MOBIA is a business technology integrator with over thirty years of experience and 500+ employees across Canada and USA. Our talented bench of technical engineers and trusted advisors deliver process improvements and business transformations within our core pillars of Cloud, Infrastructure, Software Development, Cybersecurity and Broadband & Wireless Services.

Our inside-out approach allows us to understand business challenges from deep within the organization, mapping the impact as it ripples outward. This insight enables us to create future-proof solutions that maximize results and repeatedly exceed our client’s expectations.

Adversary Simulation Workshop

Lab Guide:
ATT&CK Automation

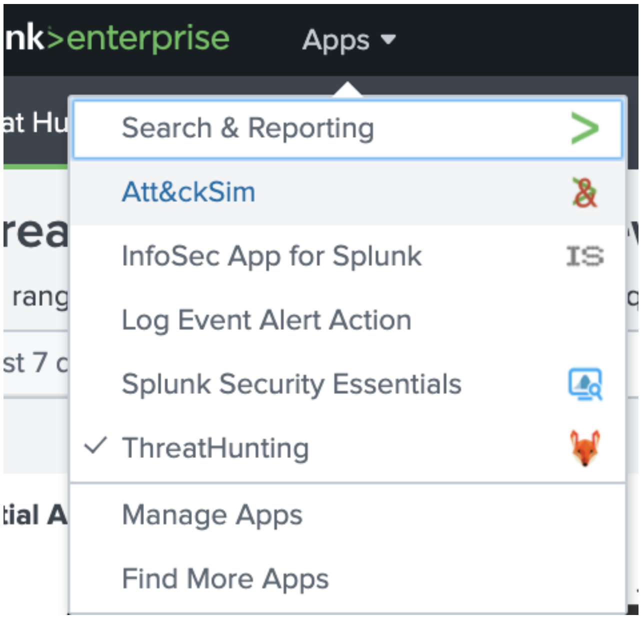
Objective:

Use the AttackSimulator app to trigger an atomic test on your student machine.

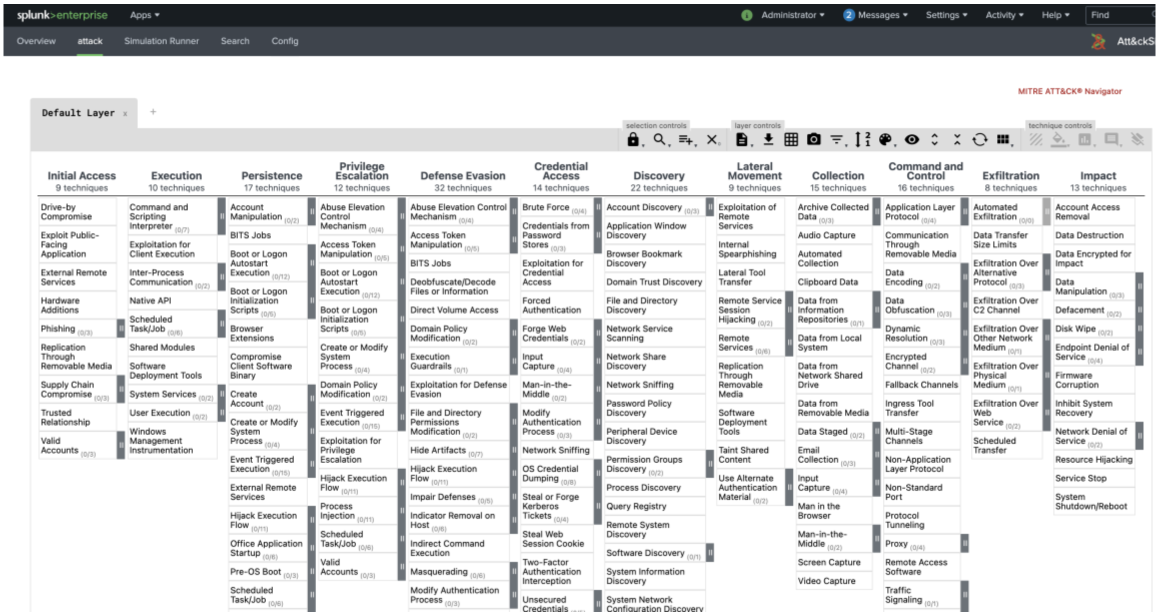
Instructions:

Note: There are various Enterprise grade commercial tools for adversary simulation, the AttackSimulator app is meant to provide a simple example of the use of automation for testing.

