FORENSICS: SHARK ON THE WATCH BY Monhal

EASY

Scenario:

During a coffee break, your colleague, Boris, teased you and said that he managed to hack your computer earlier that day and planted a hidden file in it. Since you always lock your computer when you leave, you suspect he did it using a network-related vulnerability. Luckily, company policy includes network traffic monitoring. The NOC team agreed to provide you with access to the recorded traffic of your computer on that same morning.

Objectives:

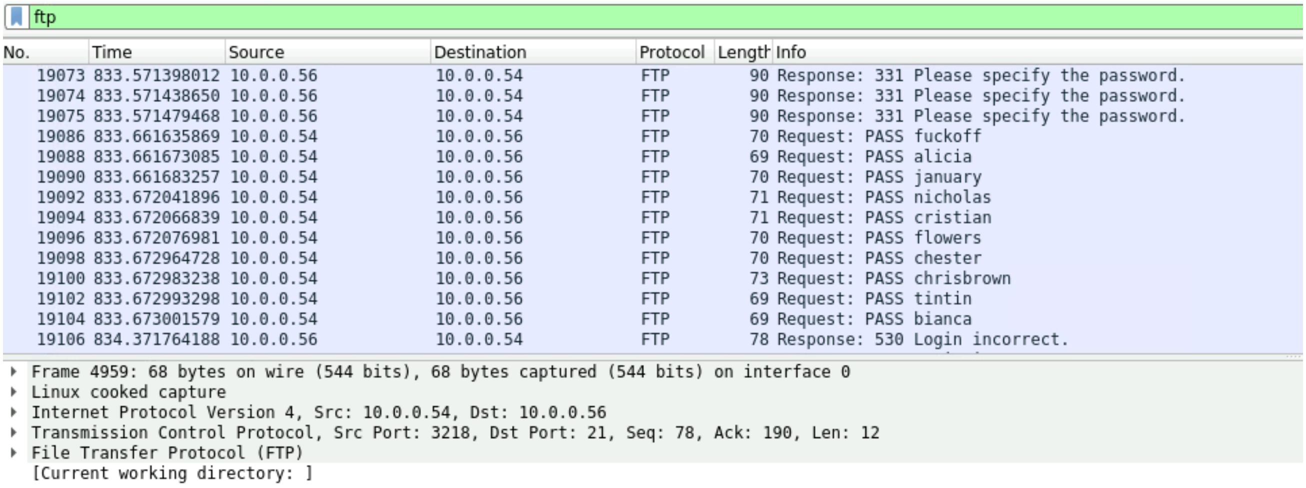
- Identify what Boris did to hack your computer.
- Find the content of the file that Boris planted on your computer.

Used tools:

WireShark

According to the scenario, a file transfer usually is done with FTP protocol, in wireshark a simple port filtering will display all the ftp traffic.

