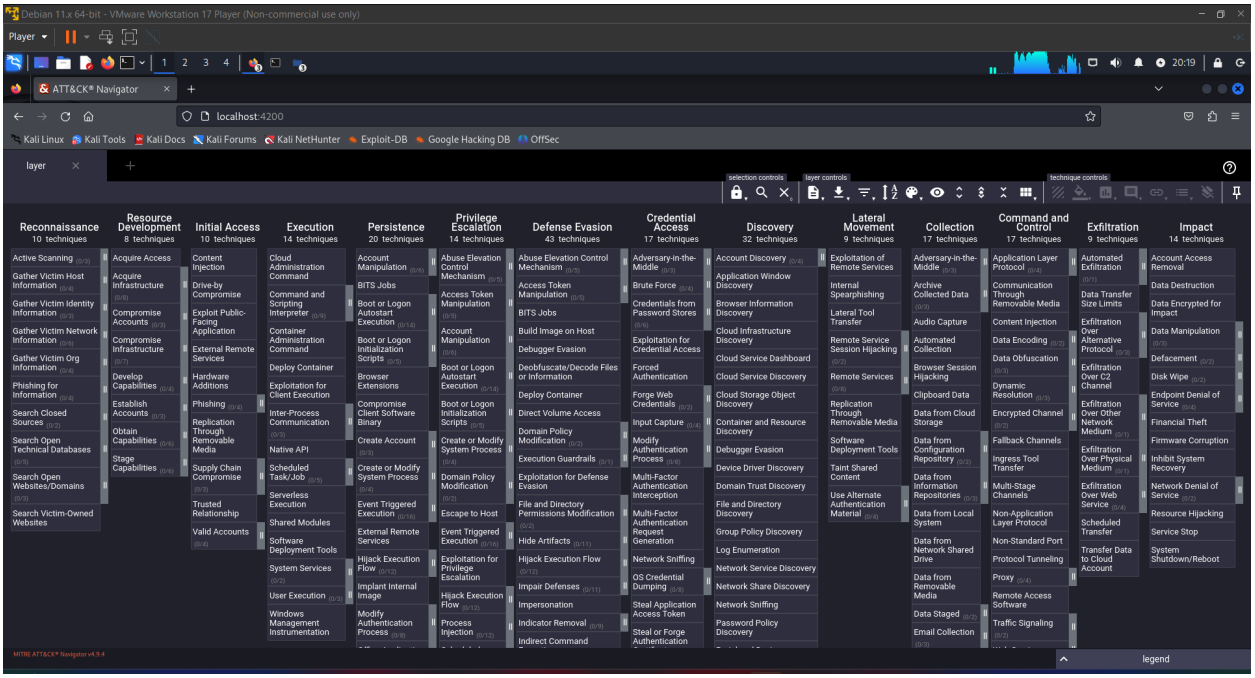
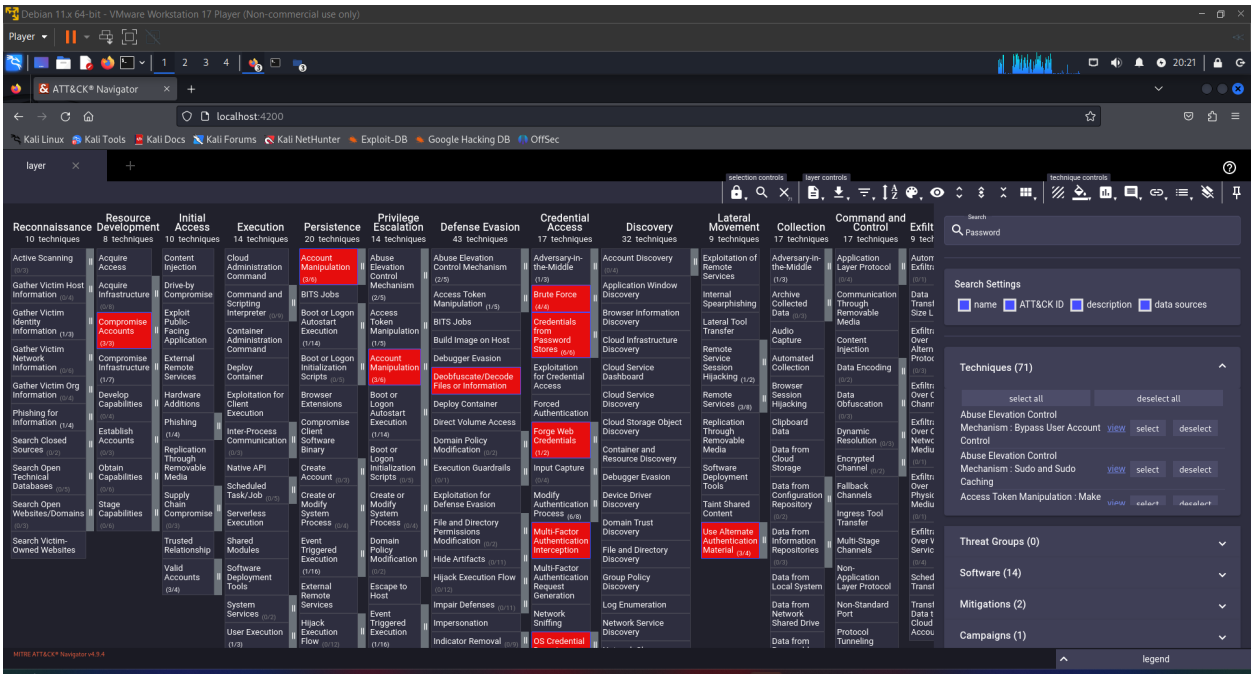
