OWASP
Open Web Application
Security Project

Cyber Attacks
Tactics & Techniques

Andres More/Leonardo Frittelli

McAfee Cordoba

Agenda

- Attacks
  - Application vs Platform
  - Tactics vs Techniques
- MITRE's ATT&CK
  - Tactics and Techniques Matrix
  - Review techniques related to OWASP

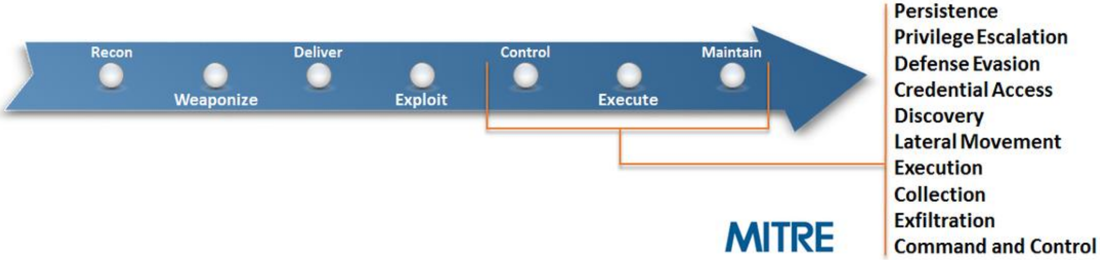
Attacks

- Definition:
  - – Technique used to exploit vulnerabilities
- Tactics vs Techniques
- Application vs Platform Attacks

OWASP Attack Reference

- Application Security Attacks
- 12 subcategories with 70 pages total
  - *Abuse of Functionality, Data Structure, Embedded Malicious Code, Exploitation of Authentication, Injection, Probabilistic Techniques, Protocol Manipulation, Resource Depletion, Resource Manipulation, Sniffing Attacks, Spoofing*.
- Described attacks may belong to +1 category

ATT&CK



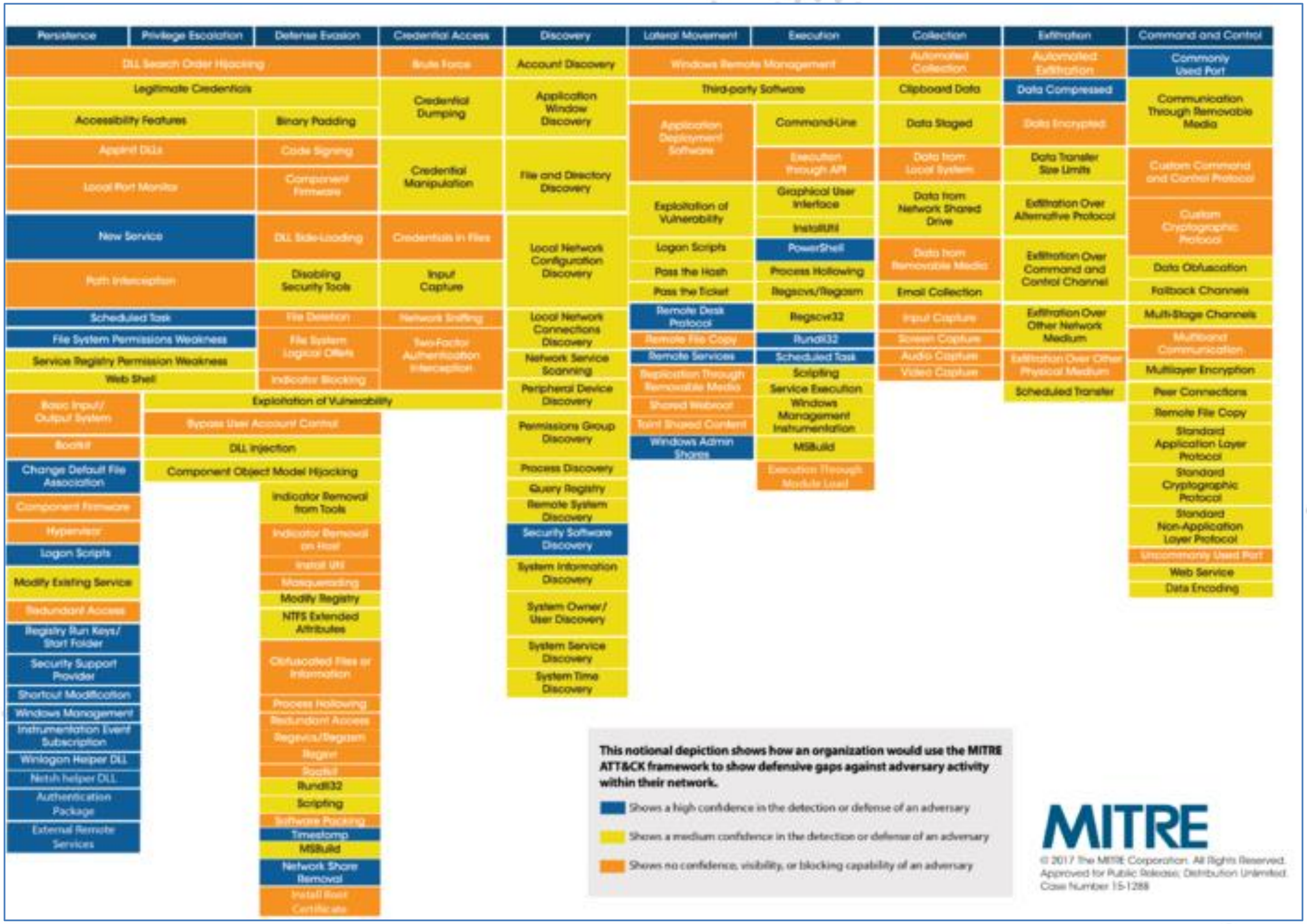
Recon
Weaponize
Deliver
Exploit
Control
Execute
Maintain

