Cybersecurity Threat Analysis

by Sean Sanders

The Common Vulnerability Scoring System

Introduced in 2005

Provides a standardized way for organizations to understand the severity of threats, which helps them prioritize patches and other responses.

Standardized Scoring

Consistent numerical severity assessment

Prioritization Aid

Helps organizations focus remediation efforts

Transparent Metrics

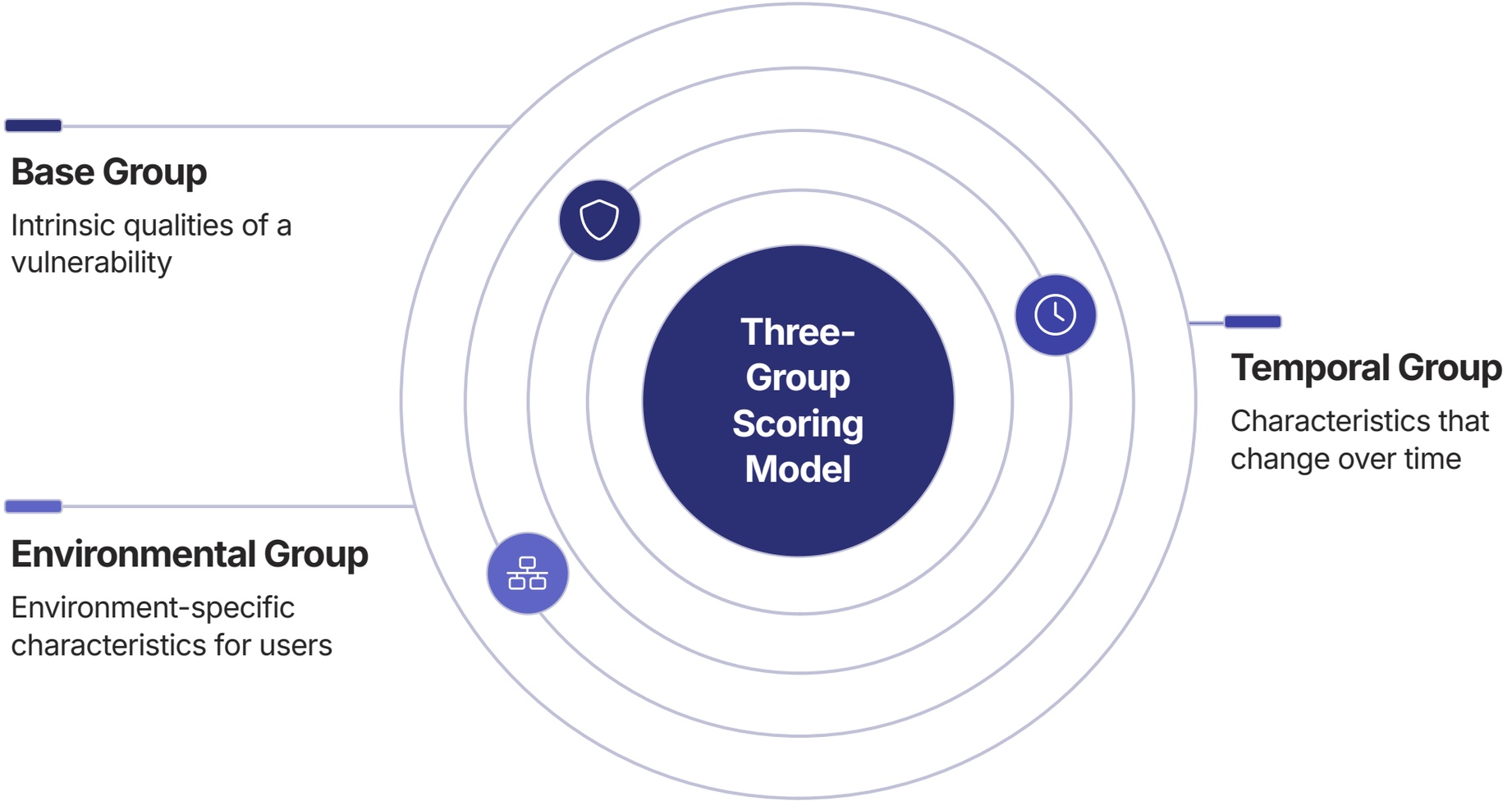
Clear, documented evaluation criteria

Open Framework

Community-driven and widely adopted

How it works

It uses three metric groups to generate a score:



Scoring: The base metrics produce a score from 0 to 10. This score is then adjusted by the temporal and environmental metrics to determine the ease and impact of a potential exploit.