Figure 1 - ftp filter



```
ftp
```

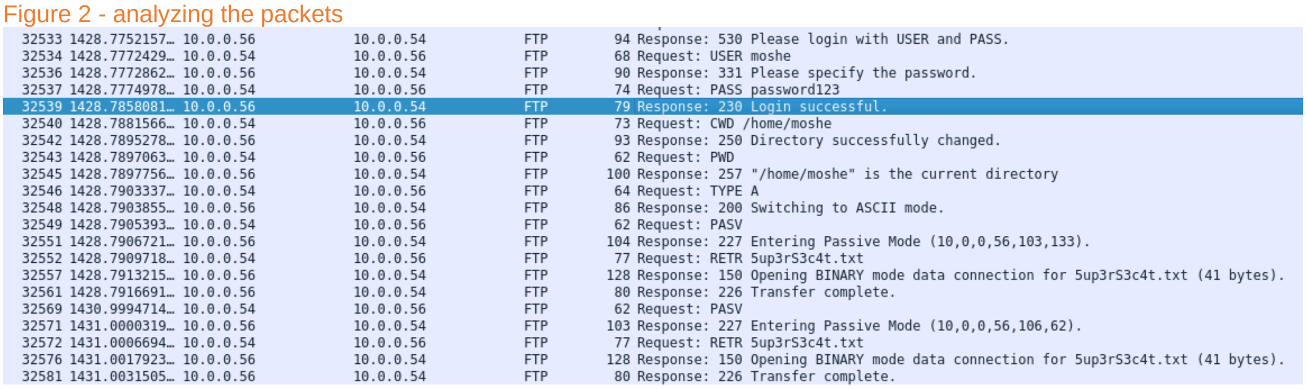
```
No.    Time         Source          Destination     Protocol Lengtł Info
 19073 833.571398012 10.0.0.56      10.0.0.54       FTP          90 Response: 331 Please specify the password.
 19074 833.571438650 10.0.0.56      10.0.0.54       FTP          90 Response: 331 Please specify the password.
 19075 833.571479468 10.0.0.56      10.0.0.54       FTP          90 Response: 331 Please specify the password.
 19086 833.661635869 10.0.0.54      10.0.0.56       FTP          70 Request: PASS fuckoff
 19088 833.661673085 10.0.0.54      10.0.0.56       FTP          69 Request: PASS alicia
 19090 833.661683257 10.0.0.54      10.0.0.56       FTP          70 Request: PASS january
 19092 833.672041896 10.0.0.54      10.0.0.56       FTP          71 Request: PASS nicholas
 19094 833.672066839 10.0.0.54      10.0.0.56       FTP          71 Request: PASS cristian
 19096 833.672076981 10.0.0.54      10.0.0.56       FTP          70 Request: PASS flowers
 19098 833.672964728 10.0.0.54      10.0.0.56       FTP          70 Request: PASS chester
 19100 833.672983238 10.0.0.54      10.0.0.56       FTP          73 Request: PASS chrisbrown
 19102 833.672993298 10.0.0.54      10.0.0.56       FTP          69 Request: PASS tintin
 19104 833.673001579 10.0.0.54      10.0.0.56       FTP          69 Request: PASS bianca
 19106 834.371764188 10.0.0.56      10.0.0.54       FTP          78 Response: 530 Login incorrect.
```

```
▸ Frame 4959: 68 bytes on wire (544 bits), 68 bytes captured (544 bits) on interface 0
▸ Linux cooked capture
▸ Internet Protocol Version 4, Src: 10.0.0.54, Dst: 10.0.0.56
▸ Transmission Control Protocol, Src Port: 3218, Dst Port: 21, Seq: 78, Ack: 190, Len: 12
▸ File Transfer Protocol (FTP)
  [Current working directory: ]
```

It is obvious that a brute-force attack has been occurred (notice all the password attempts and the login incorrect response [530]) – also we can see that the attacker IP is: 10.0.0.54 and the target IP is: 10.0.0.56

After further investigating of the packets, found the attacker activity on the target machine.

