# TTP Detail – T1595

## TTP Information

Name: Active Scanning

Description: Adversaries may execute active reconnaissance scans to gather information that can be used during targeting. Active scans are those where the adversary probes victim infrastructure via network traffic, as opposed to other forms of reconnaissance that do not involve direct interaction.

Adversaries may perform different forms of active scanning depending on what information they seek to gather. These scans can also be performed in various ways, including using native features of network protocols such as ICMP.(Citation: Botnet Scan)(Citation: OWASP Fingerprinting) Information from these scans may reveal opportunities for other forms of reconnaissance (ex: [Search Open Websites/Domains](https://attack.mitre.org/techniques/T1593) or [Search Open Technical Databases](https://attack.mitre.org/techniques/T1596)), establishing operational resources (ex: [Develop Capabilities](https://attack.mitre.org/techniques/T1587) or [Obtain Capabilities](https://attack.mitre.org/techniques/T1588)), and/or initial access (ex: [External Remote Services](https://attack.mitre.org/techniques/T1133) or [Exploit Public-Facing Application](https://attack.mitre.org/techniques/T1190)).

## Threat-Mapped Scoring

Score: 1.8

Priority: P4 - Informational (Low)

## Kill Chain Phases

**•** mitre-attack: reconnaissance