CVSS Calculator

Bit Sentinel

Common Vulnerability Scoring System (CVSS) 2.0 Online Calculator – Bit Sentinel

Common Vulnerability Scoring System (CVSS) is a free and open industry standard for assessing the severity of computer system security vulnerabilities. It is under the custodianship of NIST. It attempts to establish a measure of how much concern a vulnerability warrants, compared...

CVSS Base Score	**2.7**
Impact Subscore	4.9
Exploitability Subscore	2.2
CVSS Temporal Score	**Not Defined**
CVSS Environmental Score	**Not Defined**
Modified Impact Subscore	0
Overall CVSS Score	**2.7**

AV:L/AC:M/Au:M/C:P/I:P/A:N

- Base Score Metrics

Access Vector (AV)*

Local (AV:L) | Adjacent Network (AV:A) | Network (AV:N)

Access Complexity (AC)*

High (AC:H) | Medium (AC:M) | Low (AC:L)

Authentification (Au)*

Multiple (Au:M) | Single (Au:S) | None (Au:N)

Confidentiality Impact (C)*

None (C:N) | Partial (C:P) | Complete (C:C)

Integrity Impact (I)*

None (I:N) | Partial (I:P) | Complete (I:C)

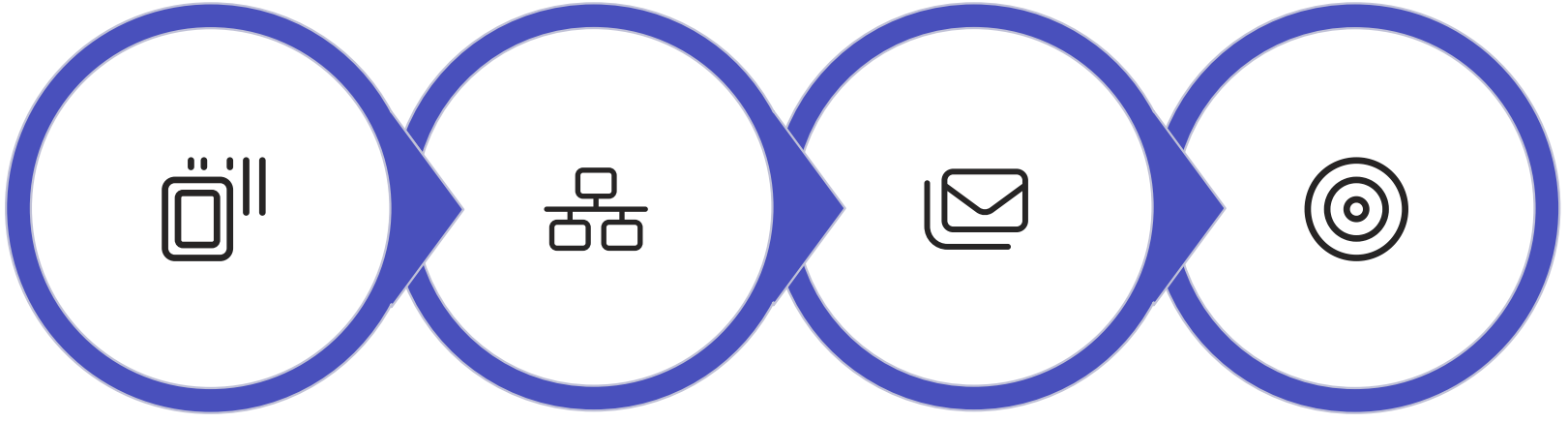
Availability Impact (A)*

None (A:N) | Partial (A:P) | Complete (A:C)