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

MITRE

- Cyber Kill Chain (Lockheed)
- PRE-ATT&CK (MITRE)
  - Outside perimeter, pre-exploit
- ATT&CK (MITRE)
  - Engaging Adversarial Tactics, Techniques, and Common Knowledge
  - Techniques across Windows, Linux and MacOS
  - Navigator Tool & STIX 2.0 JSON Mapping Available

ATT&CK - Gap Analysis Example



Persistence

- 🟧 DLL Search Order Hijacking
- 🟨 Legitimate Credentials
- 🟨 Accessibility Features
- 🟧 AppInit DLLs
- 🟧 Local Port Monitor
- 🟦 New Service
- 🟧 Path Interception
- 🟦 Scheduled Task
- 🟦 File System Permissions Weakness
- 🟨 Service Registry Permission Weakness
- 🟨 Web Shell
- 🟧 Basic Input/Output System
- 🟧 Bootkit
- 🟦 Change Default File Association
- 🟧 Component Firmware
- 🟧 Hypervisor
- 🟦 Logon Scripts
- 🟨 Modify Existing Service
- 🟧 Redundant Access
- 🟦 Registry Run Keys/Start Folder
- 🟦 Security Support Provider
- 🟦 Shortcut Modification
- 🟦 Windows Management Instrumentation Event Subscription
- 🟦 Winlogon Helper DLL
- 🟦 Netsh helper DLL
- 🟦 Authentication Package
- 🟦 External Remote Services

Privilege Escalation

- 🟨 Exploitation of Vulnerability
- 🟧 Bypass User Account Control
- 🟨 DLL Injection
- 🟨 Component Object Model Hijacking

Defense Evasion

- 🟨 Binary Padding
- 🟧 Code Signing
- 🟧 Component Firmware
- 🟧 DLL Side-Loading
- 🟨 Disabling Security Tools
- 🟧 File Deletion
- 🟧 File System Logical Offsets
- 🟧 Indicator Blocking
- 🟨 Indicator Removal from Tools
- 🟧 Indicator Removal on Host
- 🟧 Install Util
- 🟧 Masquerading
- 🟨 Modify Registry
- 🟨 NTFS Extended Attributes
- 🟧 Obfuscated Files or Information
- 🟧 Process Hollowing
- 🟧 Redundant Access
- 🟧 Regsvcs/Regasm
- 🟧 Regsvr
- 🟧 Rootkit
- 🟨 Rundll32
- 🟨 Scripting
- 🟧 Software Packing
- 🟦 Timestomp
- 🟨 MSBuild
- 🟦 Network Share Removal
- 🟧 Install Root Certificate

