

Contenidos



Marco teórico

01

- Ransomware y APT
- Framework Mitre ATT&CK
- Controles CIS y CIS Benchmarks
- Ansible Lockdown

Grupo Lazarus

02

- Introducción
- Matriz con sus TTP

Procedimiento

03

- Mapeo de TTPs a CIS
- Selección de CIS Benchmark
- Selección de recomendaciones
- Construcción del script
- Ejecución del script y auditoría



Marco teórico

Ransomware y APT

Ransomware

“El ***ransomware*** es un tipo de *malware* que toma por completo el control del equipo bloqueando o cifrando la información del usuario para, a continuación, pedir dinero a cambio de liberar o descifrar los ficheros del dispositivo.” - [INCIBE]



Entonces... ¿Por qué grupos ransomware y no APTs?

- *Es una definición más frecuente*
- *Los ataques estudiados se caracterizan por el uso de ransomware*

Amenaza persistente avanzada (APT)

- Es un ciberataque dirigido y prolongado
- Conocimientos y técnicas de alto nivel
- Cinco etapas:
 1. Acceso
 2. Mantener la posición
 3. Escalado de privilegios
 4. Movimiento lateral
 5. Exfiltración

Framework MITTRE ATT&CK®

Definición

El framework **MITRE ATT&CK®** es una base de conocimiento, globalmente accesible, que contiene las tácticas y técnicas utilizadas por los ciberdelincuentes durante todo el ciclo de vida del ciberataque.

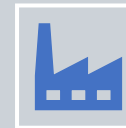
Tipos de matrices



Enterprise: Contiene información relacionada con los entornos corporativos.



Mobile: Abarca las técnicas que involucran dispositivos móviles. Por un lado, el acceso a dispositivos, y por otro, los efectos originados en la red que pueden ser utilizados por los adversarios sin acceso a dispositivos.



ICS: Hace referencia a las siglas de “Industrial Control Systems”. Contiene información para identificar, definir y combatir ataques cibernéticos en redes OT, es decir, está enfocada en los entornos industriales.

Framework MITTRE ATT&CK®

¿Qué contiene una matriz?

Todas las matrices están formadas por sus tácticas, técnicas y procedimientos, **TTPs** para abreviar.

El nombre de cada columna de la matriz conforma la táctica; con un total de catorce, mientras que las técnicas y sub-técnicas se encuentran bajo el nombre de la columna a la que pertenecen e identificadas con su nombre o ID.

TTP

- **Táctica:** Representa el “por qué” el atacante lleva a cabo una acción.
- **Técnica:** Representa “cómo” un atacante alcanza la táctica que tiene como objetivo.
- **Procedimiento:** Describe la acción específica que ha llevado a cabo el atacante de una técnica para lograr una táctica.

Ejemplo: “El atacante ha empleado en comando `nmap -sn 192.168.1.0/24` para escanear las direcciones IP de la red y, así, obtener información.”