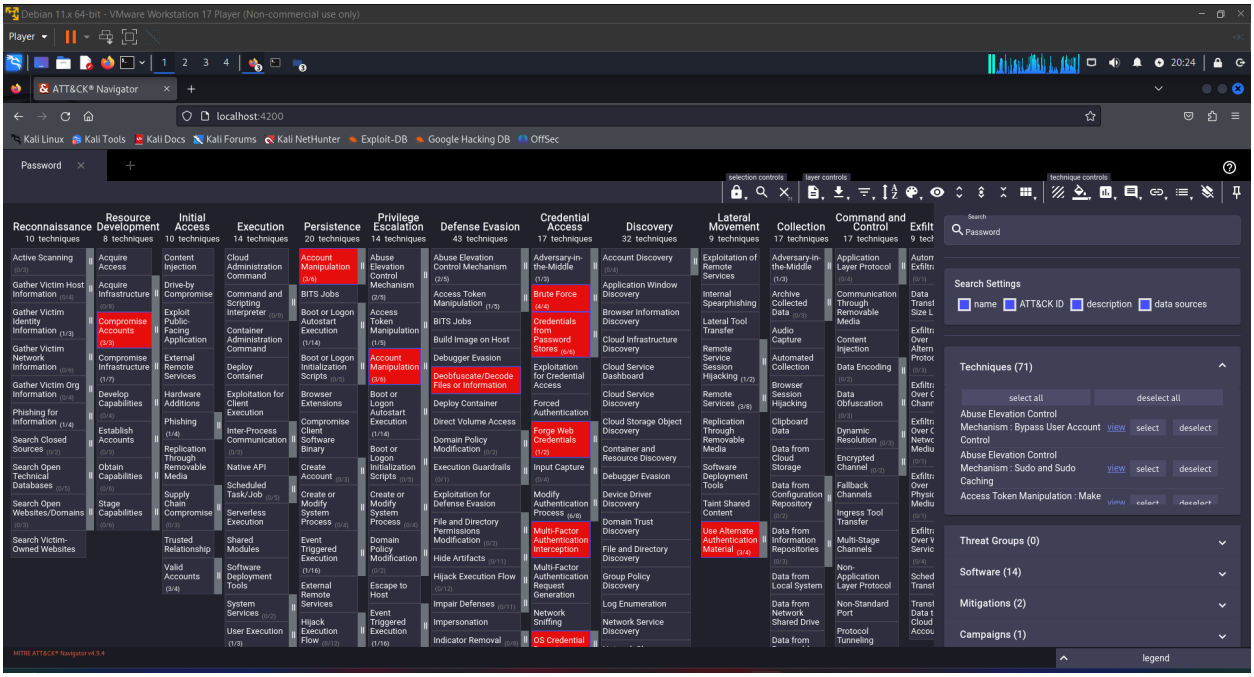
Application of ATT&CK Navigator

