MITRE ATT&CK Framework BY P3NGU1N

- **Introduction to MITRE**
- **MITRE was founded in 1958 in the USA**
- **produces innovative solutions to advance national security in new ways**

What is MITRE ATT&CK Framework?

- MITRE ATT&CK that stands for Adversarial Tactics, Techniques, and Common Knowledge
- introduced in 2013
- to analyze cyber attacks systematically through the MITRE ATT&CK framework

Why is the MITRE ATT&CK Framework important to SOC Analyst?

- SOC Analysts can clearly see the actions that should be taken for each stage of the cyber attack
- attack detection and mitigation techniques developed against cyber attacks can be used more effectively
- provides a clear roadmap of cyber attacks, research can be conducted on other possible cyber attacks that have not occurred yet

> 🎯 QUESTION:
>
> In what year was the MITRE founded?
>
> ANSWER: 1958

🎯 QUESTION:

In what year was MITRE ATT&CK Framework started to be developed?

ANSWER: 2013

What is MITRE ATT&CK Matrix?

- **visualization method used to classify and see attack methods**
- **matrices to visualize the details of attacker behavior using the matrices**

Types of Matrices:

- Enterprise Matrix
- Mobile Matrix
- ICS (Industrial Control Systems) Matrix

Enterprise Matrix:

- Enterprise matrix is mainly used to understand the cyber attacks on large organizations.

here are 7 sub-matrices under the Enterprise Matrix

- PRE
- Windows
- macOS
- Linux
- Cloud
- Network
- Containers

Mobile Matrix:

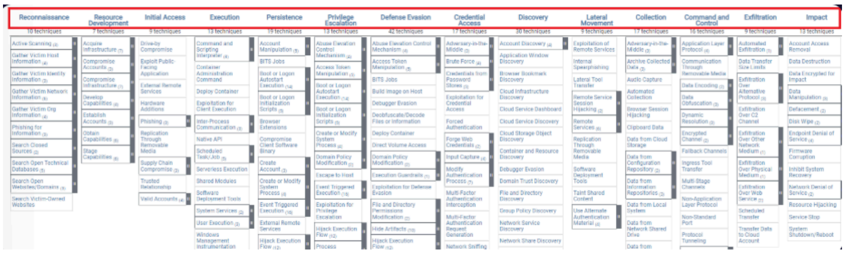
- prepared for mobile devices and contains information about the cyber security of mobile devices.
- ensure the security of individual and corporate mobile devices
- less informative compared to enterprise matrix

ICS Matrix

- Contains the information collected for the cyber security of devices in the industrial control systems
- matrix can be used to provide cyber security and analyses of an ICS.

What is Tactic?

- **Tactic expresses the purpose of the cyber attacker**
- **used to group cyber attacker behaviors**
- **see the attack steps**



Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion
10 techniques	7 techniques	9 techniques	13 techniques	19 techniques	13 techniques	42 techniques
Active Scanning (3)	Acquire Infrastructure (7)	Drive-by Compromise	Command and Scripting Interpreter (8)	Account Manipulation (5)	Abuse Elevation Control Mechanism (4)	Abuse Elevation Control Mechanism (4)
Gather Victim Host Information (4)	Compromise Accounts (3)	Exploit Public-Facing Application	Container Administration Command	BITS Jobs	Access Token Manipulation (5)	Access Token Manipulation (5)
Gather Victim Identity Information (3)	Compromise Infrastructure (7)	External Remote Services	Deploy Container	Boot or Logon Autostart Execution (14)	Boot or Logon Autostart Execution (14)	BITS Jobs
Gather Victim Network Information (6)	Develop Capabilities (4)	Hardware Additions	Exploitation for Client Execution	Boot or Logon Initialization Scripts (5)	Boot or Logon Initialization Scripts (5)	Build Image on Host
Gather Victim Org Information (4)	Establish Accounts (3)	Phishing (3)	Inter-Process Communication (3)	Browser Extensions	Create or Modify System Process (4)	Debugger Evasion
Phishing for Information (3)	Obtain Capabilities (6)	Replication Through Removable Media	Native API	Compromise Client Software Binary	Domain Policy Modification (2)	Deobfuscate/Decode Files or Information
Search Closed Sources (2)	Stage Capabilities (6)	Supply Chain Compromise (3)	Scheduled Task/Job (5)	Create Account (3)	Escape to Host	Deploy Container
Search Open Technical Databases (5)		Trusted Relationship	Serverless Execution	Create or Modify System Process (4)	Event Triggered Execution (16)	Direct Volume Access
Search Open Websites/Domains (3)		Valid Accounts (4)	Shared Modules	Event Triggered Execution (16)	Exploitation for Privilege Escalation	Domain Policy Modification (2)
Search Victim-Owned Websites			Software Deployment Tools	External Remote Services	Hijack Execution Flow (12)	Execution Guardrails (1)
			System Services (2)	Hijack Execution Flow (12)	Process	Exploitation for Defense Evasion
			User Execution (3)			File and Directory Permissions Modification (2)
			Windows Management Instrumentation			Hide Artifacts (10)
						Hijack Execution Flow (12)

Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
17 techniques	30 techniques	9 techniques	17 techniques	16 techniques	9 techniques	13 techniques
Adversary-in-the-Middle (3)	Account Discovery (4)	Exploitation of Remote Services	Adversary-in-the-Middle (3)	Application Layer Protocol (4)	Automated Exfiltration (1)	Account Access Removal
Brute Force (4)	Application Window Discovery	Internal Spearphishing	Archive Collected Data (3)	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction
Credentials from Password Stores (5)	Browser Bookmark Discovery	Lateral Tool Transfer	Audio Capture	Data Encoding (2)	Exfiltration Over Alternative Protocol (3)	Data Encrypted for Impact
Exploitation for Credential Access	Cloud Infrastructure Discovery	Remote Service Session Hijacking (2)	Automated Collection	Data Obfuscation (3)	Exfiltration Over C2 Channel	Data Manipulation (3)
Forced Authentication	Cloud Service Dashboard	Remote Services (6)	Browser Session Hijacking	Dynamic Resolution (3)	Exfiltration Over Other Network Medium (1)	Defacement (2)
Forge Web Credentials (2)	Cloud Service Discovery	Replication Through Removable Media	Clipboard Data	Encrypted Channel (2)	Exfiltration Over Physical Medium (1)	Disk Wipe (2)
Input Capture (4)	Cloud Storage Object Discovery	Software Deployment Tools	Data from Cloud Storage	Fallback Channels	Exfiltration Over Web Service (2)	Endpoint Denial of Service (4)
Modify Authentication Process (7)	Container and Resource Discovery	Taint Shared Content	Data from Configuration Repository (2)	Ingress Tool Transfer	Scheduled Transfer	Firmware Corruption
Multi-Factor Authentication Interception	Debugger Evasion	Use Alternate Authentication Material (4)	Data from Information Repositories (3)	Multi-Stage Channels	Transfer Data to Cloud Account	Inhibit System Recovery
Multi-Factor Authentication Request Generation	Domain Trust Discovery		Data from Local System	Non-Application Layer Protocol		Network Denial of Service (2)
Network Sniffing	File and Directory Discovery		Data from Network Shared Drive	Non-Standard Port		Resource Hijacking
	Group Policy Discovery		Data from	Protocol Tunneling		Service Stop
	Network Service Discovery					System Shutdown/Reboot
	Network Share Discovery					

Types of Tactics

Enterprise Tactics

There are 14 tactics in the Enterprise matrix as in the list below:

- Reconnaissance
- Resource Development

- Initial Access
- Execution
- Persistence
- Privilege Escalation
- Defense Evasion
- Credential Access
- Discovery
- Lateral Movement
- Collection
- Command and Control
- Exfiltration
- Impact

Mobile Tactics

There are 14 tactics in the Mobile matrix as in the list below:

- Initial Access
- Execution
- Persistence
- Privilege Escalation
- Defense Evasion
- Credential Access
- Discovery
- Lateral Movement
- Collection
- Command and Control
- Exfiltration
- Impact
- Network Effects

- Remote Service Effects

ICS Tactics

There are 12 tactics in the ICS matrix as in the list below:

- Initial Access
- Execution
- Persistence
- Privilege Escalation
- Evasion
- Discovery
- Lateral Movement
- Collection
- Command and Control
- Inhibit Response Function
- Impair Process Control
- Impact

🎯 QUESTION:

What is the ID of the "Lateral Movement" tactic in the Enterprise matrix?