Framework MITTRE ATT&CK®

Reconnaissance 10 techniques	Resource Development 8 techniques	Initial Access 10 techniques	Execution 14 techniques	Persistence 20 techniques	Privilege Escalation 14 techniques	Defense Evasion 43 techniques	Credential Access 17 techniques	Discovery 32 techniques	Lateral Movement 9 techniques	Collection 17 techniques	Command and Control 17 techniques	Exfiltration 9 techniques	Impact 14 techniques
<div>Active Scanning (0/3)</div> <div>Gather Victim Host Information (0/4)</div> <div>Gather Victim Identity Information (0/3)</div> <div>Gather Victim Network Information (0/6)</div> <div>Gather Victim Org Information (0/4)</div> <div>Phishing for Information (0/4)</div> <div>Search Closed Sources (0/2)</div> <div>Search Open Technical Databases (0/5)</div> <div>Search Open Websites/Domains (0/3)</div> <div>Search Victim-Owned Websites</div>	<div>Acquire Access</div> <div>Acquire Infrastructure (0/8)</div> <div>Compromise Accounts (0/3)</div> <div>Compromise Infrastructure (0/7)</div> <div>Develop Capabilities (0/4)</div> <div>Establish Accounts (0/3)</div> <div>Obtain Capabilities (0/6)</div> <div>Stage Capabilities (0/6)</div>	<div>Content Injection</div> <div>Drive-by Compromise</div> <div>Exploit Public-Facing Application</div> <div>External Remote Services</div> <div>Hardware Additions</div> <div>Phishing (4/4)</div> <div>Replication Through Removable Media</div> <div>Supply Chain Compromise (0/3)</div> <div>Trusted Relationship</div> <div>Valid Accounts (0/4)</div>	<div>Cloud Administration Command</div> <div>Command and Scripting Interpreter (0/9)</div> <div>Container Administration Command</div> <div>Deploy Container</div> <div>Exploitation for Client Execution</div> <div>Inter-Process Communication (0/3)</div> <div>Native API</div> <div>Scheduled Task/Job (0/5)</div> <div>Serverless Execution</div> <div>Shared Modules</div> <div>Software Deployment Tools</div> <div>System Services (0/2)</div> <div>User Execution (0/3)</div> <div>Windows Management Instrumentation</div>	<div>Account Manipulation (0/6)</div> <div>BITS Jobs</div> <div>Boot or Logon Autostart Execution (0/14)</div> <div>Boot or Logon Initialization Scripts (0/5)</div> <div>Browser Extensions</div> <div>Compromise Client Software Binary</div> <div>Create Account (0/3)</div> <div>Create or Modify System Process (0/4)</div> <div>Event Triggered Execution (0/16)</div> <div>External Remote Services</div> <div>Hijack Execution Flow (0/12)</div> <div>Implant Internal Image</div> <div>Modify Authentication Process (0/8)</div> <div>Office Application Startup (0/6)</div> <div>Power Settings</div> <div>Pre-OS Boot (0/5)</div>	<div>Abuse Elevation Control Mechanism (0/5)</div> <div>Access Token Manipulation (0/5)</div> <div>Account Manipulation (0/6)</div> <div>Boot or Logon Autostart</div> <div>Browser Extensions (T1176)</div> <div>pin/unpin tooltip initialization select</div> <div>add to selection</div> <div>remove from selection</div> <div>select all</div> <div>deselect all</div> <div>invert selection</div> <div>select annotated</div> <div>select unannotated</div> <div>select all techniques in tactic</div> <div>deselect all techniques in tactic</div> <div>view technique</div> <div>view tactic</div> <div>Process Injection (0/12)</div> <div>Scheduled Task/Job (0/5)</div> <div>Valid Accounts (0/4)</div>	<div>Abuse Elevation Control Mechanism (0/5)</div> <div>Access Token Manipulation (0/5)</div> <div>BITS Jobs</div> <div>Build Image on Host</div> <div>Debugger Evasion</div> <div>Decode/Encode Files or Information</div> <div>Deploy Container</div> <div>Direct Volume Access</div> <div>Domain Policy Modification (0/2)</div> <div>Execution Guardrails (0/1)</div> <div>Exploitation for Defense Evasion</div> <div>File and Directory Permissions Modification (0/2)</div> <div>Hide Artifacts (0/11)</div> <div>Hijack Execution Flow (0/12)</div> <div>Impair Defenses (0/11)</div> <div>Impersonation</div> <div>Indicator Removal (0/9)</div>	<div>Adversary-in-the-Middle (0/3)</div> <div>Brute Force (0/4)</div> <div>Credentials from Password Stores (0/6)</div> <div>Exploitation for Credential Access</div> <div>Forced Authentication</div> <div>Forge Web Credentials (0/2)</div> <div>Input Capture (0/4)</div> <div>Modify Authentication Process (0/8)</div> <div>Multi-Factor Authentication Interception</div> <div>Multi-Factor Authentication Request Generation</div> <div>Network Sniffing</div> <div>OS Credential Dumping (0/8)</div> <div>Steal Application Access Token</div> <div>Steal or Forge Authentication Certificates</div> <div>Steal or Forge Kerberos Tickets (0/4)</div>	<div>Account Discovery (0/4)</div> <div>Application Window Discovery</div> <div>Browser Information Discovery</div> <div>Cloud Infrastructure Discovery</div> <div>Cloud Service Dashboard</div> <div>Cloud Service Discovery</div> <div>Cloud Storage Object Discovery</div> <div>Container and Resource Discovery</div> <div>Debugger Evasion</div> <div>Device Driver Discovery</div> <div>Domain Trust Discovery</div> <div>File and Directory Discovery</div> <div>Group Policy Discovery</div> <div>Log Enumeration</div> <div>Network Service Discovery</div>	<div>Exploitation of Remote Services</div> <div>Internal Spearphishing</div> <div>Lateral Tool Transfer</div> <div>Remote Service Session Hijacking (0/2)</div> <div>Remote Services (0/8)</div> <div>Replication Through Removable Media</div> <div>Software Deployment Tools</div> <div>Taint Shared Content</div> <div>Use Alternate Authentication Material (0/4)</div>	<div>Adversary-in-the-Middle (0/3)</div> <div>Archive Collected Data (0/3)</div> <div>Audio Capture</div> <div>Automated Collection</div> <div>Browser Session Hijacking</div> <div>Clipboard Data</div> <div>Data from Cloud Storage</div> <div>Data from Configuration Repository (0/2)</div> <div>Data from Information Repositories (0/3)</div> <div>Data from Local System</div> <div>Data from Network Shared Drive</div> <div>Data from Removable Media</div> <div>Data Staged (0/2)</div> <div>Email Collection (0/3)</div> <div>Input Capture (0/4)</div> <div>Screen Capture</div>	<div>Application Layer Protocol (0/4)</div> <div>Communication Through Removable Media</div> <div>Content Injection</div> <div>Data Encoding (0/2)</div> <div>Data Obfuscation (0/3)</div> <div>Dynamic Resolution (0/3)</div> <div>Encrypted Channel (0/2)</div> <div>Fallback Channels</div> <div>Ingress Tool Transfer</div> <div>Multi-Stage Channels</div> <div>Non-Application Layer Protocol</div> <div>Non-Standard Port</div> <div>Protocol Tunneling</div> <div>Proxy (0/4)</div> <div>Remote Access Software</div> <div>Traffic Signaling (0/2)</div> <div>Web Service (0/3)</div>	<div>Automated Exfiltration (0/1)</div> <div>Data Transfer Size Limits</div> <div>Exfiltration Over Alternative Protocol (0/3)</div> <div>Exfiltration Over C2 Channel (0/2)</div> <div>Exfiltration Over Other Network Medium (0/1)</div> <div>Exfiltration Over Physical Medium (0/1)</div> <div>Exfiltration Over Web Service (0/4)</div> <div>Scheduled Transfer</div> <div>Transfer Data to Cloud Account</div>	<div>Account Access Removal</div> <div>Data Destruction</div> <div>Data Encrypted for Impact</div> <div>Data Manipulation (0/3)</div> <div>Defacement (0/2)</div> <div>Disk Wipe (0/2)</div> <div>Endpoint Denial of Service (0/4)</div> <div>Financial Theft</div> <div>Firmware Corruption</div> <div>Inhibit System Recovery</div> <div>Network Denial of Service (0/2)</div> <div>Resource Hijacking</div> <div>Service Stop</div> <div>System Shutdown/Reboot</div>

Spearphishing Attachment
Spearphishing Link
Spearphishing via Service
Spearphishing Voice

Sub-técnicas

Procedimiento

Tácticas

Técnicas

Controles CIS y CIS Benchmarks

Controles de Seguridad Críticos de CIS

Los Controles de Seguridad Críticos de CIS son un conjunto de acciones prioritarias que conforman una colección de mejores prácticas de defensa para mitigar los ataques más comunes a sistemas y redes.



