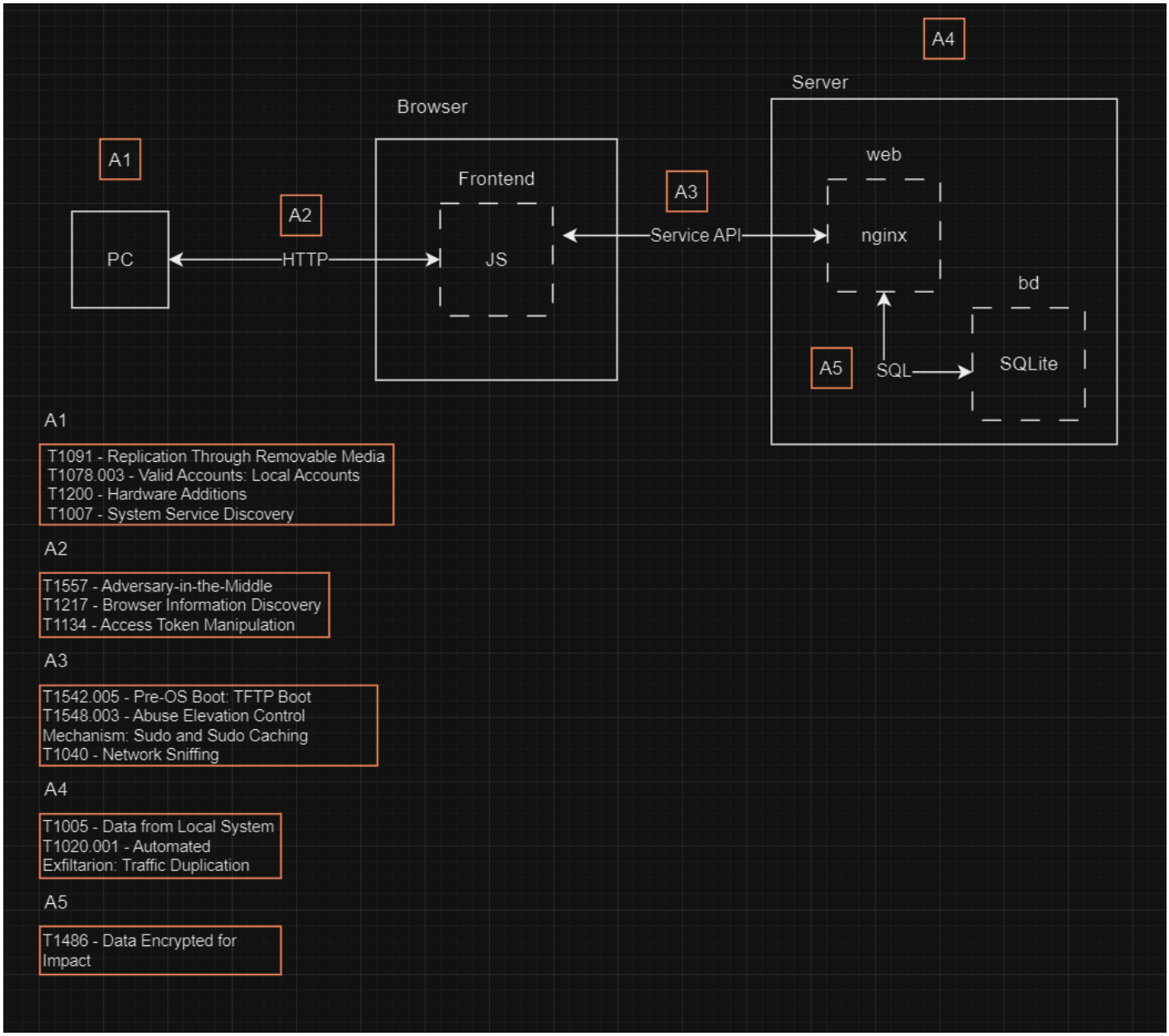


A1

T1091 - Replication Through Removable Media
T1078.003 - Valid Accounts: Local Accounts
T1200 - Hardware Additions
T1007 - System Service Discovery

A2

T1557 - Adversary-in-the-Middle
T1217 - Browser Information Discovery
T1134 - Access Token Manipulation

