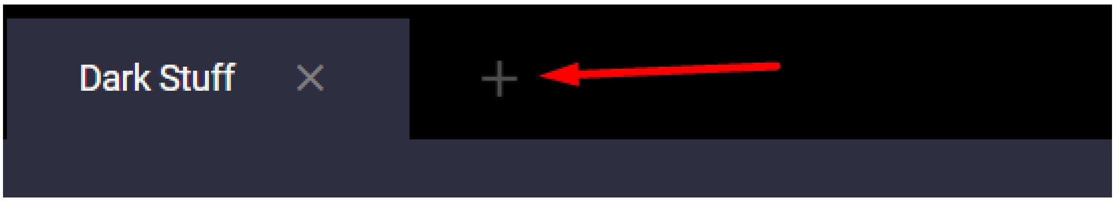
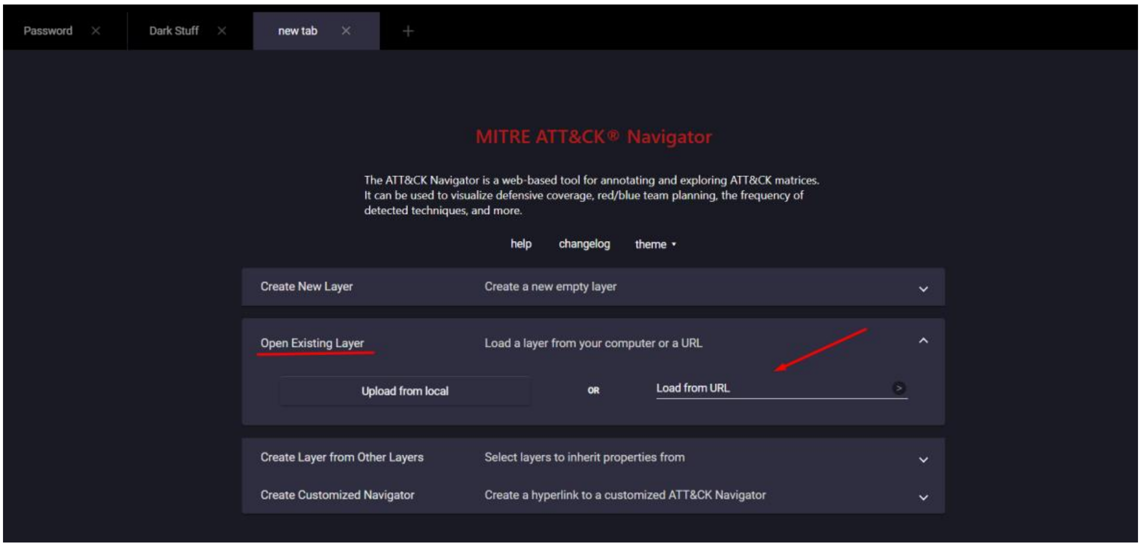
Lab 3 - Importing Navigator Layers

In this lab You overheard your colleagues discussing NIST 800-53 controls and their importance to your company while at lunch. When you return to your desk, you are curious about the types of attacker behaviors from ATT&CK that map to the NIST 800-53 AC-2 control. Use your newfound ATT&CK Navigator skills so create a visual representation of NIST 800-53 AC-2 mapped to the ATT&CK framework.

1. Return to your open Navigator page and click on the + sign next to the Dark Stuff Tab. This creates a new layer.



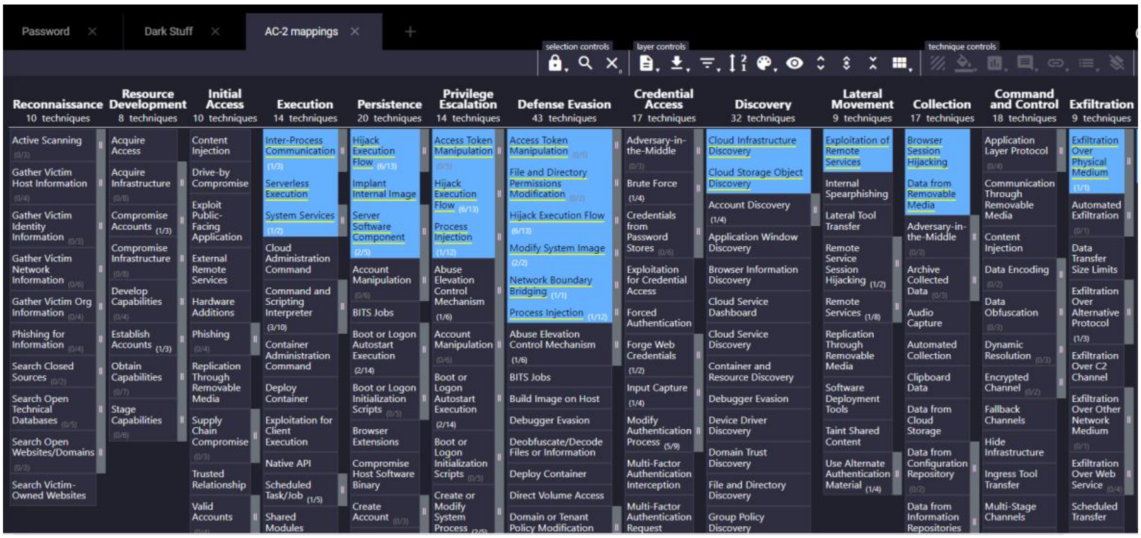
2. Click on **Open Existing Layer.**


Password ×
Dark Stuff ×
new tab ×
+
MITRE ATT&CK® Navigator
help
changelog
theme ▾
Create New Layer
Create a new empty layer
Open Existing Layer
Load a layer from your computer or a URL
Upload from local
OR
Load from URL
Create Layer from Other Layers
Select layers to inherit properties from
Create Customized Navigator
Create a hyperlink to a customized ATT&CK Navigator

The ATT&CK Navigator is a web-based tool for annotating and exploring ATT&CK matrices. It can be used to visualize defensive coverage, red/blue team planning, the frequency of detected techniques, and more.

