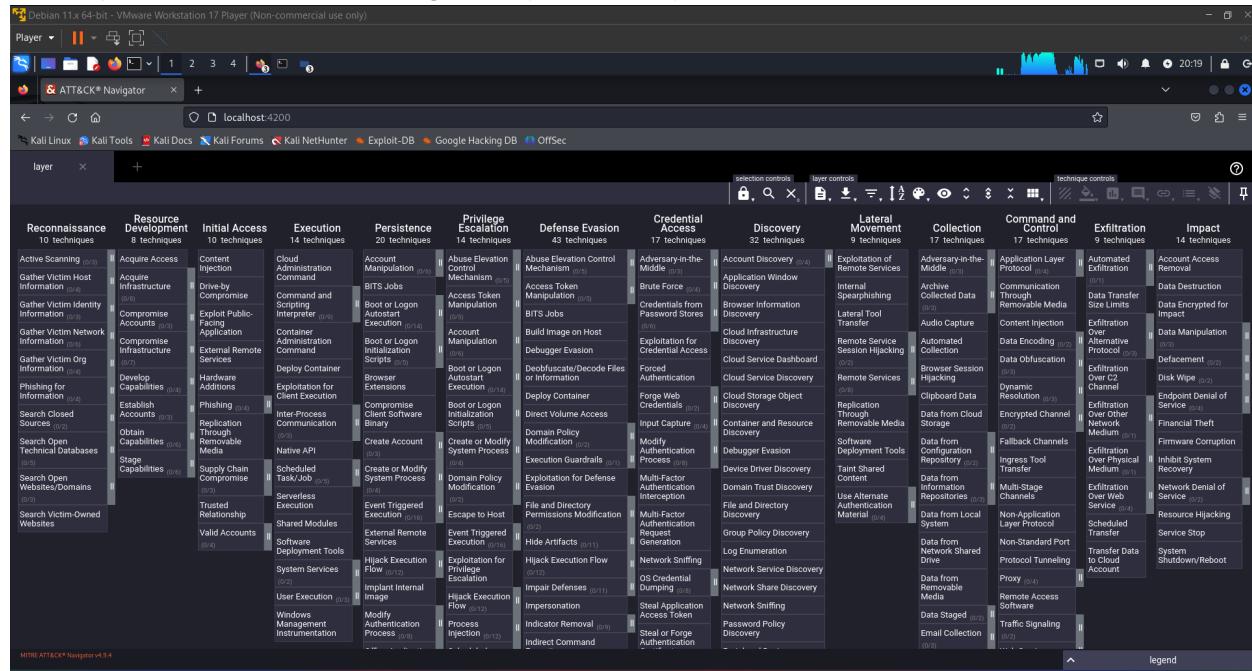


Application of ATT&CK Navigator

Getting to know the toolbar:

1. Click on Create New Layer
2. Expand More Options
3. Set the version to ATT&CK v12
4. Click the Enterprise button
5. Use the search button under selection controls and search for the term Password
6. Click the select all button
7. Using the background color button under technique controls, change the background color of your selection from steps 5 and 6 to red.
8. Click the toggle state button to disable the selected techniques.
9. Click the show/hide disabled button to hide the disabled techniques from view.
10. Click the show/hide disabled button to show the disabled techniques in the view.
11. Click the toggle state button to enable the selected techniques.
12. Rename the Navigator Layer from “layer” to “Password”.



Debian 11.x 64-bit - VMware Workstation 17 Player (Non-commercial use only)

Player | < > ⌛ 🔍 +

localhost:4200

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

layer +

The screenshot shows the ATT&CK Navigator interface with the matrix view. The columns represent tactics: Reconnaissance, Resource Development, Initial Access, Execution, Persistence, Privilege Escalation, Defense Evasion, Credential Access, Discovery, Lateral Movement, Collection, Command and Control, and Exit. The rows represent techniques, many of which are highlighted in red. The right side of the screen features a search bar, search settings, and a sidebar with sections for Techniques, Threat Groups, Software, Mitigations, and Campaigns.

Debian 11x 64-bit - VMware Workstation 17 Player (Non-commercial use only)

