T1046 Core-network scanning

Description: An adversary may discover operator network related information (identifiers).

Adversaries may attempt to get a listing of earlier generation systems (e.g. 3G) that do not use IP address, hostname, but instead, other identifiers, such as point codes (like IP addresses for SS7 protocols, point to point) and Global Titles. Examples are GTScan, SigPloit, SCTPScan and GTPScan.

Note: This is scanning for 3G, 4G and 5G core components address info (part of 5G nonstandalone deployments). This is scanning for open ports to determine protocol use without compromising the host/NF.

Labelling:

* Sub-technique(s): No sub-techniques
* Applicable Tactics: Discovery

Metadata:

* Architecture segment: OA&M
* Platforms: 5G Network
* Permissions Required: none
* Data Sources:
* Theoretical/Proof of Concept/Observed: Observed

Procedure Examples:

|  |  |
| --- | --- |
| **Name** | **Description** |
| Specific example if known | If there is a documented instance of this technique occurring in earlier generation or a notional example |
| Use of pen testing tools. | Adversaries may employ pen testing tools such as GTScan, SigPloit, SCTPScan and GTPScan. |

Mitigations

|  |  |
| --- | --- |
| **ID** | **Use** |
| If known | Short description of potential mitigations. |
| M1042 | Ensure that unnecessary ports and services are closed to prevent risk of discovery and potential exploitation. |
| M1031 | Use network intrusion detection/prevention systems to detect and prevent remote service scans. |
| M1030 | Ensure proper network segmentation is followed to protect critical servers and devices. |

Pre-Conditions

|  |  |
| --- | --- |
| **Name** | **Description** |
| If known | Short description of conditions that must be present for technique to be used. |
| Access to scanning tool | Adversaries need access to such tools |

Critical Assets

|  |  |
| --- | --- |
| **Name** | **Description** |
| If known | Short description of the assets that adversary wants to target or that are at risk such as data (system/user, access token, crypto key etc.), capability, service. |
| MNO core network component data. | Data (IP address or FQDN, ports) relating to network nodes |

Detection

|  |  |
| --- | --- |
| **ID** | **Detects** |
| If known | Short description of possible detection techniques such as logs or sensors. |
| DS0029 | SIEM tools using network firewalls. Detect port scanners |

Post-Conditions

|  |  |
| --- | --- |
| **Name** | **Description** |
| If known | Short description of potential capabilities achieved by the technique (e.g. escape from container gives control of the host) |
| Identifier of some network nodes revealed | Adversary now knows identifiers of some network nodes, and so these nodes can now be spoofed or targeted for Denial of Service. |

References:

|  |  |
| --- | --- |
| **Name** | **URL** |
| S.P. Rao, S. Holtmanns, T. Aura: “Threat modeling framework for mobile communication systems”, May 2020 | https://arxiv.org/abs/2005.05110v1 |

#doNotParse

(from Muddasar 6/12/22): Port scanning is usually done on multiaccess network. On host-to-host direct connections, it probably not useful, as these direct network connections are limited. IDS, and NetFlow’s software determine based on activity that port scanning is being performed. Nmap open source tool can map IPs and ports on a network.

I don’t think Port scanning is possible on traditional SS7 MTP3, SS7 used dedicated link types (A, C, and D-links). Although a whole lot of SS7 traffic may be carried over IP. In that case port scanning can be effective to determine IP based Message transfer points (MTPs) or ISUP/EISUP software servers.

PCAP can be detected if adversary is using compromised host on the network to sniff traffic on the vLAN. This will be possible by logging alerts when a new PCAP process is executed. I am sure an adversary that has compromised to run PCAP knows how to disable logging and alerting first