MITRE ATT&CK Daily Analysis Report

Tactic and Technique Deep Dive – Learning Documentation by Darrshan

Technique ID	: T1595
Technique Name	: Active Scanning
Tactic	: Reconnaissance
Platform	: PRE
Date	: 3/11/2025
Analyst	: Darrshan S/O Erettai Muniandy

Contents

Overview

Active scanning is a reconnaissance technique where adversaries deliberately scan target networks to identify live hosts, open ports, or services. It helps attackers map a network's surface before exploitation. This activity often precedes intrusions or phishing campaigns and is a key step for assessing potential attack vectors.

Common scanning method

- ICMP or ping sweeps
- TCP/UDP port scans
- Web application scanning or vulnerability scanning\
- Service fingerprinting

Sub-Techniques

Sub-technique ID	Sub-technique Name	Description
.001	Scanning IP blocks	Scanning large IP ranges to find active systems.
.002	Vulnerability Scanning	Searching for known vulnerabilities in target systems.
.003	Wordlist Scanning	Using dictionaries to identify valid subdomains, directories, or parameters.

Objective

To understand how adversaries use scanning activities to discover potential entry points and how defenders can detect or mitigate such reconnaissance behavior.

Example Scenario

An adversary performs a mass scan using tools like "**Masscan**" or "**Nmap**" targeting a specific organization's IP range. Results reveal open SSH and HTTP services. This information later supports brute-force attacks or exploit delivery.

Example tools

1. Nmap
2. Masscan
3. ZMap
4. Shodan – for passive scanning context.

Detection & Mitigation

Detection Ideas

- Monitor network traffic for high-frequency connection attempts from a single source to multiple IPs or ports.
- Use IDS/IPS signatures to detect known scanning patterns.
- Track unusual external reconnaissance behavior scanning activity.

Mitigation

- Implement network segmentation & rate-limiting.
- Block unnecessary inbound connections.
- Use honeypots to mislead and detect scanning activity.

Analytical Notes

Factor	Description
Difficulty to detect	**Moderate** Scanning is noisy but can be disguised in low-volume bursts.
Impact Potential	**Low on its own** Critical for successful follow-on attacks.
Defensive Priority	**Medium** Focus on visibility & logging (Make sure your firewall, IDS and network monitoring tools **logs these scan patterns clearly**), we can simply block everything in the name of defense. Not an emergency but ensure scan don't go unnoticed.
Score	**3** Pretty common, but dangerous if ignored.
Reason	Common reconnaissance activity with moderate detection and containment difficulty.

Real-World Example

Incident

Log4Shell Scanning Campaign (December 2021)

Description

Right after the Log4Shell (CVE-2021-44228) vulnerability was disclosed, adversaries and security researchers worldwide launch a massive **active scanning** campaigns to identify vulnerable systems. These scans targeted public-facing servers running Java applications using the vulnerable Log4j library. Attackers probed networks using HTTP headers, URLs and payloads designed to trigger a DNS callback or command execution, a classic case of large-scale reconnaissance and exploitation preparation.

Techniques used

- T1595 (Active Scanning) – to find potential vulnerable endpoints.
- T1595.002 (Vulnerability Scanning) – automated discovery of systems exposing Log4j.
- T1190 (Exploit Public-facing Application) – Follow-up exploitation phase.

Tools and infrastructure

- Attackers used **Masscan**, **Nmap** and custom scripts to scan entire IP ranges.
- Some scans originated from compromised cloud servers and anonymized VPNs.

Impact

The scan led to thousands of compromised systems within days, affecting enterprise and cloud environments globally. It demonstrated how reconnaissance (T1595) directly fuels widespread exploitation in real-world campaigns.

Detection indicators

- Repeated inbound HTTP requests with **"${jndi:"** patterns in headers.
- Abnormal scan traffic from foreign cloud providers.
- DNS callback activity resolving to attacker-controlled domains.

Terminology & Definitions

TERM	DEFINITION	CONTEXT / USAGE
RECONNAISSANCE	The phase where attackers collect information about targets to identify possible entry points.	Overall MITRE tactic category.
ACTIVE SCANNING	Direct interaction with target systems to discover live hosts, open ports, or services.	Primary technique (T1595).
PASSIVE SCANNING	Gathering target information indirectly (e.g., via Shodan or public sources) without touching the target's network.	Contrast with active scanning.
IP BLOCK	A range of IP addresses belonging to the same organization or ISP.	Often scanned to map external assets.
FINGERPRINTING	Analyzing system responses to identify OS, version, or service type.	Sub-technique of reconnaissance.

MASSCAN	A high-speed port scanner capable of scanning the entire Internet in minutes.	Common attacker and researcher tool.
NMAP	A network scanning tool used to detect hosts, ports, and services with more detailed probes.	Legitimate admin and attacker tool.
VULNERABILITY SCANNING	Automated searching for known weaknesses in systems or applications.	Sub-technique T1595.002.
SHODAN	A search engine for Internet-connected devices. Used for passive reconnaissance.	Often leveraged pre-attack.
LOG4SHELL (CVE-2021-44228)	A critical remote code execution vulnerability in Apache Log4j, heavily scanned and exploited in 2021.	Real-world scanning example.
HONEYPOT	A decoy system designed to attract and log attacker activity without risk to production networks.	Mitigation / detection tool.
INDICATOR OF COMPROMISE (IOC)	Observable evidence that an attack or compromise has occurred (e.g., malicious IP, hash, domain).	Used in detection and response.
C2 (COMMAND AND CONTROL)	A channel used by attackers to communicate with compromised hosts.	Later stage following reconnaissance.

References

[1] MITRE ATT&CK, “T1595: Active Scanning,” *MITRE Corporation*, 2024. [Online]. Available: https://attack.mitre.org/techniques/T1595/. [Accessed: Nov. 3, 2025].

[2] MITRE ATT&CK, “T1595.002: Vulnerability Scanning,” *MITRE Corporation*, 2024. [Online]. Available: https://attack.mitre.org/techniques/T1595/002/. [Accessed: Nov. 3, 2025].

[3] Cybersecurity and Infrastructure Security Agency (CISA), “Mitigating Log4Shell Vulnerability (CVE-2021-44228),” *Alert AA21-356A*, Dec. 17, 2021. [Online]. Available: https://www.cisa.gov/news-events/alerts/2021/12/17/aa21-356a.

[4] SANS Institute, “Detecting and Preventing Network Reconnaissance,” *SANS Whitepapers*, 2023. [Online]. Available: https://www.sans.org/white-papers/. [Accessed: Nov. 3, 2025].

[5] G. Lyon, *Nmap Network Scanning: The Official Nmap Project Guide to Network Discovery and Security Scanning*, Nmap Project, 2022. [Online]. Available: https://nmap.org/book/.

[6] R. D. Graham, “Masscan: Mass IP port scanner,” *GitHub Repository*, 2024. [Online]. Available: https://github.com/robertdavidgraham/masscan. [Accessed: Nov. 3, 2025].

[7] Shodan, “Understanding Internet-Wide Scanning Data,” *Shodan Documentation*, 2024. [Online]. Available: https://help.shodan.io/. [Accessed: Nov. 3, 2025].

[8] CrowdStrike, “Log4Shell Exploitation and Global Scanning Trends,” *CrowdStrike Blog*, Dec. 2021. [Online]. Available: https://www.crowdstrike.com/blog/log4shell-exploitation/.

[9] Microsoft Threat Intelligence, “Tracking Reconnaissance and Scan-Based Intrusions,” *Microsoft Security Blog*, 2023. [Online]. Available: https://www.microsoft.com/security/blog/.