

# 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

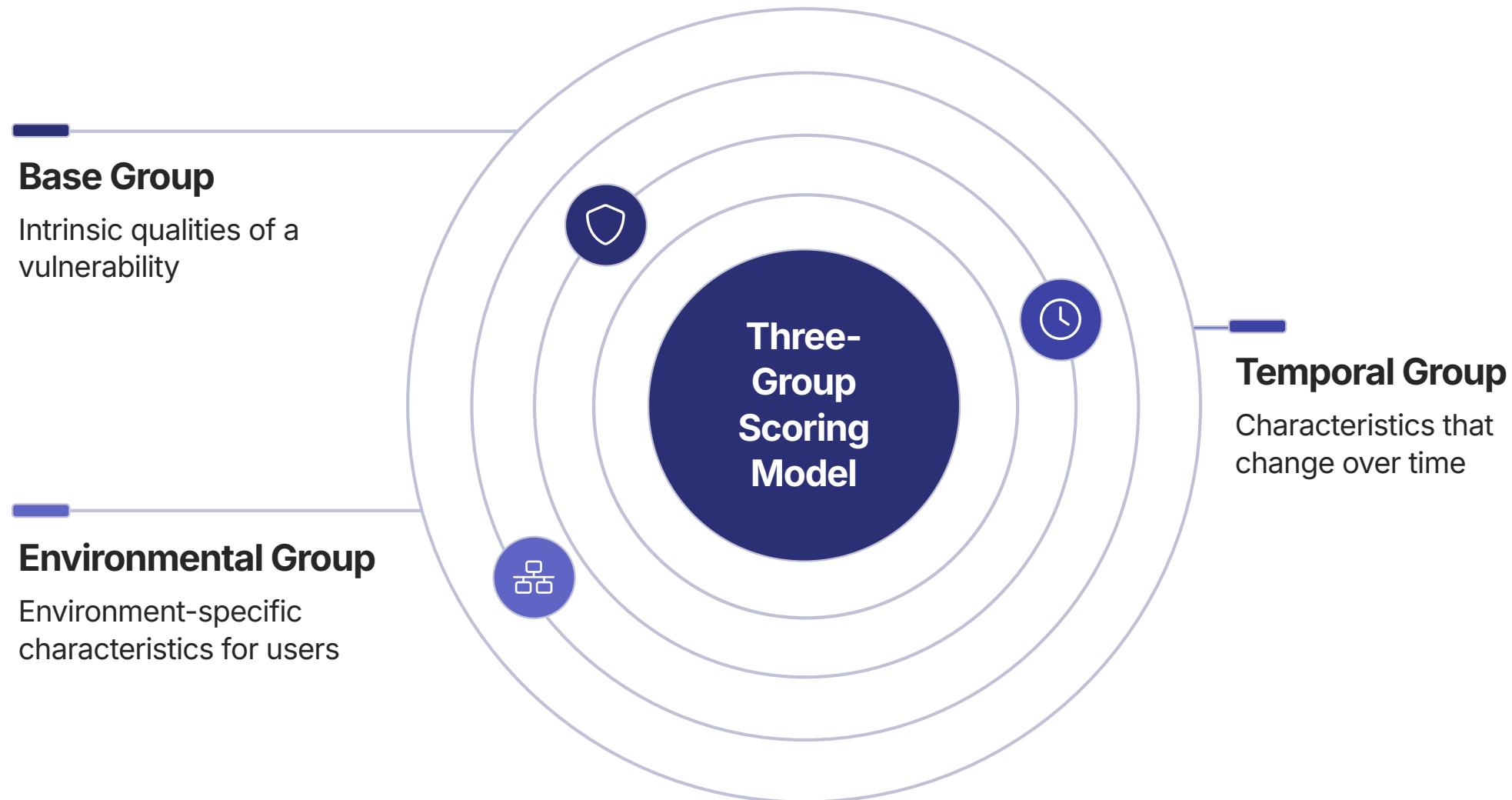
---

### 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 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...



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)