CIS Benchmarks

Los CIS Benchmarks son un conjunto de mejores prácticas y directrices técnicas de hardening para una configuración segura de un sistema objetivo.



¿Qué es hardening?

El hardening o robustecimiento se refiere a práctica de fortalecer un sistema informático o una red con el fin de hacerlo más resistente a ataques, intrusiones y vulnerabilidades.

Ejemplo apartado CIS Benchmark

1.3.1 Ensure sudo is installed (Scored)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

sudo allows a permitted user to execute a command as the superuser or another user, as specified by the security policy. The invoking user's real (not effective) user ID is used to determine the user name with which to query the security policy.

Rationale:

sudo supports a plugin architecture for security policies and input/output logging. Third parties can develop and distribute their own policy and I/O logging plugins to work seamlessly with the sudo front end. The default security policy is sudoers, which is configured via the file /etc/sudoers.

The security policy determines what privileges, if any, a user has to run sudo. The policy may require that users authenticate themselves with a password or another authentication mechanism. If authentication is required, sudo will exit if the user's password is not entered within a configurable time limit. This limit is policy-specific.

Audit:

Verify that sudo is installed.

Run the following command and inspect the output to confirm that sudo is installed:

```
# dpkg -s sudo
```

OR

```
# dpkg -s sudo-ldap
```

Remediation:

Install sudo using the following command.

```
# apt install sudo
```

OR

```
# apt install sudo-ldap
```

References:

1. SUDO(8)
2. <http://www.sudo.ws/>

Notes:

Use the sudo-ldap package if you need LDAP support for sudoers.

CIS Controls:

Version 7

4.3 Ensure the Use of Dedicated Administrative Accounts

Ensure that all users with administrative account access use a dedicated or secondary account for elevated activities. This account should only be used for administrative activities and not internet browsing, email, or similar activities.

Ansible Lockdown

Introducción

Ansible Lockdown es una herramienta de código abierto que automatiza los procesos necesarios para cumplir con los controles de seguridad *CIS* o *STIG*, desarrollada y mantenida por la empresa “Lockdown Enterprise”.

Utiliza Ansible, por lo que cuenta con la estructura de *Playbooks* que están escritos en el lenguaje YAML.

```
1  ---
2  # If you would like a report at the end according to OpenSCAP as to the report results
3  # then you should set ubtu18cis_oscap_scan to true/yes.
4  # NOTE: This requires the python_xmltojson package on the control host.
5  ubtu18cis_oscap_scan: false
6  ubtu18cis_report_dir: /tmp
7
8  ubtu18cis_section1_patch: true
9  ubtu18cis_section2_patch: true
10 ubtu18cis_section3_patch: true
11 ubtu18cis_section4_patch: true
12 ubtu18cis_section5_patch: true
13 ubtu18cis_section6_patch: true
14
15 # System will reboot if false, can give better audit results
16 ubtu18_skip_reboot: True
17
18 ## Benchmark name used by auditing control role
19 # The audit variable found at the base
20 benchmark: UBUNTU18-CIS
21
22 ### Audit Binary is required on the remote host
23 setup_audit: false
24 # How to retrieve audit binary
25 # Options are copy or download - detailed settings at the bottom of this file
26 # you will need to access to either github or the file already downloaded
27 get_audit_binary_method: download
28
29 # how to get audit files onto host options
30 # options are git/copy/get_url other e.g. if you wish to run from already downloaded conf
31 audit_content: git
32
33 # enable audits to run - this runs the audit and get the latest content
34 run_audit: false
```

