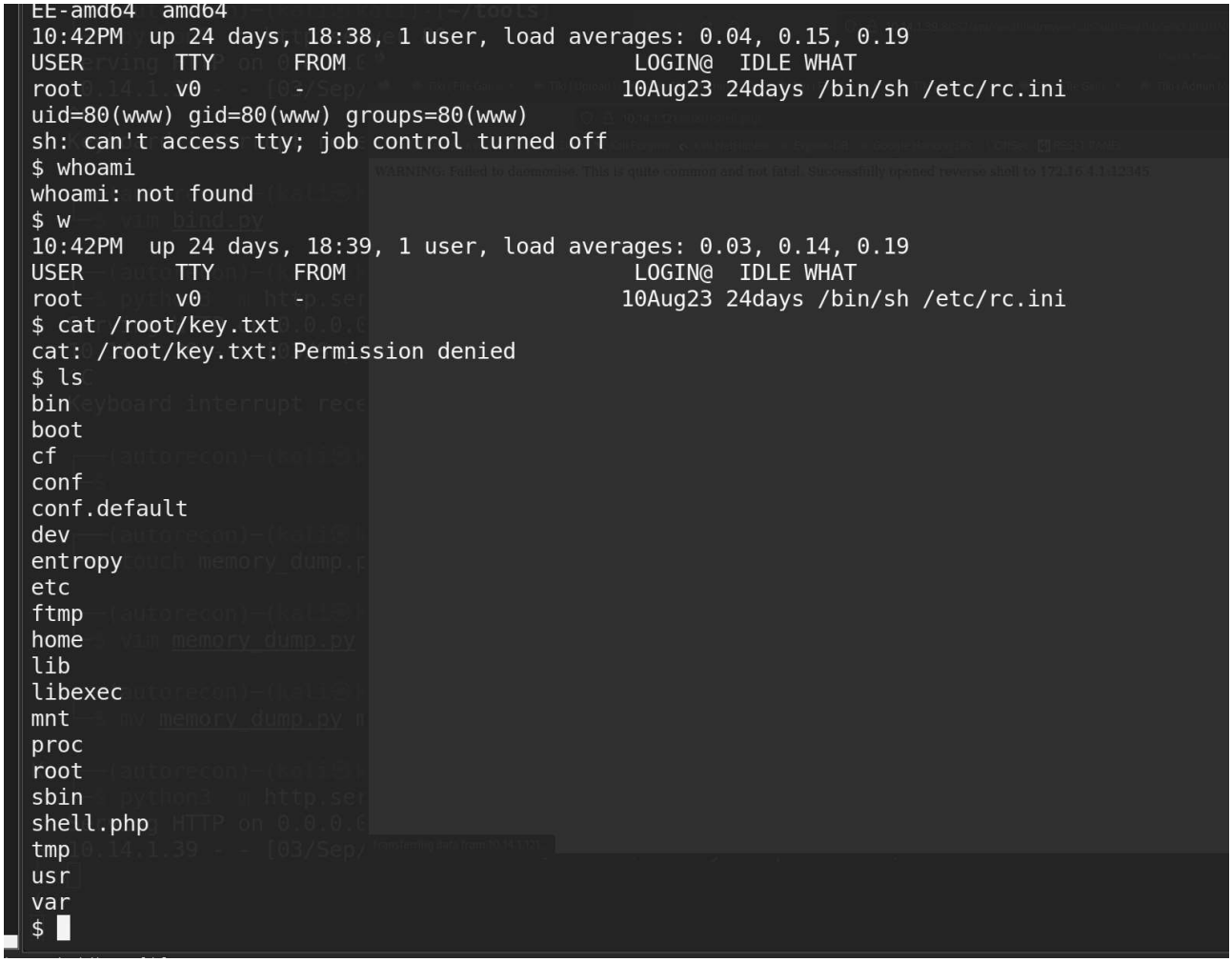
Initial Access

I already had the password from Anthony, which was `admin:nas4free123` . Once I connected, I poked around the browser, finding a file uploader AND editor.