Figure 2 - analyzing the packets



```
 32533 1428.7752157… 10.0.0.56      10.0.0.54       FTP      94 Response: 530 Please login with USER and PASS.
 32534 1428.7772429… 10.0.0.54      10.0.0.56       FTP      68 Request: USER moshe
 32536 1428.7772862… 10.0.0.56      10.0.0.54       FTP      90 Response: 331 Please specify the password.
 32537 1428.7774978… 10.0.0.54      10.0.0.56       FTP      74 Request: PASS password123
 32539 1428.7858081… 10.0.0.56      10.0.0.54       FTP      79 Response: 230 Login successful.
 32540 1428.7881566… 10.0.0.54      10.0.0.56       FTP      73 Request: CWD /home/moshe
 32542 1428.7895278… 10.0.0.56      10.0.0.54       FTP      93 Response: 250 Directory successfully changed.
 32543 1428.7897063… 10.0.0.54      10.0.0.56       FTP      62 Request: PWD
 32545 1428.7897756… 10.0.0.56      10.0.0.54       FTP     100 Response: 257 "/home/moshe" is the current directory
 32546 1428.7903337… 10.0.0.54      10.0.0.56       FTP      64 Request: TYPE A
 32548 1428.7903855… 10.0.0.56      10.0.0.54       FTP      86 Response: 200 Switching to ASCII mode.
 32549 1428.7905393… 10.0.0.54      10.0.0.56       FTP      62 Request: PASV
 32551 1428.7906721… 10.0.0.56      10.0.0.54       FTP     104 Response: 227 Entering Passive Mode (10,0,0,56,103,133).
 32552 1428.7909718… 10.0.0.54      10.0.0.56       FTP      77 Request: RETR 5up3rS3c4t.txt
 32557 1428.7913215… 10.0.0.56      10.0.0.54       FTP     128 Response: 150 Opening BINARY mode data connection for 5up3rS3c4t.txt (41 bytes).
 32561 1428.7916691… 10.0.0.56      10.0.0.54       FTP      80 Response: 226 Transfer complete.
 32569 1430.9994714… 10.0.0.54      10.0.0.56       FTP      62 Request: PASV
 32571 1431.0000319… 10.0.0.56      10.0.0.54       FTP     103 Response: 227 Entering Passive Mode (10,0,0,56,106,62).
 32572 1431.0006694… 10.0.0.54      10.0.0.56       FTP      77 Request: RETR 5up3rS3c4t.txt
 32576 1431.0017923… 10.0.0.56      10.0.0.54       FTP     128 Response: 150 Opening BINARY mode data connection for 5up3rS3c4t.txt (41 bytes).
 32581 1431.0031505… 10.0.0.56      10.0.0.54       FTP      80 Response: 226 Transfer complete.
```

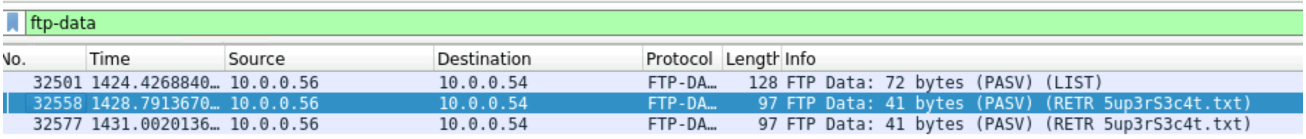
Notice the credentials ‘moshe:password123’, the attacker then transferred a file to the target machine called ‘5upers3cr4t.txt’ – a plain text file.

FORENSICS: SHARK ON THE WATCH ***BY Monhal***

EASY

In order to get the data inside the .txt file, the filer ftp-data is needed.

Figure 3 - ftp-data filter

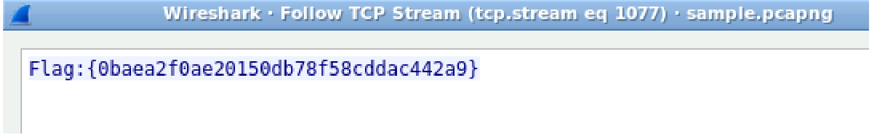


ftp-data

No.	Time	Source	Destination	Protocol	Length	Info
32501	1424.4268840…	10.0.0.56	10.0.0.54	FTP-DA…	128	FTP Data: 72 bytes (PASV) (LIST)
32558	1428.7913670…	10.0.0.56	10.0.0.54	FTP-DA…	97	FTP Data: 41 bytes (PASV) (RETR 5up3rS3c4t.txt)
32577	1431.0020136…	10.0.0.56	10.0.0.54	FTP-DA…	97	FTP Data: 41 bytes (PASV) (RETR 5up3rS3c4t.txt)

At ftp-data filter we can see 3 files, investigating the packets by right-clicking on the packet > follow > TCP stream will show the data inside the file which is the flag.

Figure 4 - Follow TCP stream result



Wireshark · Follow TCP Stream (tcp.stream eq 1077) · sample.pcapng

```
Flag:{0baea2f0ae20150db78f58cddac442a9}
```

CHALLENGE PWNED!

Please feel free to contact me on: **Monhalsarbouch@gmail.com**