From the Apps menu choose the Att&ckSim app:



You will notice that when the app load you are presented with an embedded version of the ATT&CK Navigator:

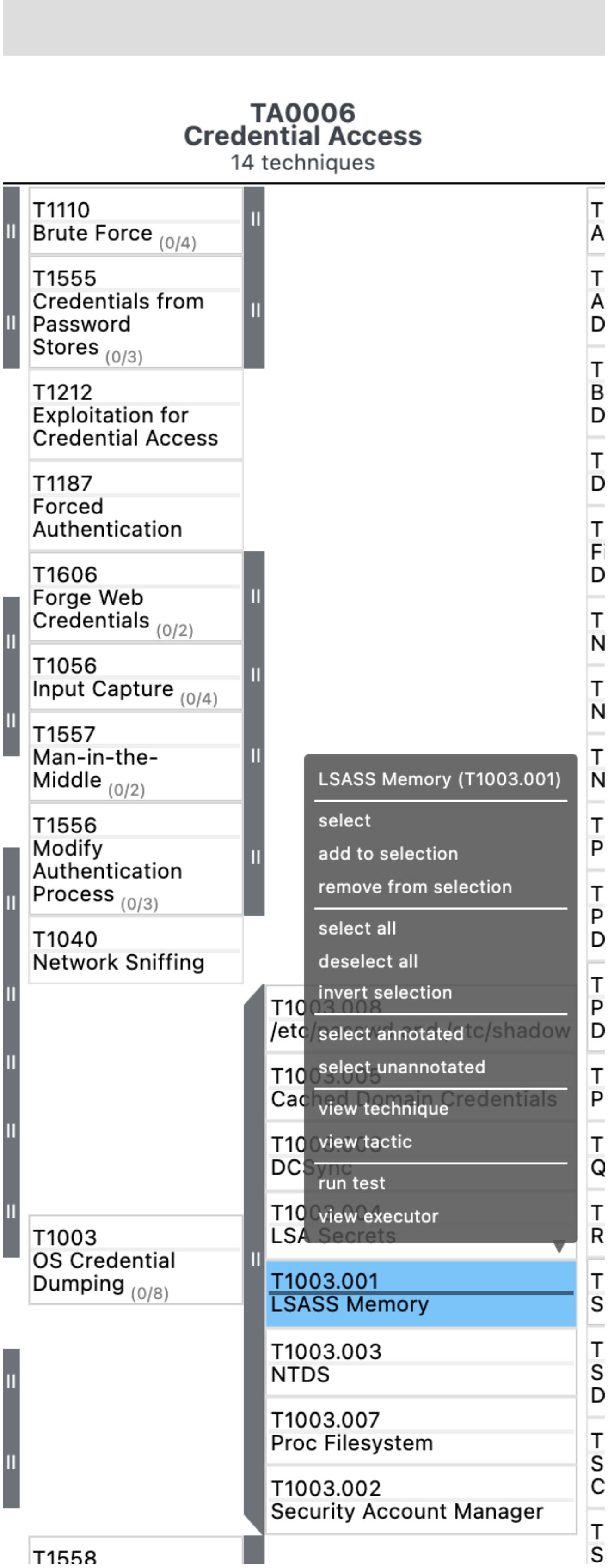


Initial Access 9 techniques	Execution 10 techniques	Persistence 17 techniques	Privilege Escalation 12 techniques	Defense Evasion 32 techniques	Credential Access 14 techniques
Drive-by Compromise	Command and Scripting Interpreter (0/7)	Account Manipulation (0/2)	Abuse Elevation Control Mechanism (0/4)	Abuse Elevation Control Mechanism (0/4)	Brute Force (0/4)
Exploit Public-Facing Application	Exploitation for Client Execution	BITS Jobs	Access Token Manipulation (0/5)	Access Token Manipulation (0/5)	Credentials from Password Stores (0/3)
External Remote Services	Inter-Process Communication (0/2)	Boot or Logon Autostart Execution (0/12)	Boot or Logon Autostart Execution (0/12)	BITS Jobs	Exploitation for Credential Access
Hardware Additions	Native API	Boot or Logon Initialization Scripts (0/5)	Boot or Logon Initialization Scripts (0/5)	Deobfuscate/Decode Files or Information	Forced Authentication
Phishing (0/3)	Scheduled Task/Job (0/6)	Browser Extensions	Create or Modify System Process (0/4)	Direct Volume Access	Forge Web Credentials (0/2)
Replication Through Removable Media	Shared Modules	Compromise Client Software Binary	Domain Policy Modification (0/2)	Domain Policy Modification (0/2)	Input Capture (0/4)
Supply Chain Compromise (0/3)	Software Deployment Tools	Create Account (0/2)	Event Triggered Execution (0/15)	Execution Guardrails (0/1)	Man-in-the-Middle (0/2)
Trusted Relationship	System Services (0/2)	Create or Modify System Process (0/4)	Exploitation for Privilege Escalation	Exploitation for Defense Evasion	Modify Authentication Process (0/3)
Valid Accounts (0/3)	User Execution (0/2)	Event Triggered Execution (0/15)	Hijack Execution Flow (0/11)	File and Directory Permissions Modification (0/2)	Network Sniffing
	Windows Management Instrumentation	External Remote Services	Process Injection (0/11)	Hide Artifacts (0/7)	OS Credential Dumping (0/8)
		Hijack Execution Flow (0/11)	Scheduled Task/Job (0/6)	Hijack Execution Flow (0/11)	Steal or Forge Kerberos Tickets (0/4)
		Office Application Startup (0/6)	Valid Accounts (0/3)	Impair Defenses (0/5)	Steal Web Session Cookie
		Pre-OS Boot (0/3)		Indicator Removal on Host (0/6)	Two-Factor Authentication Interception
