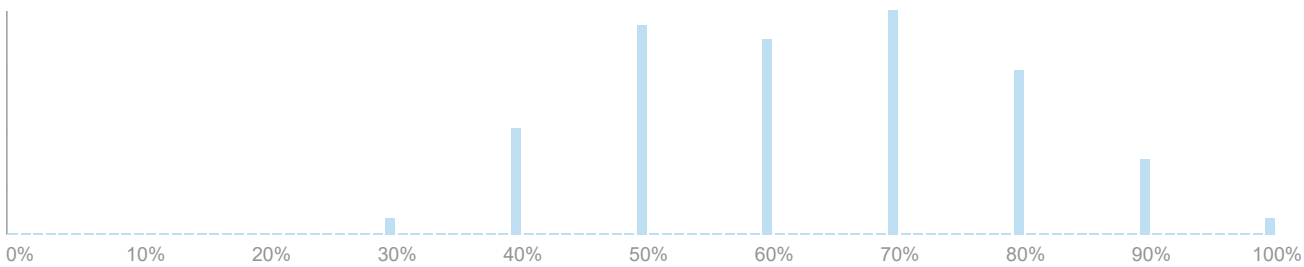
Quiz Summary

Section Filter ▾ | Student analysis | Item analysis

Average score	High score	Low score	Standard deviation	Average time
64%	100%	30%	1.55	24:33



Question Breakdown

Attempts: 67 out of 67

Which of the following statements about Amplification (D)DoS attack is WRONG?

+0.4

Discrimination Index

Amplification attack often misuses open DNS resolvers on the Internet		0 %
Amplification attack utilizes a large number of bots.	1 respondent	1 %

To counter amplification attack, prevention of IP spoofing is effective.	20 respondents	30 %
Blocking incoming DNS traffic is a good solution to counter amplification attack.	44 respondents	**66 %**
None of the above	2 respondents	3 %

66% answered correctly

Attempts: 67 out of 67

Recall SIFF studied in Week 9 lecture. Which of the following will NOT increase the difficulty DoS attack?

+0.48

Discrimination Index

Increase the number of SIFF routers between the source and destination	4 respondents	6 %
Increase the number of valid (active) keys maintained on each SIFF router at each time slot	17 respondents	**25 %**
Increase the size of router marking	22 respondents	33 %
None of the options 1-3 above	17 respondents	25 %
All of the options 1-3 above	7 respondents	10 %

25% answered correctly

Attempts: 67 out of 67

+0.38

Discrimination Index

Which of the following statements is CORRECT about SIFF?

SIFF enables the reciever to select who can send a privileged traffic to it.	53 respondents	**79 %**
If any of the routers en route is not SIFF-capable, SIFF does not reduce (D)DOS traffic at all.	2 respondents	3 %
SIFF routers need to establish a (shared) secret key with the source.	6 respondents	9 %
Collusion with a SIFF router closer to the source can significantly reduce attackers' effort to guess capability.	2 respondents	3 %
None of the above	4 respondents	6 %

79% answered correctly

Attempts: 67 out of 67

Recall Crossfire attack studied in Week 9 lecture. Which of the following statements is WRONG?

+0.31

Discrimination Index

Crossfire attack typically starts with collecting route information by using a tool like traceroute		0 %
Crossfire attack targets links with high flow density.	10 respondents	15 %
Crossfire attack changes target links over time.	5 respondents	7 %
Crossfire attack uses a large number of bots to send traffic to servers in the	23 respondents	**34 %**

target area.

None of the above.	29 respondents	43 %

34%
answered
correctly

Attempts: 66 out of 67

Assume you are running a server in the target area of Crossfire attack. Which of the following is a good countermeasure against Crossfire attack?

+0.45

Discrimination
Index

Trace back the sources of the traffic and filter them.	17 respondents	25 %
Enhance the server's computatioal power and network bandwidth.	1 respondent	1 %
Block traceroute	12 respondents	18 %
Block DNS traffic	1 respondent	1 %
None of the above.	35 respondents	**52 %**
No Answer	1 respondent	1 %

52%
answered
correctly

Attempts: 67 out of 67

Which of the following statements is correct about anonymity on the Internet?

+0.33

Discrimination Index

Anonymity can be attained by encryption		0 %
Secure communication (e.g., TLS) can hide who is communicating with whom.		0 %
Anonymity is often demanded for freedom of speech.	64 respondents	**96 %**
Anonymity still ensures accountability.	1 respondent	1 %
None of the above.	2 respondents	3 %

96% answered correctly

Attempts: 67 out of 67

Recall MIX studied in Week 10. Which of the following statements is CORRECT about MIX?

+0.39

Discrimination Index

MIX relies on symmetric key encryption.		0 %
MIX is designed to ensure sender anonymity.	56 respondents	**84 %**
MIX requires TLS for each communication.	1 respondent	1 %
In Mixnet (Mix cascade), anonymity cannot be provided if less than half of the MIX servers are honest.	3 respondents	4 %
None of the above.	7 respondents	10 %

84%
answered
correctly

Attempts: 67 out of 67

+0.56

Discrimination Index

Which of the following statements is CORRECT about Tor?

Tor Proxy (client software) establishes shared secret key directly with all Tor routers on the circuit.	20 respondents	30 %
When a client (browser) is sending HTTP request to a web server via Tor, nobody but B can see the HTTP request in plaintext.	11 respondents	16 %
Tor can hide who is connecting to Tor network.	11 respondents	16 %
Tor can hide who is accessed via Tor network.	10 respondents	15 %
None of the above.	15 respondents	**22 %** ✓

22%
answered
correctly

Attempts: 66 out of 67

+0.35

Discrimination Index

Which of the following attack strategy is effective against Tor?

Traffic analysis using timing and packet size	5 respondents	7 %
Hacking of directory servers	1 respondent	1 %
Deployment of malicious routers		0 %
Routing attack		0 %

All of the above.	60 respondents	**90 %**
No Answer	1 respondent	1 %

90% answered correctly

Attempts: 67 out of 67

Which of the following statement is CORRECT about Hidden Services in Tor?

+0.21

Discrimination Index

Hidden services are often used for illegal purposes.	60 respondents	**90 %**
Rendezvous Point knows the server's IP address.		0 %
Rendezvous Point knows the client's IP address.	2 respondents	3 %
Client can find the server's IP address from the Tor directory server.	3 respondents	4 %
All of the above.	2 respondents	3 %

90% answered correctly