**Ziyang Lin Lab3 Report**

**Zlin32 Team2**

**Team 2 report**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Date** | **Team 1** | **Team 3** | **Team 4** | **Team 5** | **Team 6** | **Team9** |
| 12-04 | None | 1C, 1P | None | None | None | None |
| 12-05 | None | 19C, 18P, 5E | 3C, 1P | None | 1C, 1P | None |
| 12-06 | 9C, 9P, 2E | 2C | None | None | None | 2C |
| 12-07 | 7C, 4P, 3E | 5C, 2P | None | None | 9C, 5P | 4C |
| 12-08 | 3C, 3P, 3E | 10C, 5P | None | None | 10C, 4P | None |
| 12-09 | 12C, 10P, 2E | 21C, 4P | 2C, 2P | 14C, 3P | 9C, 6P | 1C |

**Team 2 rules**

1. First cert in handshake packet's certChain should be verifiable by root cert and have an issuer name equal to "20194."

2. Subject name of last cert in handshake packet's certChain should be equal to the issuer name of the cert in handshake packet's cert field.

3. Cert in handshake packet's cert field should have a subject name equal to the IP address of the incoming connection.

4. The subject name of the cert in the handshake packet's cert field should match the subject name of the last cert in the certChain, up to the length of the latter subject name (eg. finalCert.subjectName[:len(lastCertInChain.subjectName)] == lastCertInChain.subjectName).

**Scanner results**

FAIL means the team’s server fail the rule, so I can make handshake with wrong cert.

PASS means the team’s server pass the rule, so I can’t make handshake with wrong cert.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Team number** | **Rule 1** | **Rule 2** | **Rule 3** | **Rule 4** |
| **1** | PASS | **FAIL** | **FAIL** | **FAIL** |
| **2** | PASS | PASS | PASS | **FAIL** |
| **3** | PASS | **FAIL** | PASS | PASS |
| **4** | PASS | PASS | PASS | **FAIL** |
| **5** | PASS | PASS | PASS | PASS |
| **6** | PASS | PASS | PASS | PASS |
| **9** | **FAIL** | **FAIL** | **FAIL** | **FAIL** |