		Scheduled Task/Job (0/6)		Indirect Command Execution	Unsecured Credentials
				Masquerading (0/6)	
				Modify Authentication Process (0/3)	

Discovery 22 techniques	Lateral Movement 9 techniques	Collection 15 techniques	Command and Control 16 techniques	Exfiltration 8 techniques	Impact 13 techniques
Account Discovery (0/3)	Exploitation of Remote Services	Archive Collected Data (0/3)	Application Layer Protocol (0/4)	Automated Exfiltration (0/0)	Account Access Removal
Application Window Discovery	Internal Spearphishing	Audio Capture	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction
Browser Bookmark Discovery	Lateral Tool Transfer	Automated Collection	Data Encoding (0/2)	Exfiltration Over Alternative Protocol (0/3)	Data Encrypted for Impact
Domain Trust Discovery	Remote Service Session Hijacking (0/2)	Clipboard Data	Data Obfuscation (0/3)	Exfiltration Over C2 Channel	Data Manipulation (0/3)
File and Directory Discovery	Remote Services (0/6)	Data from Information Repositories (0/1)	Dynamic Resolution (0/3)	Exfiltration Over Other Network Medium (0/1)	Defacement (0/2)
Network Service Scanning	Replication Through Removable Media	Data from Local System	Encrypted Channel (0/2)	Exfiltration Over Physical Medium (0/1)	Disk Wipe (0/2)
Network Share Discovery	Software Deployment Tools	Data from Network Shared Drive	Fallback Channels	Exfiltration Over Web Service (0/2)	Endpoint Denial of Service (0/4)
Network Sniffing	Taint Shared Content	Data from Removable Media	Ingress Tool Transfer	Scheduled Transfer	Firmware Corruption
Password Policy Discovery	Use Alternate Authentication Material (0/2)	Data Staged (0/2)	Multi-Stage Channels		Inhibit System Recovery
Peripheral Device Discovery		Email Collection (0/3)	Non-Application Layer Protocol		Network Denial of Service (0/2)
Permission Groups Discovery (0/2)		Input Capture (0/4)	Non-Standard Port		Resource Hijacking
Process Discovery		Man in the Browser	Protocol Tunneling		Service Stop
Query Registry		Man-in-the-Middle (0/2)	Proxy (0/4)		System Shutdown/Reboot
Remote System Discovery		Screen Capture	Remote Access Software		
Software Discovery (0/1)		Video Capture	Traffic Signaling (0/1)		
System Information Discovery					
System Network Configuration Discovery					

There are a few difference with regards to the extended capabilities but generally it's the same view that you would see on the github version of ATT&CK.

