

# Overview

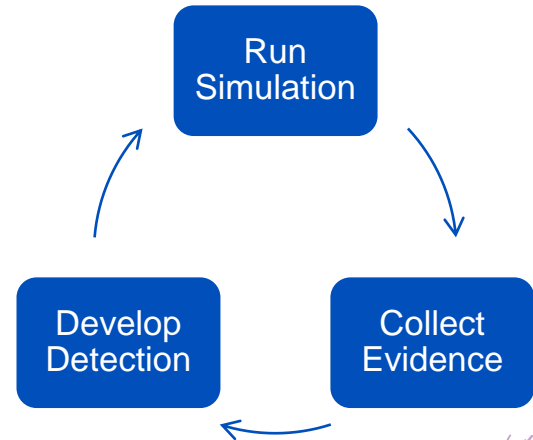
- What is Breach and Attack Simulation (BAS)
- Why Use BAS tools
  - Measure defensive capabilities
- Overview of the MITRE ATT&CK Matrix
  - Compare with Trickbot
- List of Open Source tools
- Overview of the various tools

# What is BAS

- Ability to simulate adversarial activities with some degree of automation. [1]
- May be adversary model based, for example the Adversarial Tactics, Techniques & Common Knowledge (ATT&CK™) project. [2]

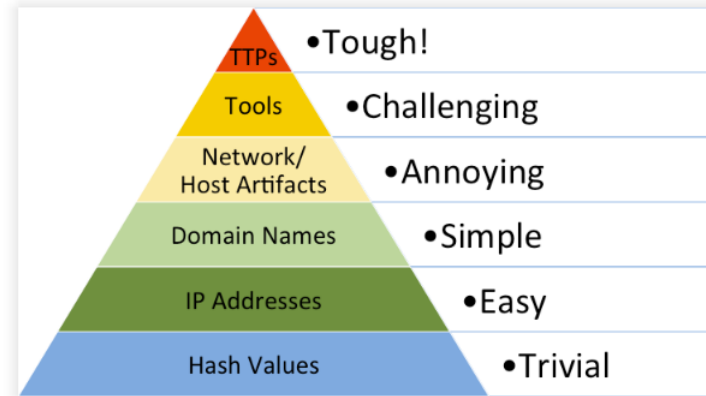
# Why use BAS tools

- Measure defensive capabilities;
- Threat hunting and incident response preparedness;
- Gain insights into areas of potential vulnerability;
- Continual simulation testing highlights critical exposures in a network.



