Question 1 ***A Tour of Tor***

As a reminder, when connecting to a normal website through Tor, your computer first queries the Tor "consensus" to get a list of all Tor nodes, and using this information it connects to the first Tor node and, from there, creates a circuit through the Tor network, eventually ending at an exit node.

Q1.1 (4 min) Consider the scenario where you are in a censored country and the censor choses not to block Tor, the censor is the adversary, and no Tor relays exist within this country. How many Tor relays must your traffic pass through, including the exit node, to prevent the censor from blocking your traffic.

- ◯ One
- ◯ Two
- ◯ Three
- ◯ Four
- ◯ Tor doesn't stop this adversary

Q1.2 (4 min) Consider the scenario where you are the only user of Tor on a network that keeps detailed logs of all IPs contacted. You use Tor to email a threat. The network operator is made aware of this threat and that it was sent through Tor and probably originated on the operator's network. How many Tor relays must your traffic pass through, including the exit node, to guarantee the network operator can't identify you as the one who sent the threat?

- ◯ One
- ◯ Two
- ◯ Three
- ◯ Four
- ◯ Tor doesn't stop this adversary

Q1.3 (4 min) Consider the scenario where there is a single hostile Tor node but you don't know that node's identitity, and that node can be an exit node. You want to keep confidential from this node what HTTP sites you are visiting through Tor. How many Tor relays must your traffic pass through, including the exit node, to guarantee this adversary can't know what sites you visit?

- ◯ One
- ◯ Two
- ◯ Three
- ◯ Four
- ◯ Tor doesn't stop this adversary

Q1.4 (4 min) Consider the scenario where there are mulitple independent hostile Tor nodes but you don't know their identities, and these nodes can be exit nodes. You want to keep confidential from all these nodes what HTTP sites you are visiting through Tor. How many Tor relays must your traffic pass through, including the exit node, to guarantee that every independent hostile node can't know what sites you visit?

- ◯ One
- ◯ Two
- ◯ Three
- ◯ Four
- ◯ Tor doesn't stop this adversary

Q1.5 (4 min) Consider the scenario where there are multiple colluding hostile Tor nodes but you don't know those nodes identities, and these nodes can be exit nodes. You want to keep confidential from all these nodes what HTTP sites you are visiting through Tor. How many Tor relays must your traffic pass through, including the exit node, to guarantee that the colluding system of hostile nodes can't know what sites you visit?

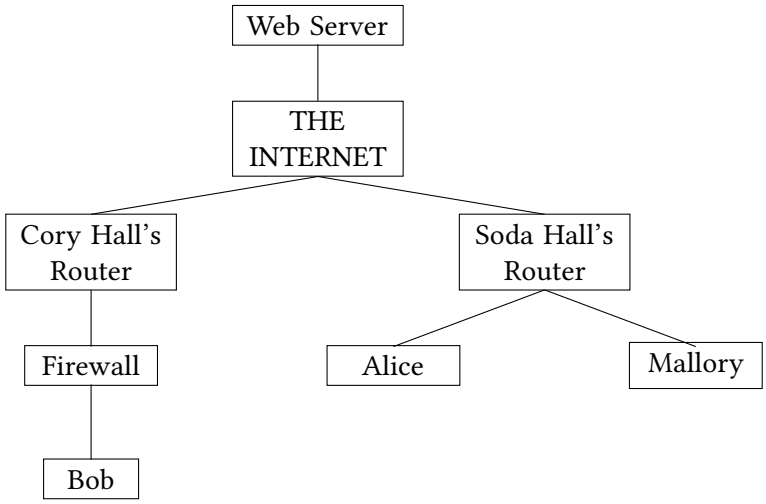
- ◯ One
- ◯ Two
- ◯ Three
- ◯ Four
- ◯ Tor doesn't stop this adversary

Q1.6 (4 min) Consider the scenario where there is a single hostile Tor node but you don't know that node's identity, and that node can be an exit node. You want to have data integrity for the HTTP sites you are visiting through Tor. How many Tor relays must your traffic pass through, including the exit node, to guarantee this adversary can't manipulate the data you receive from the sites you visit?

- ◯ One
- ◯ Two
- ◯ Three
- ◯ Four
- ◯ Tor doesn't stop this adversary

Question 2 ***Making New Friends***

Consider two local broadcast networks, as shown in the diagram below.



Q2.1 (2 min) Alice broadcasts an ARP request for Mallory's MAC address.

Which of these entities, if malicious, can poison Alice's ARP cache? Select all that apply.

☐ Mallory ☐ Bob ☐ None of the above

☐ Soda Hall's router ☐ Cory Hall's router

Q2.2 (4 min) Mallory and Bob form a TLS connection. Then, Bob adds a rule to the firewall disallowing all inbound packets from Mallory.

EvanBot argues that TLS messages are encrypted, so the firewall cannot stop Mallory from sending more TLS messages to Bob. Is EvanBot correct? Justify your answer in 10 words or fewer.

○ Yes ○ No

Q2.3 (3 min) Bob adds a rule to the firewall disallowing all inbound packets from anybody in Soda Hall's local network.

Which of the following attacks can Mallory still perform on Bob? Assume that Mallory cannot spoof packets. Select all that apply.

☐ DoS ☐ TLS hijacking

☐ XSS ☐ None of the above