Player | < > ⌛ 🔍 +

localhost:4200

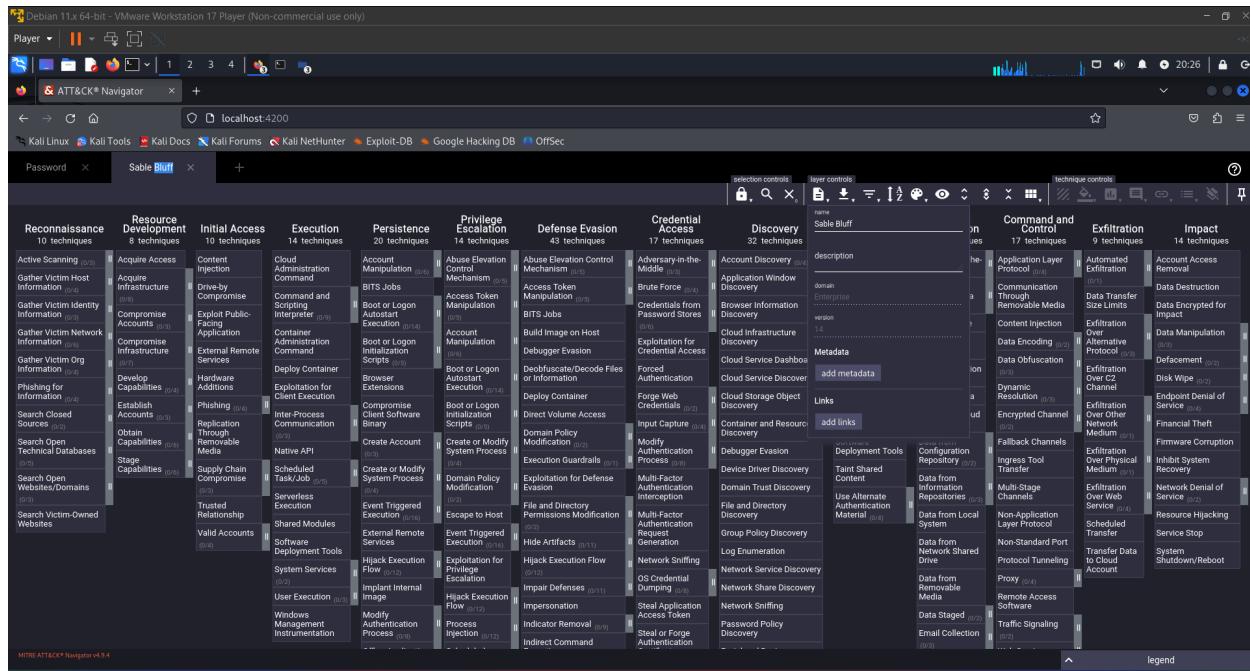
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

Password +

This screenshot is identical to the one above, but it includes a search term 'Password' in the search bar, which has filtered the results to show only techniques related to password manipulation.

Lab 2 - Assigning Risk Score in Navigator

1. By clicking the + sign next to our Password Layer.
2. Use the same settings as you did in Lab 1.
3. Click on the name of the tab currently titled “layer” to edit the name and change it to Sable Bluff.
4. Click on the color selection icon under the layer controls menu.
5. On the presets drop-down, at the bottom of the menu, click on blue to red to change the score gradient to blue for a low score and red for a high score.
6. Under selection controls, click on the search icon.
7. Find APT29 under Threat Groups and click the select button.
8. Click on the scoring button under technique controls, and give the selected techniques a score of 80
9. Click the deselect button under selection controls to unselect the 20 techniques that were chosen in step 7.
10. Under selection controls click the search icon.
11. Under software, locate DarkComet and click view to open the MITRE ATT&CK web page for DarkComet.
12. Return to the ATT&CK Navigator and click the select button for DarkComet.
13. Give the selected DarkComet techniques a score of 50.
14. Use the deselect button to unselect all the DarkComet techniques.
15. Use what you’ve learned so far to add a score of 25 to techniques that can be mitigated with Active Directory Configuration.



Debian 11.x 64-bit - VMware Workstation 17 Player (Non-commercial use only)

Player | < > | +

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

localhost:4200

Sable Bluff

selection controls layer controls technique controls

Techniques (625)

select all deselect all

Abuse Elevation Control Mechanism: Elevated Execution with Prompt

Abuse Elevation Control Mechanism: Setuid and Setgid

Abuse Elevation Control Mechanism: Sudo and Sudo

Threat Groups (141)

select all deselect all

APT19

APT28

APT29

select all deselect all

APT3

Software (648)

Mitigations (43)

legend

Debian 11.x 64-bit - VMware Workstation 17 Player (Non-commercial use only)

Player | < > | +

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

localhost:4200

Sable Bluff

selection controls layer controls technique controls

Techniques (625)

select all deselect all

Abuse Elevation Control Mechanism: Elevated Execution with Prompt

Abuse Elevation Control Mechanism: Setuid and Setgid

Abuse Elevation Control Mechanism: Sudo and Sudo

Threat Groups (141)

select all deselect all

APT19

APT28

APT29

select all deselect all

APT3

Software (648)

Mitigations (43)

legend

Debian 11x 64-bit - VMware Workstation 17 Player (Non-commercial use only)

Player | < > | 1 2 3 4 | + | & ATT&CK® Navigator | localhost:4200 | Kali Linux | Kali Tools | Kali Docs | Kali Forums | Kali NetHunter | Exploit-DB | Google Hacking DB | OffSec

Password X Sable Bluff +

The screenshot shows the ATT&CK Navigator interface with a large tree of attack techniques. The categories include:

