Exercise 1: Mapping Adversary Behavior

You will use the MITRE ATT&CK Navigator to map the fictional adversary behaviors based on tactics, techniques, and procedures (TTPs) using the MITRE ATT&CK Enterprise Matrix. The security incidents have not occurred yet, but you will work on creating the security incidents in a later exercise.

You will map the behaviors based on the mock threat report, which describes the fictional adversary TTPs. This will allow you to *translate* the behaviors into the MITRE ATT&CK model.

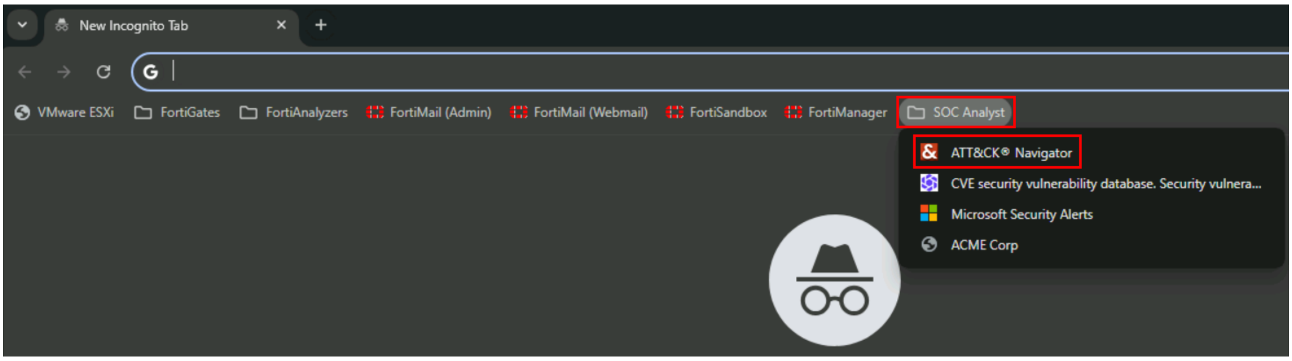
With every update of MITRE ATT&CK, MITRE also updates the ATT&CK Navigator to reflect the changes. The tool may look different from the images in this lab guide, depending on the current live version. If you are not able to follow any of the steps in this exercise, tell your instructor.

Configure the ATT&CK Navigator Settings

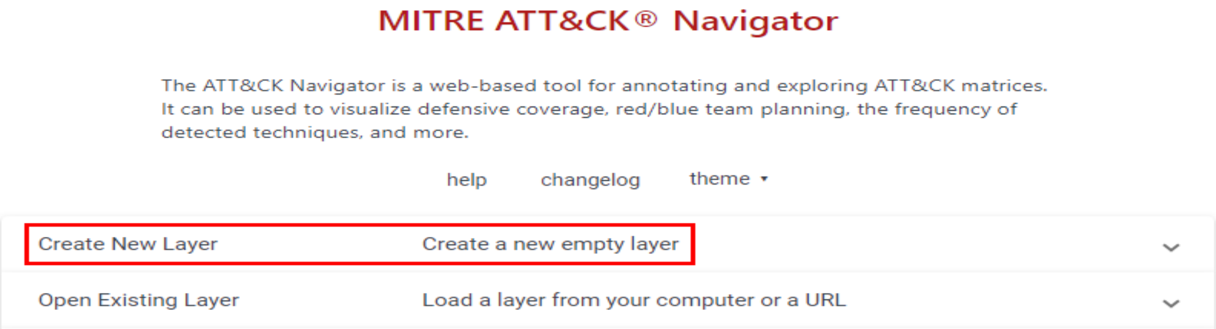
You will access the ATT&CK Navigator and configure the settings to what you require for your mapping.

To configure the ATT&CK Navigator settings

1. On the bastion host, open Google Chrome, click the **SOC Analyst** bookmark folder, and then click the **ATT&CK Navigator** bookmark (https://mitre-attack.github.io/attack-navigator/).



2. Click **Create New Layer**.

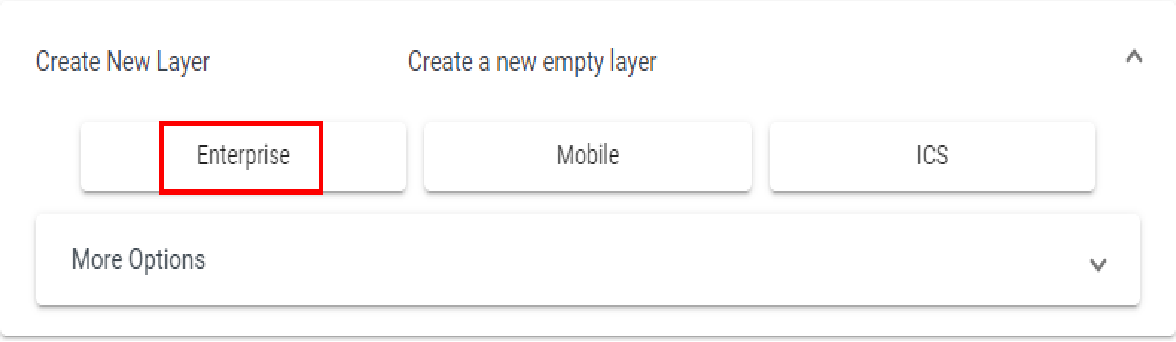

MITRE ATT&CK® Navigator

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.

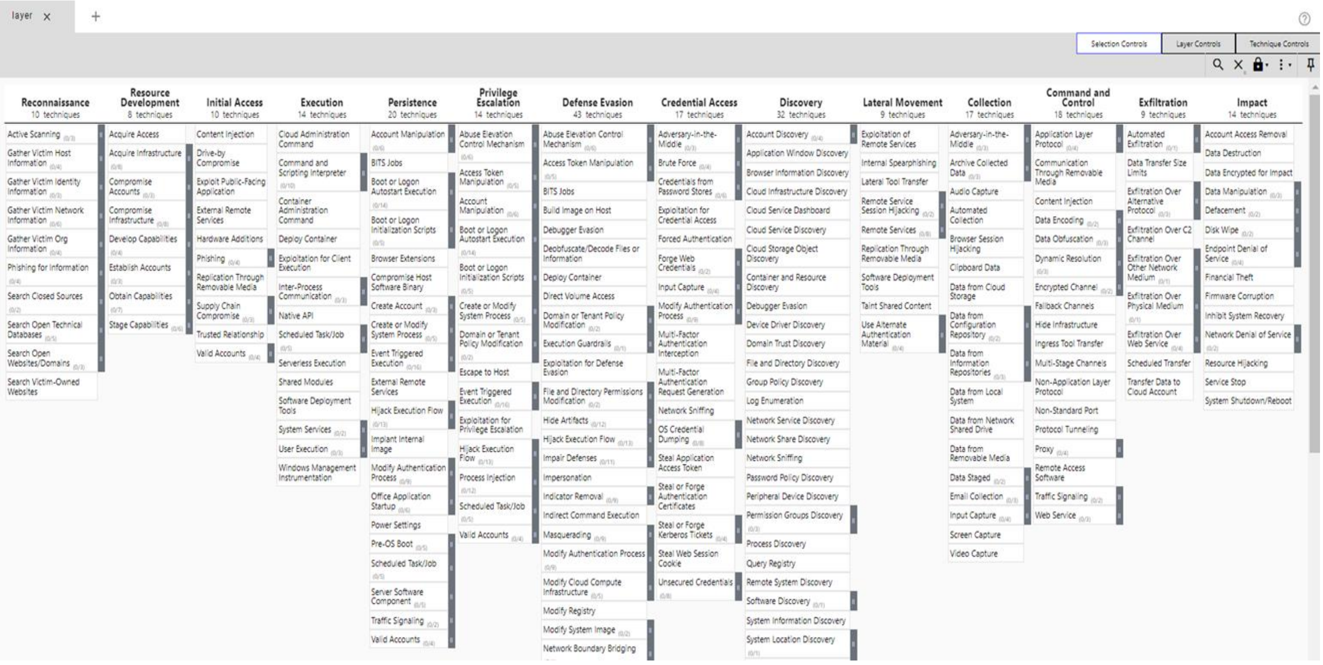
Create New Layer — Create a new empty layer

Open Existing Layer — Load a layer from your computer or a URL

3. Click **Enterprise**.


Create New Layer — Create a new empty layer

The ATT&CK Navigator opens.