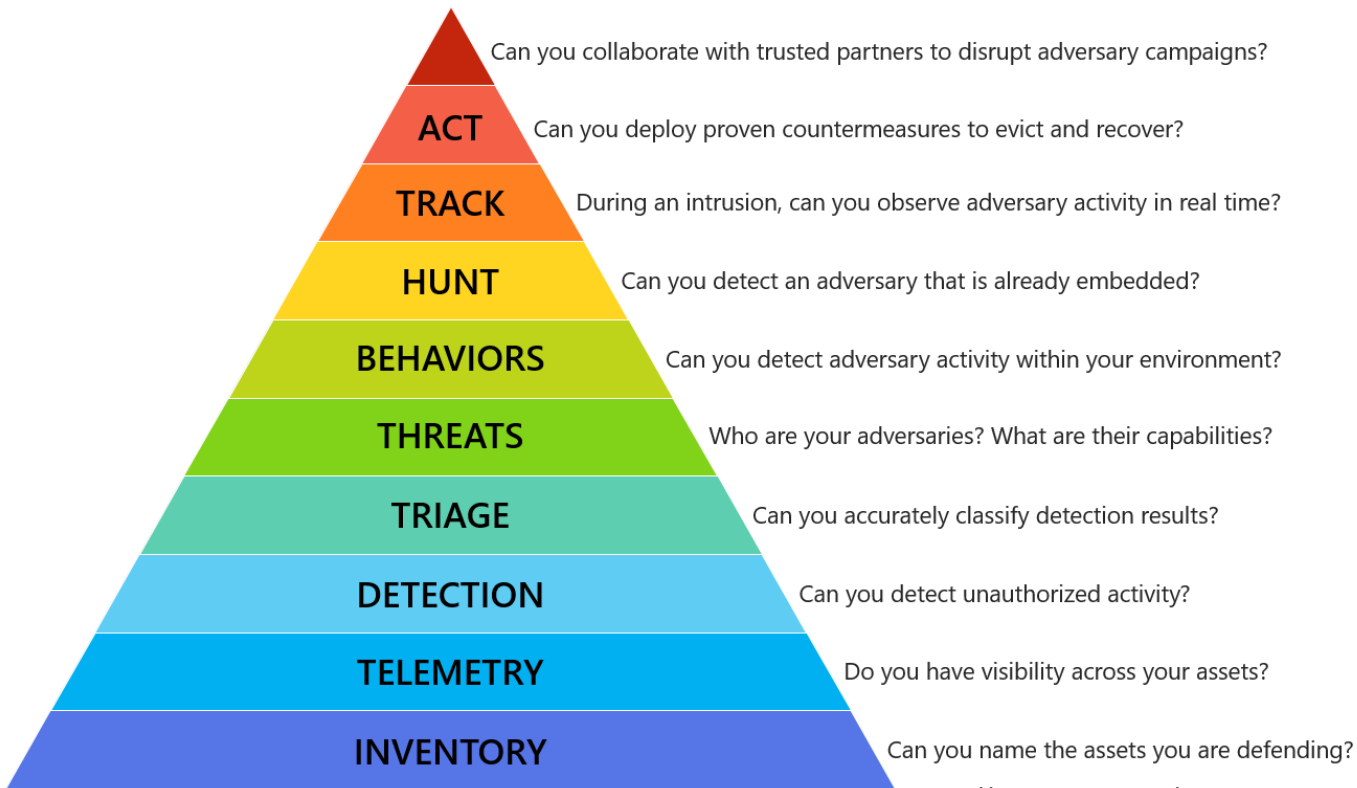
# Measure defensive capabilities

- Do your systems detect these malicious activities:
  - CLI or PowerShell attacks
  - C2 server communications
  - Ransomware
  - Trojans
  - Malicious scripts or executables
  - Man in the Middle attacks
  - Disabling Security Tools (T1089)
  - ... and many more
- Can you prove it?