Encabezado de un archivo *main.yml* de Ansible Lockdown



Grupo Lazarus

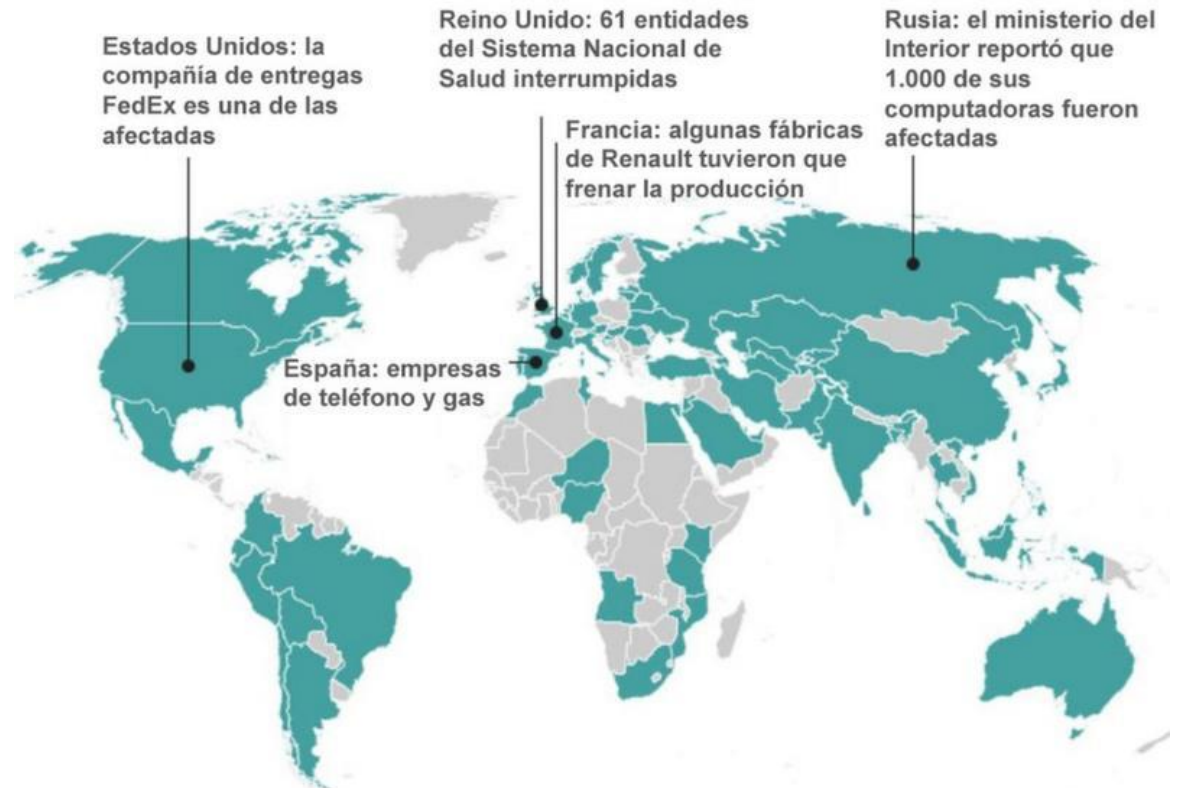
Introducción

¿Qué es el grupo Lazarus?

El Grupo Lazarus (también conocido como **HIDDEN COBRA** o Whois Team) es un conjunto de ciberdelincuentes norcoreano financiado por el gobierno. Se trata de una amenaza persistente avanzada (APT) debido a su nivel de amenaza y los múltiples métodos que utilizan para llevar a cabo una operación.

Llevan operando desde 2009 y han participado en numerosos ataques, varios de ellos enfocados en Corea del Sur, hasta el famoso ataque de WannaCry en 2017.

Países afectados en las primeras horas del ciberataque



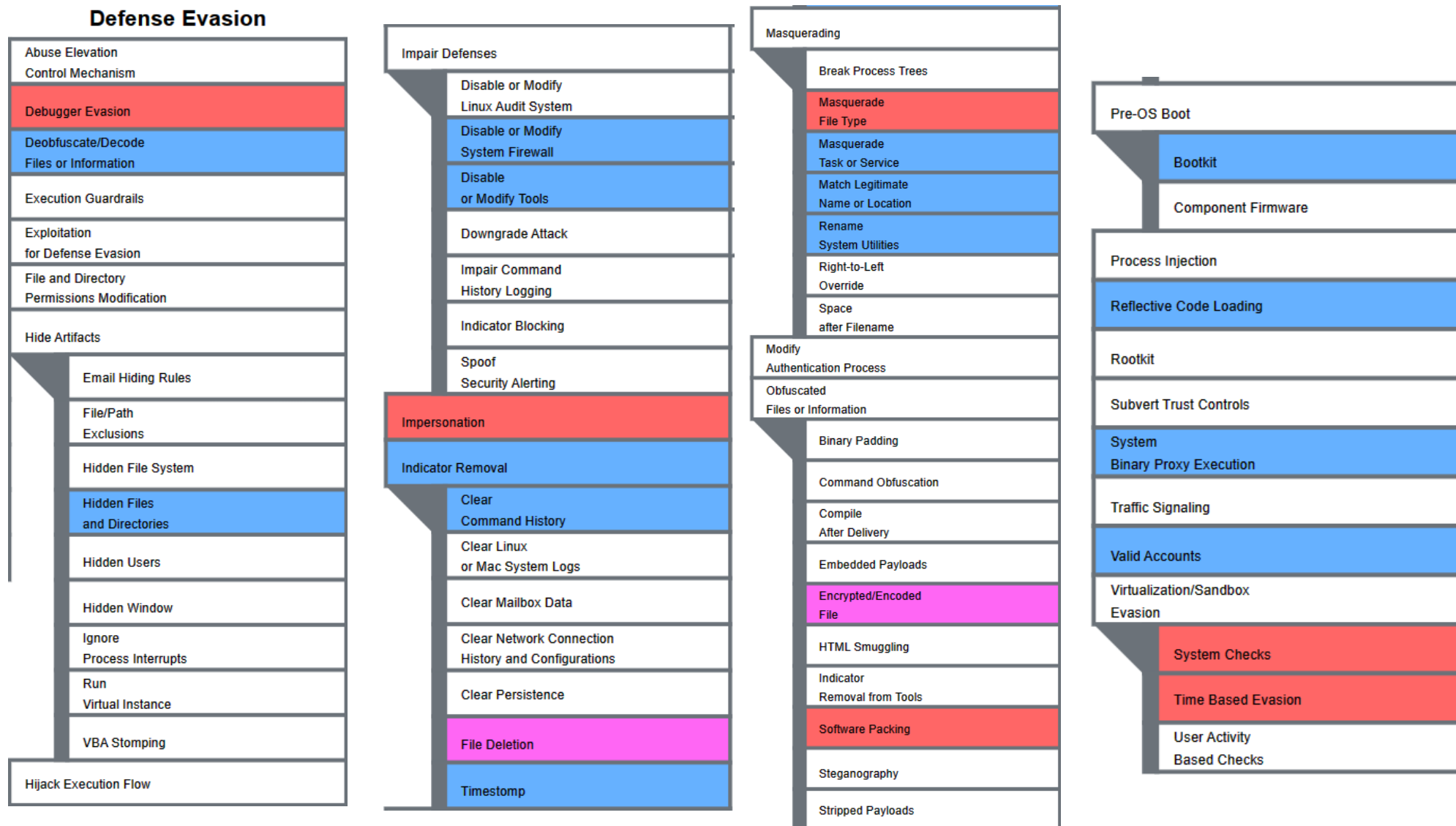
Fuente: Equipo de análisis e investigación global de Kaspersky



