

Lab 0:

Network Fundamentals Review

ITSC 206: Advanced Networking for Offensive

and Defensive Environments

Table of Contents

[Lab Outcomes 3](#_Toc71486140)

[Files/Downloads 3](#_Toc71486141)

[Introduction 3](#_Toc71486142)

[“beaconing.pcap” analysis 3](#_Toc71486143)

[1. Answer the following questions: 3](#_Toc71486144)

[a. What is a \*.pcap file? *(1 mark)* 3](#_Toc71486145)

[b. What is a C&C beaconing? *(1 mark)* 3](#_Toc71486146)

[2. Name 3 packet analysis tools: *(1 mark)* 3](#_Toc71486147)

[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: 3](#_Toc71486148)

[a. Name the beacon URL found in this capture. Attach proof *(1 mark)* 3](#_Toc71486149)

[b. Please explain your URL choice and attach supporting proof *(1 mark)* 4](#_Toc71486150)

[c. What is the hostname of the traffic sending machine? Attach proof *(1 mark)* 4](#_Toc71486151)

[d. What is the destination country for the “malicious traffic”? Attach proof *(1 mark)* 4](#_Toc71486152)

[e. Locate any user account details in the capture. Attach proof *(1 mark)* 4](#_Toc71486153)

[f. Recover plain-text passwords associated with these user accounts? Attach proof *(1 mark)* 4](#_Toc71486154)

[“Bob-PC-EncryptedZip.pcap” analysis 4](#_Toc71486155)

[1. Answer the following question: 4](#_Toc71486156)

[a. What is FTP protocol? *(1 mark)* 4](#_Toc71486157)

[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). 4](#_Toc71486158)

[3. Extract a file from FTP session found in this capture. What is this file? Attach proof *(1 mark)* 5](#_Toc71486159)

[4. Open the file. What is inside it? Attach proof *(1 mark)* 5](#_Toc71486160)

[5. Extract the internal file. Attach proof *(1 mark)* 5](#_Toc71486161)

[6. Explain password recovery process. Attach proof *(1 mark)* 5](#_Toc71486162)

[7. What is the extracted file? Attach proof (1 mark) 5](#_Toc71486163)

Lab Outcomes

* Review general network analysis skills.

Files/Downloads

* beaconing.pcap – D2L
* Bob-PC-EncryptedZip.pcap – D2L

Introduction

This lab reviews your practical packet and protocol analysis skills. You will use knowledge acquired previously to solve multiple challenges throughout this exercise.

“beaconing.pcap” analysis

1. Answer the following questions:
   1. What is a \*.pcap file? *(1 mark)*
   2. What is a C&C beaconing? *(1 mark)*
2. Name 3 packet analysis tools: *(1 mark)*
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 *(1 mark)*
   2. Please explain your URL choice and attach supporting proof *(1 mark)*
   3. What is the hostname of the traffic sending machine? Attach proof *(1 mark)*
   4. What is the destination country for the “malicious traffic”? Attach proof *(1 mark)*
   5. Locate any user account details in the capture. Attach proof *(1 mark)*
   6. Recover plain-text passwords associated with these user accounts? Attach proof *(1 mark)*

“Bob-PC-EncryptedZip.pcap” analysis

1. Answer the following question:
   1. What is FTP protocol? *(1 mark)*
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 *(1 mark)*
4. Open the file. What is inside it? Attach proof *(1 mark)*
5. Extract the internal file. Attach proof *(1 mark)*
6. Explain password recovery process. Attach proof *(1 mark)*
7. What is the extracted file? Attach proof (1 mark)