Exploring Database Defensive Methods Lab Report

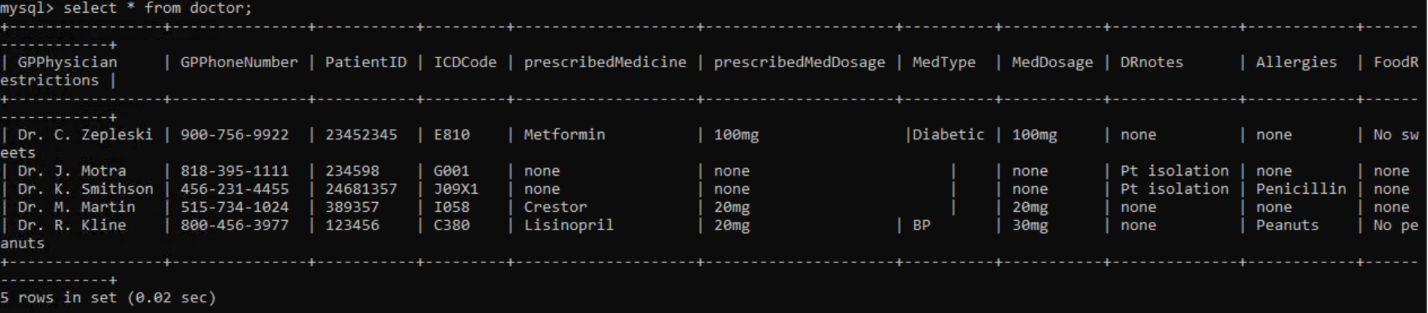
CST 620

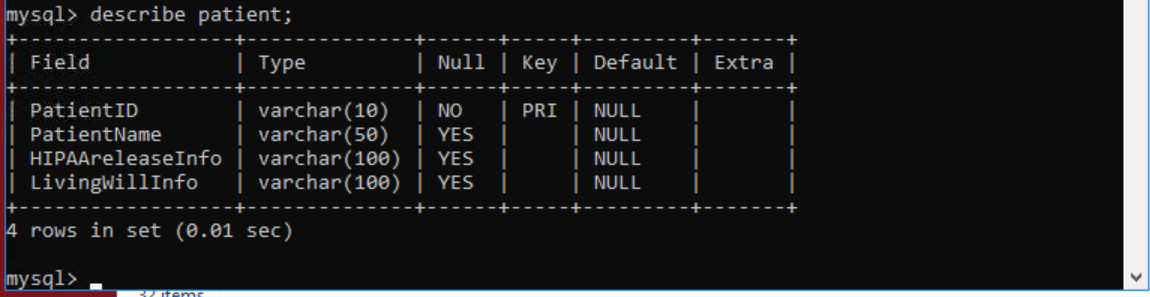
Ifeanyi Uzoukwu

**Part 1**

Here is a summary of the issues I found while using SNORT to analyze the user accounts and permissions.

* Patient Billing has access to more fields than it’s supposed to have access to
* Certain fields, such as Nursing were not accessible at all. This could be indicative of a bigger issue regarding certain parts of the database needing to be reconfigured.
* There should be a limited amount of information that is deemed available on the database for all parties to view.