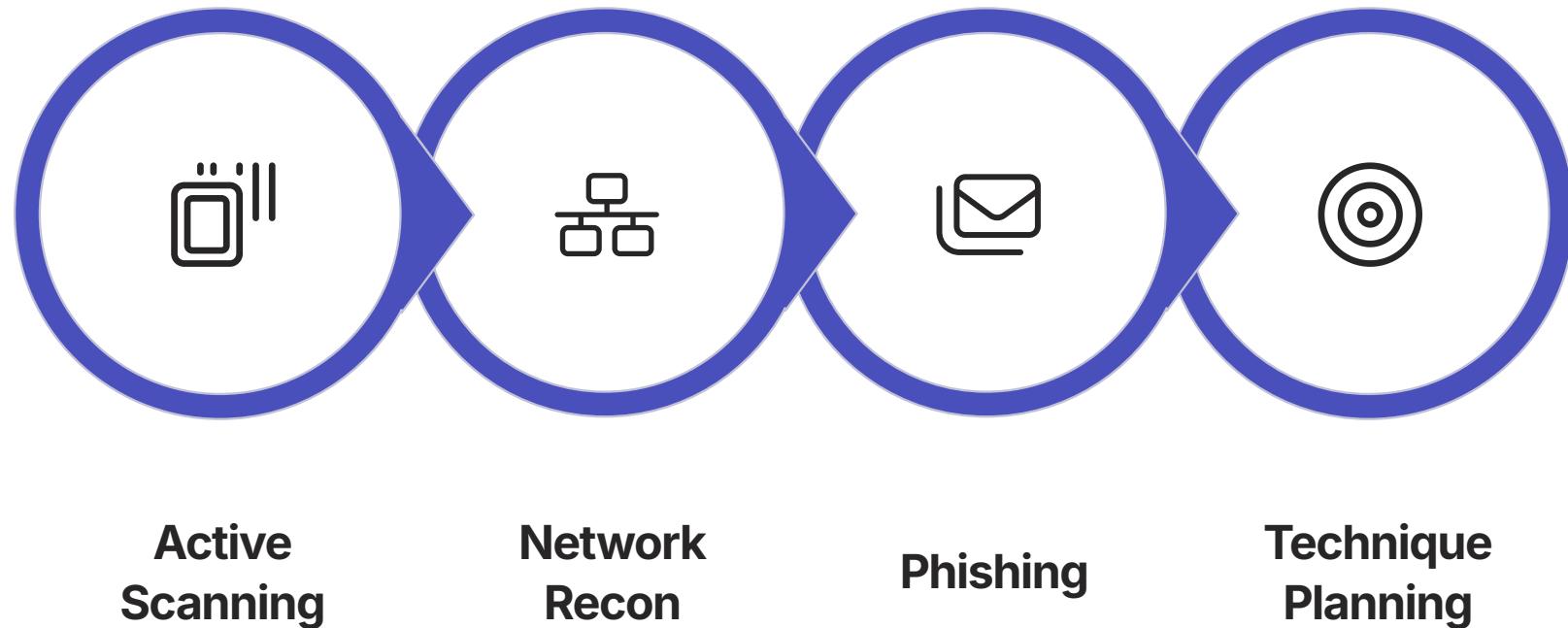
Partial (A:P)

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

The screenshot shows a user interface for managing attack layers. At the top left is a red icon with a white ampersand (&) and the URL "mitre-attack.github.io". To the right is a blue square icon with a white diagonal line. Below this is a dark navigation bar with the following elements:

- "Create New Layer" on the left.
- "Create a new empty layer" in the center.
- A small upward-pointing arrow icon on the right side of the bar.
- Three tabs at the bottom: "Enterprise ATT&CK", "Mobile ATT&CK", and "ICS ATT&CK".

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.

## T1552.001: Unsecured Credentials - Credentials in Files

By exploiting the IDOR, the attacker downloaded a packet capture file. Analyzing this file revealed plaintext FTP credentials (nathan / Buck3tH4TFORM3!).