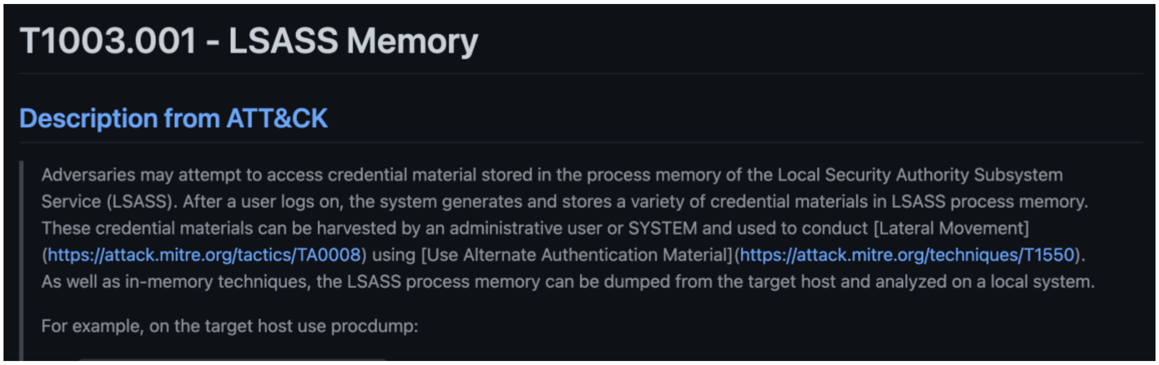
Right-click on the technique T1003.001.



TA0006
Credential Access
14 techniques

- T1110 Brute Force (0/4)
- T1555 Credentials from Password Stores (0/3)
- T1212 Exploitation for Credential Access
- T1187 Forced Authentication
- T1606 Forge Web Credentials (0/2)
- T1056 Input Capture (0/4)
- T1557 Man-in-the-Middle (0/2)
- T1556 Modify Authentication Process (0/3)
- T1040 Network Sniffing
- T1003 OS Credential Dumping (0/8)
  - T1003.008 /etc/passwd and /etc/shadow
  - T1003.005 Cached Domain Credentials
  - T1003.006 DCSync
  - T1003.004 LSA Secrets
  - T1003.001 LSASS Memory
  - T1003.003 NTDS
  - T1003.007 Proc Filesystem
  - T1003.002 Security Account Manager
- T1558

There are two new menu items available in the list, run test and view executor. Click the “view executor” link to see the atomic test from atomicredteam. Click the T1003.001.md file to see the write-up.

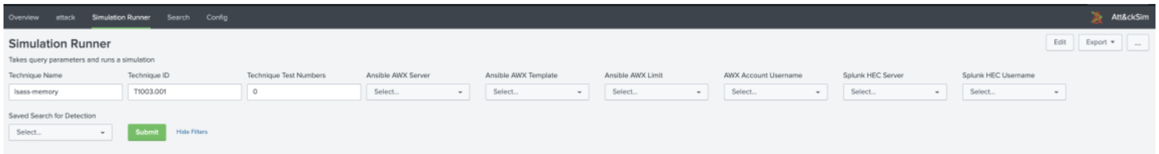


T1003.001 - LSASS Memory

Description from ATT&CK

> Adversaries may attempt to access credential material stored in the process memory of the Local Security Authority Subsystem Service (LSASS). After a user logs on, the system generates and stores a variety of credential materials in LSASS process memory. These credential materials can be harvested by an administrative user or SYSTEM and used to conduct [Lateral Movement](https://attack.mitre.org/tactics/TA0008) using [Use Alternate Authentication Material](https://attack.mitre.org/techniques/T1550). As well as in-memory techniques, the LSASS process memory can be dumped from the target host and analyzed on a local system.
>
> For example, on the target host use procdump:

Now click the “run test” link and you’ll be taken to a new dashboard called the Simulation Runner:

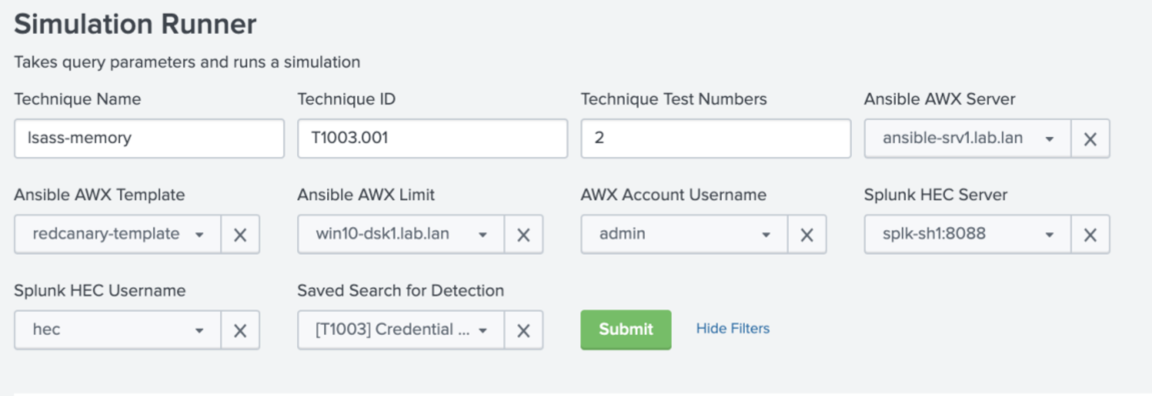


Simulation Runner

Takes query parameters and runs a simulation

Technique Name: lsass-memory
Technique ID: T1003.001
Technique Test Numbers: 0
Ansible AWX Server: Select...
Ansible AWX Template: Select...
Ansible AWX Limit: Select...
AWX Account Username: Select...
Splunk HEC Server: Select...
Splunk HEC Username: Select...
Saved Search for Detection: Select...

A number of the fields have been pre-populated based on where you launched the test from in the navigator. Fill out the rest of the fields and click search to launch the test:



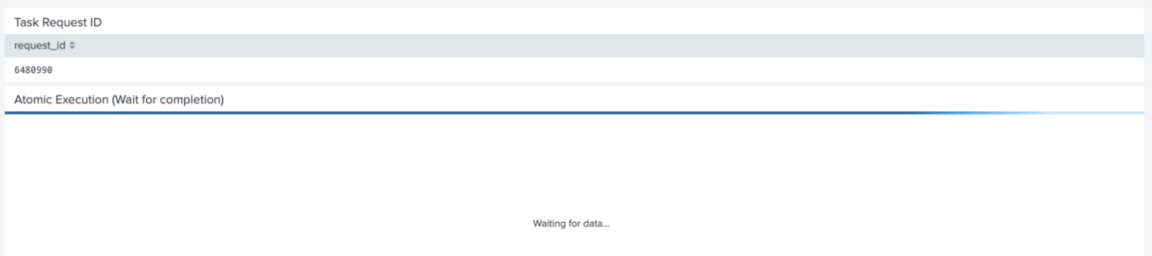
Simulation Runner

Takes query parameters and runs a simulation

Technique Name: lsass-memory
Technique ID: T1003.001
Technique Test Numbers: 2
Ansible AWX Server: ansible-srv1.lab.lan
Ansible AWX Template: redcanary-template
Ansible AWX Limit: win10-dsk1.lab.lan
AWX Account Username: admin
Splunk HEC Server: splk-sh1:8088
Splunk HEC Username: hec
Saved Search for Detection: [T1003] Credential ...

This version of the AttackSimulator hooks into our ansible instance but the original version was written to integrate with Splunk’s Phantom tool (SOAR).