Advanced|File Manager
Directory: HOME » var » www » html » files
Name
.websrv_htpasswd
License_keys.txt
info.txt
3 Item(s) (Free: 1.65 GiB)

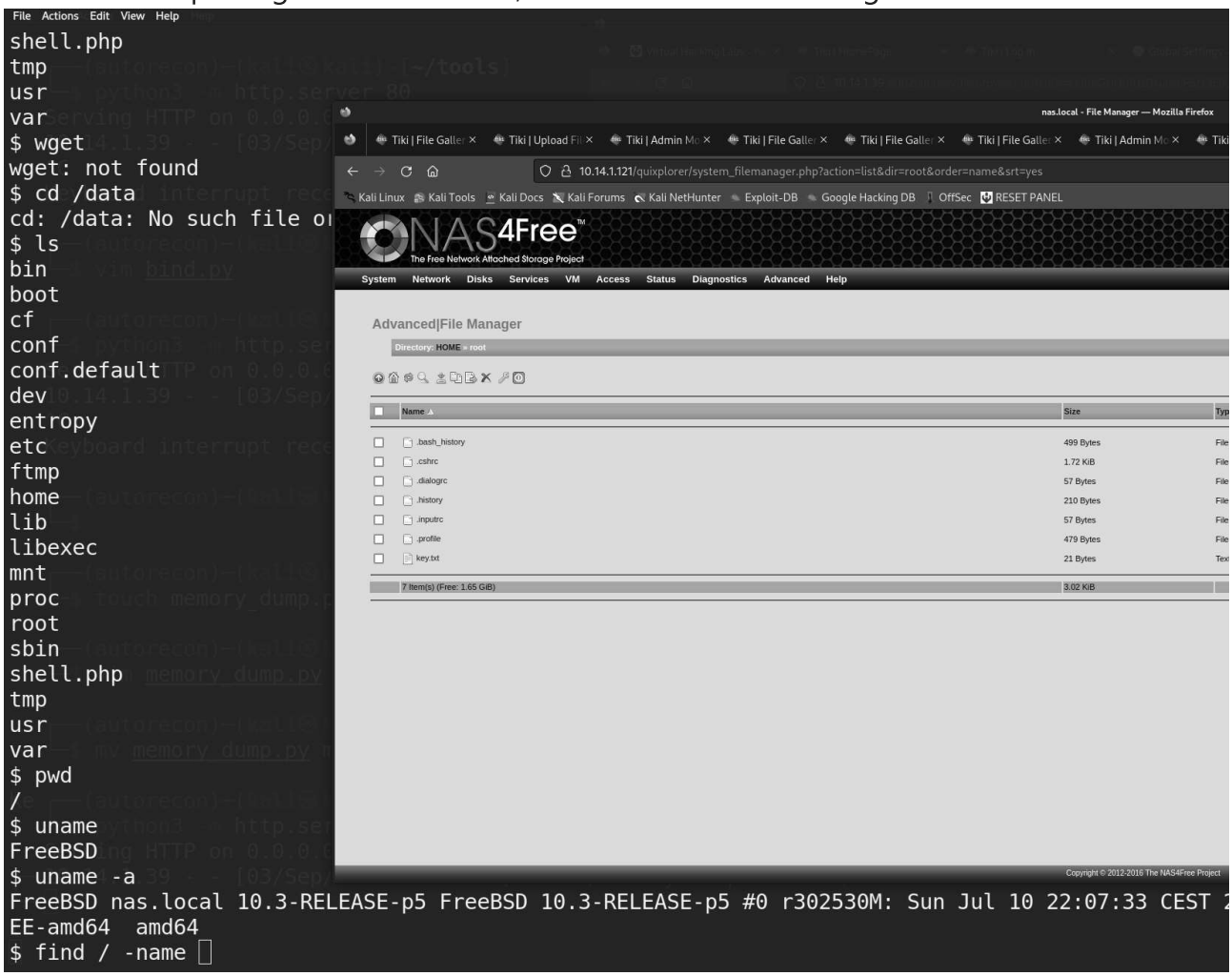

(kali㉿kali)-[~]
$ ifconfig
eth0: flags=4163<UP,BROADC
inet 192.168.174.1
inet6 fe80::20c:29
ether 00:0c:29:4d:
RX packets 81497
RX errors 0 dropp
TX packets 48056
TX errors 0 dropp
lo: flags=73<UP,LOOPBACK,R
inet 127.0.0.1 ne
inet6 ::1 prefixl
loop txqueuelen 1
RX packets 362 by
RX errors 0 dropp
TX packets 362 by
TX errors 0 dropp
ppp0: flags=4305<UP,POINTO
inet 172.16.4.1
ppp txqueuelen 3
RX packets 47843
RX errors 0 dropp
TX packets 35225
TX errors 0 dropp
(kali㉿kali)-[~]
$ nc -lvp 12345
listening on [any] 12345 ...
Virtual Hacking Labs - Re
Tiki | HomePage
Tiki | Log In
10.14.1.39:8082/api/raw/filebrowser.db?auth
Tiki | File Galler
Tiki | Upload Fil
Tiki | Admin Mo
10.14.1.121:8080
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
RESET PANEL
Index of /
Name
Last Modified
Size
Type
Parent Directory/
-
Directory
License_keys.txt
2016-Oct-26 18:12:54
0.1K
text/plain
info.txt
2016-Oct-27 16:40:39
0.6K
text/plain
shell.php
2023-Sep-03 22:41:24
6.1K
application/octet-stream
webserv