Matriz con sus TTPs - I

Initial Access	Execution	Persistence	Privilege Escalation
Content Injection	Command and Scripting Interpreter	Account Manipulation	Abuse Elevation Control Mechanism
Drive-by Compromise	JavaScript Python Unix Shell Visual Basic	Boot or Logon Autostart Execution	Account Manipulation
Exploit Public-Facing Application		Boot or Logon Initialization Scripts	Boot or Logon Autostart Execution
External Remote Services		Browser Extensions	Boot or Logon Initialization Scripts
Hardware Additions		Compromise Host Software Binary	Create or Modify System Process
Phishing	Exploitation for Client Execution	Create Account	Escape to Host
Spearphishing Attachment	Inter-Process Communication	Create or Modify System Process	Event Triggered Execution
Spearphishing Link	Native API	Event Triggered Execution	Exploitation for Privilege Escalation
Spearphishing via Service	Scheduled Task/Job	External Remote Services	Hijack Execution Flow
Spearphishing Voice	Shared Modules	Hijack Execution Flow	Process Injection
Supply Chain Compromise	Software Deployment Tools	Modify Authentication Process	Scheduled Task/Job
Trusted Relationship	System Services	Power Settings	Valid Accounts
Valid Accounts	User Execution	Pre-OS Boot	
	Malicious File	Bootkit	
	Malicious Link	Component Firmware	
		Scheduled Task/Job	
		Server Software Component	
		Traffic Signaling	
		Valid Accounts	

Matriz con sus TTPs - II



Matriz con sus TTPs - III

Credential Access	Discovery		Lateral Movement	Collection
Adversary-in-the-Middle	Account Discovery		Exploitation of Remote Services	Adversary-in-the-Middle
Brute Force	Domain Account		Internal Spearphishing	Archive Collected Data
Credential Stuffing	Local Account		Lateral Tool Transfer	Archive via Custom Method
Password Cracking	Application Window Discovery		Remote Service Session Hijacking	Archive via Library
Password Guessing	Browser Information Discovery		Remote Services	Archive via Utility
Password Spraying	Debugger Evasion		SSH	Audio Capture
Credentials from Password Stores	Device Driver Discovery	System Network Connections Discovery	VNC	Automated Collection
Exploitation for Credential Access	File and Directory Discovery	System Owner/User Discovery	Software Deployment Tools	Clipboard Data
Forge Web Credentials	Log Enumeration	System Service Discovery	Taint Shared Content	Data from Information Repositories
Input Capture	Network Service Discovery	System Time Discovery		Data from Local System
GUI Input Capture	Network Share Discovery	Virtualization/Sandbox Evasion		Data from Network Shared Drive
Keylogging	Network Sniffing	System Checks		Data from Removable Media
Web Portal Capture	Password Policy Discovery	Time Based Evasion		Data Staged
Modify Authentication Process	Peripheral Device Discovery	User Activity Based Checks		Local Data Staging
Multi-Factor Authentication Interception	Permission Groups Discovery			Remote Data Staging
Multi-Factor Authentication Request Generation	Process Discovery			Email Collection
Network Sniffing	Remote System Discovery			Input Capture
OS Credential Dumping	Software Discovery			GUI Input Capture
Steal or Forge Authentication Certificates	System Information Discovery			Keylogging
Steal or Forge Kerberos Tickets	System Location Discovery			Web Portal Capture
Steal Web Session Cookie	System Language Discovery			Screen Capture
Unsecured Credentials	System Network Configuration Discovery			Video Capture