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 button5. Use the search button under selection controls and search for the term Password6. Click the select all button7. 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”.

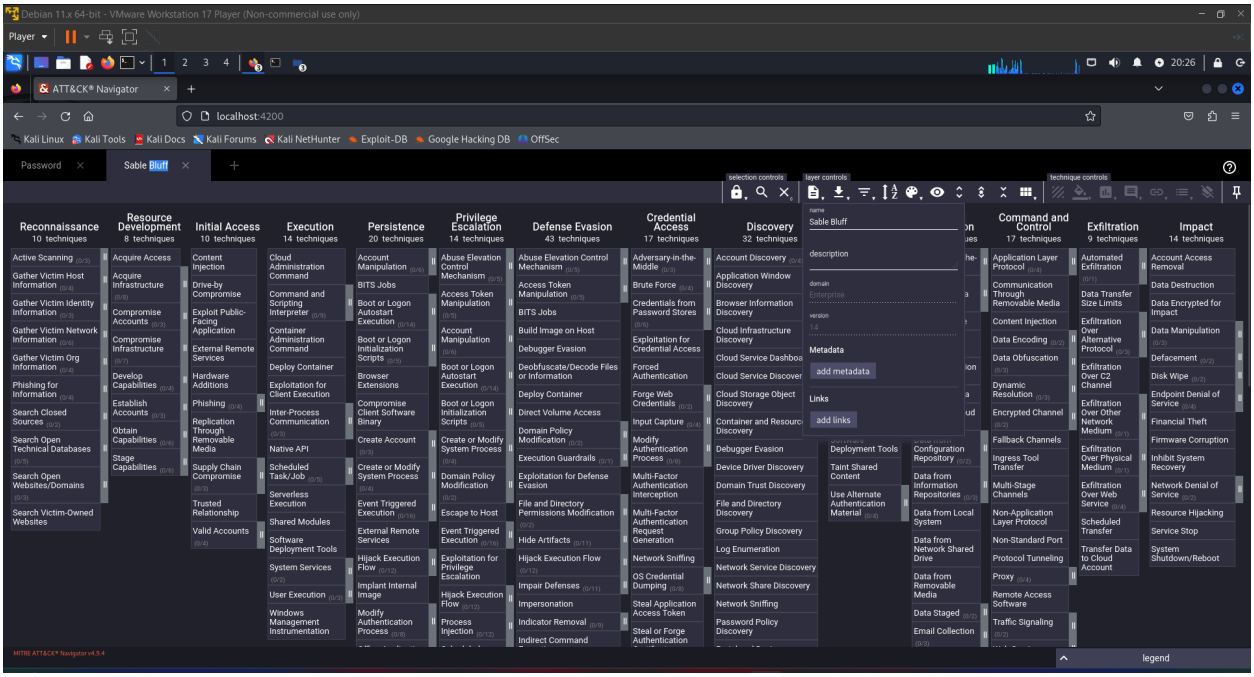


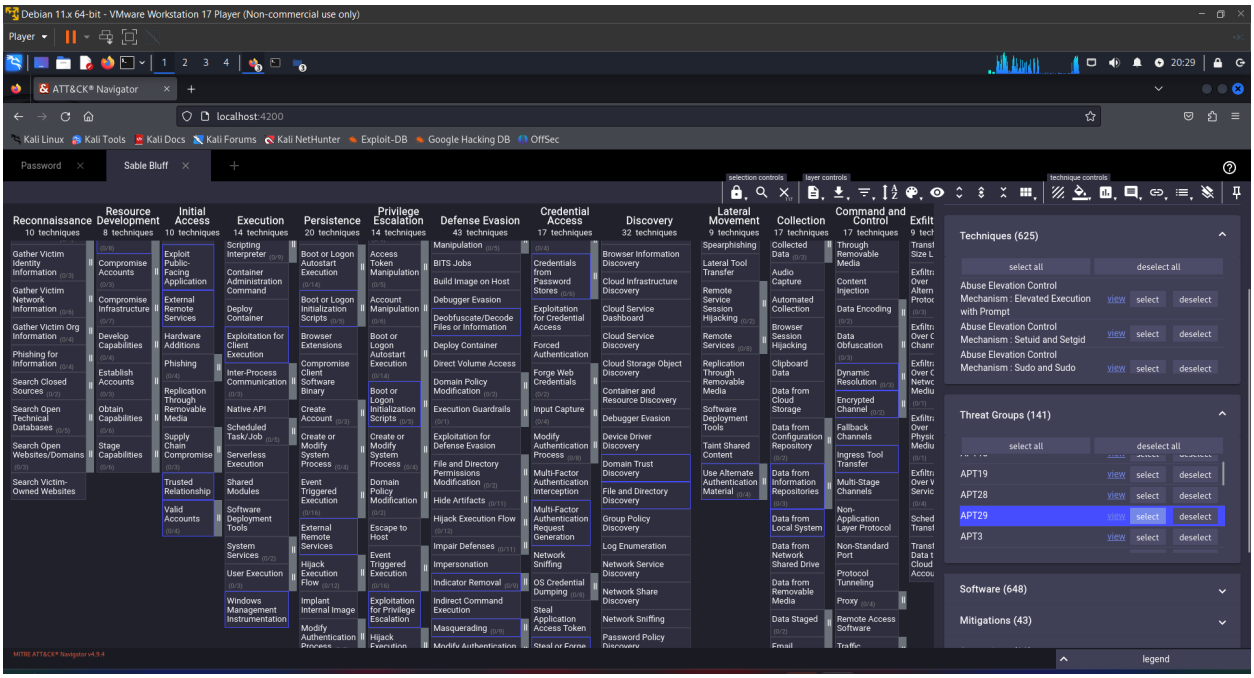

Debian 11.x 64-bit - VMware Workstation 17 Player (Non-commercial use only)
ATT&CK® Navigator
localhost:4200
layer
Reconnaissance
Resource Development
Initial Access
Execution
Persistence
Privilege Escalation
Defense Evasion
Credential Access
Discovery
Lateral Movement
Collection
Command and Control
Search Settings
name
ATT&CK ID
description
data sources
Techniques (71)
select all
deselect all
Threat Groups (0)
Software (14)
Mitigations (2)
Campaigns (1)
legend