Click submit and wait for the test to run:



Task Request ID

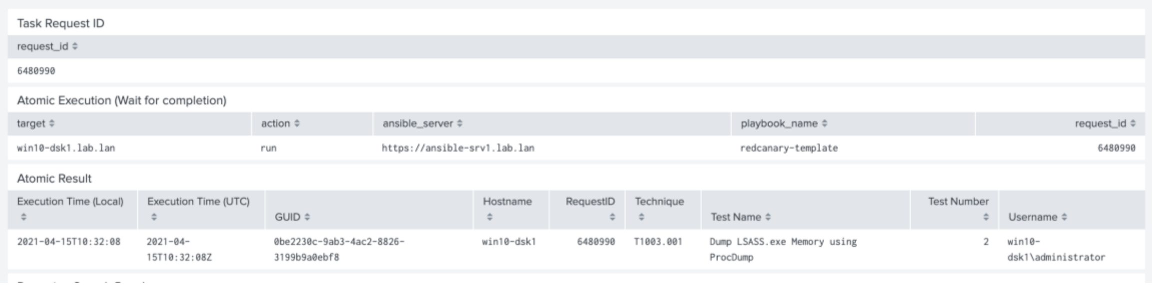
request_id ⇕
6480990

Atomic Execution (Wait for completion)

Waiting for data...

While waiting for the test to complete check back with your student machine to see evidence of the test running.

Once completed the test will display the results of the execution:



Task Request ID

request_id ⇕
6480990

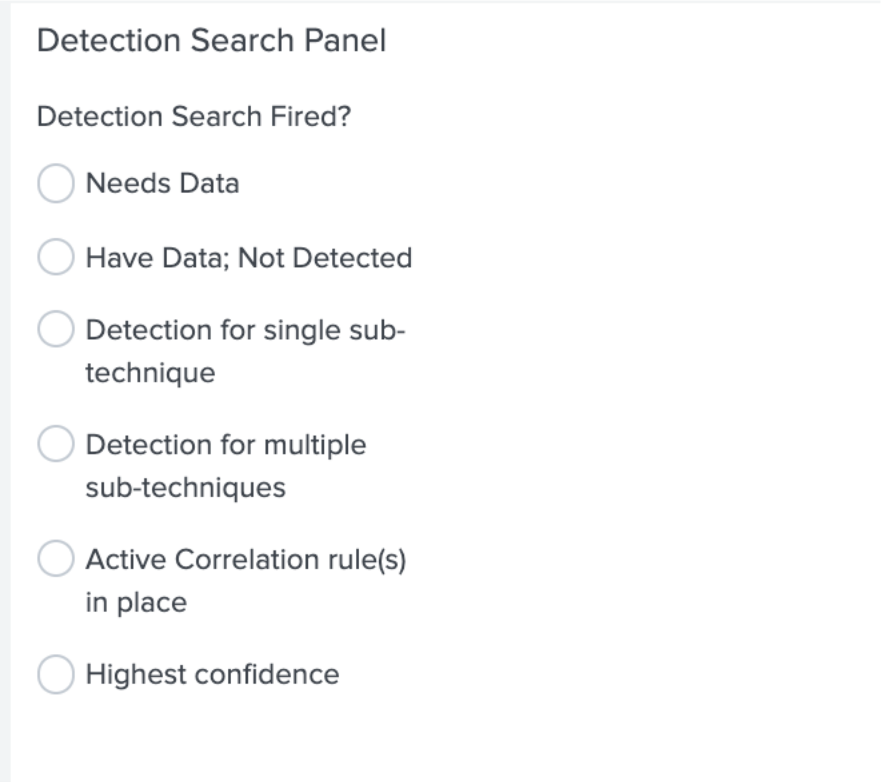
Atomic Execution (Wait for completion)

target ⇕	action ⇕	ansible_server ⇕	playbook_name ⇕	request_id ⇕
win10-dsk1.lab.lan	run	https://ansible-srv1.lab.lan	redcanary-template	6480990

Atomic Result

Execution Time (Local) ⇕	Execution Time (UTC) ⇕	GUID ⇕	Hostname ⇕	RequestID ⇕	Technique ⇕	Test Name ⇕	Test Number ⇕	Username ⇕
2021-04-15T10:32:08	2021-04-15T10:32:08Z	0be2230c-9ab3-4ac2-8826-3199b9a0ebf8	win10-dsk1	6480990	T1003.001	Dump LSASS.exe Memory using ProcDump	2	win10-dsk1\administrator

In the panel below the search results, as an investigator you can use Splunk and the data provided back form the test to understand and track how well your alerts are working.