## 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

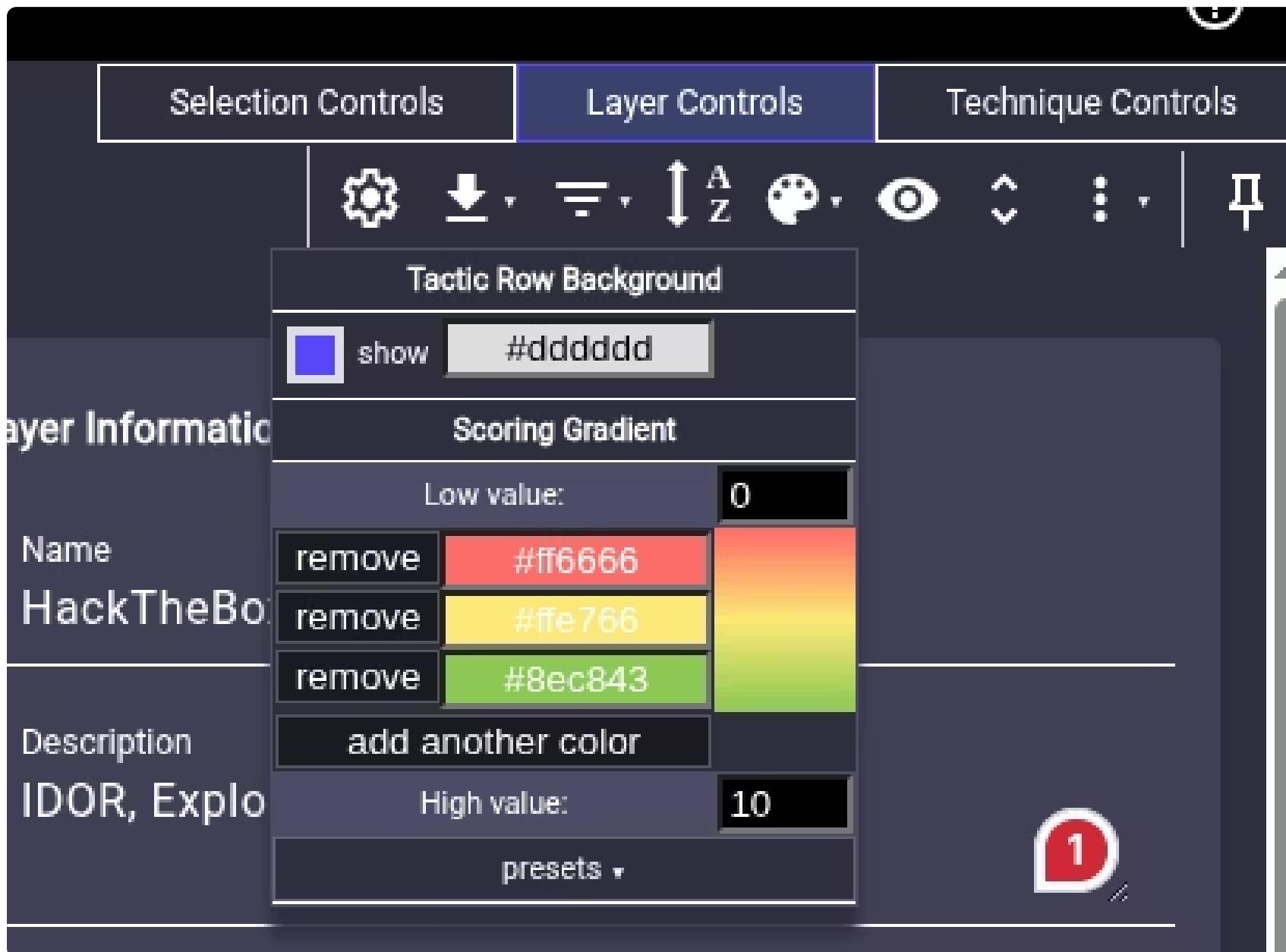
about		layer		domain		Enterprise ATT&CK v17		platforms					
Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Active Scanning	Acquire Access	Content Injection	Cloud Infrastructure	Account Manipulation	Abuse Mechanism	Adversary-in-the-Middle	Account Discovery	Replication of Remote Services	Adversary-in-the-Middle	Adaptation Layer Protocol	Adversary	Access Removal	
Gather Victim Host Information	Acquire Infrastructure	Drive-by Compromise	Command and Scripting Interpreter	Access Token Manipulation	Brute Force	Application Internal Spoofing	Windows Discovery	Communication Through Removable Media	Data Transfer	Archive Collected Data	Data Transfer	Data Decimation	
Gather Victim Identity Information	Compromise Accounts	Delivery Platform Application	Administrator Command	Boot or Logon Automation	Credentials from Password Stores	Browser Information Disclosure	Device Discovery	File Transfer	File Transfer	File Transfer over Alternative Protocol	File Transfer	Data Encrypted for Impact	
Gather Victim Network Information	Compromise Infrastructure	External Remote Services	Deploy Container	Boot or Logon Installation Scripts	SelfSigned and Signed	Exploitation for Credential Access	Cloud Infrastructure Discovery	Remote Service Collection	Automated Data Encoding	Data Exfiltration Over C2 Channel	Data Manipulation		
Gather Victim Org Information	Delivery Capabilities	Internal Remote Services	EDS Administration	Cloud Infrastructure Installation Scripts	Forge TCC Manipulation	Forge Web Credentials	Cloud Service Discovery	Session Hijacking	Blind Denial of Service	Session Hijacking	Session Hijacking	Defacement	
Phishing for Information	Establish Accounts	Phishing	Exploitation for Client Execution	Compromised Host Software Library	Input Injection	Input Capture	Cloud Object Discovery	Replication Through Removable Media	DYNAMIC Resolution	Clipboard Data Removal	Exfiltration Over Physical Medium	Disk Wipe	
Find Closed Sources	Obtain Capabilities	Redteam Through Removable Media	Internal Process	Create Account	Device-Based Policy Modification	Cloud Shared Object Discovery	Container and Resource Discovery	Data from Cloud Storage	Data from Encrypted Channel	Endpoint Transfer	Email Bombing		
Search Open Technical Databases	Stage Capabilities	Supply Chain Compromise	Inter-Process Communication	Create or Modify System Process	Finance to Host Manipulation	Cloud Deployment Tools	Taint Shared Content	Data from Configuration Repository	Fallback Channels	Scheduled Transfer	Endpoint Denial of Service		
Discover WellKnown Domains	Establish Relationship	Native API	Event Triggered Execution	Event Triggered Execution	BITS jobs	Cloud Debugger Evasion	Device Authentication Infrastructure	Data from Shared Information Repositories	Data Staged	Hide Infrastructure	Transmit Data to Cloud Account	Financial Theft	
Search Victim-Owned Websites	Valid Accounts	Scheduled TaskJobs	Exclusive Control	Exploitation for Privilege Escalation	Build Image on Host	Device Driver Discovery	Device Driver Discovery	Data Ingress	Data Ingestion	Ingress from Local System	Total Transfer	Firmware Corruption	