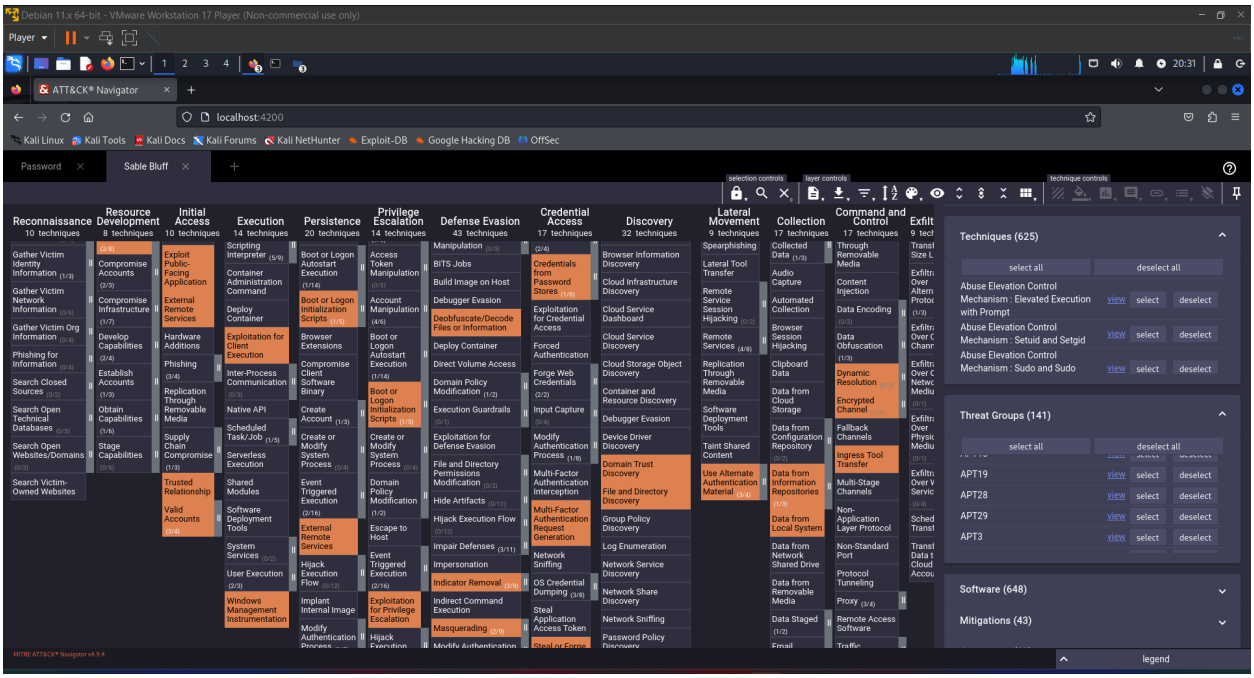

Debian 11.x 64-bit - VMware Workstation 17 Player (Non-commercial use only)
ATT&CK® Navigator
localhost:4200
Password
Reconnaissance
Resource Development
Initial Access
Execution
Persistence
Privilege Escalation
Defense Evasion
Credential Access
Discovery
Lateral Movement
Collection
Command and Control
Search Settings
name
ATT&CK ID
description
data sources
Techniques (71)
select all
deselect all
Threat Groups (0)
Software (14)
Mitigations (2)
Campaigns (1)
legend

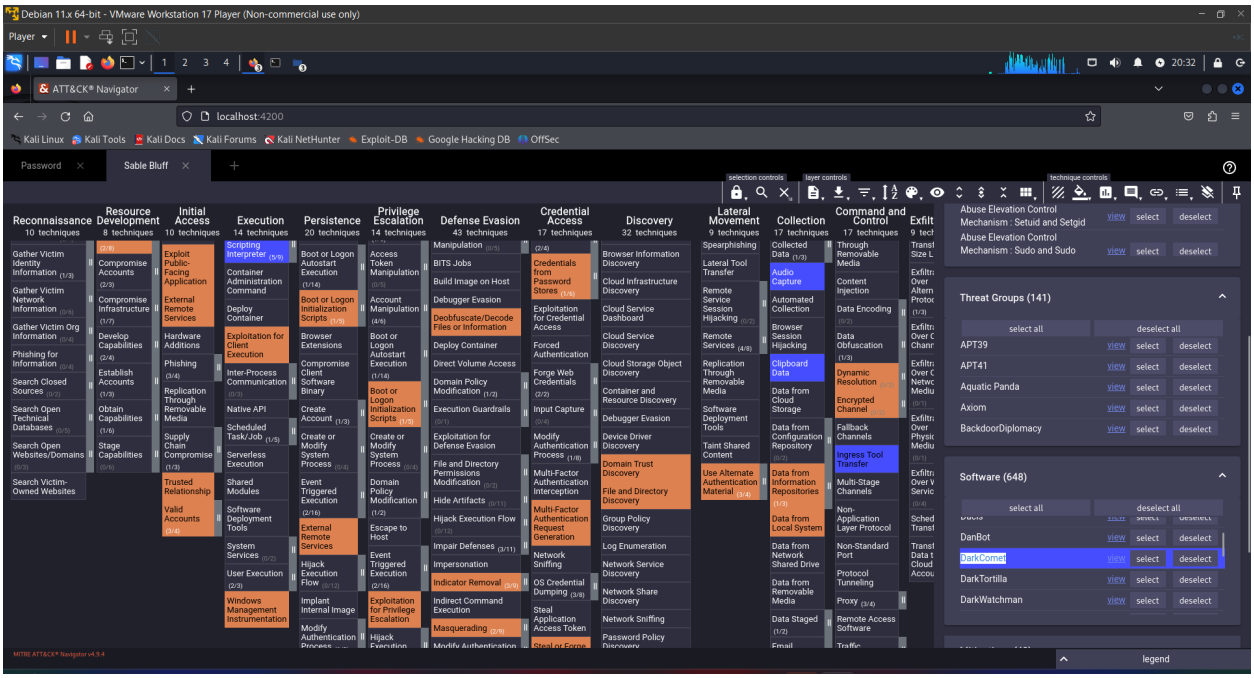
Lab 2 - Assigning Risk Score in Navigator