MITRE Attack Navigator

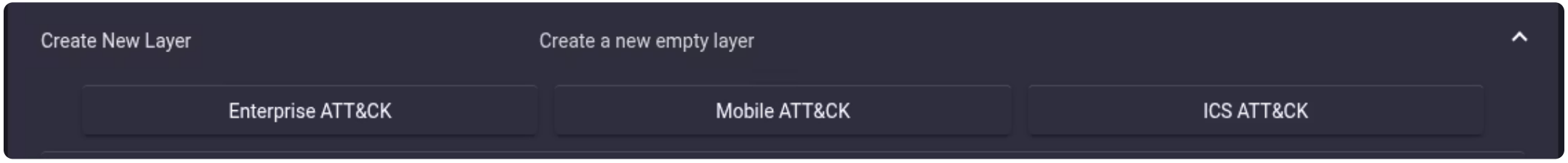
Red Teaming and Pentesting

Use the Navigator to plan and visualize red team engagements and penetration tests by selecting and color-coding specific techniques.



Attack Navigator Layers

mitre-attack.github.io



Each of these represents a comprehensive knowledge base of tactics and techniques used by cyber adversaries in specific environments.

Attack Navigator Layers Continued…

Enterprise ATT&CK

- **Scope:** Covers enterprise systems and cloud platforms.
- **Use Case:** Security professionals use this layer for threat modeling and testing defenses against Advanced Persistent Threat (APT) groups.

Mobile ATT&CK

- **Scope:** Covers Android and iOS mobile platforms.
- **Use Case:** Helps organizations secure mobile devices and applications, and understand mobile malware threats to develop detection and mitigation strategies.

ICS ATT&CK

- **Scope:** Focuses on industrial control systems (ICS) and physical processes.
- **Use Case:** Essential for protecting critical infrastructure and operational technology (OT) environments against attacks that disrupt physical processes.

CAP and Attack Navigator

Lab covers:

- Insecure Direct Object Reference (IDOR)
- Packet capture analysis
- Exploiting Linux capabilities for privilege escalation

Initial Access

This tactic represents the methods used to get your initial foothold on the system. In this lab, the attacker exploited a web vulnerability to find credentials and then used them to log in.

T1190: Exploit Public-Facing Application

The attacker's first step was to interact with the HTTP server running on port 80. The core vulnerability was an

Insecure Direct Object Reference (IDOR), which allowed access to a packet capture file that was not intended for the user. This is a direct exploitation of a flaw in the web application.

T**1552.001: Unsecured Credentials - Credentials in Files**

By exploiting the IDOR, the attacker downloaded a packet capture file. Analyzing this file revealed plaintext FTP credentials (

nathan / Buck3tH4TF0RM3!).

T1078: Valid Accounts

The credentials found in the capture file were successfully used to log in to the machine via SSH, granting the initial foothold.

Privilege Escalation

This tactic covers actions taken to gain higher-level permissions on a system. The lab demonstrates escalating from the user nathan to root.

T1548.003: Abuse Elevation Control Mechanism - SUID and SGID

- After gaining access, the attacker used a script to find privilege escalation vectors.
- The script discovered that the Python 3.8 binary had the cap_setuid Linux capability. This capability is a mechanism that controls elevation and allows a process to change its user ID (UID).
- The attacker then used Python to execute `os.setuid(0)`, abusing this capability to become the root user. While not a traditional SUID bit, exploiting `cap_setuid` is a direct abuse of a system's elevation control mechanism and falls under this technique.