- Reconnaissance**: 10 techniques (e.g., Gather Victim Identity Information, Gather Victim Network Information).
- Resource Development**: 8 techniques (e.g., Compromise Accounts, Compromise Infrastructure).
- Initial Access**: 10 techniques (e.g., Exploit Public-Facing Application, Container Administration Command).
- Execution**: 14 techniques (e.g., Scripting Interpreter, Container Administration Command).
- Persistence**: 20 techniques (e.g., Boot or Logon Autostart Execution, Account Manipulation).
- Privilege Escalation**: 14 techniques (e.g., Bits Jobs, Build Image on Host).
- Defense Evasion**: 43 techniques (e.g., Exploit for Defense Evasion, Deploy Container).
- Credential Access**: 17 techniques (e.g., Credentials from Password Stores, Exploitation for Credential Access).
- Discovery**: 32 techniques (e.g., Browser Information Discovery, Cloud Infrastructure Discovery).
- Lateral Movement**: 9 techniques (e.g., Lateral Tool Transfer, Remote Service Session Hijacking).
- Collection**: 17 techniques (e.g., Collected Data, Automated Collection).
- Command and Control**: 17 techniques (e.g., Exitf: Over C Channel, Exitf: Over Network Medium).
- Exfiltration**: 9 techniques (e.g., Through Removable Media, Content Injection).
- Threat Groups (141)**: A list of threat groups including APT39, APT41, Aquatic Panda, Axiom, and BackdoorDiplomacy.
- Software (648)**: A list of software including DanBot, DarkComet, DarkTortilla, and DarkWatchman.

Legend: view, select, deselect

MITRE ATT&CK® Navigator v3.4

Debian 11x 64-bit - VMware Workstation 17 Player (Non-commercial use only)

Player | < > | 1 2 3 4 | + | & ATT&CK® Navigator | localhost:4200 | Kali Linux | Kali Tools | Kali Docs | Kali Forums | Kali NetHunter | Exploit-DB | Google Hacking DB | OffSec

Password X Sable Bluff +

The screenshot shows the ATT&CK Navigator interface with a simplified tree of attack techniques. The categories include:

- Reconnaissance**: 10 techniques (e.g., Gather Victim Identity Information, Gather Victim Network Information).
- Resource Development**: 8 techniques (e.g., Compromise Accounts, Compromise Infrastructure).
- Initial Access**: 10 techniques (e.g., Exploit Public-Facing Application, Container Administration Command).
- Execution**: 14 techniques (e.g., Scripting Interpreter, Container Administration Command).
- Persistence**: 20 techniques (e.g., Boot or Logon Autostart Execution, Account Manipulation).
- Privilege Escalation**: 14 techniques (e.g., Bits Jobs, Build Image on Host).
- Defense Evasion**: 43 techniques (e.g., Exploit for Defense Evasion, Deploy Container).
- Credential Access**: 17 techniques (e.g., Credentials from Password Stores, Exploitation for Credential Access).
- Discovery**: 32 techniques (e.g., Browser Information Discovery, Cloud Infrastructure Discovery).
- Lateral Movement**: 9 techniques (e.g., Lateral Tool Transfer, Remote Service Session Hijacking).
- Collection**: 17 techniques (e.g., Collected Data, Automated Collection).
- Command and Control**: 17 techniques (e.g., Exitf: Over C Channel, Exitf: Over Network Medium).
- Exfiltration**: 9 techniques (e.g., Through Removable Media, Content Injection).
- Impact**: 14 techniques (e.g., Data Encrypted for Impact, Data Manipulation).

Legend: view, select, deselect

MITRE ATT&CK® Navigator v3.4

Lab 3 - Importing Navigator Layers

1. Return to your open Navigator page and click on the + sign next to the Sable Bluff Tab. This creates a new layer. Click on Open Existing Layer. 3. Paste the following URL into the Load from URL text box: https://raw.githubusercontent.com/center-for-threat-informed-defense/attack-control-8-frameworkmappings/main/frameworks/attack_10_1/nist800_53_r4/layers/by_family/Access_Control/AC-2.json 4. Click on the little arrow next to where you pasted the URL to import the layers. 5. You will receive a warning about the imported layer's version being different than Navigator's Layer Version. Click OK. 6. You will be asked if you want to upgrade the layer version. Click No.

The screenshot shows the ATT&CK Navigator interface with the 'Sable Bluff' tab selected. A new layer, 'AC-2 mappings', has been imported and is visible in the center grid. The grid is organized into columns representing different attack families: Reconnaissance, Resource Development, Initial Access, Execution, Persistence, Privilege Escalation, Defense Evasion, Credential Access, Discovery, Lateral Movement, Collection, Command and Control, Exfiltration, and Impact. Each column contains several specific techniques, many of which are highlighted in yellow or blue. The bottom right corner of the interface includes a legend for color-coding.