<https://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html>

# The Incident Response Hierarchy of Needs



<https://github.com/swannman/ircapabilities>

# ATT&CK Matrix for Enterprise

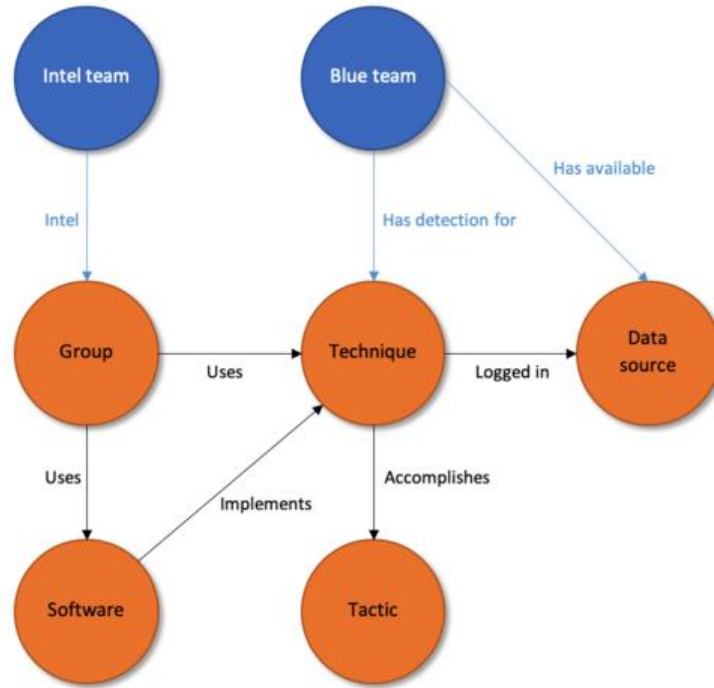
ATT&CK Matrix for Enterprise

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Automated Exfiltration	Commonly Used Port
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	BITS Jobs	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Data Compressed	Communication Through Removable Media
Hardware Additions	Command-Line Interface	Account Manipulation	AppCert DLLs	Binary Padding	Brute Force	Browser Bookmark Discovery	Distributed Component Object Model	Clipboard Data	Data Encrypted	Connection Proxy
Replication Through Removable Media	Compiled HTML File	AppCert DLLs	AppInit DLLs	Bypass User Account Control	Credential Dumping	File and Directory Discovery	Exploitation of Remote Services	Data Staged	Data Transfer Size Limits	Custom Command and Control Protocol
Spearphishing Attachment	Control Panel Items	AppInit DLLs	Application Shimming	CMSTP	Credentials in Files	Network Service Scanning	Logon Scripts	Data from Information Repositories	Exfiltration Over Alternative Protocol	Custom Cryptographic Protocol
Spearphishing Link	Dynamic Data Exchange	Application Shimming	Bypass User Account Control	Clear Command History	Credentials in Registry	Network Share Discovery	Pass the Hash	Data from Local System	Exfiltration Over Command and Control Channel	Data Encoding
Spearphishing via Service	Execution through API	Authentication Package	DLL Search Order Hijacking	Code Signing	Exploitation for Credential Access	Network Sniffing	Pass the Ticket	Data from Network Shared Drive	Exfiltration Over Other Network Medium	Data Obfuscation
Supply Chain Compromise	Execution through Module Load	BITS Jobs	Dylib Hijacking	Compiled HTML File	Forced Authentication	Password Policy Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Physical Medium	Domain Fronting
Trusted Relationship	Exploitation for Client Execution	Bootkit	Exploitation for Privilege Escalation	Component Firmware	Hooking	Peripheral Device Discovery	Remote File Copy	Email Collection	Scheduled Transfer	Fallback Channels
Valid Accounts	Graphical User Interface	Browser Extensions	Extra Window Memory Injection	Component Object Model Hijacking	Input Capture	Permission Groups Discovery	Remote Services	Input Capture		Multi-Stage Channels

# ATT&CK Matrix for Enterprise

- Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK);
- MITRE started this project in 2013 to document common tactics, techniques, and procedures (TTPs) an adversary takes while operating within an enterprise network;
- Help organizations understand the stages of attack events;
- Stage of event across top axis and the mechanism for that stage down the column.