Reconnaissance 10 techniques	Resource Development 8 techniques	Initial Access 10 techniques	Execution 14 techniques	Persistence 20 techniques
Active Scanning (0/3)	Acquire Access	Content Injection	Cloud Administration Command	Account Manipulation (0/6)
Gather Victim Host Information (0/4)	Acquire Infrastructure (0/8)	Drive-by Compromise	Command and Scripting Interpreter (0/10)	BITS Jobs
Gather Victim Identity Information (0/3)	Compromise Accounts (0/3)	Exploit Public-Facing Application	Container Administration Command	Boot or Logon Autostart Execution (0/14)
Gather Victim Network Information (0/6)	Compromise Infrastructure (0/8)	External Remote Services	Deploy Container	Boot or Logon Initialization Scripts (0/5)
Gather Victim Org Information (0/4)	Develop Capabilities (0/4)	Hardware Additions	Exploitation for Client Execution	Browser Extensions
Phishing for Information (0/4)	Establish Accounts (0/3)	Phishing (0/4)	Inter-Process Communication (0/3)	Compromise Host Software Binary
Search Closed Sources (0/2)	Obtain Capabilities (0/7)	Replication Through Removable Media	Native API	Create Account (0/3)
Search Open Technical Databases (0/5)	Stage Capabilities (0/6)	Supply Chain Compromise (0/3)	Scheduled Task/Job (0/5)	Create or Modify System Process (0/5)
Search Open Websites/Domains (0/3)		Trusted Relationship	Serverless Execution	Event Triggered Execution (0/16)
Search Victim-Owned Websites		Valid Accounts (0/4)	Shared Modules	External Remote Services
			Software Deployment Tools	Hijack Execution Flow (0/13)
			System Services (0/2)	Implant Internal Image
			User Execution (0/3)	Modify Authentication Process (0/9)
			Windows Management Instrumentation	Office Application Startup (0/6)
				Power Settings
				Pre-OS Boot (0/5)
				Scheduled Task/Job (0/5)
				Server Software Component (0/5)
				Traffic Signaling (0/2)
				Valid Accounts (0/4)

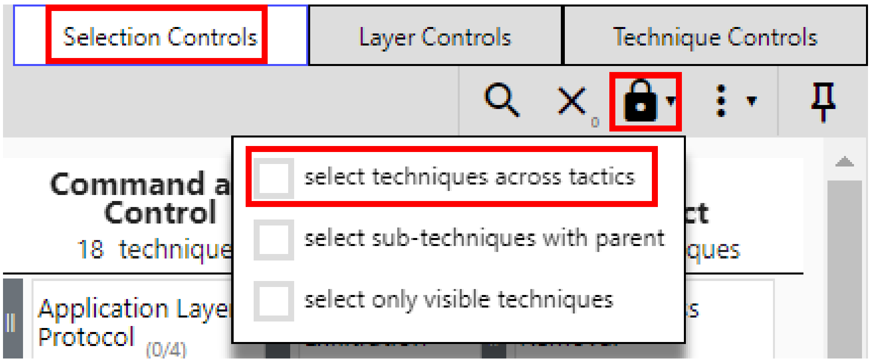
Privilege Escalation 14 techniques	Defense Evasion 43 techniques	Credential Access 17 techniques	Discovery 32 techniques
Abuse Elevation Control Mechanism (0/6)	Abuse Elevation Control Mechanism (0/6)	Adversary-in-the-Middle (0/3)	Account Discovery (0/4)
Access Token Manipulation (0/5)	Access Token Manipulation (0/5)	Brute Force (0/4)	Application Window Discovery
Account Manipulation (0/6)	BITS Jobs	Credentials from Password Stores (0/6)	Browser Information Discovery
Boot or Logon Autostart Execution (0/14)	Build Image on Host	Exploitation for Credential Access	Cloud Infrastructure Discovery
Boot or Logon Initialization Scripts (0/5)	Debugger Evasion	Forced Authentication	Cloud Service Dashboard
Create or Modify System Process (0/5)	Deobfuscate/Decode Files or Information	Forge Web Credentials (0/2)	Cloud Service Discovery
Domain or Tenant Policy Modification (0/2)	Deploy Container	Input Capture (0/4)	Cloud Storage Object Discovery
Escape to Host	Direct Volume Access	Modify Authentication Process (0/9)	Container and Resource Discovery
Event Triggered Execution (0/16)	Domain or Tenant Policy Modification (0/2)	Multi-Factor Authentication Interception	Debugger Evasion
Exploitation for Privilege Escalation	Execution Guardrails (0/1)	Multi-Factor Authentication Request Generation	Device Driver Discovery
Hijack Execution Flow (0/13)	Exploitation for Defense Evasion	Network Sniffing	Domain Trust Discovery
Process Injection (0/12)	File and Directory Permissions Modification (0/2)	OS Credential Dumping (0/8)	File and Directory Discovery
Scheduled Task/Job (0/5)	Hide Artifacts (0/12)	Steal Application Access Token	Group Policy Discovery
Valid Accounts (0/4)	Hijack Execution Flow (0/13)	Steal or Forge Authentication Certificates	Log Enumeration
	Impair Defenses (0/11)	Steal or Forge Kerberos Tickets (0/4)	Network Service Discovery
	Impersonation	Steal Web Session Cookie	Network Share Discovery
	Indicator Removal (0/9)	Unsecured Credentials (0/8)	Network Sniffing
	Indirect Command Execution		Password Policy Discovery
	Masquerading (0/9)		Peripheral Device Discovery
	Modify Authentication Process (0/9)		Permission Groups Discovery (0/3)
	Modify Cloud Compute Infrastructure (0/5)		Process Discovery
	Modify Registry		Query Registry
	Modify System Image (0/2)		Remote System Discovery
	Network Boundary Bridging		Software Discovery (0/1)
			System Information Discovery
			System Location Discovery (0/1)

Lateral Movement 9 techniques	Collection 17 techniques	Command and Control 18 techniques	Exfiltration 9 techniques	Impact 14 techniques
Exploitation of Remote Services	Adversary-in-the-Middle (0/3)	Application Layer Protocol (0/4)	Automated Exfiltration (0/1)	Account Access Removal
Internal Spearphishing	Archive Collected Data (0/3)	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction
Lateral Tool Transfer	Audio Capture	Content Injection	Exfiltration Over Alternative Protocol (0/3)	Data Encrypted for Impact
Remote Service Session Hijacking (0/2)	Automated Collection	Data Encoding (0/2)	Exfiltration Over C2 Channel	Data Manipulation (0/3)
Remote Services (0/8)	Browser Session Hijacking	Data Obfuscation (0/3)	Exfiltration Over Other Network Medium (0/1)	Defacement (0/2)
Replication Through Removable Media	Clipboard Data	Dynamic Resolution (0/3)	Exfiltration Over Physical Medium (0/1)	Disk Wipe (0/2)
Software Deployment Tools	Data from Cloud Storage	Encrypted Channel (0/2)	Exfiltration Over Web Service (0/4)	Endpoint Denial of Service (0/4)
Taint Shared Content	Data from Configuration Repository (0/2)	Fallback Channels	Scheduled Transfer	Financial Theft
Use Alternate Authentication Material (0/4)	Data from Information Repositories (0/3)	Hide Infrastructure	Transfer Data to Cloud Account	Firmware Corruption
	Data from Local System	Ingress Tool Transfer		Inhibit System Recovery
	Data from Network Shared Drive	Multi-Stage Channels		Network Denial of Service (0/2)
	Data from Removable Media	Non-Application Layer Protocol		Resource Hijacking
	Data Staged (0/2)	Non-Standard Port		Service Stop
	Email Collection (0/3)	Protocol Tunneling		System Shutdown/Reboot
	Input Capture (0/4)	Proxy (0/4)		
	Screen Capture	Remote Access Software		
	Video Capture	Traffic Signaling (0/2)		
		Web Service (0/3)		

To get a more precise mapping of Group ABC behaviors, you must set a specific configuration of the ATT&CK Navigator.