A3

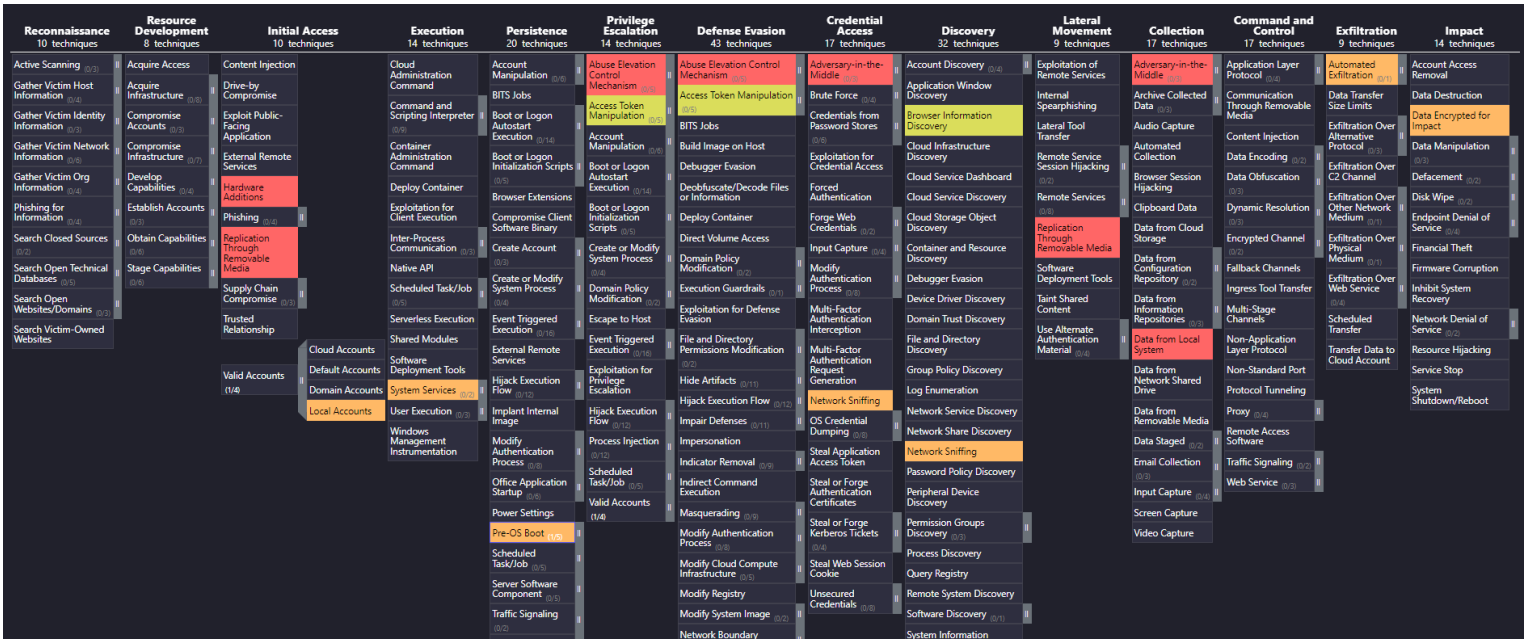
T1542.005 - Pre-OS Boot: TFTP Boot
T1548.003 - Abuse Elevation Control Mechanism: Sudo and Sudo Caching
T1040 - Network Sniffing

A4

T1005 - Data from Local System
T1020.001 - Automated Exfiltarion: Traffic Duplication

A5

T1486 - Data Encrypted for Impact



Красный – высокая опасность

Оранжевый – средняя опасность

Зеленый – низкая опасность

Угрозы:

T1091 - Replication Through Removable Media – красный

T1078.003 - Valid Accounts: Local Accounts – оранжевый

T1200 - Hardware Additions – красный

T1007 - System Service Discovery – оранжевый

T1557 - Adversary-in-the-Middle – красный

T1217 - Browser Information Discovery – зеленый

T1134 - Access Token Manipulation – зеленый

T1542.005 - Pre-OS Boot: TFTP Boot – оранжевый

T1548.003 - Abuse Elevation Control Mechanism: Sudo and Sudo Caching – красный

T1040 - Network Sniffing – оранжевый

T1005 - Data from Local System – красный

T1020.001 - Automated Exfiltarion: Traffic Duplication – оранжевый

T1486 - Data Encrypted for Impact – оранжевый