Detection Search Panel

Detection Search Fired?

○ Needs Data

○ Have Data; Not Detected

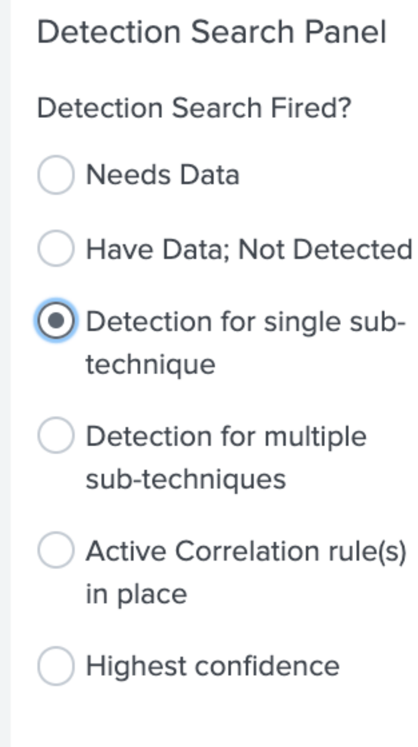
○ Detection for single sub-technique

○ Detection for multiple sub-techniques

○ Active Correlation rule(s) in place

○ Highest confidence

The results of for this test are tracked in the embedded ATT&CK navigator. Click any one of the colours and in a new tab re-open the embedded navigator.



Detection Search Panel

Detection Search Fired?