4. In the **Selection Controls** toolbar, click the lock icon (□), and then clear the **select techniques across tactics** checkbox.

Your configuration should match the following example:



☐ select techniques across tactics

☐ select sub-techniques with parent

☐ select only visible techniques

According to the MITRE ATT&CK model definition, a technique and subtechnique can span across multiple tactics. The default configuration of the ATT&CK Navigator is set for the automatic selection of a technique or subtechnique across all applicable tactics. In this exercise, this would eventually create inaccurate selections that would not reflect the described behaviors of Group ABC.

Map the Reconnaissance Tactic

According to the mock report, Group ABC first performs **Reconnaissance** (tactic) by accessing a target's public website, learning about the organization, its employees, and roles, and downloading hosted documents to find a vulnerability. These actions are included in **Search Victim-Owned Websites** (technique).

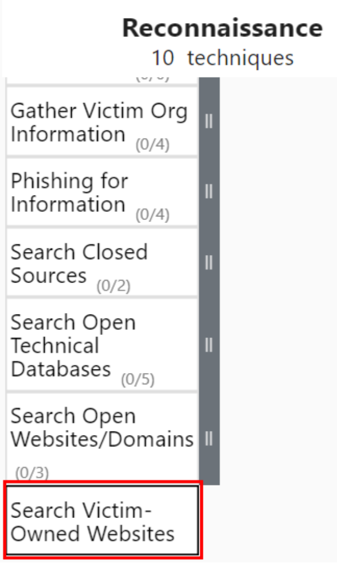
The group also uses a list of common usernames to probe the target email systems, in order to **Gather Victim Identity Information** (technique) and obtain valid **Email Addresses** (subtechnique) that exist on the target.

The group is also known to perform **Active Scanning** (technique) by **Scanning IP Blocks** (subtechnique) and using **Vulnerability Scanning** (subtechnique).

You will use the ATT&CK Navigator to map the **Reconnaissance** tactic.

To map the Reconnaissance tactic

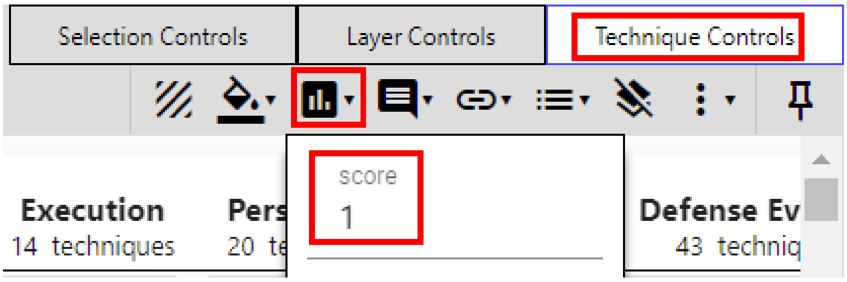
1. In the ATT&CK Navigator, in the **Reconnaissance** column, select **Search Victim-Owned Websites**.



Reconnaissance
10 techniques

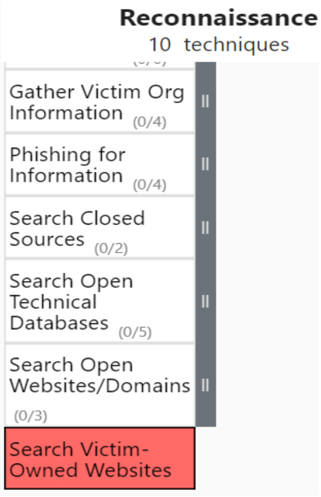
Gather Victim Org Information (0/4)
Phishing for Information (0/4)
Search Closed Sources (0/2)
Search Open Technical Databases (0/5)
Search Open Websites/Domains (0/3)
Search Victim-Owned Websites

2. In the **Technique Controls** toolbar, click the **score** icon, and then set the **score** to 1.



score
1

The selection is highlighted.

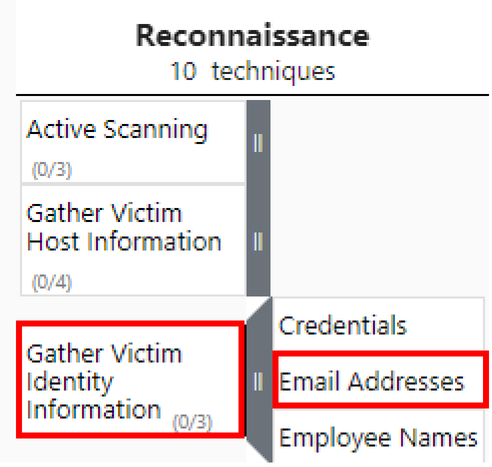


Reconnaissance
10 techniques

Gather Victim Org Information (0/4)
Phishing for Information (0/4)
Search Closed Sources (0/2)
Search Open Technical Databases (0/5)
Search Open Websites/Domains (0/3)
Search Victim-Owned Websites

3. In the **Reconnaissance** column, to the right of the **Gather Victim Identity Information** technique, click **||** to expand the subtechniques.

4. Hold the Shift key, and then in the **Reconnaissance** column, select both the **Gather Victim Identity Information** technique and **Email Addresses** subtechnique.



Reconnaissance
10 techniques

Active Scanning (0/3)

Gather Victim Host Information (0/4)

Gather Victim Identity Information (0/3)

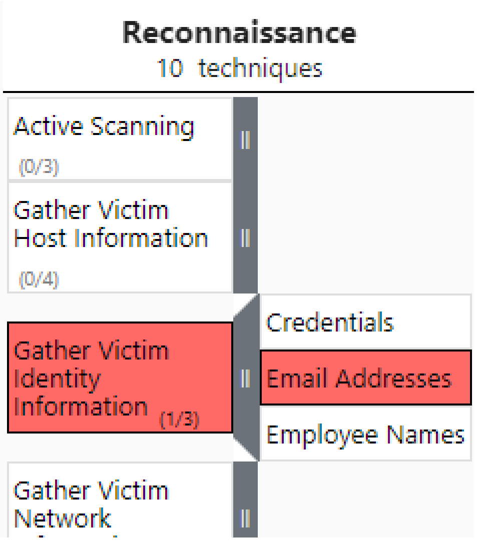
Credentials

Email Addresses

Employee Names

5. In the **Technique Controls** toolbar, click the **score** icon, and then set the **score** to 1.

The selections are highlighted.



Reconnaissance
10 techniques

Active Scanning (0/3)

Gather Victim Host Information (0/4)

Gather Victim Identity Information (1/3)

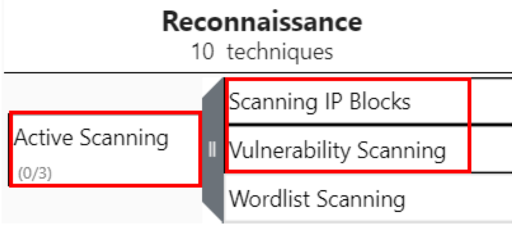
Credentials

Email Addresses

Employee Names

Gather Victim Network

6. To the right of the **Gather Victim Identity Information** technique, click **||** to collapse the subtechniques.
7. In the **Reconnaissance** column, to the right of the **Active Scanning** technique, click **||** to expand the subtechniques.
8. Hold the Shift key, and then in the **Reconnaissance** column, select both the **Active Scanning** technique and **Scanning IP Blocks** and **Vulnerability Scanning** subtechniques.



Reconnaissance
10 techniques

Active Scanning (0/3)

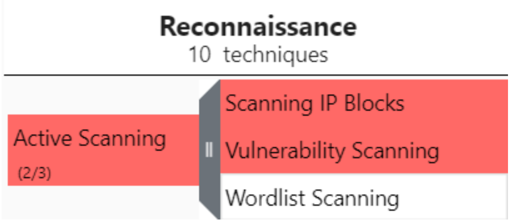
Scanning IP Blocks

Vulnerability Scanning

Wordlist Scanning

9. In the **Technique Controls** toolbar, click the **score** icon, and then set the **score** to 1.

The selections are highlighted.



10. To the right of the **Active Scanning** technique, click **||** to collapse the subtechniques.

In this case, you are using the score system to create a visual cue for the selections. You can use the score system for other purposes such as indicating priorities and risk-level associated with specific techniques and subtechniques.