	Cloud Accounts	External Remote Services	External	Exploit for Privilege Escalation	Image on Host	Driver Sniffing	Driver Trust Discovery	Data Ingestion	Data Ingestion	Driver Malicious Channels	Malicious Driver	Network Recovery	
	Default Accounts	File Execution	File	Execution Flow	Image on Host	Fileless Sniffing	Fileless Trust Discovery	Data Ingestion	Data Ingestion	Fileless Malicious Channels	Malicious Fileless	Denial of Service	
	Shared Modules	Hijack Execution Flow	Fileless	Desfuscate/Decode Files or Information	OS Credential Dumping	Fileless Deployment	Fileless Drift	Data from Non-Application Removable Media	Data from Non-Standard Port	Fileless Protocol	Protocol Tunneling	Service Stop	
	Custom Accounts	Impersonate	Fileless	Deployment	Fileless Exploitation	Fileless Persistence	Fileless Policy Discovery	Data from Non-Standard Port	Email Collection	Fileless Registry	Protocol Tunneling	System Shutdown/Reboot	
	System Accounts	Internal Image	Fileless	Deploy Container	Fileless Access Token	Fileless Shared Cache	Fileless Share Discovery	Input Capture	Input Capture	Fileless Service Discovery	Protocol Tunneling		
	Local Accounts	TaskJobs	Fileless	Direct Access	Fileless Shared Cache	Fileless Service Discovery	Fileless Share Discovery	Screen Capture	Screen Capture	Fileless System Discovery	Protocol Tunneling		
	System Services	Modify Authentication Process	Fileless	Direct Access	Fileless Shared Cache	Fileless Service Discovery	Fileless Share Discovery	Video Capture	Video Capture	Fileless System Discovery	Protocol Tunneling		
	Wi-Fi Networks	User Execution	Fileless	Forge Registry	Fileless Shared Cache	Fileless Service Discovery	Fileless Share Discovery	Web Service	Web Service	Fileless System Discovery	Protocol Tunneling		
	Windows Management	Office Application	Fileless	Fileless Shared Cache	Fileless Shared Cache	Fileless Service Discovery	Fileless Share Discovery						
	Instrumentation	Startups	Fileless	Fileless Shared Cache	Fileless Shared Cache	Fileless Service Discovery	Fileless Share Discovery						
			Power Settings	Fileless Shared Cache	Fileless Shared Cache	Fileless Service Discovery	Fileless Share Discovery						
				Pre-OS Boot	Fileless Shared Cache	Fileless Service Discovery	Fileless Share Discovery						
				Scheduled TaskJobs	File and Directory Permissions Modification	Fileless Service Discovery	Fileless Share Discovery						
				Server Software Components	Fileless Shared Cache	Fileless Service Discovery	Fileless Share Discovery						
				Software Extensions	Fileless Shared Cache	Fileless Service Discovery	Fileless Share Discovery						
				Traffic Signaling	Fileless Shared Cache	Fileless Service Discovery	Fileless Share Discovery						
				Valid Accounts	Fileless Shared Cache	Fileless Service Discovery	Fileless Share Discovery						
				Cloud Accounts	Fileless Shared Cache	Fileless Service Discovery	Fileless Share Discovery						
				Default Accounts	Fileless Shared Cache	Fileless Service Discovery	Fileless Share Discovery						
				Delegated Accounts	Fileless Shared Cache	Fileless Service Discovery	Fileless Share Discovery						
				Domain Accounts	Fileless Shared Cache	Fileless Service Discovery	Fileless Share Discovery						
				Local Accounts	Fileless Shared Cache	Fileless Service Discovery	Fileless Share Discovery						