○ Needs Data

○ Have Data; Not Detected

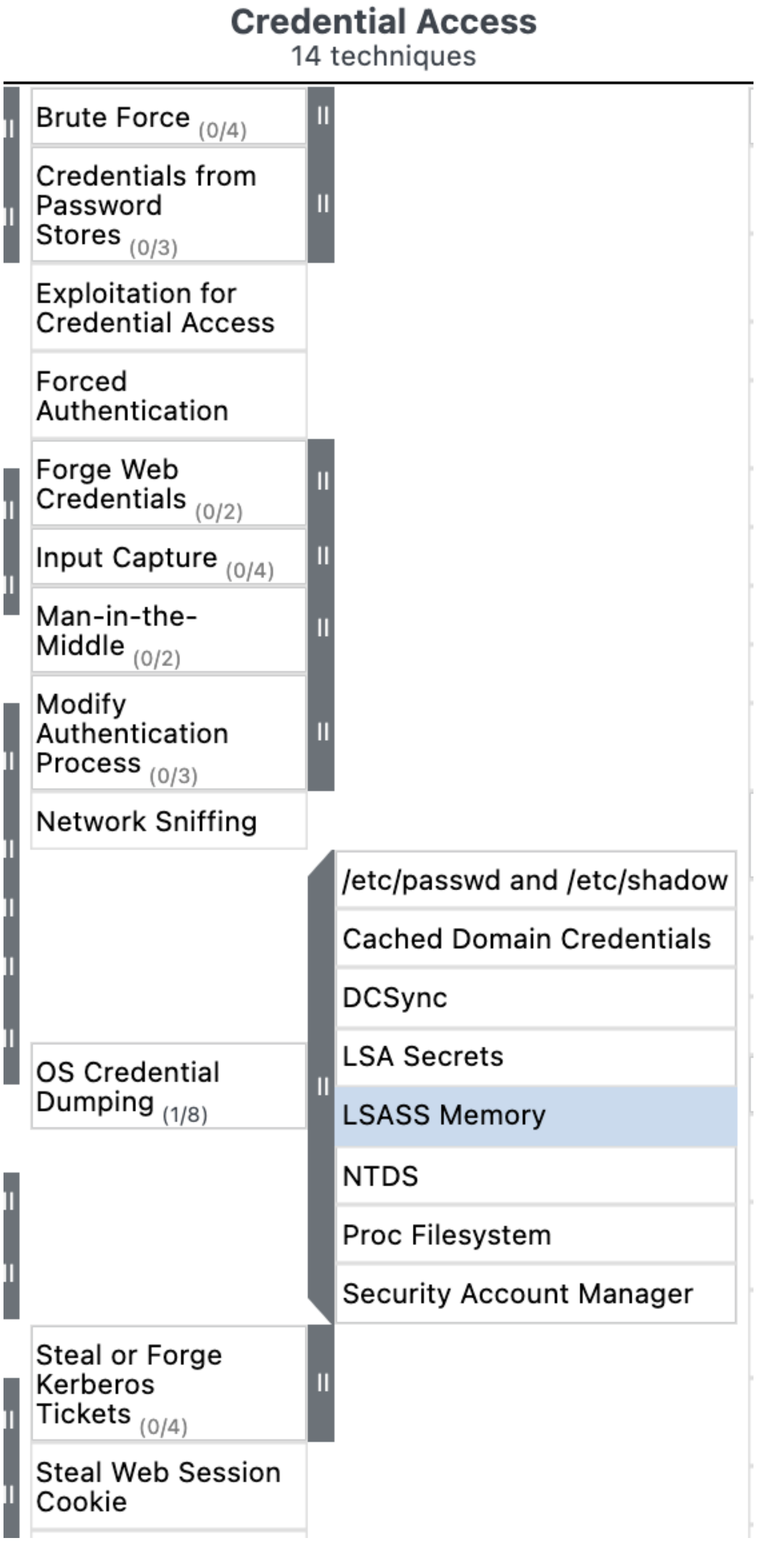
● Detection for single sub-technique

○ Detection for multiple sub-techniques

○ Active Correlation rule(s) in place

○ Highest confidence

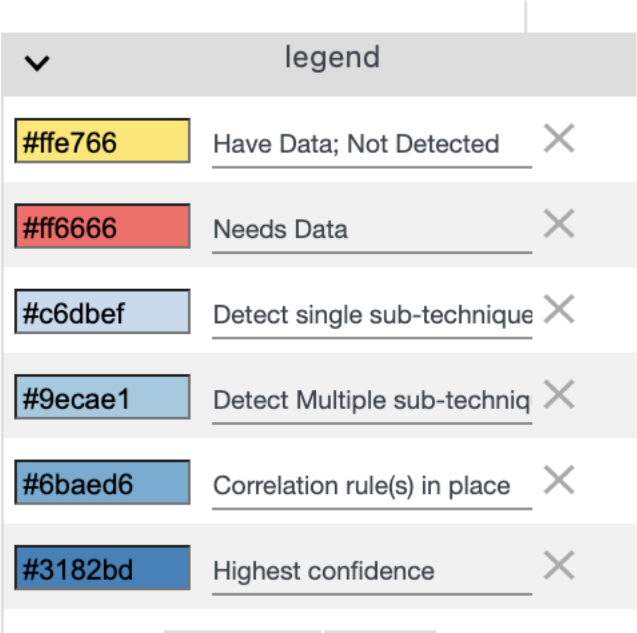
Now notice that a colour has been assigned to the T1003.001 technique:



Credential Access
14 techniques

- Brute Force (0/4)
- Credentials from Password Stores (0/3)
- Exploitation for Credential Access
- Forced Authentication
- Forge Web Credentials (0/2)
- Input Capture (0/4)
- Man-in-the-Middle (0/2)
- Modify Authentication Process (0/3)
- Network Sniffing
- OS Credential Dumping (1/8)
  - /etc/passwd and /etc/shadow
  - Cached Domain Credentials
  - DCSync
  - LSA Secrets
  - LSASS Memory
  - NTDS
  - Proc Filesystem
  - Security Account Manager
- Steal or Forge Kerberos Tickets (0/4)
- Steal Web Session Cookie

Pop open the legend at the bottom to see the mapping for each colour:



legend

#ffe766	Have Data; Not Detected
#ff6666	Needs Data
#c6dbef	Detect single sub-technique
#9ecae1	Detect Multiple sub-techniq
#6baed6	Correlation rule(s) in place
#3182bd	Highest confidence

Using the atomic redteam as our attack simulation tool, coupled with automation and integrated tracking we can start to build a continuous assessment loop!

End of Lab