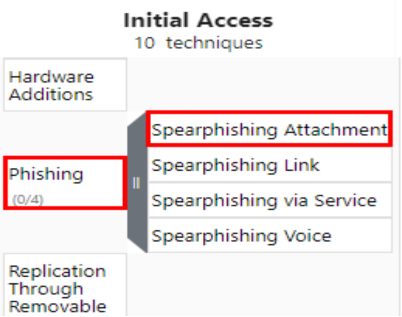
Map the Initial Access Tactic

According to the mock report, Group ABC uses spear phishing for initial access. Specifically, the group uses *spear phishing with a malicious file attachment*, which is a subtechnique of the broader **Phishing** technique.

You will use the ATT&CK Navigator to map the **Initial Access** tactic.

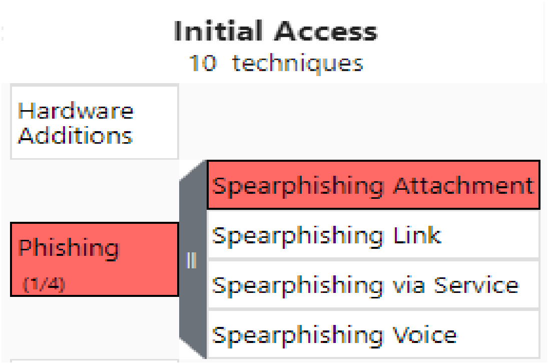
To map the Initial Access tactic

1. In the ATT&CK Navigator, in the **Initial Access** column, to the right of the **Phishing** technique, click **||** to expand the subtechniques.
2. Hold the Shift key, and then in the **Initial Access** column, select both the **Phishing** technique and **Spearphishing Attachment** subtechnique.



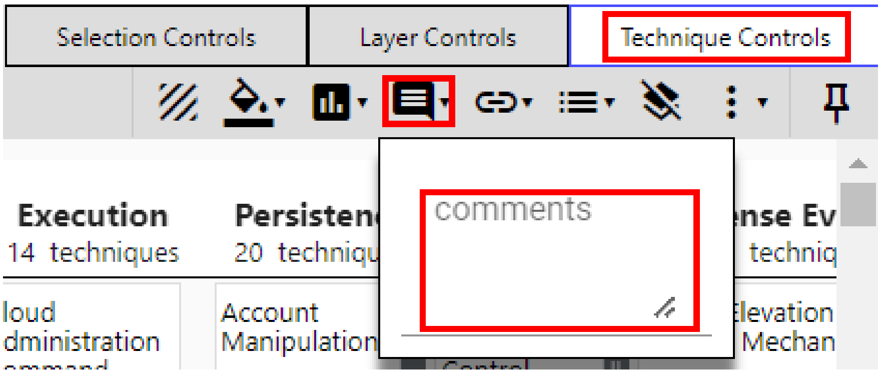
3. In the **Technique Controls** toolbar, click the **score** icon, and then set the **score** to 1.

The selections are highlighted.



You mapped the Group ABC technique and subtechnique for the **Initial Access** tactic. However, in the lesson, you learned another aspect of an adversary behavior that is a component of the ATT&CK model—procedures. Since the ATT&CK Navigator does not have a specific object to map procedures, you will use the comment section of the **Spearphishing Attachment** subtechnique to annotate the Group ABC procedure of attaching a malicious document to the spear-phishing email.

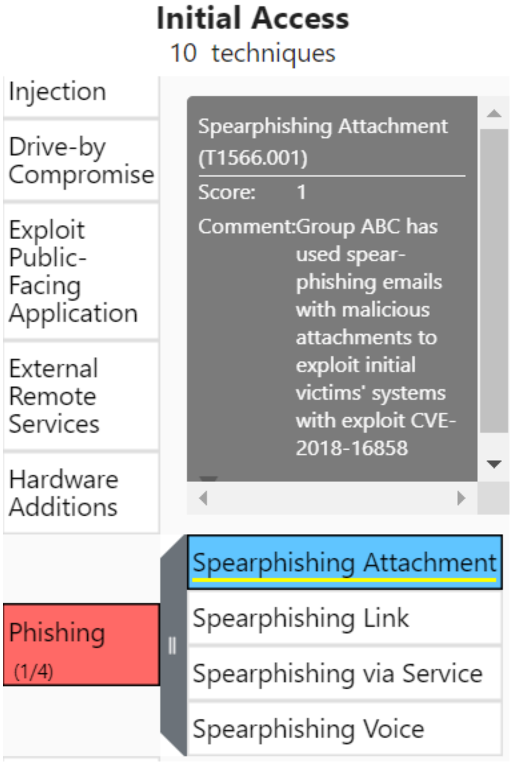
4. Click the **Spearphishing Attachment** subtechnique to select it, and then in the **Technique Controls** toolbar, click the comment icon to open the comment field.



5. In the comment field, type something like the following text:

Group ABC has used spear-phishing emails with malicious attachments to exploit initial victims' systems with exploit CVE-2018-16858.

The **Spearphishing Attachment** subtechnique is now underlined, and you can hover over it to see the comment that you added.



Initial Access
10 techniques

Injection
Drive-by Compromise
Exploit Public-Facing Application
External Remote Services
Hardware Additions
Phishing (1/4)

Spearphishing Attachment (T1566.001)
Score: 1
Comment:Group ABC has used spear-phishing emails with malicious attachments to exploit initial victims' systems with exploit CVE-2018-16858

Spearphishing Attachment
Spearphishing Link
Spearphishing via Service
Spearphishing Voice

Because procedures do not affect future labs, and for time management reasons, this is the only procedure from Group ABC that you will detail in the ATT&CK Navigator. However, in a real-world situation, you should collect and document as many details as possible about an adversary.

6. To the right of the **Phishing** technique, click **||** to collapse the subtechniques.

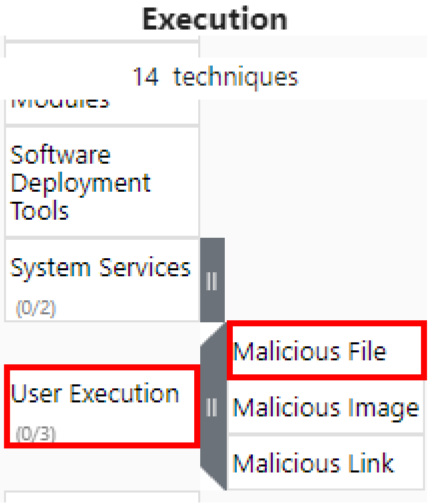
Map the Execution Tactic

You will map the **Execution** behavior of the Group ABC attacks. According to the mock report, the group's attacks require the target user to execute the malicious file.

You will use the ATT&CK Navigator to map the **Execution** tactic.

To map the Execution tactic

1. In the **Execution** column, to the right of the **User Execution** technique, click **||** to expand the subtechniques.
2. Hold the Shift key, and then in the **Execution** column, select both the **User Execution** technique and **Malicious File** subtechnique.



Execution
14 techniques

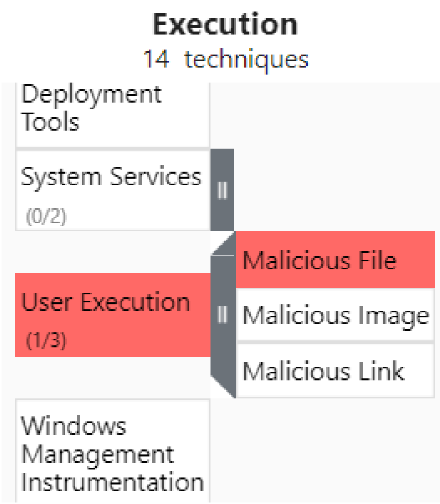
Modules
Software Deployment Tools
System Services (0/2)
User Execution (0/3)

Malicious File
Malicious Image
Malicious Link

You may need to scroll down to see these items.

3. In the **Technique Controls** toolbar, click the **score** icon, and then set the **score** to 1.

The selections are highlighted.