# ATT&CK Matrix for Enterprise





# Trickbot mapped to ATT&CK Matrix

MITRE ATT&CK® Navigator

TrickBot (S0266) 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	34 items	62 items	32 items	69 items	21 items	23 items	18 items	13 items	22 items	9 items	16 items
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Commonly Used Port	Automated Exfiltration	Account Access Removal
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	Binary Padding	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Communication Through Removable Media	Data Compressed	Data Destruction
	Command-Line Interface			BITS Jobs	Brute Force	Browser Bookmark Discovery	Clipboard Data	Data Encrypted for Impact			
External Remote Services	Compiled HTML File	Account Manipulation	AppCert DLLs	Bypass User Account Control	Credential Dumping	Domain Trust Discovery	Component Object Model and Distributed COM	Data from Information Repositories	Connection Proxy	Data Transfer Size Limits	Defacement
				AppInIt DLLs					Clear Command History	File and Directory Discovery	Exploitation of Remote Services
Hardware Additions	Component Object Model and Distributed COM	AppInIt DLLs	Application Shimming	CMSTP	Credentials from Web Browsers	File and Directory Discovery	Internal Spearphishing	Data from Local System	Exfiltration Over Alternative Protocol	Disk Structure Wipe	
Replication Through Removable Media	Control Panel Items	Application Shimming	Bypass User Account Control	Code Signing	Credentials in Files	Network Service Scanning	Logon Scripts	Data from Network Shared Drive	Custom Cryptographic Protocol	Endpoint Denial of Service	
	Dynamic Data Exchange	Authentication Package	DLL Search Order Hijacking	Compile After Delivery	Credentials in Registry	Network Share Discovery	Pass the Hash	Data from Removable Media	Data Encoding	Exfiltration Over Command and Control Channel	
Spearphishing Attachment	Execution through API	BITS Jobs	Dylib Hijacking	Compiled HTML File	Exploitation for Credential Access	Network Sniffing	Pass the Ticket	Domain Fronting	Exfiltration Over Other Network Medium	Firmware Corruption	
Spearphishing Link	Execution through Module Load	Bootkit	Elevated Execution with Prompt	Component Firmware	Forced Authentication	Password Policy Discovery	Remote Desktop Protocol	Data Staged	Domain Generation Algorithms	Exfiltration Over Physical Medium	Inhibit System Recovery
Spearphishing via Service	Exploitation for Client Execution	Browser Extensions	Change Default File Association	Component Object Model Hijacking	Hooking	Peripheral Device Discovery	Remote File Copy	Email Collection	Fallback Channels	Network Denial of Service	
Supply Chain Compromise	Graphical User Interface	Component Firmware	Emond	Connection Proxy	Input Capture	Permission Groups Discovery	Remote Services	Man in the Browser	Multi-hop Proxy	Resource Hijacking	
Trusted Relationship	InstallUtil	Component Object Model Hijacking	Exploitation for Privilege Escalation	Control Panel Items	Input Prompt	Process Discovery	Replication Through Removable Media	Screen Capture	Multi-Stage Channels	Scheduled Transfer	Runtime Data Manipulation
			Extra Window Memory Injection	DCShadow	Query Registry	Remote System Discovery	Video Capture	Multiband Communication	Stored Data Manipulation		
Valid Accounts	Launchctl	File System Permissions Weakness	Deobfuscate/Decode Files or Information	Kernelboasting	Keychain	Security Software Discovery	Shared Webroot	SSH Hijacking	Multilayer Encryption	System Shutdown/Reboot	
	Local Job Scheduling	Create Account	Disabling Security Tools	LLMNR/NBT-NS Poisoning and Relay	Software Discovery	Taint Shared Content	Screen Capture	Port Knocking	Transmitted Data		
LSASS Driver	DLL Search Order Hijacking	DLL Side-Loading	DLL Search Order Hijacking	Network Sniffing	System Information Discovery	Third-party	Port Knocking				
Mshst	Dylib Hijacking	Hooking	DLL Side-Loading	Network Sniffing	System Information Discovery						
PowerShell			Execution Guardrails	Password Filter							

^ legend

# Open source tools

- Guardicore's Infection Monkey
  - <http://infectionmonkey.com>
- Uber's Metta -
  - <https://github.com/uber-common/metta>
- AlphaSOC's FlightSIM
  - <https://github.com/alphasoc/flightsim>
- Synex Caldera
  - <https://github.com/mitre/caldera>
- Blue team training toolkit (BT3)
  - <https://www.encrypted.no/en/downloads-2/tools/>
- Atomic Red Team
  - <https://atomicredteam.io>
- Redhunt OS
  - <https://github.com/redhuntlabs/RedHunt-OS>

# Infection Monkey

- Available for download, and as a virtual instance on Azure and Amazon marketplace.
- Designed to test the resilience of modern data centers and clouds against cyber attacks.
- Developed by GuardiCore Labs under the GPL v3 open source license.
- Comprised of two parts:
  - Monkey – A tool which infects other machines and propagates to them
  - Monkey Island – A Command & Control server with a dedicated UI to visualize the Chaos Monkey's progress

<https://github.com/guardicore/monkey>

# Infection Monkey

Microsoft Azure

All services >

## Marketplace

Get Started

Service Providers

### Management

Private Marketplace

Private Offer Management

### My Marketplace

Favorites

Recently created

Private products

### Categories

Networking (4)

Security (4)

infection

Showing results for 'infection'.