ANSWER: TA0008

🎯 QUESTION:

When was the "Persistence" tactic in the mobile matrix created?

Answer Format: DD Month YYYY

ANSWER: 17 October 2018

🎯 QUESTION:

What is the name of the tactic in Enterprise, Mobile and ICS matrices which is under the techniques related to obtaining higher-level permission on the target system/network?

ANSWER: Privilege Escalation

Techniques and Sub-Techniques:

- Tactics contain the attackers aim not detailed information
- techniques contain the attackers method used to achieve goal
- each tactic has multiple techniques and sub techniques
- some techniques have sub techniques and some do not

Types of Techniques and Sub Techniques:

divided into 3 groups:

- enterprise techniques
- mobile techniques
- ICS techniques

What is a procedure:

consists of examples of techniques and sub-tech

it explains the use of technique

🎯 QUESTION:

What is the name of the technique with the ID T1055 among the Enterprise techniques?

ANSWER: Process Injection

🎯 QUESTION:

Among the Enterprise techniques, which platform is the technique with the ID T1112 for?

ANSWER: Windows

🎯 QUESTION:

Under which tactic is the "Supply Chain Compromise" technique which is among the Enterprise techniques?

ANSWER: Initial Access

Mitigations:

actions taken in response to techniques

mitigation has a unique id and description

Types of mitigations:

- Enterprise Mitigation
- mobile mitigation
- ICS mitigation

all have mitigations which apply to different techniques

🎯 QUESTION:

What is the name of the mitigation with the ID M1032 among the Enterprise mitigations?

ANSWER: multi-factor authentication

🎯 QUESTION:

What is the name of enterprise mitigation that recommends “digital signature verification should be implemented to prevent the untrusted codes from working on enterprise devices”?

ANSWER: code signing

Groups:

- APT groups are hacker groups, they carryout cyber attacks with gov support
- in mitre info about apt groups is collected which helps identify which apt group is targetting

- with mitre the attack map of an apt group can be revealed
- we can see what techniques they used in order to achieve their goals
- Under the “Techniques” column, you can see what tools, software or techniques that the APT group was leveraged for the attack.

Total groups : 170

🎯 QUESTION:

What is the name of the software that is associated only with the "System Information Discovery" technique among the software utilized by the OilRig APT group?

ANSWER: systeminfo

🎯 QUESTION:

What is the name of the APT group whose “Associated Groups” information includes the names “GOLD NIAGARA”, “ITG14” and “Carbon Spider”?

ANSWER: FIN7

Software:

- programs developed to work on digital systems
- software used by apt groups are mentioned in mitre
- each software has unique id and description
- u can slick on software and get to know which group used to achieve which goal

total software: 877

🎯 QUESTION:

For which platform is the software named “Cryptoistic” utilized by “Lazarus Group” APT group meant for?

ANSWER: macOS

🎯 QUESTION:

What is the type of software named “Rotexy” for Android platforms?

ANSWER: malware

🎯 QUESTION:

What is the name of the APT group that utilizes the software named “PUNCHBUGGY” targeting POS networks?

ANSWER: fin8

QUIZ:

1.**What is the concept that expresses the motivation for the action of the cyber attacker within the MITRE ATT&CK Framework?**

ANSWER: Tactic

2.**What is the concept that explains how the cyber attacker performs his action within the MITRE ATT&CK Framework?**

ANSWER: Technique

3.**What is the concept that expresses the application examples of the method used by the cyber attacker within the MITRE ATT&CK Framework?**

Answer: Procedure

4.**Which of the following is an ID of a technique in the MITRE ATT&CK Framework?**

ANSWER: T1426

5.**Which of the following enterprise techniques belongs to a different tactic?**

ANSWER: Exploit Public-Facing Application

6.**In which matrix is the "Impair Process Control" tactic located?**

ANSWER: ICS Matrix

7.**What is the tool used for credential dumping specifically only for Linux systems by the "TeamTNT" APT group?**

ANSWER: LaZagne