4. To the right of the **User Execution** technique, click **||** to collapse the subtechniques.

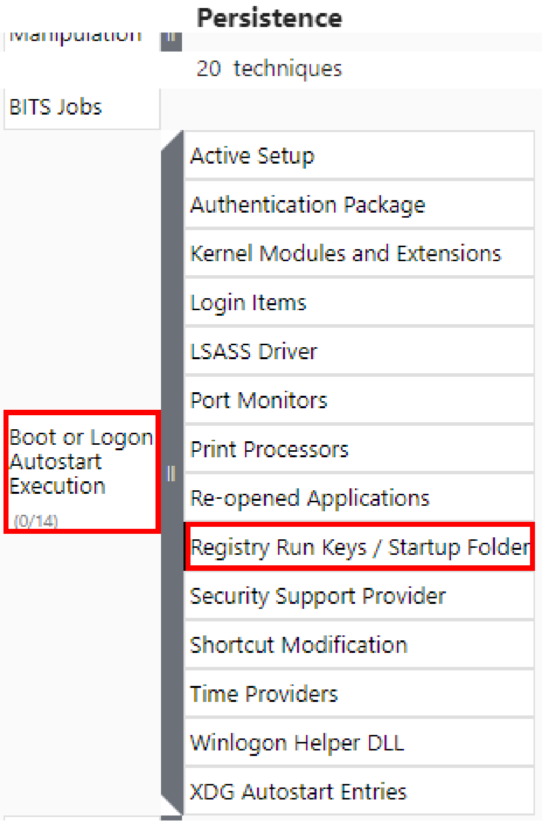
Map the Persistence Tactic

For the **Persistence** stage, according to the threat report, Group ABC creates a new Windows system service that starts automatically when the operating system starts up.

You will use the ATT&CK Navigator to map the **Persistence** tactic.

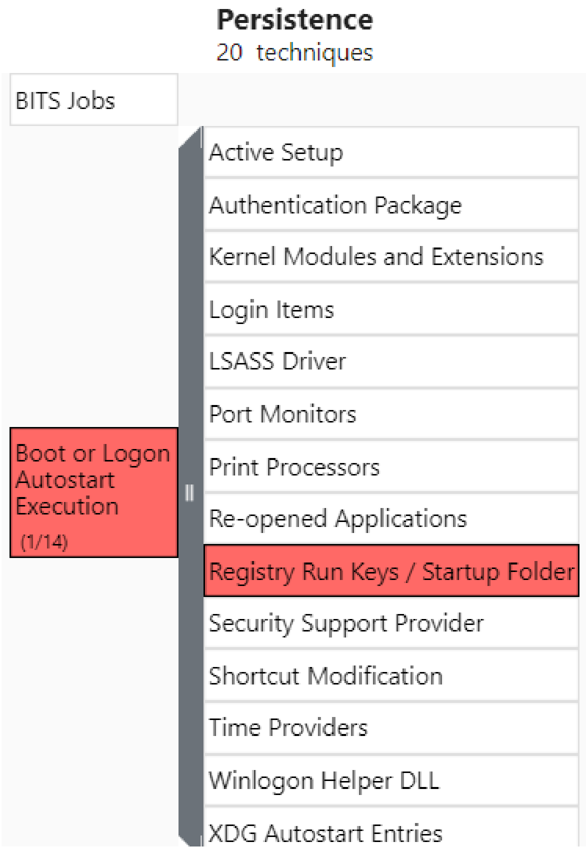
To map the Persistence tactic

1. In the **Persistence** column, to the right of the **Boot or Logon Autostart Execution** technique, click **||** to expand the subtechniques.
2. Hold the Shift key, and then in the **Persistence** column, select both the **Boot or Logon Autostart Execution** technique and **Registry Run Keys / Startup Folder** subtechnique.



3. In the **Technique Controls** toolbar, click the **score** icon, and then set the **score** to 1.

The selections are highlighted.



Persistence

20 techniques

BITS Jobs

Boot or Logon Autostart Execution (1/14)

Active Setup

Authentication Package

Kernel Modules and Extensions

Login Items

LSASS Driver

Port Monitors

Print Processors

Re-opened Applications

Registry Run Keys / Startup Folder

Security Support Provider

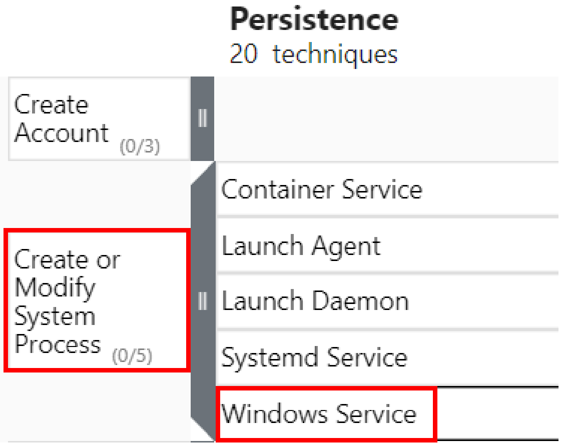
Shortcut Modification

Time Providers

Winlogon Helper DLL

XDG Autostart Entries

4. To the right of the **Boot or Logon Autostart Execution** technique, click **||** to collapse the subtechniques.
5. In the **Persistence** column, to the right of the **Create or Modify System Process** technique, click **||** to expand the subtechniques.
6. Hold the Shift key, and then in the **Persistence** column, select both the **Create or Modify System Process** technique and **Windows Service** subtechnique.



Persistence

20 techniques

Create Account (0/3)

Create or Modify System Process (0/5)

Container Service

Launch Agent

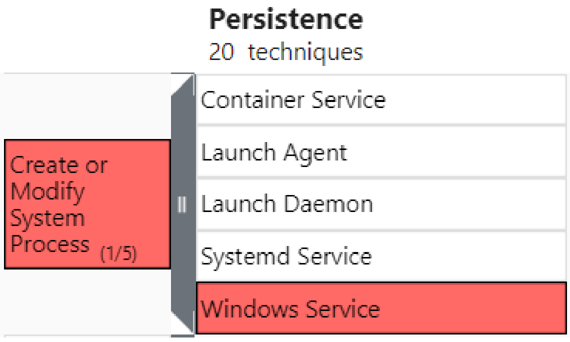
Launch Daemon

Systemd Service

Windows Service

7. In the **Technique Controls** toolbar, click the **score** icon, and then set the **score** to 1.

The selections are highlighted.



Persistence

20 techniques

Create or Modify System Process (1/5)

Container Service

Launch Agent

Launch Daemon

Systemd Service

Windows Service

8. To the right of the **Create or Modify System Process** technique, click **||** to collapse the subtechniques.

Map the Defense Evasion Tactic

The mock report describes that after establishing persistence, Group ABC tries to clear the Windows Audit Log Security entries on the compromised target in order to evade detection.

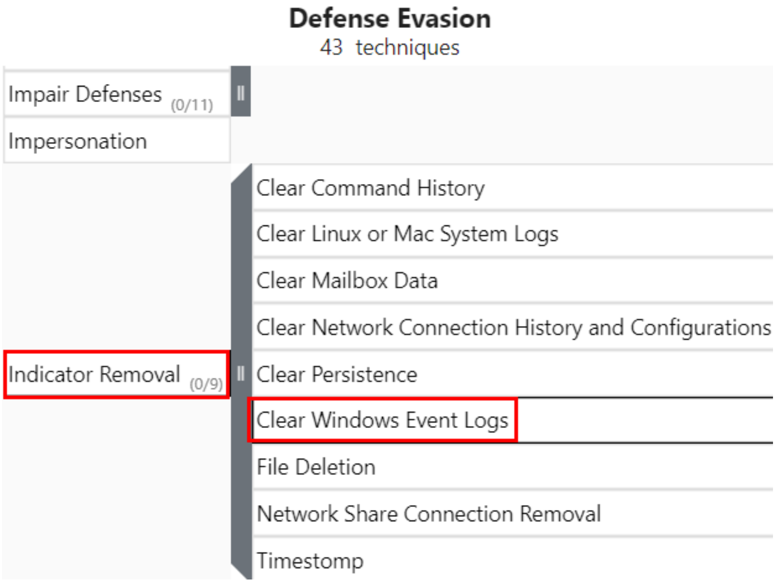
You will use the ATT&CK Navigator to map the **Defense Evasion** tactic.