Credential Access

- 🟧 Brute Force
- 🟨 Credential Dumping
- 🟨 Credential Manipulation
- 🟧 Credentials in Files
- 🟨 Input Capture
- 🟧 Network Sniffing
- 🟧 Two-Factor Authentication Interception

Discovery

- 🟨 Account Discovery
- 🟨 Application Window Discovery
- 🟨 File and Directory Discovery
- 🟨 Local Network Configuration Discovery
- 🟨 Local Network Connections Discovery
- 🟨 Network Service Scanning
- 🟨 Peripheral Device Discovery
- 🟨 Permissions Group Discovery
- 🟨 Process Discovery
- 🟨 Query Registry
- 🟨 Remote System Discovery
- 🟦 Security Software Discovery
- 🟨 System Information Discovery
- 🟨 System Owner/User Discovery
- 🟨 System Service Discovery
- 🟨 System Time Discovery

Lateral Movement

- 🟧 Windows Remote Management
- 🟨 Third-party Software
- 🟧 Application Deployment Software
- 🟨 Exploitation of Vulnerability
- 🟨 Logon Scripts
- 🟨 Pass the Hash
- 🟨 Pass the Ticket
- 🟦 Remote Desktop Protocol
- 🟧 Remote File Copy
- 🟦 Remote Services
- 🟧 Replication Through Removable Media
- 🟧 Shared Webroot
- 🟧 Taint Shared Content
- 🟦 Windows Admin Shares

Execution

- 🟨 Command-Line
- 🟧 Execution through API
- 🟨 Graphical User Interface
- 🟨 InstallUtil
- 🟦 PowerShell
- 🟨 Process Hollowing
- 🟨 Regsvcs/Regasm
- 🟨 Regsvr32
- 🟦 Rundll32
- 🟦 Scheduled Task
- 🟨 Scripting
- 🟨 Service Execution
- 🟨 Windows Management Instrumentation
- 🟨 MSBuild
- 🟧 Execution Through Module Load

Collection

- 🟧 Automated Collection
- 🟨 Clipboard Data
- 🟨 Data Staged
- 🟧 Data from Local System
- 🟨 Data from Network Shared Drive
- 🟧 Data from Removable Media
- 🟨 Email Collection
- 🟧 Input Capture
- 🟧 Screen Capture
- 🟧 Audio Capture
- 🟧 Video Capture

Exfiltration

- 🟧 Automated Exfiltration
- 🟦 Data Compressed
- 🟧 Data Encrypted
- 🟨 Data Transfer Size Limits
- 🟨 Exfiltration Over Alternative Protocol
- 🟨 Exfiltration Over Command and Control Channel
- 🟨 Exfiltration Over Other Network Medium
- 🟧 Exfiltration Over Other Physical Medium
- 🟨 Scheduled Transfer

Command and Control

- 🟦 Commonly Used Port
- 🟨 Communication Through Removable Media
- 🟧 Custom Command and Control Protocol
- 🟧 Custom Cryptographic Protocol
- 🟨 Data Obfuscation
- 🟨 Fallback Channels
- 🟨 Multi-Stage Channels
- 🟧 Multiband Communication
- 🟨 Multilayer Encryption
- 🟨 Peer Connections
- 🟨 Remote File Copy
- 🟨 Standard Application Layer Protocol
- 🟨 Standard Cryptographic Protocol
- 🟨 Standard Non-Application Layer Protocol
- 🟧 Uncommonly Used Port
- 🟨 Web Service
- 🟨 Data Encoding

This notional depiction shows how an organization would use the MITRE ATT&CK framework to show defensive gaps against adversary activity within their network.

