Network Service Scanning (version 1.0)

**Cloud Service Label: IaaS**

Adversaries may attempt to get a listing of services running on remote hosts, including those that may be vulnerable to remote software exploitation. Methods to acquire this information include port scans and vulnerability scans using tools that are brought onto a system.

Within cloud environments, adversaries may attempt to discover services running on other cloud hosts or cloud services enabled within the environment. Additionally, if the cloud environment is connected to a on-premises environment, adversaries may be able to identify services running on non-cloud systems. The most frequently targeted services and ports on the cloud are port 22 (SSH) and port 3389 (RDP). Cloud administrators often leave these services open to enable quick remote access to IaaS resources. In Azure by default these ports are open to the world when a VM is first created and need to be purposefully secured after creation.

## Examples

|  |  |
| --- | --- |
| **Name** | **Description** |
| Flan Scan | Lightweight network vulnerability scanner created by Cloudflare that can be used to find open ports, identify services, and provide list of CVEs and vulnerabilities. Easier to run inside cloud environment |

Mitigations

|  |  |
| --- | --- |
| **Name** | **Description** |
| Disable or Remove Feature or Program | Ensure that unnecessary ports and services are closed to prevent risk of discovery and potential exploitation. |
| Network Intrusion Prevention | Use network intrusion detection/prevention systems to detect and prevent remote service scans. |
| Network Segmentation | Ensure proper network segmentation is followed to protect critical servers and devices. |

Detection

System and network discovery techniques normally occur throughout an operation as an adversary learns the environment. Data and events should not be viewed in isolation, but as part of a chain of behavior that could lead to other activities, such as Lateral Movement, based on the information obtained.

Normal, benign system and network events from legitimate remote service scanning may be uncommon, depending on the environment and how they are used. Legitimate open port and vulnerability scanning may be conducted within the environment and will need to be deconflicted with any detection capabilities developed. Network intrusion detection systems can also be used to identify scanning activity. Monitor for process use of the networks and inspect intra-network flows to detect port scans. Routinely inspect SSH and RDP logs on hosts to detect brute force or other probing attacks.

References

1. <https://github.com/cloudflare/flan>. Accessed July 24, 2020.