To map the Defense Evasion tactic

In the **Defense Evasion** column, to the right of the **Indicator Removal** technique, click **||** to expand the subtechniques.

Depending on your screen resolution, you may have to scroll down to see this technique.

2. Hold the Shift key, and then in the **Defense Evasion** column, select both the **Indicator Removal** technique and **Clear Windows Event Logs** subtechnique.



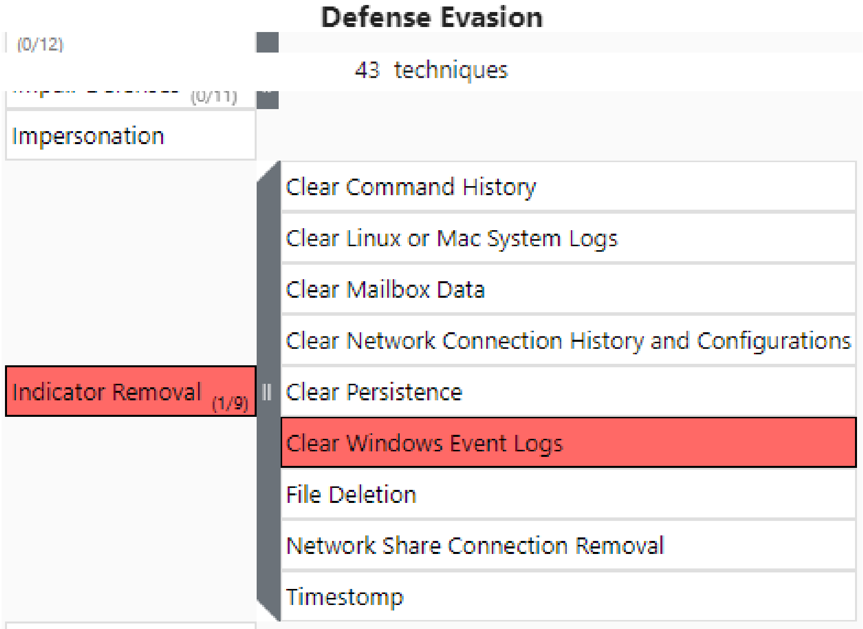
Defense Evasion
43 techniques

Impair Defenses (0/11)
Impersonation
Indicator Removal (0/9)

Clear Command History
Clear Linux or Mac System Logs
Clear Mailbox Data
Clear Network Connection History and Configurations
Clear Persistence
Clear Windows Event Logs
File Deletion
Network Share Connection Removal
Timestomp

3. In the **Technique Controls** toolbar, click the **score** icon, and then set the **score** to 1.

The selections are highlighted.



Defense Evasion
43 techniques

(0/12)
(0/11)
Impersonation
Indicator Removal (1/9)

Clear Command History
Clear Linux or Mac System Logs
Clear Mailbox Data
Clear Network Connection History and Configurations
Clear Persistence
Clear Windows Event Logs
File Deletion
Network Share Connection Removal
Timestomp

4. To the right of the **Indicator Removal** technique, click **||** to collapse the subtechniques.

Map the Command and Control Tactic

The next tactic you will map is the **Command and Control** tactic. You will map the following two behaviors of Group ABC under this tactic:

- The download of the malicious file that, along with the setup of Run keys, will automatically reestablish the Command and Control (C&C) channel once a user logs in to the compromised host
- The use of port TCP/443 to establish the C&C channel between the compromised host and the C&C server

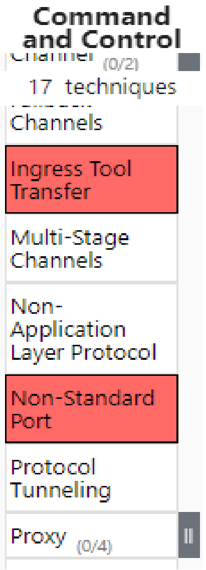
The first behavior of the two listed above—the download of additional artifacts—maps to the **Ingress Tool Transfer** technique. The second behavior—related to the establishment of a raw TCP C&C channel over a well-known port that is associated with another protocol (in this case, HTTPS)—maps to the **Non-Standard Port** technique.

You will use the ATT&CK Navigator to map the **Command and Control** tactic.

To map the Command and Control tactic

1. In the **Command and Control** column, hold the Shift key, and then select both the **Ingress Tool Transfer** technique and **Non-Standard Port** technique.
2. In the **Technique Controls** toolbar, click the **score** icon, and then set the **score** to 1.

The selections are highlighted.



Command and Control

17 techniques

Channel (0/2)

Channels

Ingress Tool Transfer

Multi-Stage Channels

Non-Application Layer Protocol

Non-Standard Port

Protocol Tunneling

Proxy (0/4)

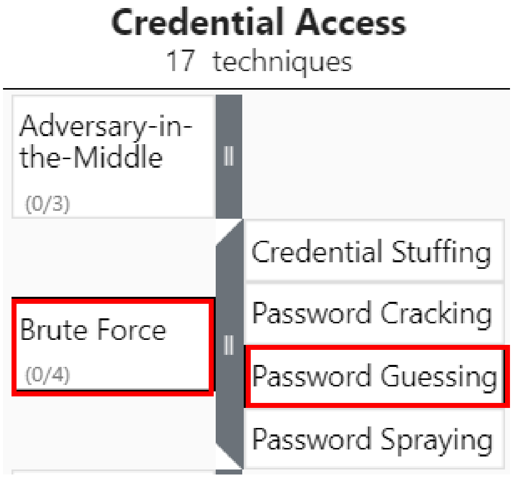
Map the Credential Access Tactic

To gain **Credential Access** (tactic), Group ABC has been known to use **Brute Force** (technique) and **Password Guessing** (subtechnique).

You will use the ATT&CK Navigator to map the **Credential Access** tactic.

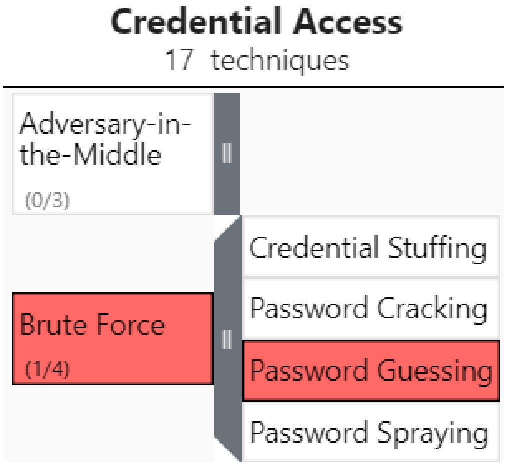
To map the Credential Access tactic

1. In the **Credential Access** column, to the right of the **Brute Force** technique, click **||** to expand the subtechniques.
2. In the **Credential Access** column, hold the Shift key, and then select both the **Brute Force** technique and **Password Guessing** subtechnique.



3. In the **Technique Controls** toolbar, click the **score** icon, and then set the **score** to 1.

The selections are highlighted.



4. To the right of the **Brute Force** technique, click **||** to collapse the subtechniques.

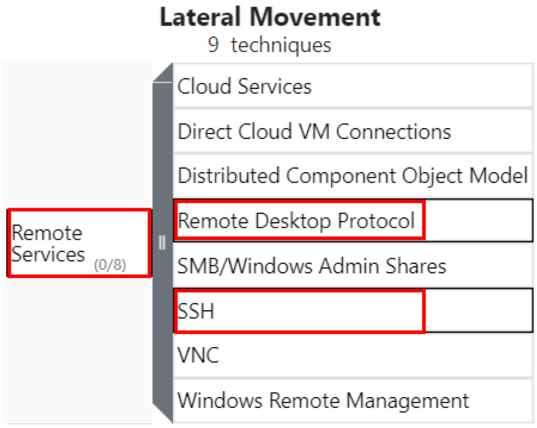
Map the Lateral Movement Tactic

The adversary group will achieve **Lateral Movement** (tactic) by using **Remote Services** (technique), specifically **Remote Desktop Protocol** (subtechnique) and **SSH** (subtechnique), to move to high-priority targets.

You will use the ATT&CK Navigator to map the **Lateral Movement** tactic.