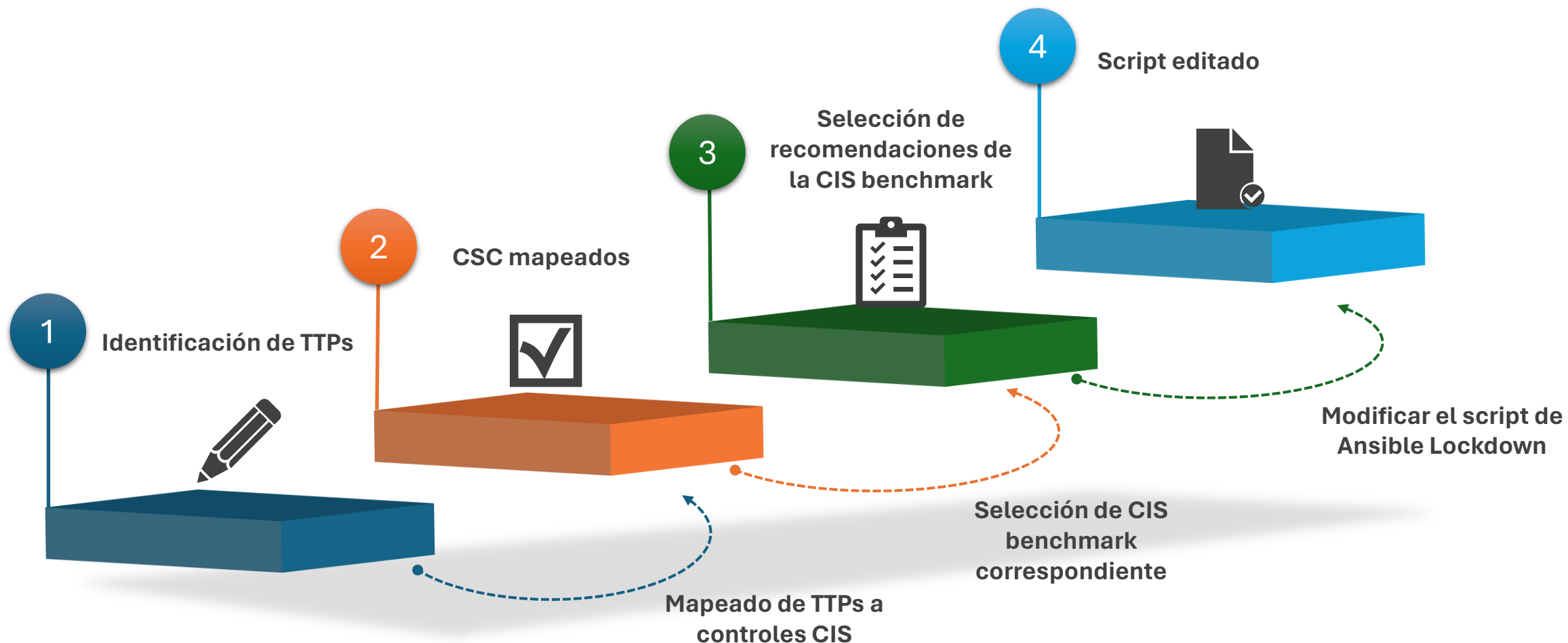
Matriz con sus TTPs - IV

Command and Control		Exfiltration		Impact	
Application Layer Protocol	Fallback Channels	Automated Exfiltration		Account Access Removal	
DNS	Hide Infrastructure	Data Transfer Size Limits		Data Destruction	
File Transfer Protocols	Ingress Tool Transfer	Exfiltration Over Alternative Protocol		Data Encrypted for Impact	
Mail Protocols	Multi-Stage Channels		Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Data Manipulation	
Web Protocols	Non-Application Layer Protocol		Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Defacement	
Communication Through Removable Media	Non-Standard Port		Exfiltration Over Unencrypted Non-C2 Protocol	External Defacement	
Content Injection	Protocol Tunneling	Exfiltration Over C2 Channel		Internal Defacement	
Data Encoding	Proxy	Exfiltration Over Other Network Medium		Disk Wipe	
Non-Standard Encoding	Domain Fronting	Exfiltration Over Physical Medium		Disk Content Wipe	
Standard Encoding	External Proxy	Exfiltration Over Web Service		Disk Structure Wipe	
Data Obfuscation	Internal Proxy		Exfiltration Over Webhook	Endpoint Denial of Service	
Junk Data	Multi-hop Proxy		Exfiltration to Cloud Storage	Financial Theft	
Protocol Impersonation	Remote Access Software		Exfiltration to Code Repository	Firmware Corruption	
Steganography	Traffic Signaling		Exfiltration to Text Storage Sites	Inhibit System Recovery	
Dynamic Resolution	Web Service	Scheduled Transfer		Network Denial of Service	
Encrypted Channel	Bidirectional Communication			Resource Hijacking	
Asymmetric Cryptography	Dead Drop Resolver			Service Stop	
Symmetric Cryptography	One-Way Communication			System Shutdown/Reboot	



