COMS 4180 Network Security Spring 2018 Written Assignment 3

Due Wednesday April 4, 2018, 10:00pm Eastern time.

- This assignment is to be done individually.
- NO LATE SUBMISSIONS WILL BE ACCEPTED.

Submission Instructions

- Assignments will be submitted in Courseworks.
- Submit one file containing all of your answers. The file formats accepted are pdf, word (.docx, .doc) and plain text with a .txt extension.
- The file name will be <your uni>.<extension> example: jld2017.pdf
- Please put your name on the first line of the file.

50 points, 8 problems

1. 5 points
From the Verizon_rp_DBIR_2018 report,
Consider the various statistics in the report. Are humans a top vulnerability that is exploited in attacks? Justify your answer the data from the Verizon report.

2. 5 points
What does GMbot use to capture user login information and what types of applications were its target?

3. 5 points
What protocol did Angler use and how did this make it difficult for analysts to analyze the malware?

4. 10 points (5 points each)
Of the topologies listed in the Damballa whitepaper Botnet Communication Topologies,
(a) What topology makes a botnet easiest to disable if the master(s) are discovered and why?
(b) Which topology do you think makes a botnet the most difficult to disable and why?

Questions 5, 6 and 7 require reading the Symantec-istr-v21-2017 report.
5. 10 points total (2 points for each part)
a. What legitimate tool was used most by hackers in 2016?
b. What windows tool was used most by hackers?
c. What percent of email was spam in 2016?
d. What type of downloader was the most popular for delivering email threats in 2016? What type of delivery method was the most popular prior to 2016?
e. What percent of web sites tested contained vulnerabilities in 2016? Were most of these vulnerabilities critical?

6. 5 points
What did Shamoon do? What legitimate tools did it use?

7. 5 points
What is Mirai? What general type of device/equipment did it use for its attacks?

8. 5 points
Run nmap with the option(s) to obtain the most information against a machine you control (such as your laptop or VM). What operating system and open ports did nmap detect? Show the output of nmap in your answer.