Showing 1 to 9 of 9 results.

### Guardicore Infection Monkey

GuardiCore

Virtual Machine

Open source attack simulation tool to test the resilience of Azure deployments against cyber attacks

Bring your own license

Create

aws marketplace

Sign In or Create a new account

About Categories Delivery Methods Solutions AWS IQ Resources Your Saved List Partners Sell In AWS Marketplace Amazon Web Services Home

## Infection Monkey

By: [Guardicore](#) Latest Version: 1.13.1

The Infection Monkey is an attack simulation tool designed to test networks against attackers. A self-propagating testing tool, it identifies and visualizes attack paths in your network and

[Show more](#)

Linux/Unix 0 AWS reviews | 3 external reviews

[Free Tier](#)

[Continue to Subscribe](#)

[Save to List](#)

Typical Total Price  
**\$0.046/hr**

Total pricing per instance for services hosted on 12 medium in US East (N. Virginia). [View Details](#)

Overview Pricing Usage Support Reviews

## Product Overview

The Infection Monkey is an open source attack simulation tool designed to test the resilience of modern data centers and clouds against cyber attacks. It scans the network, checking for open ports and fingerprinting machines using multiple network protocols. After detecting accessible machines, it attempts to attack every single machine using methods such as intelligent password guessing and safe exploits. The Infection Monkey provides detailed information about the specific vulnerability exploited and the effect vulnerable segments can have on the entire network, giving security teams the insights they need to make informed decisions and enforce tighter security policies. The Infection Monkey is designed to be 100 percent safe, with no reconnaissance or propagation features that can impact server or network stability.

Version	1.13.1 <a href="#">Show other versions</a>
By	<a href="#">Guardicore</a>
Categories	<a href="#">Security</a> <a href="#">Testing</a> <a href="#">Network Infrastructure</a>
Operating System	Linux/Unix, Ubuntu 18.04
Delivery Methods	<a href="#">Amazon Machine Image</a>

## Highlights

- Attack simulation tool designed to test post breach defenses.
- Provides actionable information to block and mitigate attack vectors.
- Provides a visual map of your network from an attacker's point of view.

# Metta

- An information security preparedness tool;
- Uses Redis/Celery, python, and vagrant to do adversarial simulation;
- Allows you to test (mostly) your host based instrumentation;
- Depending on how vagrant is setup. It may test network based detection and controls;
- Parses YAML files with actions and uses celery to queue these actions up and run them one at a time without interaction.

<https://github.com/uber-common/metta>

# Metta

- What protection is in place to detect this?
- Event logs?
  - 4661
  - 4662
  - 4663
- Command line process auditing?

The image displays four terminal windows from a host named 'apnic@ubuntu' in the directory '~/metta'.  
1. Top-left: Shows the process of starting a virtual machine named 'metta'. It lists various default settings like WinRM address, usernames, and execution time limits, and concludes with 'Machine booted and ready!'.  
2. Top-right: Shows the output of 'redis-server' starting. It displays the Redis version (3.0.6), mode (standalone), port (6379), and PID (1939). A warning about the TCP backlog setting is also visible.  
3. Bottom-left: Shows the execution of a Python script 'run\_simulation.yml.py'. It displays a progress bar and logs the execution of various actions like 'net user', 'net user /domain', and 'net localgroup administrators'.  
4. Bottom-right: Shows a system log snippet with timestamps and process IDs, detailing the booting of 'vagrant@ubuntu v4.2.1 (windowlicker)' and the start of 'simulation.log' and 'start\_vagrant\_celery.sh'.



