Homework 06

Due: 11:59 pm, Monday April 30

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

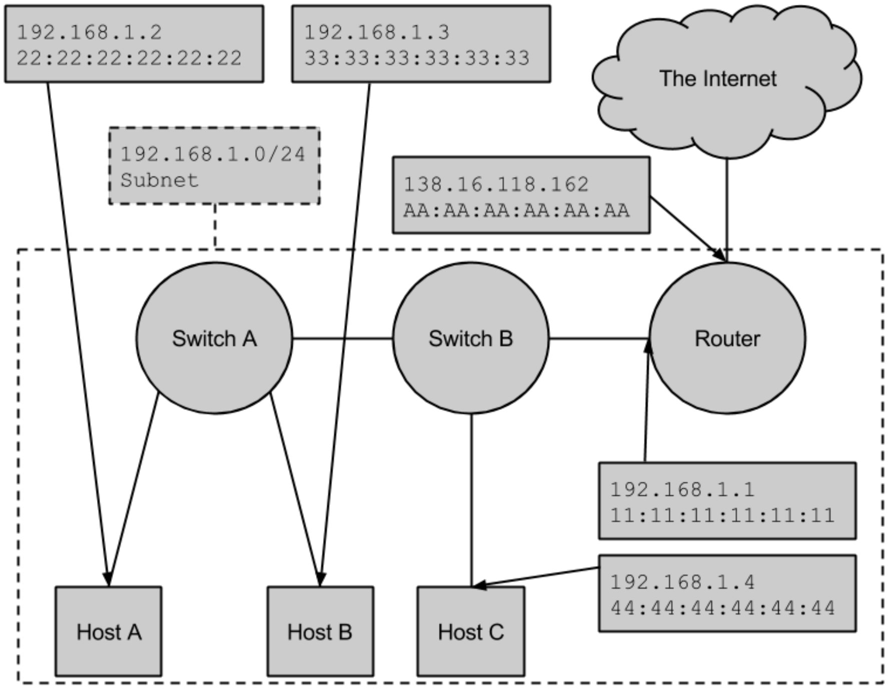

Figure 1: A subnet whose addresses all take the form `192.168.1.*`. Each router and host interface is labeled with the interface's IP address and MAC address.

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) You might think that, for a space consisting of 2^n IDs, you couldn't do better than having a $\frac{1}{2}^n$ probability of guessing a query ID correctly. Explain how the birthday attack manages to do better than this.

d) 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 http://tor.eff.org/about/overview.html.en. This method is based on the following approach:

1. Messages travel from source to destination via a sequence of proxies ("onion routers") along a randomly-selected path.

2. The last router in the path establishes a connection with the intended recipient. To prevent eavesdropping attacks, messages are encrypted between routers.

The "onion" metaphor illustrates the essence of the method: as each router receives the message, it "peels" a layer off of the packet by decrypting it with its private key, thus revealing the routing instructions meant for that router. Due to this arrangement, the data in an onion packet can only be revealed if it is transmitted to every router in the path in the order specified by the layering.

a) Navigate to the following URL: `http://matrixtxri745dfw.onion/neo/uploads/180409/MATRIX_184549_iRK_question_3.jpg`. Describe briefly how you were able to access this URL.

b) Describe why onion routing is considered trustworthy. Think about what an intermediate node needs to know in order to complete its step.

c) What do the sender and recipient know?

d) How can an adversary controlling entry and exit nodes be a problem?

Applications Security

Problem 4

a) The Voting Village will return to DEFCON this year. Imagine you are in attendance, and want to compromise a piece of voting system equipment. What would you check/probe to uncover the machine's vulnerabilities? What would you do to exploit them?

b) A local election official with no computer systems experience is confused about the risks of direct recording electronic (DRE) voting machines. Briefly explain the cost-benefit analysis of DREs and advise the official on any relevant security precautions the district should take in order to ensure the accuracy of election results.

Problem 5

a) Explain what are the advantages of storing in the header of each Bitcoin block the Merkle root hash of the transactions in the block instead of the hash of the concatenation of the transactions in the block.

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

c) Which technical limitation of the Bitcoin protocol prevents its use as a replacement for large-volume payments systems (such as credit cards) that process thousands of payment transactions per second?