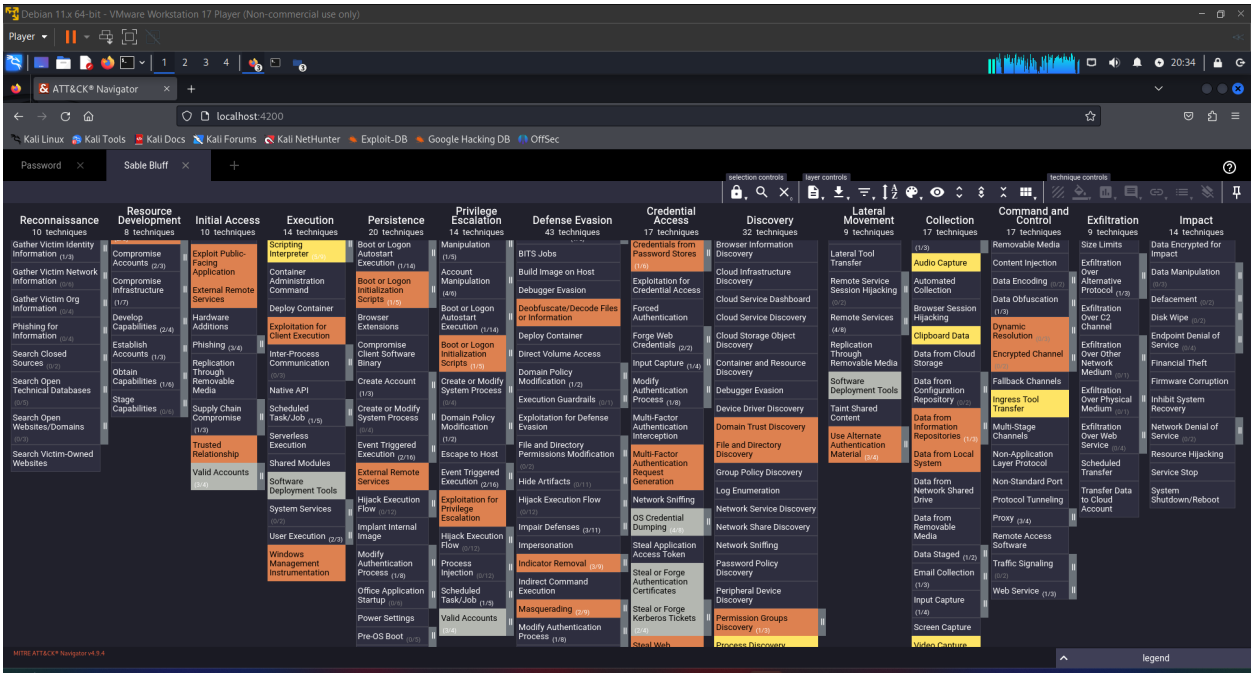
1. By clicking the + sign next to our Password Layer. 2. Use the same settings as you did in Lab 1. 3. Click on the name of the tab currently titled “layer” to edit the name and change it to Sable Bluff. 4. Click on the color selection icon under the layer controls menu. 5. On the presets drop-down, 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)
ATT&CK® Navigator
localhost:4200
Techniques (625)
Threat Groups (141)
Software (648)
Mitigations (43)
legend


Debian 11.x 64-bit - VMware Workstation 17 Player (Non-commercial use only)
ATT&CK® Navigator
localhost:4200
Techniques (625)
Threat Groups (141)
Software (648)
Mitigations (43)
legend


Debian 11.x 64-bit - VMware Workstation 17 Player (Non-commercial use only)
ATT&CK® Navigator
localhost:4200
Password
Sable Bluff
Reconnaissance
Resource Development
Initial Access
Execution
Persistence
Privilege Escalation
Defense Evasion
Credential Access
Discovery
Lateral Movement
Collection
Command and Control
Threat Groups (141)
APT39
APT41
Aquatic Panda
Axiom
BackdoorDiplomacy
Software (648)
DanBot
DarkComet
DarkTortilla
DarkWatchman
legend


Debian 11.x 64-bit - VMware Workstation 17 Player (Non-commercial use only)
ATT&CK® Navigator
localhost:4200
Password
Sable Bluff
Reconnaissance
Resource Development
Initial Access
Execution
Persistence
Privilege Escalation
Defense Evasion
Credential Access
Discovery
Lateral Movement
Collection
Command and Control
Exfiltration
Impact
legend

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_Contr ol/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.