Additionally, based on my scanning results, I could see on 8080 there were files being enumerated in `/var/www/html`. I re-used my `shell.php` and triggered this - I got a shell!

Privilege Escalation

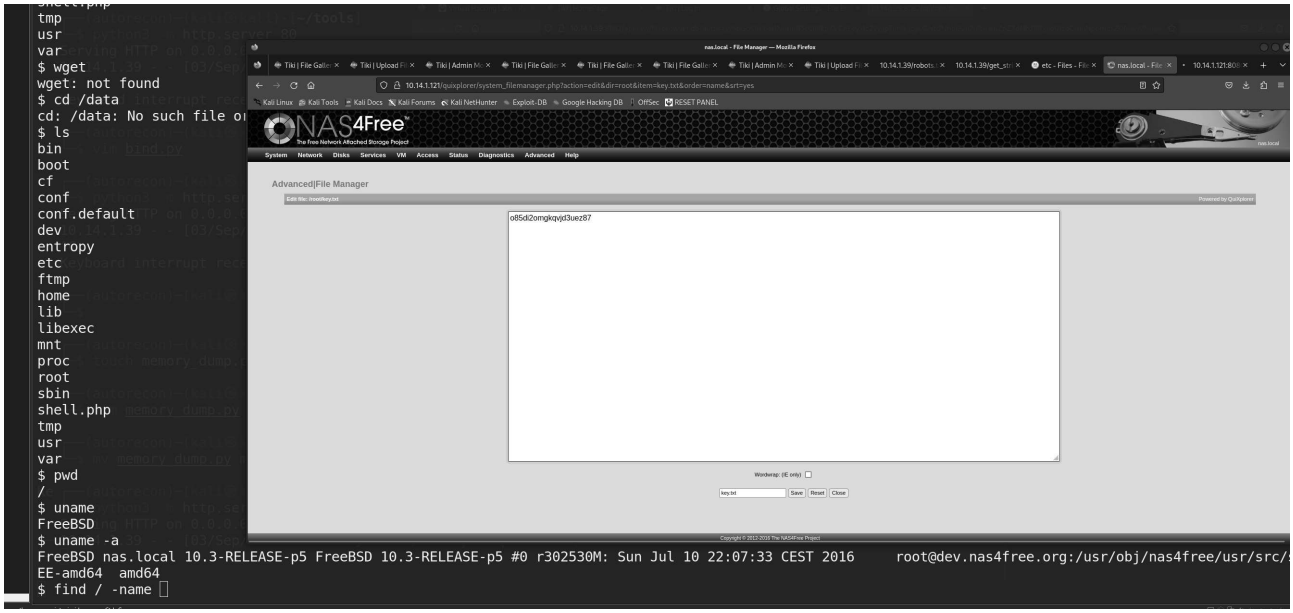
There was no privilege escalation here, but I was also not running as root in this case.



I didnt have uname, or wget, to enumerate. Going back and reading the notes, it seems like I just needed to get the `key.txt` ? What I noticed interesting, was that the filebrowser had the path in the URL that it was constructing like : `?`

`action=list&dir=var%2Fwww%2Fhtml%2Ffiles&order=name&srt=yes`

What if I just checked `/root?`



Success!

Identified Vulnerabilities

- CVE

Remediation

The main factor(s) leading to initial access included:

- The administrator password was saved in a previous scenario, allowing me access to the administrator panel.

The main factor(s) leading to privilege escalation here were:

- The web browser was running with root permissions, allowing me to enumerate the filesystem as root through the web interface.

Remediation steps then include:

- Run as a lesser privileged user
- Change the password