screenshot.  
png



XTerm



# FlightSim

- Lightweight utility used to generate malicious network traffic
- Performs tests to simulate
  - Domain Name Service (DNS) tunneling,
  - Domain generation algorithms (DGA) traffic,
    - requests to known active C2 destinations.
  - and other suspicious traffic patterns.
- Help security teams to evaluate security controls and network visibility.

```
$ flightsim run dga
```

```
AlphaSOC Network Flight Simulator™ (https://github.com/alphasoc/flightsim)  
The IP address of the network interface is 172.31.84.103  
The current time is 10-Jan-18 09:30:28
```

```
Time      Module  Description  
-----
```

```
09:30:28 dga      Starting  
09:30:28 dga      Generating list of DGA domains  
09:30:30 dga      Resolving rdumomx.xyz  
09:30:31 dga      Resolving rdumomx.biz  
09:30:31 dga      Resolving rdumomx.top  
09:30:32 dga      Resolving qtovmrn.xyz  
09:30:32 dga      Resolving qtovmrn.biz  
09:30:33 dga      Resolving qtovmrn.top  
09:30:33 dga      Resolving pbuzkkk.xyz  
09:30:34 dga      Resolving pbuzkkk.biz  
09:30:34 dga      Resolving pbuzkkk.top  
09:30:35 dga      Resolving wfoheoz.xyz  
09:30:35 dga      Resolving wfoheoz.biz  
09:30:36 dga      Resolving wfoheoz.top  
09:30:36 dga      Resolving lhceftf.xyz  
09:30:37 dga      Resolving lhceftf.biz  
09:30:37 dga      Resolving lhceftf.top  
09:30:38 dga      Finished
```

```
All done! Check your SIEM for alerts using the timestamps and details above.
```



