# TTP Detail – T1595.002

## TTP Information

Name: Vulnerability Scanning

Description: Adversaries may scan victims for vulnerabilities that can be used during targeting. Vulnerability scans typically check if the configuration of a target host/application (ex: software and version) potentially aligns with the target of a specific exploit the adversary may seek to use.

These scans may also include more broad attempts to [Gather Victim Host Information](https://attack.mitre.org/techniques/T1592) that can be used to identify more commonly known, exploitable vulnerabilities. Vulnerability scans typically harvest running software and version numbers via server banners, listening ports, or other network artifacts.(Citation: OWASP Vuln Scanning) 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: [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

## APTs (Intrusion Sets)

* APT28
* APT29
* APT41
* Aquatic Panda
* Dragonfly
* Earth Lusca
* Ember Bear
* Leviathan
* Magic Hound
* Sandworm Team
* TeamTNT
* Volatile Cedar
* Winter Vivern