				Local Accounts	Fileless Shared Cache	Fileless Service Discovery	Fileless Share Discovery						
				Pre-OS Boot	Fileless Shared Cache	Fileless Service Discovery	Fileless Share Discovery						
				Process Injection	Fileless Shared Cache	Fileless Service Discovery	Fileless Share Discovery						
				Reflection	Fileless Shared Cache	Fileless Service Discovery	Fileless Share Discovery						
				Code Loading	Fileless Shared Cache	Fileless Service Discovery	Fileless Share Discovery						
				Impersonation	Fileless Shared Cache	Fileless Service Discovery	Fileless Share Discovery						
				Indicator Removal	Fileless Shared Cache	Fileless Service Discovery	Fileless Share Discovery						
				Indirect Command Execution	Fileless Shared Cache	Fileless Service Discovery	Fileless Share Discovery						
				Masquerading	Fileless Shared Cache	Fileless Service Discovery	Fileless Share Discovery						
				Modify Authentication Process	Fileless Shared Cache	Fileless Service Discovery	Fileless Share Discovery						
				Modify Cloud Compute Infrastructure	Fileless Shared Cache	Fileless Service Discovery	Fileless Share Discovery						
				Modify Cloud Resource Hierarchy	Fileless Shared Cache	Fileless Service Discovery	Fileless Share Discovery						
				Modify Registry	Fileless Shared Cache	Fileless Service Discovery	Fileless Share Discovery						
				Modify System Image	Fileless Shared Cache	Fileless Service Discovery	Fileless Share Discovery						
				Network	Fileless Shared Cache	Fileless Service Discovery	Fileless Share Discovery						
				Boundary Bridging	Fileless Shared Cache	Fileless Service Discovery	Fileless Share Discovery						
				Obliterate Files or Information	Fileless Shared Cache	Fileless Service Discovery	Fileless Share Discovery						
				Plan for Modification	Fileless Shared Cache	Fileless Service Discovery	Fileless Share Discovery						
				Pre-OS Boot	Fileless Shared Cache	Fileless Service Discovery	Fileless Share Discovery						
				Process Injection	Fileless Shared Cache	Fileless Service Discovery	Fileless Share Discovery						
				Reflection	Fileless Shared Cache	Fileless Service Discovery	Fileless Share Discovery						
				Code Loading	Fileless Shared Cache	Fileless Service Discovery	Fileless Share Discovery						
				Impersonation	Fileless Shared Cache	Fileless Service Discovery	Fileless Share Discovery						
				Indicator Removal	Fileless Shared Cache	Fileless Service Discovery	Fileless Share Discovery						
				Indirect Command Execution	Fileless Shared Cache	Fileless Service Discovery	Fileless Share Discovery						
				Masquerading	Fileless Shared Cache	Fileless Service Discovery	Fileless Share Discovery						
				Modify Authentication Material	Fileless Shared Cache	Fileless Service Discovery	Fileless Share Discovery						
				Valid Accounts	Fileless Shared Cache	Fileless Service Discovery	Fileless Share Discovery						
				Virtualization/Sandbox	Fileless Shared Cache	Fileless Service Discovery	Fileless Share Discovery						
				Duration	Fileless Shared Cache	Fileless Service Discovery	Fileless Share Discovery						
				Weaken Encryption	Fileless Shared Cache	Fileless Service Discovery	Fileless Share Discovery						
				XSL Script Processing	Fileless Shared Cache	Fileless Service Discovery	Fileless Share Discovery						