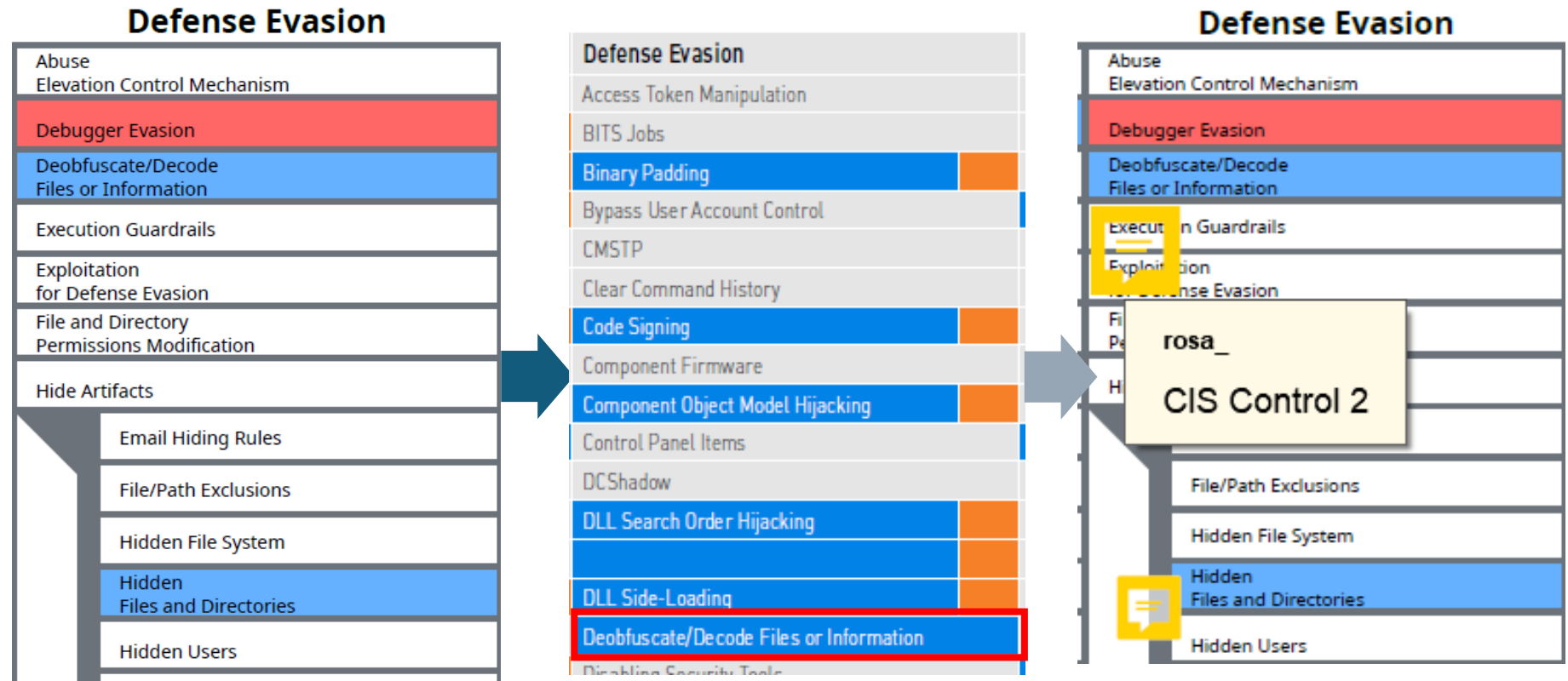
Procedimiento

Pasos del procedimiento



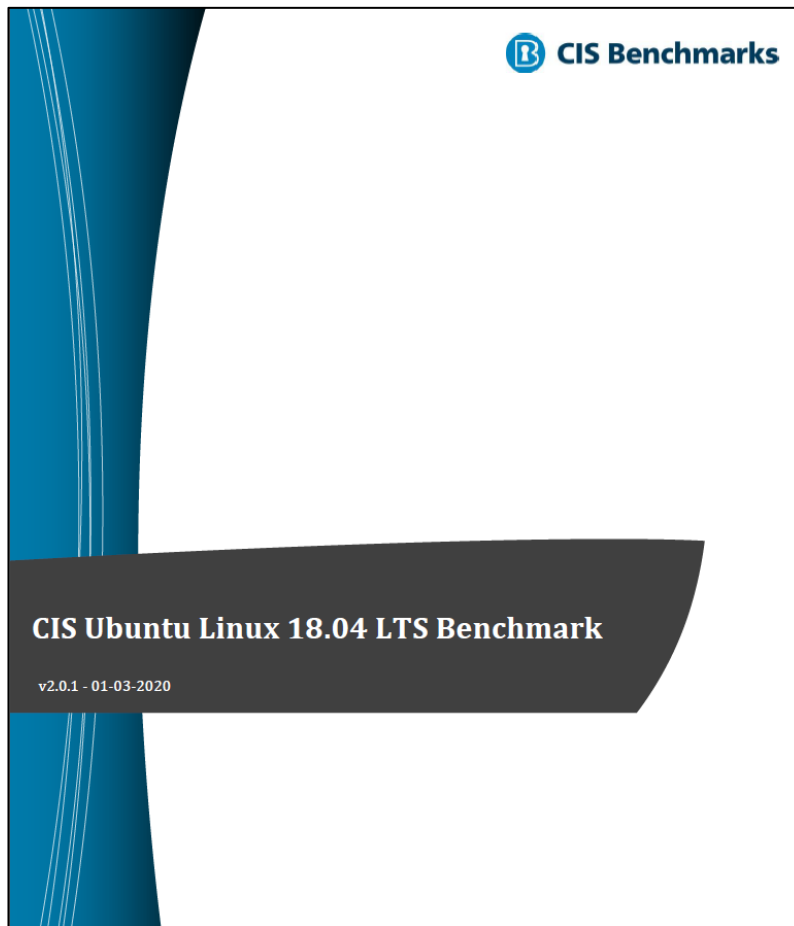
1. Mapeo de TTPs a CSC

Se mapean los TTPs del grupo Lazarus a los Controles CIS (CSC) 2-6 teniendo como referencia el mapeo realizado por Tripwire.



2. Selección de CIS Benchmark

Para este ejemplo he seleccionado la versión 2.0.1 del Benchmark “CIS Ubuntu Linux 18.04 LTS”.



También se selecciona el playbook de Ansible Lockdown correspondiente al que se le editará el script

CIS-Linux		
OS	Remediate	Audit
Amazon2	Amazon2-CIS	Amazon2-CIS-Audit
Amazon2023	Amazon2023-CIS	Amazon2023-CIS-Audit
DEBIAN11	DEBIAN11-CIS	DEBIAN11-CIS-Audit
DEBIAN12	In Development	In Development
RHEL7	RHEL7-CIS	RHEL7-CIS-Audit
RHEL8	RHEL8-CIS	RHEL8-CIS-Audit
RHEL9	RHEL9-CIS	RHEL9-CIS-Audit
UBUNTU18	UBUNTU18-CIS	UBUNTU18-CIS-Audit
UBUNTU20	UBUNTU20-CIS	UBUNTU20-CIS-Audit
UBUNTU22	UBUNTU22-CIS	UBUNTU22-CIS-Audit

3. Selección de recomendaciones

4.1.7 Ensure login and logout events are collected (Scored)

Remediation:

Edit or create a file in the `/etc/audit/rules.d/` directory ending in `.rules`

Example: `vi /etc/audit/rules.d/logins.rules`

and add the following lines:

```
-w /var/log/faillog -p wa -k logins  
-w /var/log/lastlog -p wa -k logins  
-w /var/log/tallylog -p wa -k logins
```

Notes:

Reloading the auditd config to set active settings requires the auditd service to be restarted, and may require a system reboot.

CIS Controls:

Version 7

4.9 Log and Alert on Unsuccessful Administrative Account Login

Configure systems to issue a log entry and alert on unsuccessful logins to an administrative account.

16.11 Lock Workstation Sessions After Inactivity

Automatically lock workstation sessions after a standard period of inactivity.

16.13 Alert on Account Login Behavior Deviation

Alert when users deviate from normal login behavior, such as time-of-day, workstation location and duration.

- En este caso la recomendación 4.1.7 forma parte del Control CIS 4; que es necesario cubrir, y también del Control CIS 16.
- Este paso se repetirá con todas las recomendaciones que haya en el CIS Benchmark elegido.