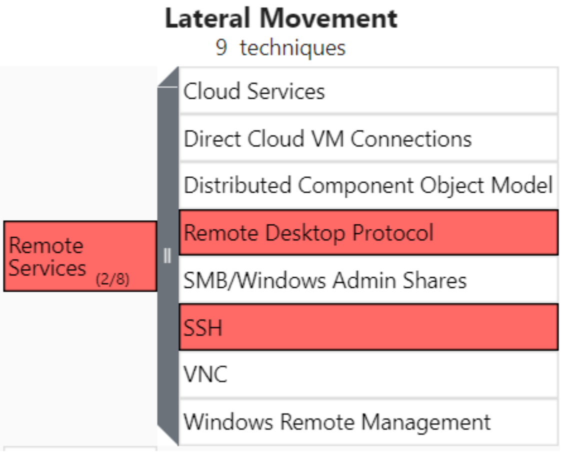
To map the Lateral Movement tactic

1. In the **Lateral Movement** column, to the right of the **Remote Services** technique, click **||** to expand the subtechniques.
2. In the **Lateral Movement** column, hold the Shift key, and then select the **Remote Services** technique and the **Remote Desktop Protocol** and **SSH** subtechniques.



3. In the **Technique Controls** toolbar, click the **score** icon, and then set the **score** to 1.

The selections are highlighted.



4. To the right of the **Remote Services** technique, click **||** to collapse the subtechniques.

Map the Exfiltration Tactic

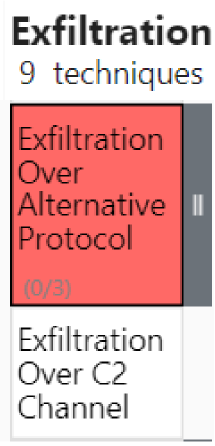
Group ABC will use **Exfiltration** (tactic) to steal sensitive files that can be used for nefarious purposes, such as for ransom or selling to other cyber criminals. They are known to use SMB to transfer files, which falls under **Exfiltration Over Alternate Protocol** (technique).

You will use the ATT&CK Navigator to map the **Exfiltration** tactic.

To map the Exfiltration tactic

1. In the **Exfiltration** column, hold the Shift key, and then select the **Exfiltration Over Alternative Protocol** technique.
2. In the **Technique Controls** toolbar, click the **score** icon, and then set the **score** to 1.

The selections are highlighted.

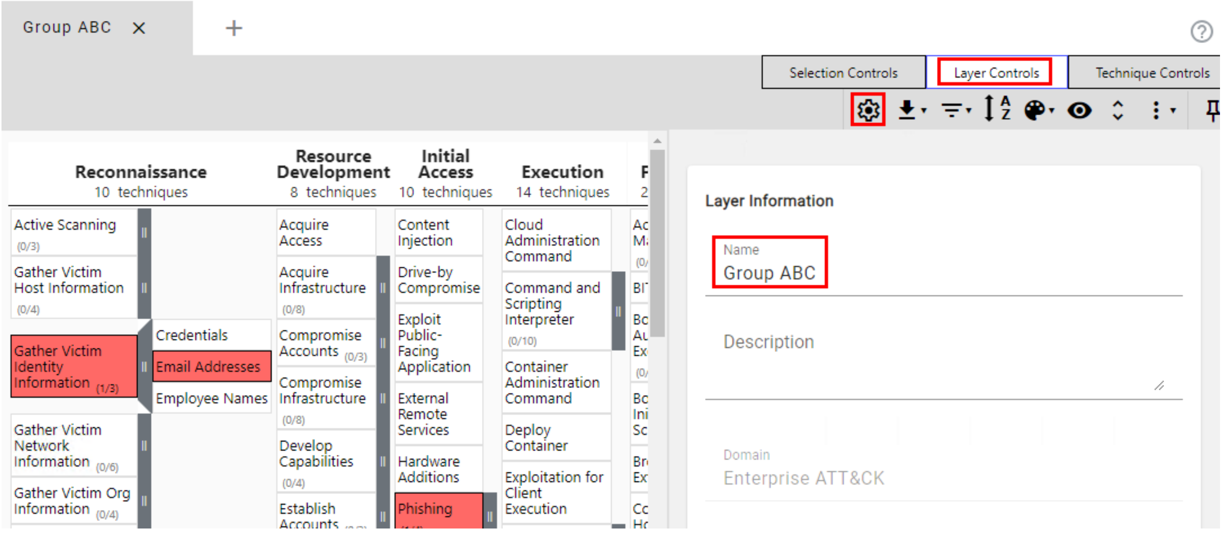

Exfiltration
9 techniques
Exfiltration Over Alternative Protocol (0/3)
Exfiltration Over C2 Channel

Finalize and Download the Security Report

You will complete the security report, and then download it. In a real-world situation, you could then send the security report to a Security Operations team, for example.

To finalize and download the security report

1. In the **Layer Controls** toolbar, click the gear icon to open the **Layer Information** window.
2. In the **Name** field, type Group ABC to change the layer name.


Group ABC
Selection Controls
Layer Controls
Technique Controls
Reconnaissance
10 techniques
Resource Development
8 techniques
Initial Access
10 techniques
Execution
14 techniques
Active Scanning
Gather Victim Host Information
Gather Victim Identity Information (1/3)
Credentials
Email Addresses
Employee Names
Gather Victim Network Information (0/6)
Gather Victim Org Information (0/4)
Acquire Access
Acquire Infrastructure (0/8)
Compromise Accounts (0/3)
Compromise Infrastructure (0/8)
Develop Capabilities (0/4)
Establish Accounts
Content Injection
Drive-by Compromise
Exploit Public-Facing Application
External Remote Services
Hardware Additions
Phishing
Cloud Administration Command
Command and Scripting Interpreter (0/10)
Container Administration Command
Deploy Container
Exploitation for Client Execution