View but not quite complete

about

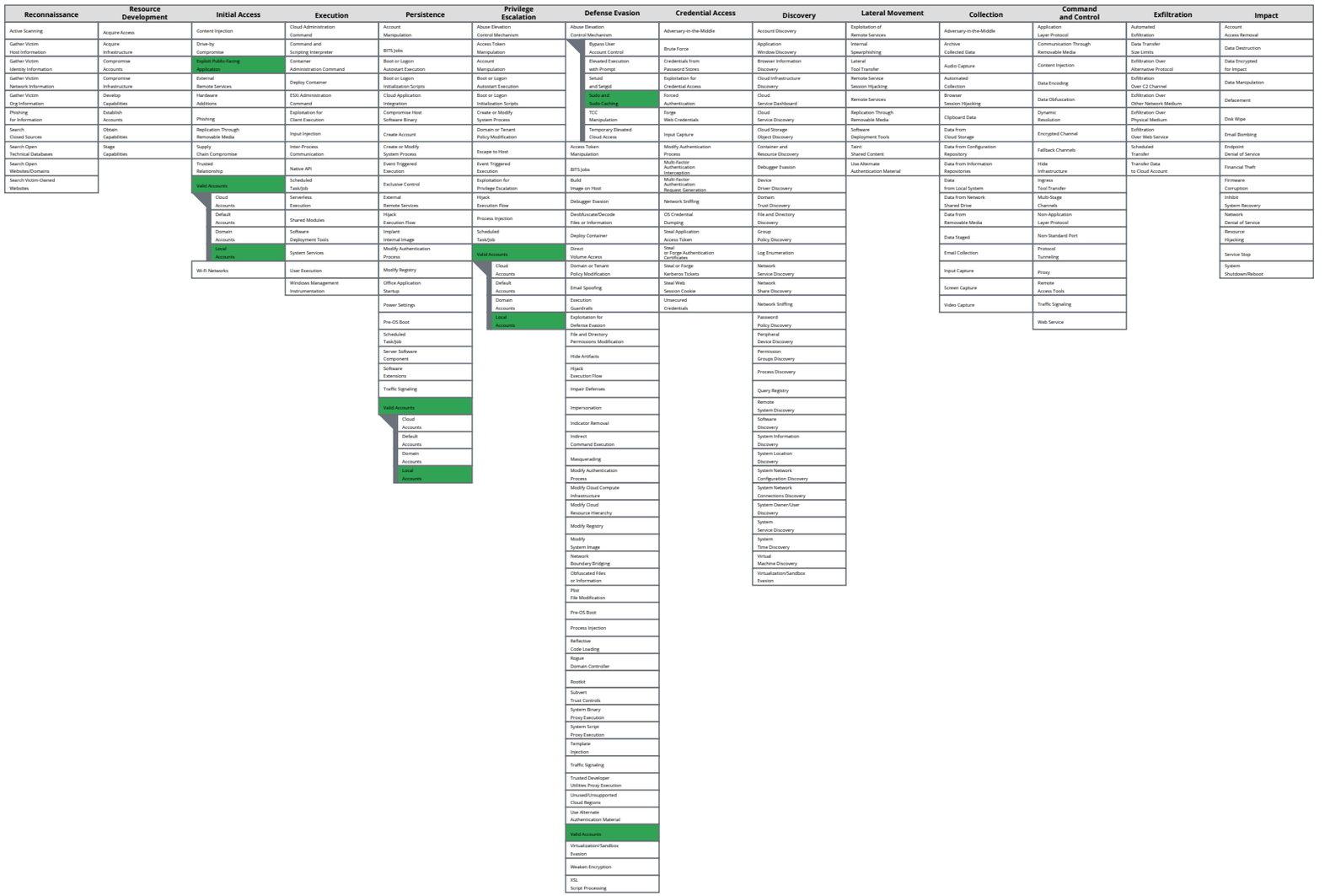
layer

domain

Enterprise ATT&CK v17

platforms

Windows, Linux, macOS, Network Devices, ESXi, PRE, Containers, IaaS, SaaS, Office Suite, Identity Provider



