

MITRE ATT&CK FRAMEWORK

Page No	INDEX
1	WHAT IS MITRE ATT&CK FRAMEWORK ?
2	ATT&CKS DESCRIPTION
3	ATT&CK MATRIX

WHAT IS MITRE ATT\$CK FRAMEWORK ?

- Mitre is a non-profitable organization which work with the companies to help them protect themselves and provide deep insight into attacker behaviour.
- Mitre attack helps to identify most of the attacks and mitigate them.
- It was created by the Mitre Corporation and released in 2013.
- Attacks stands for Adversarial, Tactics, Techniques, and Common Knowledge.

ATTACKS DESCRIPTION OF TACTICS, TECHNIQUES, AND PROCEDURES (TTPS) PROVIDES DEEP INSIGHT INTO ATTACKER BEHAVIOUR.

- **ADVERSARIAL TACTICS** : Describe their goals, like getting inside your network or stealing credentials.
- **TECHNIQUES** : Show how they do it, Spear phishing
- **Procedures/ Common knowledge** : Highly detailed examples of the tools and actions of specific attacker groups.

ATT\$CK MATRIX

Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement
10 techniques	8 techniques	10 techniques	14 techniques	20 techniques	14 techniques	43 techniques	17 techniques	32 techniques	9 techniques
Active Scanning (3)	Acquire Access	Content Injection	Cloud Administration Command	Account Manipulation (6)	Abuse Elevation Control Mechanism (6)	Abuse Elevation Control Mechanism (6)	Adversary-in-the-Middle (3)	Account Discovery (4)	Exploitation of Remote Services
Gather Victim Host Information (4)	Acquire Infrastructure (8)	Drive-by Compromise	Command and Scripting Interpreter (10)	BITS Jobs	Access Token Manipulation (5)	Access Token Manipulation (5)	Brute Force (4)	Application Window Discovery	Internal Spearphishing
Gather Victim Identity Information (3)	Compromise Accounts (8)	Exploit Public-Facing Application	Container Administration Command	Boot or Logon Autostart Execution (14)	Account Manipulation (6)	BITS Jobs	Credentials from Password Stores (6)	Browser Information Discovery	Lateral Tool Transfer
Gather Victim Network Information (6)	Compromise Infrastructure (8)	External Remote Services	Deploy Container	Boot or Logon Initialization Scripts (5)	Boot or Logon Autostart Execution (14)	Build Image on Host	Exploitation for Credential Access	Cloud Infrastructure Discovery	Remote Service Session Hijacking (2)
Gather Victim Org Information (4)	Develop Capabilities (4)	Hardware Additions	Exploitation for Client Execution	Browser Extensions	Boot or Logon Initialization Scripts (5)	Debugger Evasion	Forced Authentication	Cloud Service Dashboard	Remote Services (8)
Phishing for Information (4)	Establish Accounts (3)	Phishing (4)	Inter-Process Communication (3)	Compromise Host Software Binary	Create or Modify System Process (5)	Deobfuscate/Decode Files or Information	Forge Web Credentials (2)	Cloud Service Discovery	Replication Through Removable Media
Search Closed Sources (2)	Obtain Capabilities (7)	Replication Through Removable Media	Native API	Create Account (3)	Domain or Tenant Policy Modification (2)	Deploy Container	Input Capture (4)	Cloud Storage Object Discovery	Software Deployment Tools
Search Open Technical Databases (5)	Stage Capabilities (6)	Supply Chain Compromise (3)	Scheduled Task/Job (5)	Create or Modify System Process (5)	Domain or Tenant Policy Modification (2)	Direct Volume Access	Modify Authentication Process (9)	Container and Resource Discovery	Taint Shared Content
Search Open Websites/Domains (3)		Trusted Relationship	Serverless Execution	Event Triggered Execution (16)	Escape to Host	Execution Guardrails (1)	Multi-Factor Authentication Interception	Debugger Evasion	Use Alternate Authentication Material (4)
Search Victim-Owned Websites		Valid Accounts (4)	Shared Modules	External Remote Services	Event Triggered Execution (16)	Exploitation for Defense Evasion	Multi-Factor Authentication Request Generation	Device Driver Discovery	
			Software Deployment Tools	Hijack	Exploitation for Privilege Escalation	File and Directory Permissions Modification (2)		Domain Trust Discovery	
			System Services (2)			Hide Artifacts (12)		File and Directory Discovery	
						Hijack Execution		Group Policy	

https://attck-matrix.com/techniques/51594