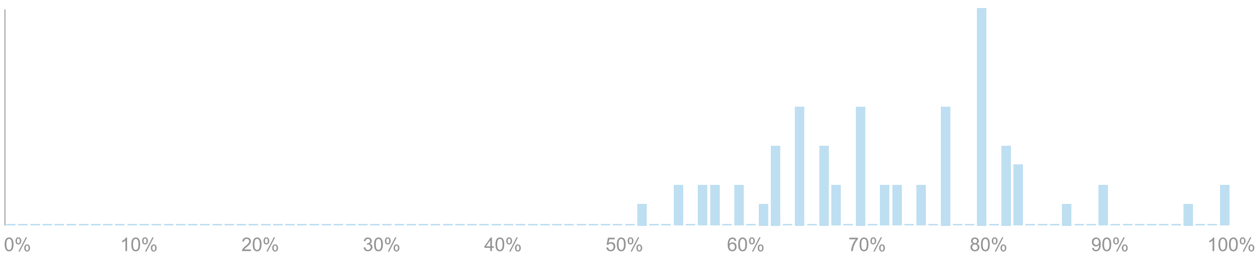
# Quiz Summary

Section Filter ▾ | Student analysis | Item analysis

| Average score | High score | Low score | Standard deviation | Average time |
|---|---|---|---|---|
| **73%** | 100% | 52% | 1.06 | 24:36 |



# Question Breakdown

Attempts: 68 out of 68

Which of the following is WRONG about IP spoofing for TCP/IP communication?

**+0.13**

Discrimination Index ?

| | | |
|---|---|---|
| IP spoofing is often used for mounting (D)DoS attacks. | 4 respondents | 6 % |
| Source routing may allow an attacker in the different network to mount IP spoofing. | | 0 % |
| **IP address can be a reliable device identifier since it uniquely identifies the device on the network.** | 60 respondents | **88 %** ✓ |

| | | |
|---|---|---|
| Knowing initial sequence number is crucial for an attacker to mount meaningful IP spoofing attack. | 3 respondents | 4 % |
| None of the above | 1 respondent | 1 % |

88% answered correctly

Attempts: 68 out of 68

Which of the following is effective as a countermeasure against IP spoofing of client IP address?

**+0.18**

Discrimination Index ?

| | | | |
|---|---|---|---|
| Promiscuous mode | | 0 % | |
| PKI | 2 respondents | 3 % | |
| Source routing | | 0 % | |
| **Ingress filtering** | 59 respondents | **87 %** | ✓ |
| None of the above. | 7 respondents | 10 % | |

87% answered correctly

Attempts: 68 out of 68

Which of the following statements is CORRECT about AIP (Accountable IP) proposal?

**+0.41**

Discrimination Index ?

| | | | |
|---|---|---|---|
| AIP is backward compatible with IPv4. | | 0 % | |
| AIP requires PKI. | 14 respondents | 21 % | |
| **Address verification can be done either at a nearest router (to the source) or intermediate router.** | 32 respondents | **47 %** | ✓ |
| Each device can have at most 1 AIP address. | 6 respondents | 9 % | |
| None of the above. | 16 respondents | 24 % | |

47% answered correctly

Attempts: 68 out of 68

In AIP, what is the network address of a device generated from?

| | | | |
|---|---|---|---|
| IPv4 address | 4 respondents | 6 % | |
| CA's public key | 1 respondent | 1 % | |
| **AD's public key** | 56 respondents | **82 %** | ✓ |
| **Device's public key** | 53 respondents | **78 %** | ✓ |
| Device's private key | 4 respondents | 6 % | |

57% answered correctly

Attempts: 68 out of 68

Which of the following statement is CORRECT about attacks discussed in "Collaborative TCP Sequence Number Inference Attack" paper discussed in

Week 5?

**+0.4**

Discrimination Index ?

| | | | |
|---|---|---|---|
| To mount client-side TCP injection attack successfully, it is better for attacker's server to be located as close to the legitimate server, with which the victim app is communicating, as possible. | 5 respondents | 7 % | |
| **Client-side TCP injection attack will work regardless of the OS version of the legitimate server.** | 10 respondents | **15 %** | ✓ |
| If a legitimate server can prepare and send response faster, it will make active TCP hijacking attack more difficult. | 19 respondents | 28 % | |
| If a legitimate server can prepare and send response faster, it will make passive TCP hijacking attack more difficult. | 26 respondents | 38 % | |
| None of the above. | 8 respondents | 12 % | |

15% answered correctly

Attempts: 68 out of 68

Which of the following would help attackers to do TCP injection and/or hijacking?

**+0.41**

Discrimination Index ?

| | | |
|---|---|---|
| Server using old version of Linux kernel | | 0 % |
| Predictable initial sequence number | 6 respondents | 9 % |

| | | | |
|---|---|---|---|
| Promiscuous mode in the same network as the victim | | 0 % | |
| Side channel using system state on a client device | | 0 % | |
| **All of the above.** | 62 respondents | **91 %** | ✓ |

91% answered correctly

Attempts: 68 out of 68

Which of the following usually can NOT be learned by using the low interaction honeypot?

**+0.26**

Discrimination Index ?

| | | | |
|---|---|---|---|
| **Attack tactics and procedure** | 56 respondents | **82 %** | ✓ |
| Statistics about attack sources | | 0 % | |
| Statistics about services (protocols) targeted | | 0 % | |
| Trend in attack traffic intensity | 1 respondent | 1 % | |
| None of the above. | 11 respondents | 16 % | |

82% answered correctly

Attempts: 68 out of 68

Which of the following tools are often used for implementing low-interaction honeypot?

| | | | |
|---|---|---|---|
| **TCP listener (e.g., netcat)** | 58 respondents | **85 %** | ✓ |

| | | | |
|---|---|---|---|
| **CONPOT** | 65 respondents | **96 %** | ✓ |
| **Network monitor (e.g., Wireshark)** | 35 respondents | **51 %** | ✓ |
| Virtual machine running real OS and servers | 14 respondents | 21 % | |
| Cowrie | 9 respondents | 13 % | |

38%
answered
correctly

Attempts: 68 out of 68

**-0**

Discrimination Index ?

What is the advantage of high-interaction honeypot?

| | | | |
|---|---|---|---|
| Feasibility to deploy | | 0 % | |
| Low resource consumption | | 0 % | |
| Good scalability | | 0 % | |
| **Better fidelity and realism** | 68 respondents | **100 %** | ✓ |
| All of the above. | | 0 % | |

100%
answered
correctly

Attempts: 68 out of 68

In Week 6, we studied CAUDIT scheme. Which of the following statements is CORRECT about CAUDIT?

**+0.36**

Discrimination Index ?

| | |
|---|---|
| CAUDIT uses Cowrie SSH honeypot for threat intelligence collection. | 0 % |

| | | | |
|---|---|---|---|
| Auditor module of CAUDIT exhaustively scan all nodes in NCSA for complete coverage. | | 0 % | |
| Black Hole Router of CAUDIT aims at avoiding overloading SSH honeypot. | 14 respondents | 21 % | |
| **Black Hole Router filters traffic from source addresses observed by the honeypot** | 49 respondents | **72 %** | ✓ |
| None of the above. | 5 respondents | 7 % | |

72%
answered
correctly