CS 4760: Network Security Midterm, spring 2024

Name
Be sure to write your name and e-mail ID on top of this page.
If you are still writing when "pens down" is called, your exam will be ripped up and not graded. So please do that first. Sorry to have to be strict on this!
There are 6 pages to this exam. Once the exam starts, please make sure you have all the pages. Questions are worth different amounts of points.
Answers for the short-answer questions should not exceed about 20 words; if your answer is too long (say, more than 30 words), you will get a zero for that question!
This exam is CLOSED text book, closed-notes, closed-calculator, closed-cell phone, closed-computer, closed-neighbor, etc. Questions are worth different amounts, so be sure to look over all the questions and plan your time accordingly. Please sign the honor pledge below.

Firewalls so mighty,

Like a sieve, they filter all,

Safety's not absolute.

Page 2: Data Link Layer

1. [3 points] Briefly, how does a WiFi Pineapple work?

2. [3 points] *Briefly* explain how to execute a MITM (in-the-middle) attack using ARP spoofing. This question is focused on the MITM aspect; you don't need to explain the ARP spoofing aspect.

3. [3 points] *Briefly* explain what a tap/tun network interface is.

4. [3 points] MAC randomization was intended to prevent tracking. *Briefly* describe how trackers can get around MAC randomization.

Page 3: Network Layer

5. [3 points] *Briefly*, what is special about the 192.168.0.0/16 address range?

6. [3 points] *Briefly*, how does traceroute work?

7. [3 points] *Briefly,* give one pro and one con of using IPsec for your VPN (virtual private network) encryption.

8. [3 points] *Briefly,* other than executing commands like you did in HW P2 (Ping Commands), give two other uses of ICMP tunneling.

Page 4: Transport Layer

9. [3 points] *Briefly,* how does a SYN cookie work?

10. [3 points] *Briefly,* why does a TCP reset attack typically not work against a video streaming service?

11. [3 points] *Briefly*, what is a reverse shell?

12. [3 points] *Briefly,* what were the 4 steps in the Mitnick attack? You don't need to describe them beyond listing what they are.

Page 5: Packet Sniffing and Firewalls

13. [3 points] <i>Briefly</i> , what is the purpose of the port numbers in a TCP heade	13.	[3 poin	nts] <i>Brie</i> j	fly, what is t	he purpos	se of the po	ort numbers	in a TCI	header
--	-----	---------	--------------------	----------------	-----------	--------------	-------------	----------	--------

14. [3 points] *Briefly,* when a firewall is also performing NAT (network address translation), what values must it keep track of for each connection?

15. [3 points] List and *briefly* describe the three types of firewalls.

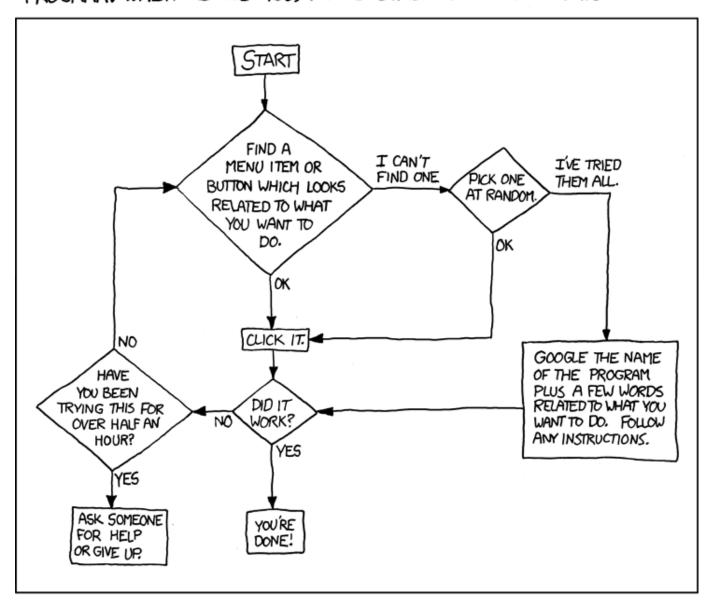
16. [3 points] *Briefly,* what is the biggest vulnerability to modern day firewalls?

Page 6: No questions here

This page unintentionally left unblank.

DEAR VARIOUS PARENTS, GRANDPARENTS, CO-WORKERS, AND OTHER "NOT COMPUTER PEOPLE."

WE DON'T MAGICALLY KNOW HOW TO DO EVERYTHING IN EVERY PROGRAM. WHEN WE HELP YOU, WE'RE USUALLY JUST DOING THIS:



PLEASE PRINT THIS FLOWCHART OUT AND TAPE IT NEAR YOUR SCREEN. CONGRATULATIONS; YOU'RE NOW THE LOCAL COMPUTER EXPERT!