Nick Weaver
Fall 2018

CS 161
Computer Security

Homework 5

Due: Monday, 3 December 2018, at 11:59pm

Instructions. This homework is due **Monday, 3 December 2018, at 11:59pm**. No late homeworks will be accepted unless you have prior accomodations from us. This assignment must be done on your own.

Create an EECS instructional class account if you have not already. To do so, visit https://inst.eecs.berkeley.edu/webacct/, click "Login using your Berkeley CalNet ID," then find the cs161 row and click "Get a new account." Be sure to take note of the account login and password, and log in to your instructional account.

Make sure you have a Gradescope account and are joined in this course. The homework *must* be submitted electronically via Gradescope (not by any other method). Your answer for each question, when submitted on Gradescope, should be a single file with each question's answer on a separate page.

Problem 1 *True/False* (12 points)

Answer True or False for each of the following questions. Explanations are not required.

(a) True or False: A virus is malware that propagates by copying itself into target systems, and a worm is malware that propagates by infecting other programs.

(b) True or False: Rootkits are often used to conceal other malware.

(c) Bob wants to prevent people from overwhelming his website, so he decides to implement proof-of-work. Let d be the number of days since January 1, 1900. The client must send $r, H(r||d)$ where r is some nonce chosen by the client. The hash must begin with 13 zero bits. If the nonce has been reused in the same day or if the hash does not begin with 13 zero bits, Bob's server ignores the request. True or False: This is a good proof-of-work scheme.

(d) True or False: A Distributed Denial of Service (DDoS) attack is executed by a botnet overwhelming the victim with large amounts of traffic coming from many sources.

(e) True or False: Tor defends against adversaries who can view all network traffic.

(f) True or False: A malicious middle relay (non-exit node) can read and modify your unencrypted traffic.

Problem 2 ***Detecting Worms*** **(15 points)**

Assume that you are working for a security company that has to monitor a network link for worm traffic. The link connects a large site with the rest of the Internet, and always has lots of traffic on it. Your company sells a monitoring box that can scan individual packets for fixed strings at very high speeds. Furthermore, the monitoring box can unencrypt traffic intended for the company.

(a) Suppose that after careful analysis you discover that a particular TCP-based worm that you need to protect against generates traffic that always contains a fixed 4-byte sequence. You program your company's specialized hardware to generate an alarm whenever it detects a packet containing this 4-byte pattern. Explain how this detector can exhibit false negatives.

(b) Propose an alternative architecture for your company's monitoring box that fixes the problem from part (a). Your alternative should not increase false positives by more than a modest amount. Does your revised approach completely eliminate false negatives? Explain why or why not.

(c) What could a worm author do to try to ensure that their worms do not have many fixed-byte sequences?

Problem 3 ***Email Denial-of-Service*** **(10 points)**

One day you try to email ten of your friends at Stanford your award-winning recipe for Big Game game-day cookies to their stanford.edu addresses. Unfortunately you typed two of their email addresses incorrectly so you received two failed-delivery notification (FDN) messages that include both the original text from the email you sent and copies of the attachment.

(a) Knowing this, how could you launch an amplified denial of service attack against some poor unsuspecting person via email?

(b) How could the developer of the Stanford mail server mitigate this issue?

Problem 4 ***Feedback*** **(0 points)**

Optionally, feel free to include feedback. Whats the single thing we could do to make the class better? Or, what did you find most difficult or confusing from lectures or the rest of class, and what would you like to see explained better?