# Correct View

about		domain		platforms	
HackTheBox-Cap		Enterprise ATT&CK v17		Windows, Linux, macOS, Network Devices, ESXi, PRE, Containers, IaaS, SaaS, Office Suite, Identity Provider	
IDOR, Exploiting Linux capabilities					
Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation
Active Scanning	Acquire Access	Content Injection	Command Manipulation	Abuse Mechanism	Control Mechanism
Gather Victim Host Information	Acquire Infrastructure	Drive-by Compromise	Command and Scripting Interpreter	Access Token Manipulation	Brute Force
Gathering Identity Information	Compromise Accounts	Deployment/Building Application	BITS Jobs	Administrator Control	Application Internal Spoofing
Gather Victim Network Information	Compromise Infrastructure	Deployment	Boot or Logon	Credentials from Password Stores	Binary Execution With Privileges
Gather Victim Org Information	External Remote Services	Deploy Container	Boot or Logon	Discovery	Code Execution
Gathering User Capabilities	Internal Remote Services	Deploy Container	Boot or Logon	Exploit for Credential Access	Command and Control
Phishing for Information	Establish Accounts	External Remote Services	Boot or Logon	Discovery	Collection
Reading Closed Sources	Obtain Capabilities	External Remote Services	BITS Administration	Exploit for Credential Access	Lateral Movement
Search Open Technical Databases	Stage Capabilities	Internal Remote Services	Cloud Automation	Session Hijacking	Command and Control
Review WellKnown Domains	Threat Relationship	Native API	Cloud Automation	Remote Services	Exfiltration
Search Victim-Owned Websites	Valid Accounts	Scheduled TaskJobs	Cloud Automation	Service Dashboard	Impact
		Cloud Accounts	Cloud Automation	Session Hijacking	Aircraft Access Removal
		Default Execution	Cloud Automation	Service Discovery	Administrated Elevation
		Shared Modules	Execution Flow	Cloud Object Discovery	Data Transfer Through Removable Media
		Dynamic Accounts	Deschedule/Decode	Cloud Deployment Tools	Archive Collected Data
		Software Deployment Tools	File or Information	Container and Resource Discovery	Removable Media
		Local Accounts	Scheduled TaskJobs	Container Shared Content	Temporary Power
		System Services	Modify Authentication	Debugger Evasion	Alternative Protocol for Impact
		Wi-Fi Networks	Cloud Accounts	Device Authentication Interception	Exfiltration Over C2 Channel
		User Execution	Cloud Accounts	Driver Discovery	Data Encoding Collection
		Windows Management	Cloud Accounts	Driver Sniffing	Delivery Through Other C2 Channel
		Instrumentation	Cloud Accounts	File System Discovery	Delivery Through Physical Medium
			Default Accounts	Driver Sniffing	Dynamic Replication Over Removable Media
			Dynamic Accounts	File System Discovery	Exfiltration Over Physical Medium
			Local Accounts	Driver Sniffing	Disk Wipe
			Local Accounts	File System Discovery	Endpoint Resolution
			Local Accounts	File System Discovery	Endpoint Transfer
			Local Accounts	File System Discovery	Endpoint Denial of Service
			Local Accounts	File System Discovery	Endpoint Hijacking
			Local Accounts	File System Discovery	Financial Theft
			Local Accounts	File System Discovery	Firmware Corruption
			Local Accounts	File System Discovery	Fileless
			Local Accounts	File System Discovery	Network Recovery
			Local Accounts	File System Discovery	Network Denial of Service
			Local Accounts	File System Discovery	Network Hijacking
			Local Accounts	File System Discovery	Protocol Tunneling
			Local Accounts	File System Discovery	Service Stop
			Local Accounts	File System Discovery	System Shutdown/Reboot
			Local Accounts	File System Discovery	Web Service

# 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