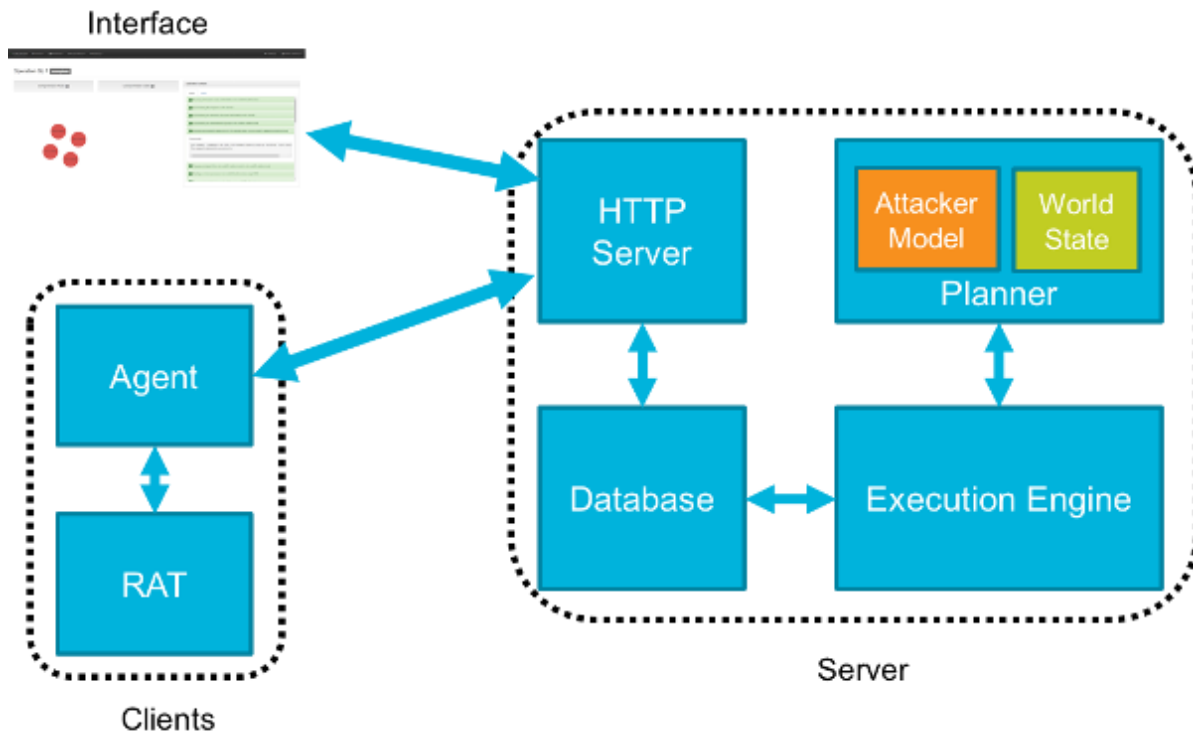


# Caldera

- CALDERA is a MITRE research project;
- An automated adversary emulation system;
- Performs post-compromise adversarial behavior within Windows Enterprise networks;
- Only supports Windows Enterprise networks that are configured as a Windows Domain;
- Generates plans during operation using a planning system and a pre-configured adversary model based on ATT&CK™

<https://github.com/mitre/caldera>

# Caldera



# Blue Team Training Toolkit (BT3)

- Created by Juan J. Güelfo;
- Used for defensive security training;
- Features include:
  - Adversary Replication and Malware Simulation - simulate malware infections or targeted attacks with specific C&C communications.
  - Network Traffic Manipulation and Replay - customise and replay network traffic stored in PCAP files.
  - Malware Sample Simulation - artifacts are harmless files that produce the same MD5 checksum as real malicious files.

# Atomic Red Team

- Library of tests;
- Mapped to the MITRE ATT&CK Framework;
- Should be able to run a test in less than five minutes;
- Test security controls and processes;
- Phased approach to running a test and evaluating results:
  1. Select a test
  2. Execute Test
  3. Collect Evidence
  4. Develop Detection
  5. Measure Progress

# Comparison

TACTIC NAME	INFECTION MONKEY	METTA	FlightSim	CALDERA	BT3	ATOMIC RED TEAM
Initial Access	Yes	No	No	No	No	Yes
Execution	Yes	Yes	Yes	Yes	Yes	Yes
Persistence	No	Yes	No	Yes	Yes	Yes
Privilege Escalation	No	Yes	No	Yes	No	Yes
Defense Evasion	No	Yes	Yes	Yes	No	Yes
Credential Access	Yes	Yes	No	Yes	Yes	Yes
Discovery	Yes	Yes	No	Yes	Yes	Yes
Lateral Movement	Yes	Yes	No	Yes	Yes	Yes
Collection	No	Yes	No	No	No	Yes
Exfiltration	No	Yes	No	Yes	No	Yes
Command & Control	Yes	Yes	Yes	No	Yes	Yes

# Threat Pursuit VM (Beta)

- <https://youtu.be/GrVj8h7uin0?t=148>
- Ubuntu Virtual machine with various tools installed, including:
  - Adversarial Emulation:
    - Caldera Apache 2.0  
<https://github.com/mitre/caldera/blob/master/LICENSE>
    - APT Simulator MIT  
<https://github.com/NextronSystems/APTSimulator/blob/master/LICENSE>
    - FlightSim Creative Commons  
<https://github.com/alphasoc/flightsim/blob/master/LICENSE>
    - Atomic Red Team MIT  
<https://github.com/redcanaryco/atomic-red-team/blob/master/LICENSE.txt>



# RedHunt-OS

- <https://github.com/redhuntlabs/RedHunt-OS>
- Ubuntu Virtual machine with various tools installed:
  - Attack Emulation:
    - Caldera
    - Atomic Red Team
    - DumpsterFire
    - Metta



# Other resources

- List of Adversary Simulation tools
  - <http://pentestit.com/adversary-emulation-tools-list/>
- Mitre ATT&CK framework
  - <https://attack.mitre.org>
- Rabobank-cdc DeTT&CT framework
  - <https://github.com/rabobank-cdc/DeTTECT>
- Risky Business Podcast
  - <https://risky.biz/RB587/> discussion about Mitre ATT&CK



# Thank You!

END OF SESSION

