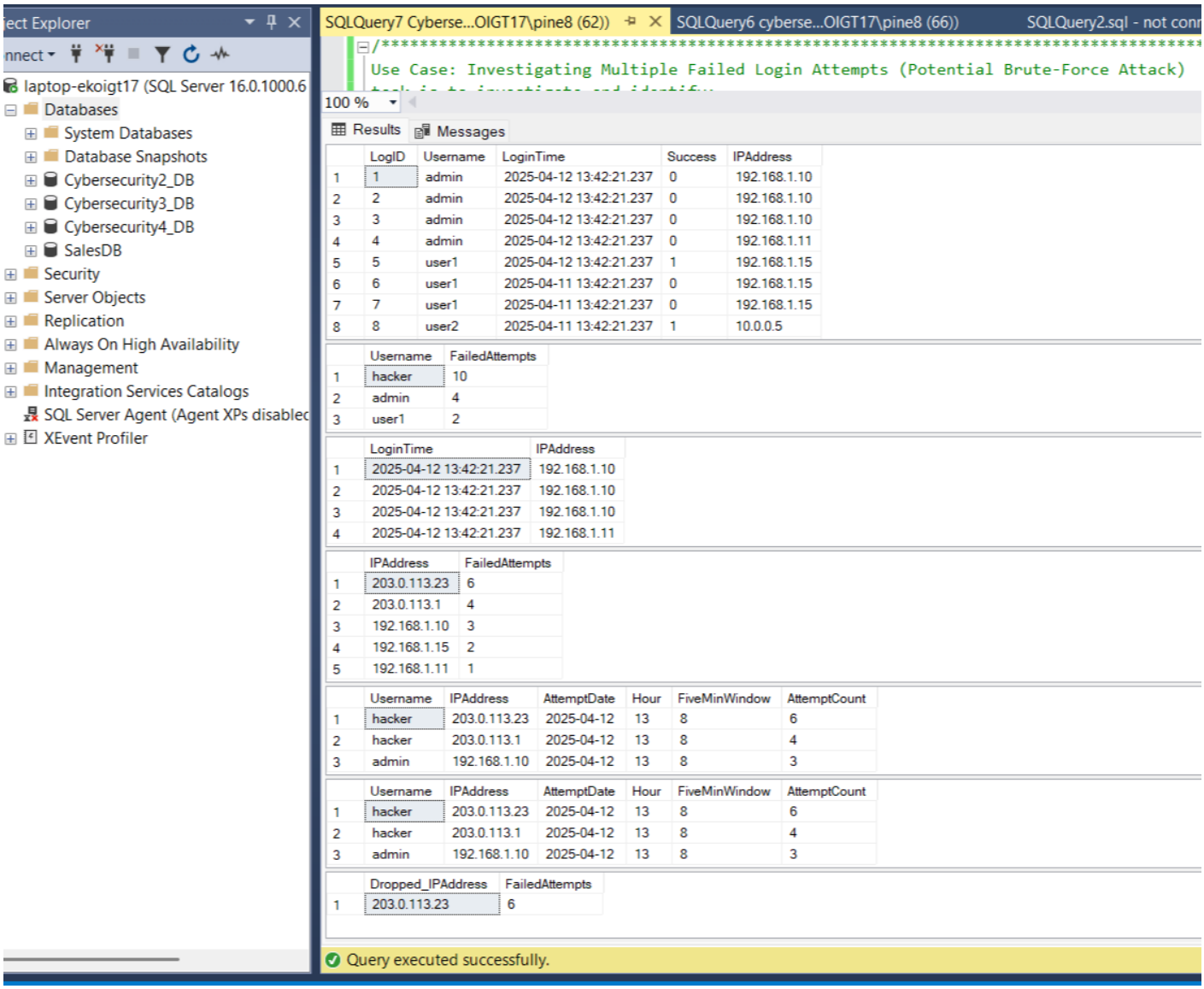
ect Explorer
nnect
laptop-ekoigt17 (SQL Server 16.0.1000.6
Databases
System Databases
Database Snapshots
Cybersecurity2_DB
Cybersecurity3_DB
Cybersecurity4_DB
SalesDB
Security
Server Objects
Replication
Always On High Availability
Management
Integration Services Catalogs
SQL Server Agent (Agent XPs disabled
XEvent Profiler
SQLQuery7 Cyberse...OIGT17\pine8 (62))
SQLQuery6 cyberse...OIGT17\pine8 (66))
SQLQuery2.sql - not conn
/*
Use Case: Investigating Multiple Failed Login Attempts (Potential Brute-Force Attack)
100 %
Results
Messages
LogID Username LoginTime Success IPAddress
1 1 admin 2025-04-12 13:42:21.237 0 192.168.1.10
2 2 admin 2025-04-12 13:42:21.237 0 192.168.1.10
3 3 admin 2025-04-12 13:42:21.237 0 192.168.1.10
4 4 admin 2025-04-12 13:42:21.237 0 192.168.1.11
5 5 user1 2025-04-12 13:42:21.237 1 192.168.1.15
6 6 user1 2025-04-11 13:42:21.237 0 192.168.1.15
7 7 user1 2025-04-11 13:42:21.237 0 192.168.1.15
8 8 user2 2025-04-11 13:42:21.237 1 10.0.0.5
Username FailedAttempts
1 hacker 10
2 admin 4
3 user1 2
LoginTime IPAddress
1 2025-04-12 13:42:21.237 192.168.1.10
2 2025-04-12 13:42:21.237 192.168.1.10
3 2025-04-12 13:42:21.237 192.168.1.10
4 2025-04-12 13:42:21.237 192.168.1.11
IPAddress FailedAttempts
1 203.0.113.23 6
2 203.0.113.1 4
3 192.168.1.10 3
4 192.168.1.15 2
5 192.168.1.11 1
Username IPAddress AttemptDate Hour FiveMinWindow AttemptCount
1 hacker 203.0.113.23 2025-04-12 13 8 6
2 hacker 203.0.113.1 2025-04-12 13 8 4
3 admin 192.168.1.10 2025-04-12 13 8 3
Username IPAddress AttemptDate Hour FiveMinWindow AttemptCount
1 hacker 203.0.113.23 2025-04-12 13 8 6
2 hacker 203.0.113.1 2025-04-12 13 8 4
3 admin 192.168.1.10 2025-04-12 13 8 3
Dropped_IPAddress FailedAttempts
1 203.0.113.23 6
Query executed successfully.