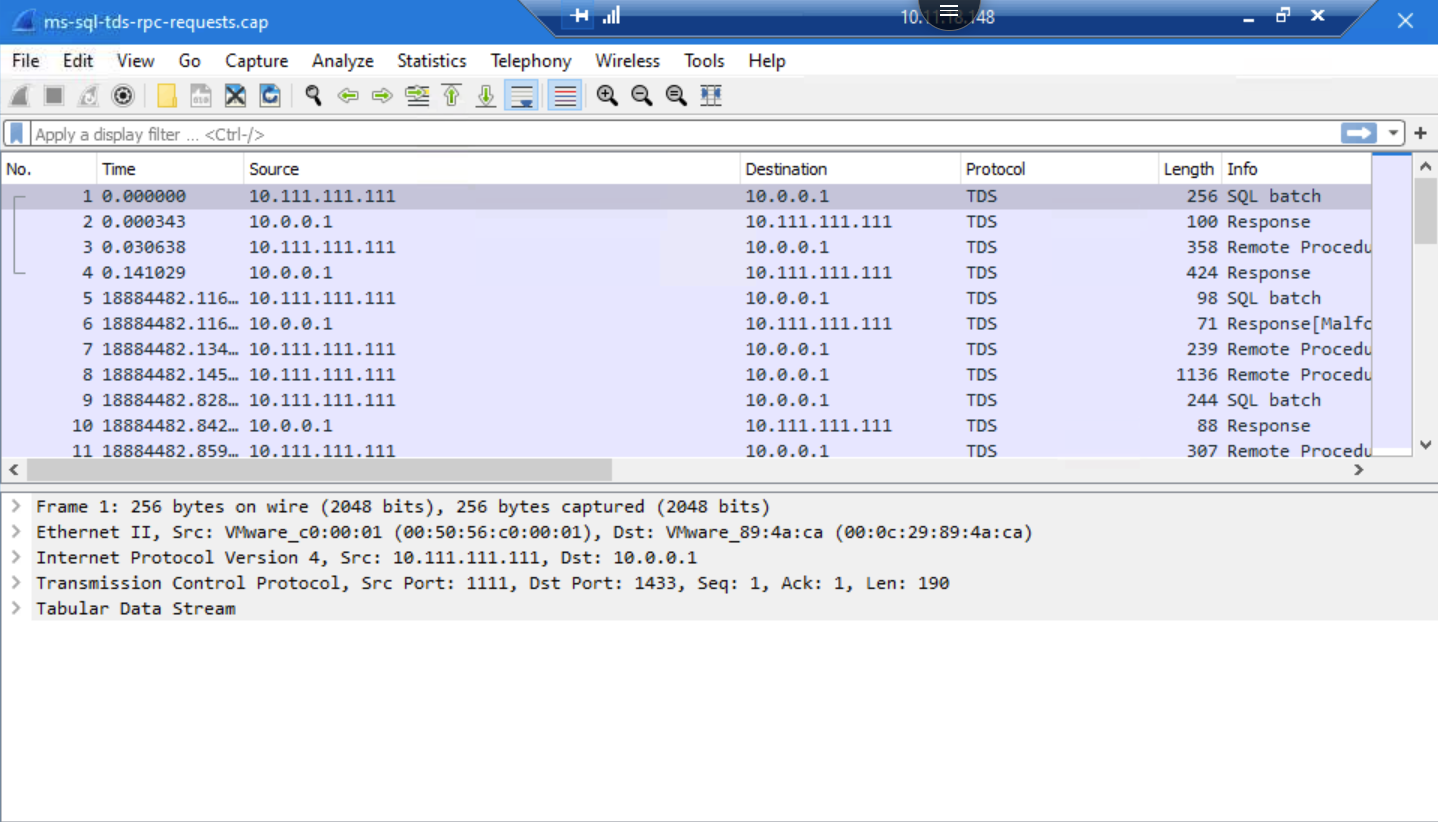


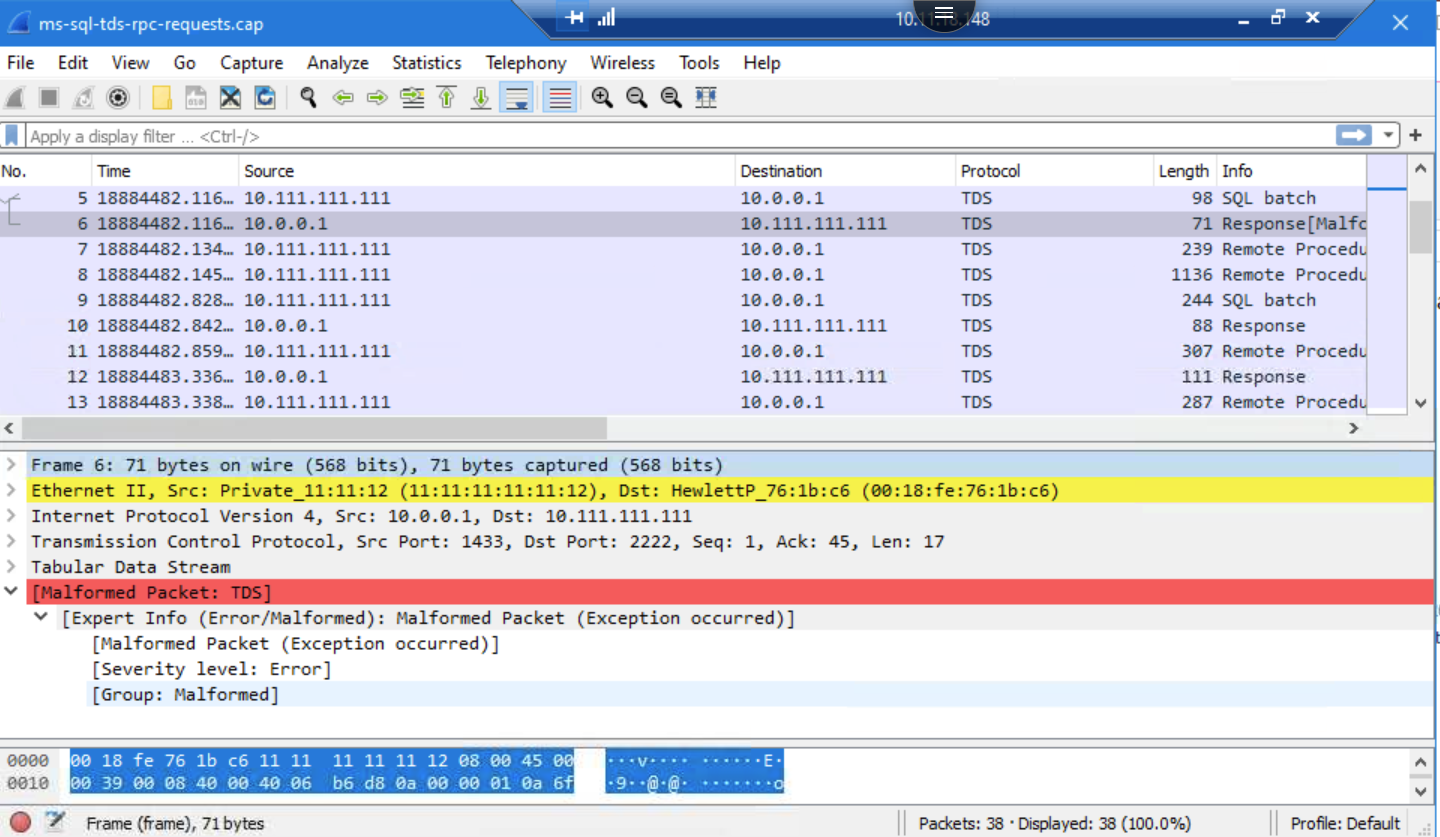


Part 2

**MS-SQL-tds-rpd-requests.cap**

There were Malformed TDS Packets detected. Record 6 in this file could be seen as an attempted injection of malicious code. Attackers could also use this kind of attack to learn about the database structure by initiating error messages. This could also be the result of Wireshark’s dissector not being able to break down a part of the code.





**Mysql\_complete.pcap**

**Records 1-2**

There was questionable traffic coming from ports 56162 and 3306.Record 1’s destination port and Record 2’s source port was 3306. Port 3306 was used for a connection establish request in record 1 and a connection establish acknowledge in record 2. Record 22 had the majority of the issues that were noticed by the expert analysis in this file. This port could be in danger of being used by a threat actor.

**Record 22**

Two warnings were issues in relation to record 22, “FIXME- dissector is incomplete” and an “End of File (EOF) found while connection was in wrong state”. There was also plaintext data found in the record, which would lead me to believe the record was not secured. This record also could have been corrupted.

