COMPSCI 215 S1 C
Assignment Two

The material submitted for this assignment must be your own work. Think carefully about any problems you come across, and try to solve them yourself before you ask anyone else for help. Under no circumstances should you work together with another student to solve problems posed in this assignment. There are

Assessment

Due: 00:00hrs 2nd June 2013

Total Points: 120

Worth: 10%

Questions

Part 1: basic networking

- Question 1 [10]: DHCP: Search the first few packets of the capture without filtering. Find the DHCP handshake.
    - a) What is the transaction id? [4]
    - b) What is the assigned IP address? [2]
    - c) What is the address of the next-hop? [3]
    - d) What are the DNS servers? [1,1]
- Question 2 [10]: DNS (filter "dns") Look at packet 50.
    - a) What is the query being made? [2]
    - b) What host the query sent to? [2]
    - c) Filter the UDP stream, and look at the response.
    - d) What is the IP address of the answer? [2]
    - e) Which servers (IP) hold the ORIGINAL record of the DNS entry? [4]
- Question 3 [10]: HTTP (filter "tcp.stream eq 2")
    - a) What program was the download made with? [2]
    - b) What was the request URL? [2]
    - c) How large was the file? [2]
    - d) How long did the entire download take (include get)? [4]
- Question 4 [10]: ICMP / Traceroute (filter "ICMP")
    - a) How do you know which ICMP packets are part of the traceroute? [2]
    - b) What was the host I was tracing? [2]
    - c) How long did the traceroute take? [4]
    - d) How many hops did it take? [2]

Part 2: W32/Sdbot malware, forensics and traffic analysis. W32/Sdbot is a minor piece of malware that uses standard unencrypted HTTP traffic. Most of the traffic is W32/Sdbot, but there is some background chatter.

Question 5 [20]: Traffic analysis

a) what is the name of the server program the bot is trying to contact? [10]

b) where do most of the infected seem servers to be, why? [10]

Question 6 [20]: Responses

a) how many requests does it make? [4]

b) how many distinct servers does it attempt to contact? [4]

c) how many successful responses are there, and whats the cause? [12]

Part 3: Broken downloader! You work for a small search engine company, and the person who you've replaced has removed all the header information the download bot, replacing them with #defime macros in the code... You have to re-configure the DNS resolution and HTTP download functions.

Question 7 [20]: DNS, In the function resolve_name

a) Correctly form the DNS header. [14]

b) Correctly get the first response address and convert it to xxx.xxx.xxx.xxx format. [6]

Thankfully, the query formation part isn't broken.

Question 8 [20]: HTTP, In the function retrieve_data

a) Correctly form the HTTP request header string. [18]

Only accept unencoded data and accept all MIME types, also identify the program as "upi001-dlbot/1.0"

b) Correctly find the end of the HTTP response header string [2]

Submission

A new submissions system (dropbox) is being put in place beginning this term. Instructions will be posted shortly indicating how you should access it.

Submit your solutions to questions 1 to 6 as a text file, clearly indicating the number for each of your answers. Also submit the file dlbot.c with your alterations.