T1078.003 Valid accounts: Infrastructure Local Accounts

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Date | Who | Current text | Proposed text | Final text |
|  |  |  |  |  |
|  |  |  |  |  |

Description: An adversary may use local administrative privileges to bypass network controls responsible for access controls and software to achieve persistence.

In a 5G deployment, unmanned locations or low security sites may be exposed to adversary using local communication, auxiliary or serial interfaces to gain access to device using device local account.

An adversary with a legitimate or compromised local network operator administrative account may perform unauthorized administration of devices and systems. Some devices always maintain local accounts in addition to networked IDAM/ICAM. Unauthorized administration of devices and systems can be done using these local administrative accounts.

Labelling:

* Sub-techniques: None
* Applicable Tactics: persistence

Metadata:

* Architecture Segment: OA&M
* Platform(s): Infrastructure, PNF
* Access type required: Administrative access
* Data Sources:
* Theoretical/Proof of concept/Observed:

Procedure Examples:

|  |  |
| --- | --- |
| **Name** | **Description** |
| Specific example if known |  |

Mitigations

|  |  |
| --- | --- |
| **ID** | **Use** |
| M1027 | Passwords Policies to ensure secure local accounts across all devices that necessitate local accounts |
| M1026 | Privileged account management |
|  |  |

Pre-Conditions

|  |  |
| --- | --- |
| **Name** | **Description** |
|  |  |

Critical Assets

|  |  |
| --- | --- |
| **Name** | **Description** |
| Physical Network Functions | Any 5G, Network, OSS and Security capability deployed as PNF supporting local accounts |
| Infrastructure servers | Any Virtualization and Network host supporting local account |

Detection

|  |  |
| --- | --- |
| **ID** | Detects |
| DS0028 | Logon session |
| DS0002 | User Account authentication |
|  |  |

Post-Conditions

|  |  |
| --- | --- |
| **Name** | **Description** |
|  |  |

References:

|  |  |
| --- | --- |
| Name | URL |
| ENISA “Threat Landscape and Good Practice Guide for Software Defined Networks/5G”, Jan. 2016, Table 1, and 2 | https://www.enisa.europa.eu/publications/sdn-threat-landscape |
| R. Pell, S. Moschoyiannis, E. Panaousis, R. Heartfield, “Towards dynamic threat modelling in 5G core networks based on MITRE ATT&CK”,  October 2021 | https://arxiv.org/abs/2108.11206 |