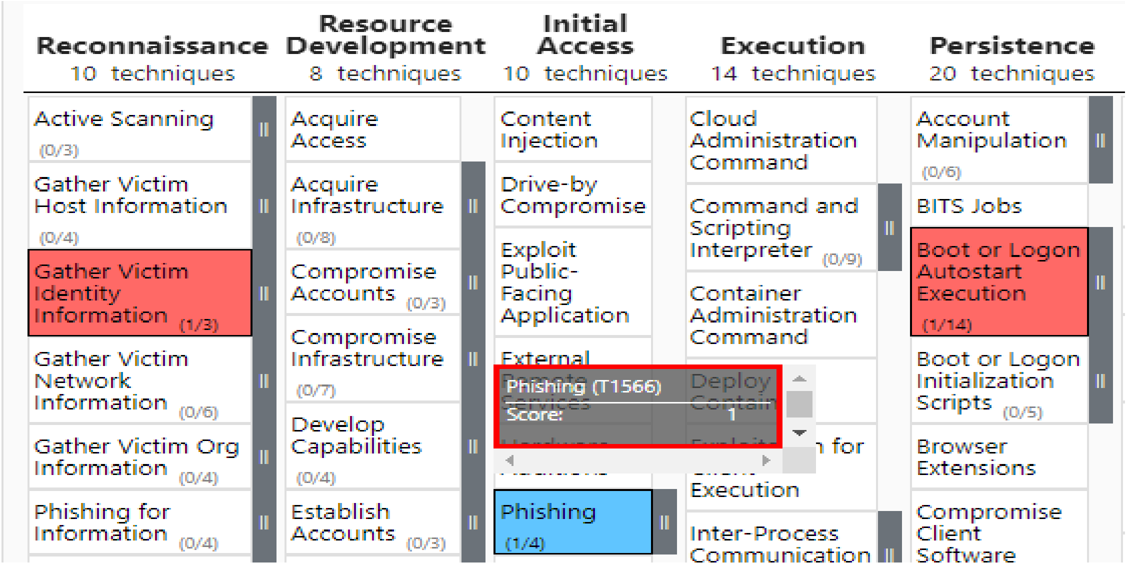
Layer Information

Name
Group ABC

Description

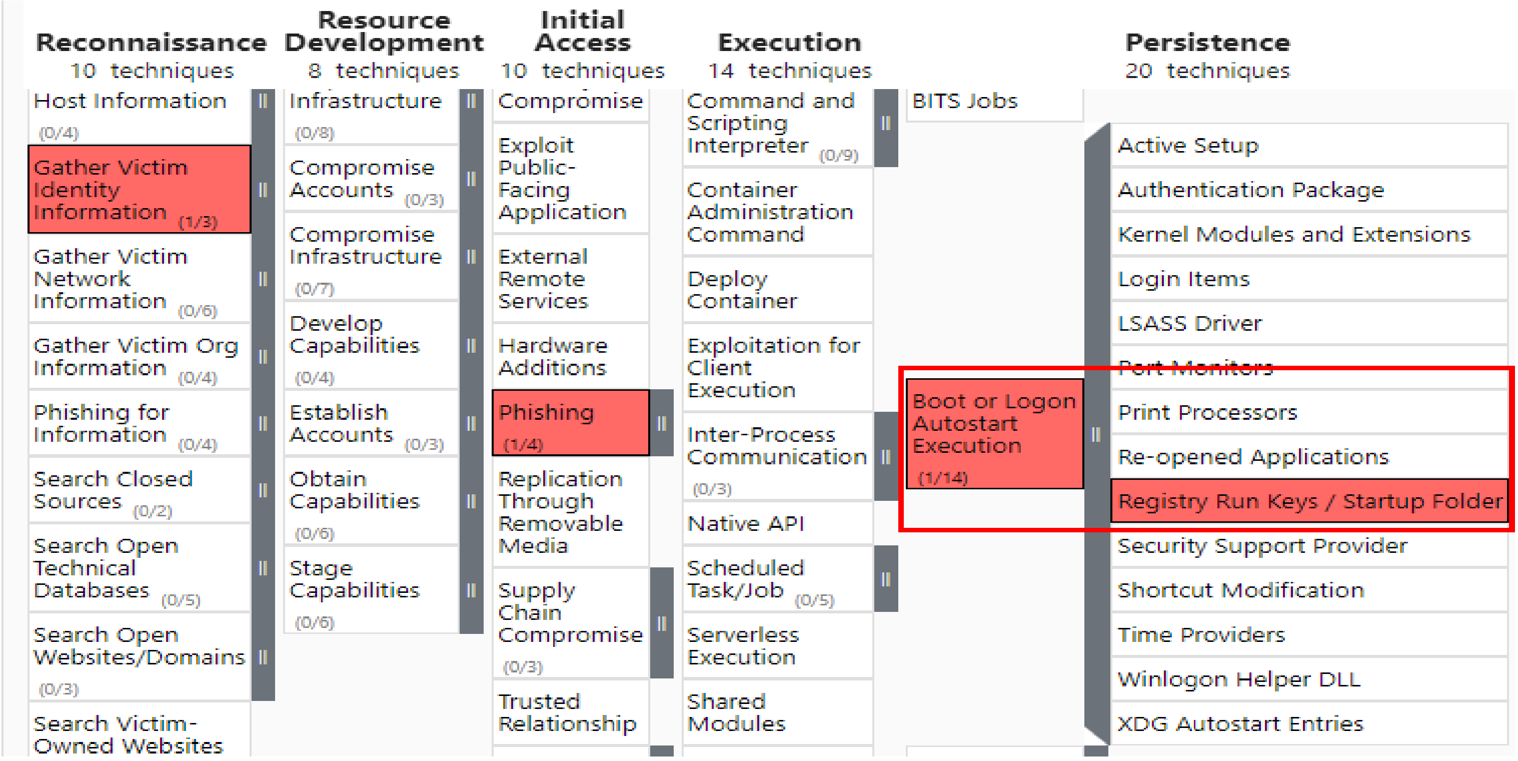
Domain
Enterprise ATT&CK

3. Hover over the highlighted techniques to see that their scores are all set to **1**.

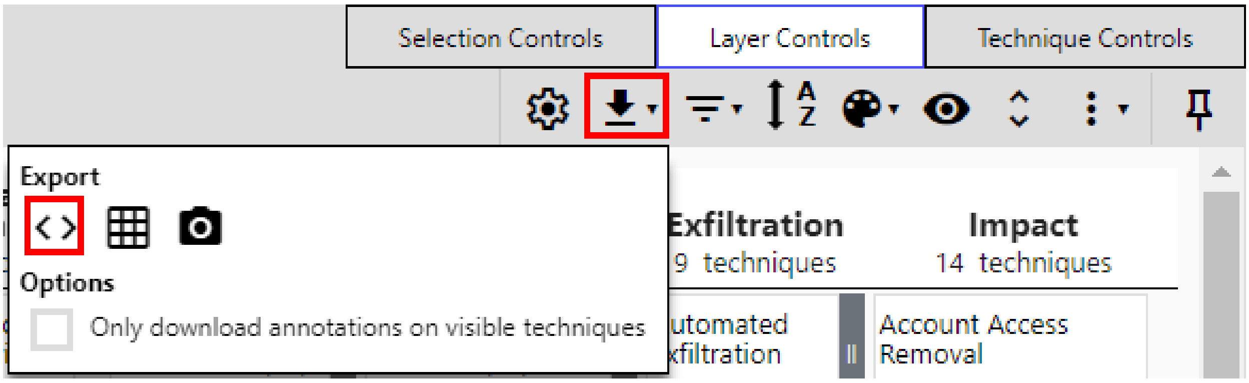

Reconnaissance
10 techniques
Resource Development
8 techniques
Initial Access
10 techniques
Execution
14 techniques
Persistence
20 techniques
Active Scanning (0/3)
Gather Victim Host Information (0/4)
Gather Victim Identity Information (1/3)
Gather Victim Network Information (0/6)
Gather Victim Org Information (0/4)
Phishing for Information (0/4)
Acquire Access
Acquire Infrastructure (0/8)
Compromise Accounts (0/3)
Compromise Infrastructure (0/7)
Develop Capabilities (0/4)
Establish Accounts (0/3)
Content Injection
Drive-by Compromise
Exploit Public-Facing Application
Phishing (1/4)
Cloud Administration Command
Command and Scripting Interpreter (0/9)
Container Administration Command
Execution
Inter-Process Communication
Account Manipulation (0/6)
BITS Jobs
Boot or Logon Autostart Execution (1/14)
Boot or Logon Initialization Scripts (0/5)
Browser Extensions
Compromise Client Software

Phishing (T1566)
Score: 1

4. Click **||** to the right of a technique to expand the subtechniques for the technique.


Reconnaissance
10 techniques
Resource Development
8 techniques
Initial Access
10 techniques
Execution
14 techniques
Persistence
20 techniques
Host Information (0/4)
Gather Victim Identity Information (1/3)
Gather Victim Network Information (0/6)
Gather Victim Org Information (0/4)
Phishing for Information (0/4)
Search Closed Sources (0/2)
Search Open Technical Databases (0/5)
Search Open Websites/Domains (0/3)
Search Victim-Owned Websites
Infrastructure (0/8)
Compromise Accounts (0/3)
Compromise Infrastructure (0/7)
Develop Capabilities (0/4)
Establish Accounts (0/3)
Obtain Capabilities (0/6)
Stage Capabilities (0/6)
Compromise
Exploit Public-Facing Application
External Remote Services
Hardware Additions
Phishing (1/4)
Replication Through Removable Media
Supply Chain Compromise (0/3)
Trusted Relationship
Command and Scripting Interpreter (0/9)
Container Administration Command
Deploy Container
Exploitation for Client Execution
Inter-Process Communication (0/3)
Native API
Scheduled Task/Job (0/5)
Serverless Execution
Shared Modules
BITS Jobs
Boot or Logon Autostart Execution (1/14)
Active Setup
Authentication Package
Kernel Modules and Extensions
Login Items
LSASS Driver
Port Monitors
Print Processors
Re-opened Applications
Registry Run Keys / Startup Folder
Security Support Provider
Shortcut Modification
Time Providers
Winlogon Helper DLL
XDG Autostart Entries

5. In the **Layer Controls** toolbar, click the **download single layer as json** icon to download your layer as a JSON file.



Downloading this file provides you with a backup of your layer that you can then upload to the ATT&CK Navigator in a later exercise.

6. In Chrome, leave the tab with the ATT&CK Navigator open for a later lab exercise.