Unorthodox Case 001

Raw Document CJ2025/XII/DFIR-CS-1290

Overview

Our client is a managed private portfolio investment company, **CoreStocks** which suffered an internal breach happening in a constraint from November to December. They believe this attack yields a severe outcome:

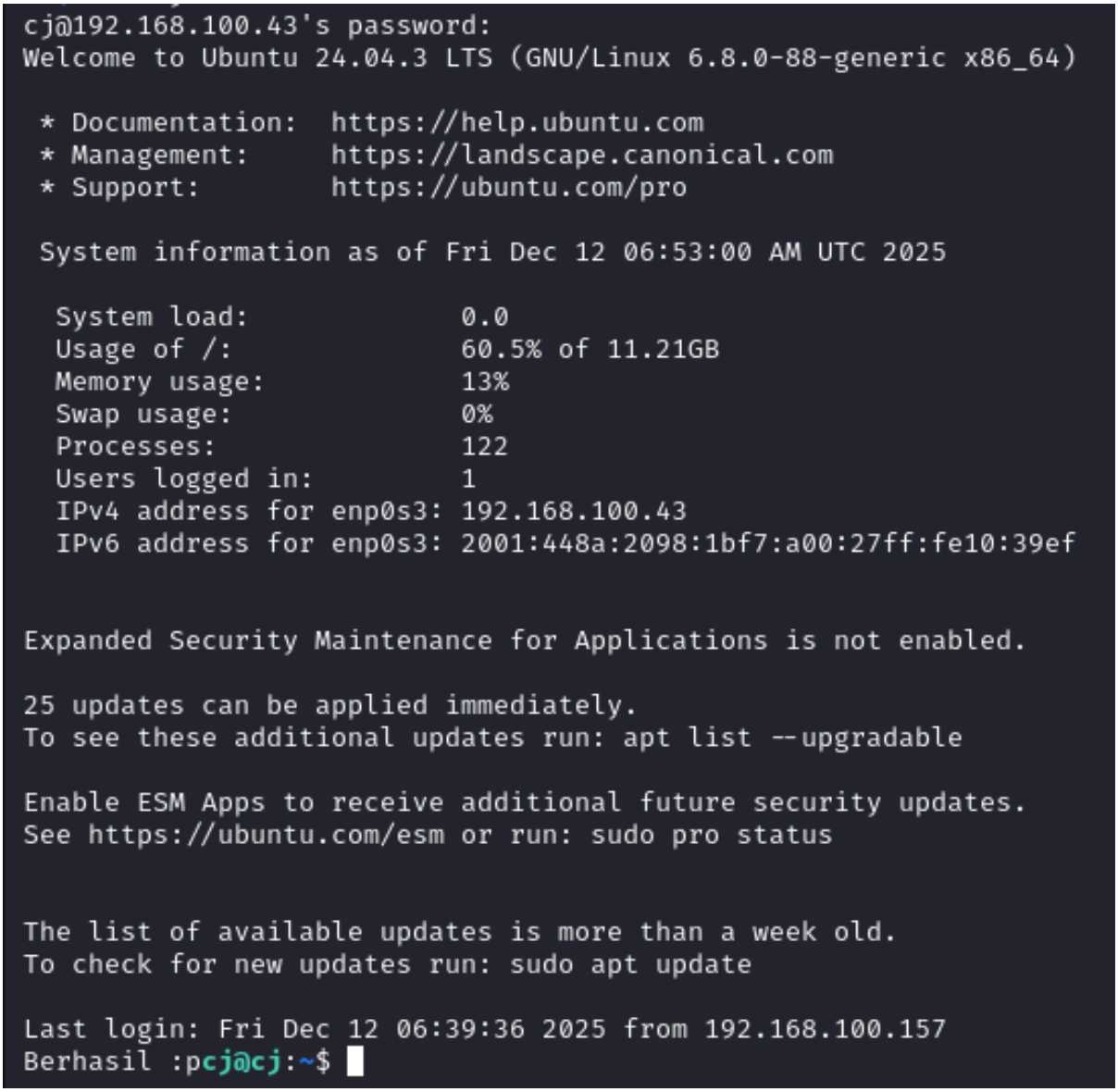
- All the last state of stock analysis (macros perspective) are deleted
- All the user login credentials have been changed by the actor
- The server is **believed to be compromised by more than just one internal threat actor.**

Evidence

There are some collected artifacts which have been retrieved for us:

- **Packet Capture File (PCAP_Captured.pcap)**
  - SHA256: 883888DE7A8F84D079A771846FC37B9A12773CA1753371E74F4B3327F27DA095
- **OVA File (CoreStock main VM server)**
  - SHA256: 499DF688F118D88B49C99197C2B68E03BB672E26DCC14BC048F3D997FEA2A2E2
- **Binary Data (exfiltrated.bin)**
  - SHA256: 2F940284901830733A303E56F3C6AC655ABB14B8A09C0110681ED137C2DB54B8

There's a screenshot from one of the employees showing a suspicious message whenever someone tries to login to the **CoreStocks** main VM server.



The screenshot was taken before the threat actor changed the credentials and removed their core stock data.