3. Paste the following URL into the Load from URL text box: https://raw.githubusercontent.com/center-for-threat-informed-defense/attack-control-framework-mappings/main/frameworks/attack_12_1/nist800_53_r5/layers/by_family/AC/AC-2.json

4. You will receive a warning about the imported layer’s version being different than Navigator’s Layer Version. Click Yes.
5. You will be asked if you want to upgrade the layer version. Click “mark all as review” option and complete all the options to the Finish.
6. Your resulting import should look similar to the screenshot below.



Reconnaissance 10 techniques	Resource Development 8 techniques	Initial Access 10 techniques	Execution 14 techniques	Persistence 20 techniques	Privilege Escalation 14 techniques	Defense Evasion 43 techniques	Credential Access 17 techniques	Discovery 32 techniques	Lateral Movement 9 techniques	Collection 17 techniques	Command and Control 18 techniques	Exfiltration 9 techniques
Active Scanning (0/3)	Acquire Access	Content Injection	Inter-Process Communication (1/3)	Hijack Execution Flow (6/13)	Access Token Manipulation (0/5)	Access Token Manipulation (0/5)	Adversary-in-the-Middle (0/3)	Cloud Infrastructure Discovery	Exploitation of Remote Services	Browser Session Hijacking	Application Layer Protocol (0/4)	Exfiltration Over Physical Medium (1/1)
Gather Victim Host Information (0/4)	Acquire Infrastructure (0/8)	Drive-by Compromise	Serverless Execution	Implant Internal Image	Hijack Execution Flow (6/13)	File and Directory Permissions Modification (0/2)	Brute Force (1/4)	Cloud Storage Object Discovery	Internal Spearphishing	Data from Removable Media	Communication Through Removable Media	Automated Exfiltration (0/1)
Gather Victim Identity Information (0/3)	Compromise Accounts (1/3)	Exploit Public-Facing Application	System Services (1/2)	Server Software Component (2/5)	Process Injection (1/12)	Hijack Execution Flow (6/13)	Credentials from Password Stores (0/6)	Account Discovery (1/4)	Lateral Tool Transfer	Adversary-in-the-Middle (0/3)	Content Injection	Data Transfer Size Limits
Gather Victim Network Information (0/6)	Compromise Infrastructure (0/8)	External Remote Services	Cloud Administration Command	Account Manipulation (0/6)	Abuse Elevation Control Mechanism (1/6)	Modify System Image (2/2)	Exploitation for Credential Access	Application Window Discovery	Remote Service Session Hijacking (1/2)	Archive Collected Data (0/3)	Data Encoding (0/2)	Exfiltration Over Alternative Protocol (1/3)
Gather Victim Org Information (0/4)	Develop Capabilities (0/4)	Hardware Additions	Command and Scripting Interpreter (3/10)	BITS Jobs	Account Manipulation (0/6)	Network Boundary Bridging (1/1)	Forced Authentication	Browser Information Discovery	Remote Services (1/8)	Audio Capture	Data Obfuscation (0/3)	Exfiltration Over C2 Channel
Phishing for Information (0/4)	Establish Accounts (1/3)	Phishing (0/4)	Container Administration Command	Boot or Logon Autostart Execution (2/14)	Boot or Logon Autostart Execution (2/14)	Process Injection (1/12)	Forge Web Credentials (1/2)	Cloud Service Dashboard	Replication Through Removable Media	Automated Collection	Dynamic Resolution (0/3)	Exfiltration Over Other Network Medium (0/1)
Search Closed Sources (0/2)	Obtain Capabilities (0/7)	Replication Through Removable Media	Deploy Container	Boot or Logon Initialization Scripts (0/5)	Boot or Logon Initialization Scripts (0/5)	Abuse Elevation Control Mechanism (1/6)	Input Capture (1/4)	Cloud Service Discovery	Software Deployment Tools	Clipboard Data	Encrypted Channel (0/2)	Exfiltration Over Web Service (0/4)
Search Open Technical Databases (0/5)	Stage Capabilities (0/6)	Supply Chain Compromise (0/3)	Exploitation for Client Execution	Browser Extensions	Create or Modify System Process (2/5)	BITS Jobs	Modify Authentication Process (5/9)	Container and Resource Discovery	Taint Shared Content	Data from Cloud Storage	Fallback Channels	Scheduled Transfer
Search Open Websites/Domains (0/3)		Trusted Relationship	Native API	Compromise Host Software Binary		Build Image on Host	Multi-Factor Authentication Interception	Debugger Evasion	Use Alternate Authentication Material (1/4)	Data from Configuration Repository (0/2)	Hide Infrastructure	
Search Victim-Owned Websites		Valid Accounts (0/4)	Scheduled Task/Job (1/5)	Create Account (0/3)		Debugger Evasion	Multi-Factor Authentication Request	Device Driver Discovery		Data from Information Repositories	Ingress Tool Transfer	
			Shared Modules			Deobfuscate/Decode Files or Information		Domain Trust Discovery			Multi-Stage Channels	
						Deploy Container		File and Directory Discovery				
						Direct Volume Access		Group Policy Discovery				
						Domain or Tenant Policy Modification						