MITRE ATT&CK®

Web Explanation

Abstract

The detailed framework for understanding and defending against cyber threats by showing adversary tactics, techniques, and procedures based on real-world observations.

Jagadish tripathy

Jagadishtripathy144@gmail.com

Contents

About: - 2

Active Scanning: - 2

Main techniques: - 3

Scanning IP Blocks: - 3

Vulnerability Scanning: - 3

Gather Victim Network Information: - 4

Network Topology: - 4

IP Addresses: - 4

Summary: - 5

About: -

MITRE ATT&CK® provides a globally recognized knowledge base of techniques and adversary behaviour's drawn from real world observations. MITRE ATT&CK® is utilized to derive threat models and methodologies to mitigate risks across different sectors. The ATT&CK framework is openly accessible to anyone, and it seeks to improve the impact of cybersecurity through regional and sectoral collaboration addressing security problems.

The ATT&CK matrix for enterprise consists of categories of techniques including the following Reconnaissance, Resource Development, Initial Access, Execution, Persistence and on. Within each of these techniques, such as Active Scanning, Gathering Victim Information, Phishing, Closed/Open-Source Searching, and Threat Intelligence seeks to help organizations protect against threats.

The techniques exhibited in the ATT&CK matrix were created from previous threat actor behaviours. This knowledge base serves as a tool for organizations to improve their cybersecurity posture while also informing organizations of threats they may be experiencing. The framework covers further topics including the Compromise of Accounts, Compromise of Infrastructure, Establish Gain and Obtain Capabilities, Phishing, Supply Chain Compromise, Valid Accounts and many other subjects in support of a comprehensive defence approach.

Active Scanning: -

Active scanning is a type of reconnaissance, where the adversary actively probes victim infrastructure over network traffic. Active scanning might be accomplished in a variety of ways, one of which is to leverage native features of network protocols, such as ICMP. The results of these scans can provide potential leads to other forms of reconnaissance, establish operational

resources, and/or provide initial access. This document will cover three sub-techniques of active scanning: IP block scanning, vulnerability scanning, and wordlist scanning. This document also includes examples of procedures, mitigations, detection, and references for further information related to active scanning.

Main techniques: -

The primary technique detailed in the web is Active Scanning. It, in fact, will provide us information on the Active Scanning technique and even discuss its sub-techniques:- Scanning IP Blocks- Vulnerability Scanning - Wordlist Scanning The web explains that active scanning is the adversaries ability to probe victim infrastructure via network traffic to obtain the information necessary to subsequently target the infrastructure.

Scanning IP Blocks: -

The method of IP Blocks Scanning is used by adversaries to find active IP addresses and open ports over a range of IP addresses. This method involves sending packets to a number of IP addresses and examining the response to learn which IP addresses are active and what services the submitted IP address is running. Adversaries can then leverage the previously gathered information on the active IP addresses to identify possible targets for exploitation. IC Block Scanning can be completed by using different tools, scripts, bots, and then can even be done surreptitiously. The method of IC Block scanning is worked into the reconnaissance phase where adversaries are gathering information about their target, in this case, a target network. This information can then be used to develop an attack strategy.

Vulnerability Scanning: -

Adversaries may gather information about the victim's network infrastructure that can be used during targeting. Information about network infrastructure may include a variety of details, including IP ranges, domain names, and network configurations. This information may help adversaries to determine the best methods for further compromise. Adversaries may gather this information in several ways, such as querying publicly available information,

using open-source intelligence (OSINT) tools, or compromising third-party services. The gathered information can be used to identify potential vulnerabilities and plan subsequent attacks.

Gather Victim Network Information: -

T1590, also known as Gather Victim Network Information, is a technique used by adversaries to collect information about a target's network infrastructure. This information can include details about IP addresses, domain names, network configurations, and other relevant data that can help adversaries in planning and executing further attacks. The gathered information can be obtained through various means such as scanning, querying publicly available data, or leveraging compromised systems. This technique is part of the reconnaissance phase, where adversaries aim to understand the target environment to identify potential vulnerabilities and plan their attack strategies effectively.

Network Topology: -

T1590.004, a technique under the MITRE ATT&CK framework, involves adversaries gathering information about an organization's network trust dependencies. This includes identifying relationships between different networks, domains, or systems that trust each other, which can be exploited to facilitate further attacks. Adversaries may use various methods to collect this information, such as analysing network traffic, querying domain name system (DNS) records, or leveraging publicly available information. Understanding these trust relationships can help adversaries move laterally within a network, escalate privileges, or exfiltrate data by exploiting the inherent trust between systems.

IP Addresses: -

T1590.005 is a tactic described in the MITRE ATT&CK framework in which the attackers gather information about trusted relationships across a victim's network. Specifically, it involves learning how networks, domains, or organizations are interconnected that is, trusted relationships, which can be used as a conduit for further attacks. Adversaries obtain and collect this information through the use of some or all of the following methods: the examination of public

sources, social engineering, and the compromise of trusted third parties. Understanding these trust relationships could help adversaries in attack planning and execution that leverage dependencies, for example, in attacks on the software supply chain or lateral movement within a network.

Summary: -

In summary, the ATT&CK framework is a resource for organizations seeking to improve their defence against cyber threats and understand the various tactics and techniques used by cyber adversary's exploits. It allows an organization to develop a strong cybersecurity program, mitigate risks and to better the organization's defences to combat the increasingly more complex and