Homework 3

CSE565 (B&C), Fall 2024, SUNY Buffalo. Due: Tue Nov 12th, 11:59PM EST.

Problems	1	2	3	4	Total
Max Score	15	5	10	10	
Your Score					

Requirements

- Save and submit your HW 2 submission to UB Learns (Brightspace) as a single typed PDF file. Name your file: Your Last Name Your First Name YourStudents ID Number Assignment Number. Example: **Doe John 55552222 HW2*3
- You should view your submission after you upload it to make sure that it is not corrupted or malformed. Submissions that are rotated, upside down, or that do not load will not receive credit. Illegible submissions may also lose credit depending on what can be read. You are responsible for making sure your submission went through successfully.
- The HW 3 deadline is **Tue Nov 12th, 11:59PM EST**. Only the most recent submission is kept on UB Learns (Brightspace). Late submissions are subject to following penalties: within 24 hours with 20 % penalty, 24~48 hours with a 40% penalty, or 48~72 hours with a 60% penalty. Submissions will close 72 hours after the deadline.

Question 1 (15 pts)

We learned three types of cache-poisoning attacks in class: ARP spoofing, BGP hijacking, and DNS poisoning. Answer the following questions

Q1.1: What is the ARP spoofing attack? Why is this attack limited to local networks rather than over the internet?

Q1.2: Give an example to explain the DNS Poisoning attack. Why can a DNS cache be easily poisoned and how to prevent it?

Q1.3: Why is it easy to recover from a BGP hijacking of `124.48.72.0/16` but difficult to recover from a BGP hijacking of `123.23.89.0/24`?

Question 2 (5 pts)

What practically prevents (*unecrypted*) HTTP responses from being spoofed by an off-path attacker who only knows client's and server's IP addresses?

Question 3 (10 pts)

The Mirai Botnet compromised hundreds of thousands of IoT devices by attempting default credentials against Telnet and SSH services. The malware then used compromised devices to DDoS popular websites.

Q3.1: Why couldn't victim websites simply drop traffic from the compromised devices to defend against the DDoS launched by Mirai?

Q3.2: Nearly all of the devices infected by Mirai were not behind Network Address Translation (NAT) gateways. Why weren't devices behind NATs infected?

Question 4 (10 pts)

Most home routers have an *HTTP-based* internal administration interface. Why is it important that you change the default password even though the interface *isn't accessible on the Internet*? Specifically,

Q2.1: Give **one** example of attack that an attacker can gain access your home router.

Q2.2: Give **two** examples of attacks that an attacker can accomplish if they can change the configuration of your home router.