Correct View

about

HackTheBox-Cap

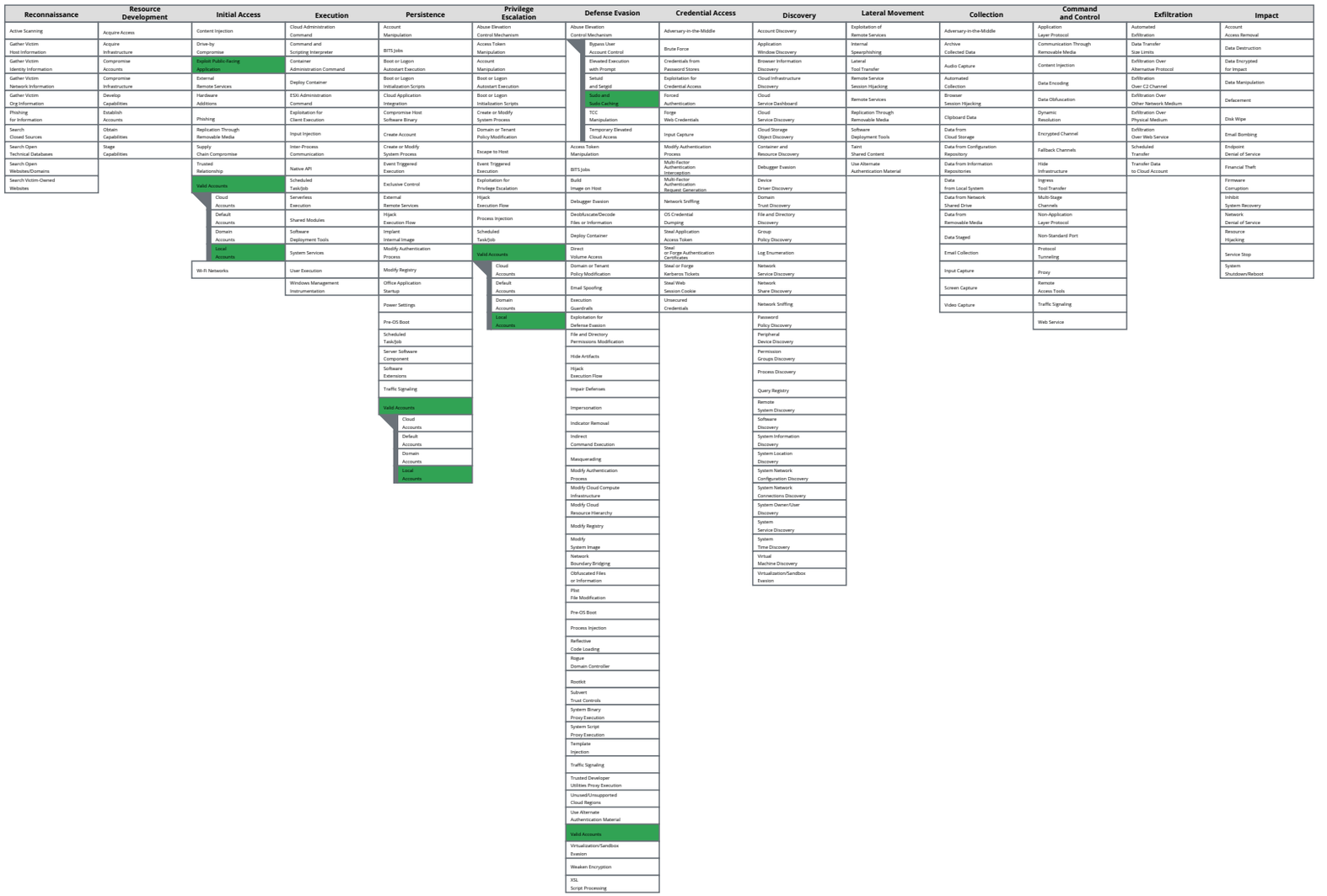
IDOR, Exploiting Linux capabilities

domain

Enterprise ATT&CK v17

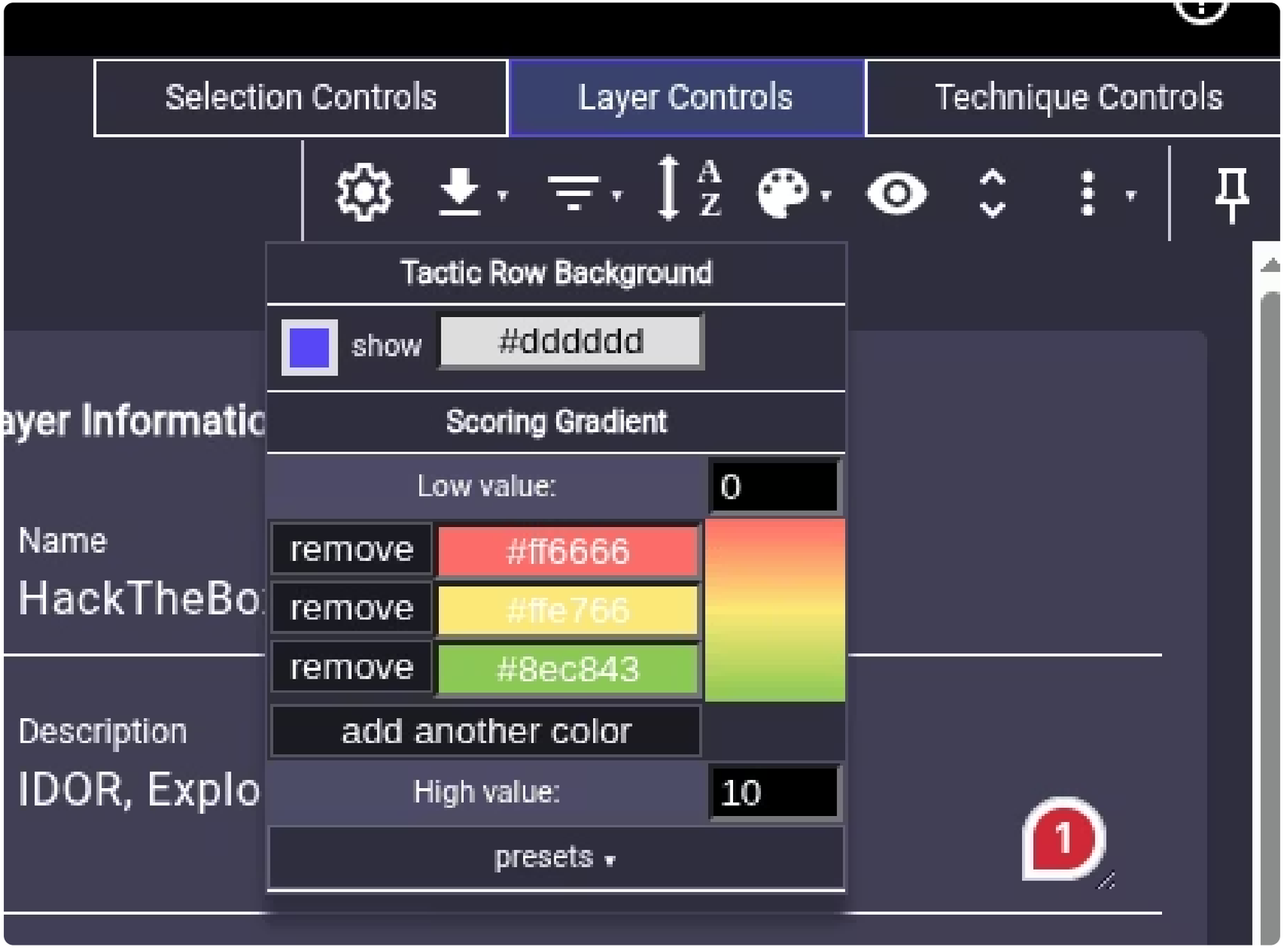
platforms

Windows, Linux, macOS, Network Devices, ESXi, PRE, Containers, IaaS, SaaS, Office Suite, Identity Provider



What now?

You must complete setting the min and max threat levels of 0 to 10



Setting the score

Select a technique and then click on `Technique Controls` Click on `Scoring` and enter in a score based on the calculated score