4. Construcción del script

- Una vez sabemos las recomendaciones que queremos implementar y las que no, se edita el archivo ya existente “main.yml” de Ansible Lockdown.
- El resto de los parámetros se mantienen con el valor por defecto.

```
# Section 2 Fixes
# Section 2 is Services (Special
ubtu18cis_rule_2_1_1_1: false
ubtu18cis_rule_2_1_1_2: false
ubtu18cis_rule_2_1_1_3: true
ubtu18cis_rule_2_1_1_4: true
ubtu18cis_rule_2_1_2: true
ubtu18cis_rule_2_1_3: false
ubtu18cis_rule_2_1_4: false
ubtu18cis_rule_2_1_5: false
ubtu18cis_rule_2_1_6: false
ubtu18cis_rule_2_1_7: false
ubtu18cis_rule_2_1_8: false
ubtu18cis_rule_2_1_9: false
ubtu18cis_rule_2_1_10: false
ubtu18cis_rule_2_1_11: false
ubtu18cis_rule_2_1_12: false
ubtu18cis_rule_2_1_13: false
ubtu18cis_rule_2_1_14: false
ubtu18cis_rule_2_1_15: false
ubtu18cis_rule_2_1_16: false
ubtu18cis_rule_2_1_17: false
ubtu18cis_rule_2_2_1: true
ubtu18cis_rule_2_2_2: true
ubtu18cis_rule_2_2_3: true
ubtu18cis_rule_2_2_4: true
ubtu18cis_rule_2_2_5: true
ubtu18cis_rule_2_2_6: true
ubtu18cis_rule_2_3: true
```

Ejecución y auditoría

Herramienta para auditar

- **Lynis** es una herramienta de auditoría de seguridad automatizada para sistemas basados en UNIX. Realiza un análisis de seguridad en profundidad y se ejecuta localmente.
- Su objetivo principal es probar las defensas de seguridad y proporcionar consejos para reforzar aún más el sistema.

```
Hardening index : 59 [##### ]
Tests performed : 220
Plugins enabled : 1

Components:
- Firewall [V]
- Malware scanner [X]

Lynis Modules:
- Compliance Status [?]
- Security Audit [V]
- Vulnerability Scan [V]

Files:
- Test and debug information : /var/log/lynis.log
- Report data : /var/log/lynis-report.dat

=====
Notice: Lynis Actualización disponible
Versión actual : 262 Latest version : 311
=====

Lynis 2.6.2

Auditing, system hardening, and compliance for UNIX-based systems
(Linux, macOS, BSD, and others)

2007-2018, CISOfy - https://cisofy.com/lynis/
Enterprise support available (compliance, plugins, interface and tools)

=====
[TIP]: Enhance Lynis audits by adding your settings to custom.prfl (see /etc/lynis/default.prfl for
all settings)
```

Al final de la ejecución nos proporciona un resumen con, entre otras cosas, una puntuación de 0 a 100

Ejecución y auditoría

```
Hardening index : 59 [##### ]
Tests performed : 220
Plugins enabled : 1

Components:
- Firewall [V]
- Malware scanner [X]

Lynis Modules:
- Compliance Status [?]
- Security Audit [V]
- Vulnerability Scan [V]

Files:
- Test and debug information : /var/log/lynis.log
- Report data : /var/log/lynis-report.dat

=====
Notice: Lynis Actualización disponible
Versión actual : 262 Latest version : 311
=====

Lynis 2.6.2

Auditing, system hardening, and compliance for UNIX-based systems
(Linux, macOS, BSD, and others)

2007-2018, CISOfy - https://cisofy.com/lynis/
Enterprise support available (compliance, plugins, interface and tools)

=====

[TIP]: Enhance Lynis audits by adding your settings to custom.prfl (see /etc/lynis/default.prfl for
all settings)
```

Salida de lynis antes de utilizar Ansible Lockdown

```
Hardening index : 63 [##### ]
Tests performed : 220
Plugins enabled : 1

Components:
- Firewall [V]
- Malware scanner [X]

Lynis Modules:
- Compliance Status [?]
- Security Audit [V]
- Vulnerability Scan [V]

Files:
- Test and debug information : /var/log/lynis.log
- Report data : /var/log/lynis-report.dat

=====
Notice: Lynis Actualización disponible
Versión actual : 262 Latest version : 311
=====

Lynis 2.6.2

Auditing, system hardening, and compliance for UNIX-based systems
(Linux, macOS, BSD, and others)

2007-2018, CISOfy - https://cisofy.com/lynis/
Enterprise support available (compliance, plugins, interface and tools)

=====

[TIP]: Enhance Lynis audits by adding your settings to custom.prfl (see /etc/lynis/default.prfl for
all settings)
```

Salida de lynis después de utilizar Ansible Lockdown

Información de contacto



[Rosa García López](#)



[@rosagl2001](#)



[rosagarlo](#)



Mención especial y
agradecimientos a



[Jose M. Redondo](#)

Referencias

- <https://github.com/ansible-lockdown/UBUNTU18-CIS/tree/devel/defaults>
- <https://attack.mitre.org/>
- <https://mitre-attack.github.io/attack-navigator/#layerURL=https%3A%2F%2Fattack.mitre.org%2Fgroups%2FG0032%2FG0032-enterprise-layer.json>
- <https://www.tripwire.com/resources/datasheets/cis-controls/mitre-attack-matrix>
- <https://www.cisecurity.org/>
- https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_glosario_ciberseguridad_2021.pdf
- <https://www.lockdownenterprise.com/>
- <https://github.com/ansible-lockdown>
- <https://github.com/CISOFY/LYNIS>
- <https://www.bbc.com/mundo/noticias-39929920>