Homework 06

Due: 11:59 pm, Thursday April 25

Please handin your homework assignment on gradescope as a PDF file with each problem on a separate page.

Network Security

Problem 1

Consider the network shown in Figure 1

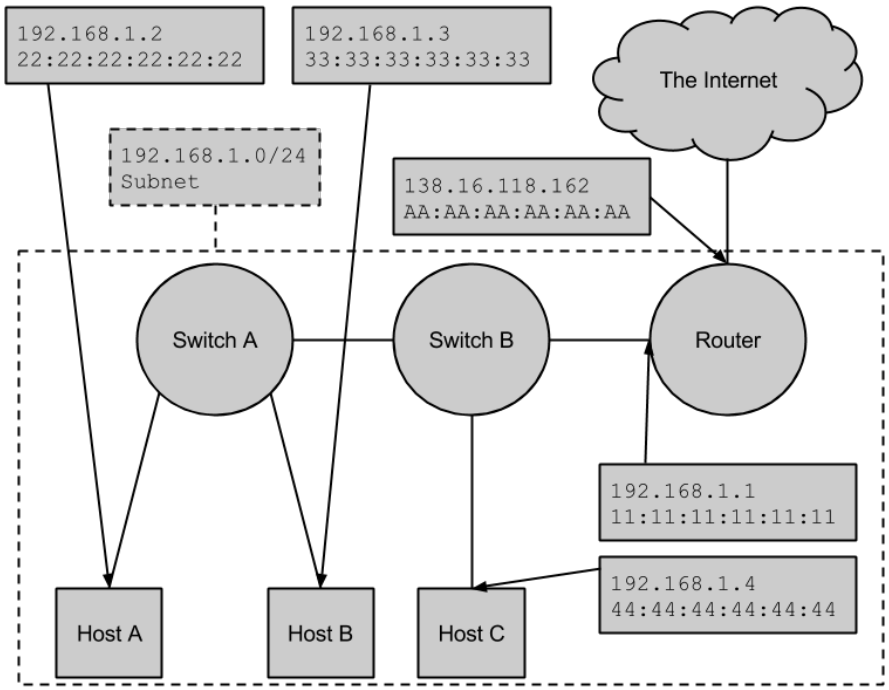

Figure 1: A subnet whose addresses all take the form `192.168.1.*`. Each router and host interface is labeled with the interface's IP address and MAC address.

a) Host B wants to observe Host A's traffic with Host C. What can Host B do to cause Host A to send their traffic to Host B instead of Host C? Be specific - don't just say "B could spoof so-and-so's IP address."

b) In carrying out this attack, Host B needs to be careful not to accidentally break other hosts' connections. How can Host B make sure that their attack only targets Host A? Again, be specific. Hint: While ARP is designed to use the broadcast MAC address (`FF:FF:FF:FF:FF:FF`) by default, it doesn't have to be used this way.

c) Host B is now intercepting Host A's traffic, but this means that Host C isn't getting the traffic, and Host A will soon notice that something is going wrong and give up, which will limit the amount of information that Host B can intercept. How can Host B make sure that the communication still works as intended, while also guaranteeing that they have access to the traffic? Again, be specific.

d) Host B is now intercepting Host A's traffic, and Host C is also getting the traffic and responding properly, so Host A is none the wiser. However, Host B would also like to intercept the responses, as they may contain important information. How can Host B accomplish this? Again, be specific.

e) Briefly, how would these techniques differ if Host B wanted to intercept Host A's communication with `128.148.32.12`? Remember that since `128.148.32.12` is not on Host B's subnet, it will not suffice to spoof `128.148.32.12`'s MAC address.

Problem 2

a) Explain why having DNS query IDs is more secure than having no query IDs.

b) Explain why having randomized DNS query IDs is more secure than having sequential query IDs.

c) Consider an intrusion detection system that analyzes network traffic to detect attacks. Which pattern in the network traffic to and from a name server would suggest that a DNS cache poisoning attack is taking place?

Problem 3

One method to protect the privacy of the sender and recipient of a message, while also providing protection for message content, is onion routing https://2019.www.torproject.org/about/overview.html.en. This method is based on the following approach:

- Messages travel from source to destination along a path of routers (proxies) randomly selected by the sender. This path is referred to as a *circuit*.
- The last router in the circuit establishes a connection with the intended destination. To defend against eavesdropping along the circuit, the sender encapsulates the message with multiple layers of encryption, one per subsequent node in the circuit, which results in the "onion." Thus, messages are always transmitted encrypted between routers.
- As each router receives the onion, it "peels" a layer off of the onion by decrypting it with its private key, which reveals the next router on the circuit.

a) Explain in your own words why onion routing protects the confidentiality of both the message content and the identity of the two communicating parties. Specifically, show why an eavesdropper observing traffic on any single link of the circuit between the sender and recipient will be able to infer *neither* (1) the content of the message *nor* (2) the identity of *both* the sender and recipient.

b) Consider an attacker who can eavesdrop traffic on both the first and last link of the circuit, but no other link. What does this adversary learn?

Social Engineering

Problem 4

Reflect on what kind of personal information an individual may share on the internet (social networks, blogs, websites, discussion forums, etc.) that could help an adversary perform a social engineering attack on the individual or their organization. Following this reflection, write a list of five recommended best practices

on internet information sharing to mitigate vulnerability to social engineering attacks. Each best practice should consist of a brief title, a description, and a justification.

For this problem, you should take into account your own online experience, what you learned in the lecture on social engineering, and the resource "The Social Engineering Framework" provided on the course website. *Please do not submit any personal information in your answer.*

To give you an idea of the answer format, here is an example of best practice (do not include it among the five ones in your answer):

> *Do not share your connections/friends:* Adjust your social network settings so that you do not publicly disclose your personal friends/relatives and work connections. Justification: knowledge of your friends, relatives, and work connections can be leveraged to craft spear phishing emails.

Bitcoin and Cloud Security

Problem 5

a) In a Bitcoin mining pool, the pool administrator assigns to each worker in the pool a range of nonces to use in trying to solve the current puzzle. The worker who finds the solution reports the successful nonce to the pool administrator, who then shares the block reward with all the workers in the pool in proportion to the work they have performed. What prevents a worker who has found the solution to the puzzle from taking the entire block reward themself?

b) Explain how the Merkle tree construction could be used to make more efficient the verification of the integrity of files outsourced to a cloud storage service. In particular, refer to the scenario of Alice outsourcing her files to Bob and wishing to check that the files she downloads from Bob have not been corrupted.

Gaming Security

Problem 6

In the gaming security lecture, we learned that a lottery ticket contains a security feature, called "SureLock number," designed to verify the authenticity of the ticket and prevent counterfeiting. Since no details were provided, your task is to design your own authentication method for lottery tickets. Your method should add to a ticket a *validation code* of short fixed length (e.g., 64 hex symbols) that is derived from the content of the ticket and a secret key that is known only to the party creating the tickets. The validation code should have the following properties:

P1. It is unfeasible to infer the secret key from the analysis of any number of issued tickets.

P2. It is unfeasible to compute the validation code from only the ticket content.

P3. Given a ticket, it is unfeasible to generate another ticket with different content and same validation code.

—

a) Explain why the above properties ensure that someone who hears about the winning ticket content should be unable to forge the winning ticket.

b) Describe your scheme for creating the ticket validation code and justify why it satisfies the above properties.