**Project Report: TimeLine**

Group 3; Ahmed, Roydon, Laksman.

1. **Initial Access:** Hardware Additions
2. **Execution:** Execution through Module Load, Exploitation for Client Execution, Graphical User interface
3. **Persistence:** Port Monitors, Redundant Access, Registry Run Keys/Startup Folder, SIP and Trust Provider Hijacking, Scheduled Task.
4. **Privilege Escalation:** Hooking, Image File Execution Options Injection, New services.
5. **Defense Evasion:** DLL Side-Loading, Deobfuscate/Decode Files or information, Disabling Security Tools; Exploitation for Defense evasion, Extra Windows Memory injection, File Deletion
6. **Credential Access:** Credentials in Registry, Exploitation for Credential Access;
7. **Discovery:** Process Discovery, Query Registry.
8. **Lateral Movement:** Pass the hash, Pass the Ticket.
9. **Collection:** Data from Network Shared Drive.
10. **Exfiltration:** Data Encrypted.
11. **Command and Control:** Custom Cryptographic Protocol, Data Encoding.

**Laks: A-d – 4, Ahmed: E-H – 4, Roydon: I-K – 3**

Weeks: 5 weeks left till Demo

**One per- week: Last week report.**

|  |  |  |
| --- | --- | --- |
| Week Feb : 17 – 23 | Date : Thursday 21st | Time Line report |
| Week Feb/March: 24 – 2 | Date: Thursday 28th | Reading Week: build and develop plan and |
| Week Mar: 3 – 9 | Date: Thursday 7th | Demo A, E, I |
| Week Mar: 10 – 16 | Date: Thursday 14th | Demo B, F, J |
| Week Mar: 17 – 23 | Date: Thursday 21st | Demo C, H, G |
| Week Mar: 24 – 30 | Date: Thursday 28th | Demo D, H |
| Week Mar/Arp: 31 -6 | Date: Thursday 4th | Report week |