- 🟦 Shows a high confidence in the detection or defense of an adversary
- 🟨 Shows a medium confidence in the detection or defense of an adversary
- 🟧 Shows no confidence, visibility, or blocking capability of an adversary

MITRE

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

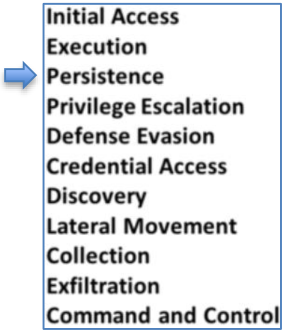
Tactic: Initial Access

- The initial access tactic represents the vectors adversaries use to **gain an initial foothold** within a network.
- 10 documented techniques
- Exploit Public-Facing Application
  - *For websites and databases, the OWASP top 10 gives a good list of the top 10 most common web-based vulnerabilities.*

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

Tactic: Execution

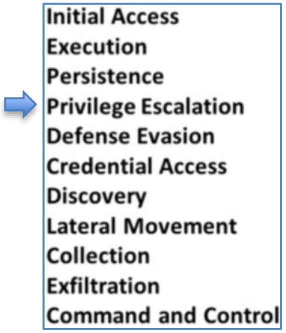
- The execution tactic represents techniques that result in **execution of adversary-controlled code** on a local or remote system.
- 31 documented techniques
- Exploitation for Client Execution
  - *Vulnerabilities can exist in software due to unsecure coding practices that can lead to unanticipated behavior.*



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

Tactic: Persistence

- Persistence gives persistent **presence** on that system. Attackers need to maintain access through **interruptions** such as system restarts, loss of credentials, or others.
- 56 documented techniques
  - *Registry Run Keys/Start Folder*



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

Tactic: Privilege Escalation

- Privilege escalation allow an adversary to obtain a **higher level** set of permissions. Adversaries can start with unprivileged access and need more privileges or permissions to access specific systems or capabilities.
- 28 documented techniques
  - *Exploitation for Privilege Escalation*

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

Tactic: Defense Evasion

- Defense evasion consists of techniques an adversary may use to **evade detection** or avoid other defenses.
- 59 documented techniques
- Exploitation for Defense Evasion
  – *OSV-Level Vulnerabilities*

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

Tactic: Credential Access

- Credential access to or control over system, domain, or service credentials allows the adversary to assume other **identities**, with all of that account's permissions.
- 21 documented techniques
- Exploitation for Credential Access
  - *Service-Level Vulnerabilities*

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

Tactic: Discovery

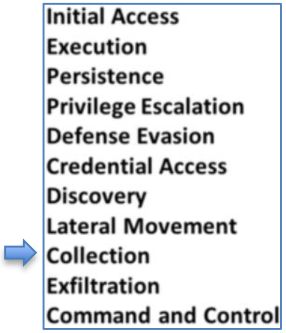
- Discovery consists of techniques that allow the adversary to gain **knowledge** about the system and internal network.
- 19 documented techniques
  - *Account discovery*
  - *Network share discovery*

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

Tactic: Lateral Movement

- Lateral movement consists of techniques that enable an adversary to **access and control remote systems** on a network and could, but does not necessarily, include execution of tools on remote systems.
- 17 documented techniques
- Exploitation of Remote Services
  - *Service Level Vulnerability*

Tactic: Collection



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

- Collection consists of techniques used to **identify and gather information**, such as sensitive files, from a target network prior to exfiltration.
- 13 documented techniques
  - *Clipboard, Input Capture*
  - *Local Data, Shared Drive Data*

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

Tactic: Exfiltration

- Exfiltration refers to techniques and attributes that result or aid in the adversary **removing files and information** from a target network.
- 9 documented techniques
  - *Compression & Encryption*
  - *Network & Alternative Protocols*

Tactic: Command and Control

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

- How adversaries **communicate** with systems under their control within a target network.
- 21 documented techniques
  - – *Standard Protocol*
  - – *Port Knocking*

References

- Application Security Attacks from OWASP
- Cyber Kill Chain from Lockheed Martin
- ATT&CK from MITRE