Submission for Lab 0

**“beaconing.pcap” analysis**

1. Answer the following questions:

1. What is a \*.pcap file?

PCAP files are files created when capturing packets using a packet capture tool

1. What is a C&C beaconing?

C&C stands for Command-and-Control and beaconing is a communication from an infected machine to a C&C server on regular intervals.

2. Name 3 packet analysis tools:

Wireshark

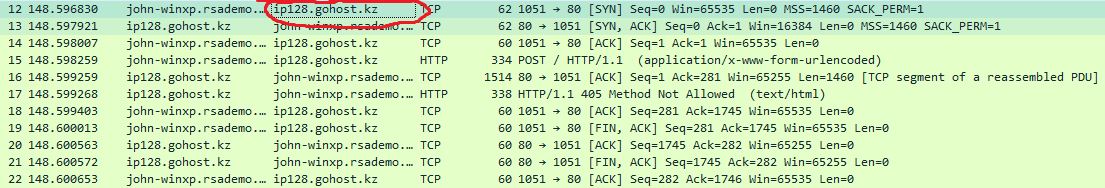
EtherApe

NetworkMiner

3. Download “beaconing.pcap” file from D2L. Open “beaconing.pcap” file using a packet analysis tool of your choice (or a combination of tools). Locate a C&C communication channel present in this PCAP. Answer following questions:

1. Name the beacon URL found in this capture. Attach proof

ip128.gohost.kz



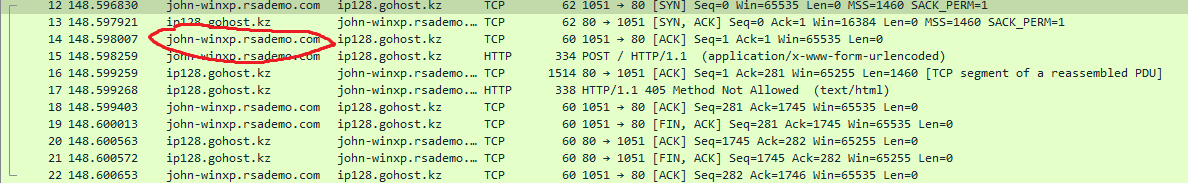
1. Please explain your URL choice and attach supporting proof

The host machine is regularly communicating to this server

(I don’t know what kind of proof to attach to this, I can see that it is regularly communicating to this server but I cant accurately display this with a screenshot)

1. What is the hostname of the traffic sending machine? Attach proof

John-winxp.rsademo.com

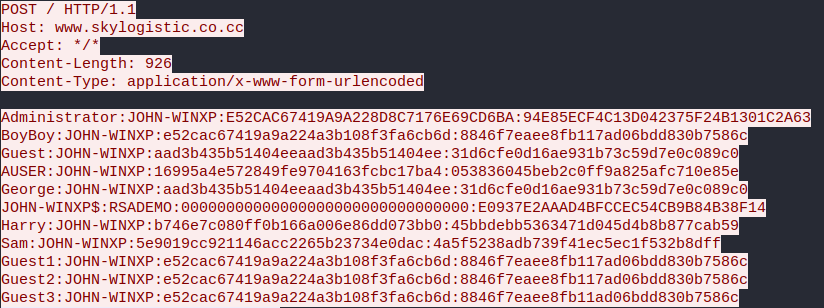


1. What is the destination country for the “malicious traffic”? Attach proof

Kazakhstan

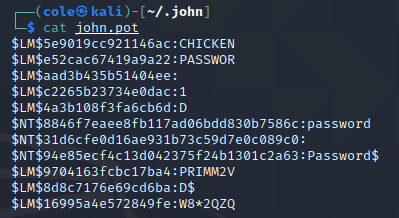


1. Locate any user accounts details in the capture. Attach proof



1. Recover plain-text passwords associated with these user accounts? Attach proof

These are the passwords I found using john the ripper, I know its not all of them but I let john run for ~20 hours and these are what it found



**“Bob-PC-EncryptedZip.pcap” analysis**

1. Answer the following question:

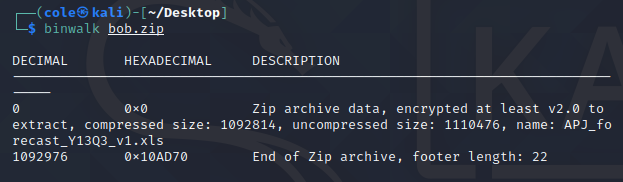
1. What is FTP protocol?

File Transfer Protocol, it transfers files over the network

2. Download “Bob-PC-EncryptedZip.pcap” file from D2L. Open “Bob-PC-EncryptedZip.pcap” file using a packet analysis tool of your choice (or a combination of tools).

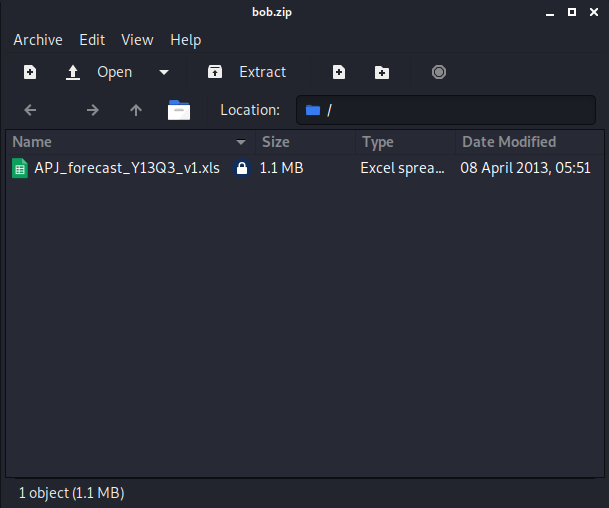
3. Extract a file from FTP session found in this capture. What is this file? Attach proof

The file is a ZIP file I named bob.zip

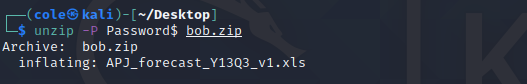


4. Open the file. What is inside of it? Attach proof

Inside the file is a spreadsheet document called APJ\_forecast\_Y13Q3\_v1.xls

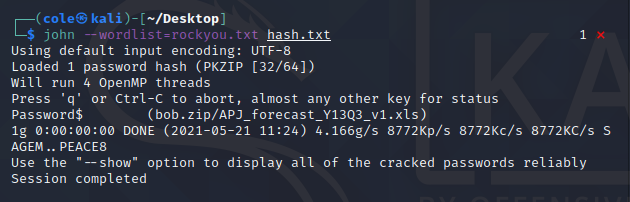


5. Extract the internal file. Attach proof



6. Explain password recovery process. Attach proof

I ran the command zip2john to create a hash which I saved under hash.txt, which when run with the john command using rockyou.txt I found the password of the zip file to be Password$



7. What is the extracted file? Attach proof

It appears to be a PE32 executable, and not actually a spreadsheet as it seemed to be

