Cómo defenderte automáticamente de las tácticas y técnicas de un grupo ransomware

Rosa García López

Contenidos

01 Marco teórico

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

02 Grupo Lazarus

- Introducción
- Matriz con sus TTP

03 Procedimiento

- 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, **TTP**s para abreviar.

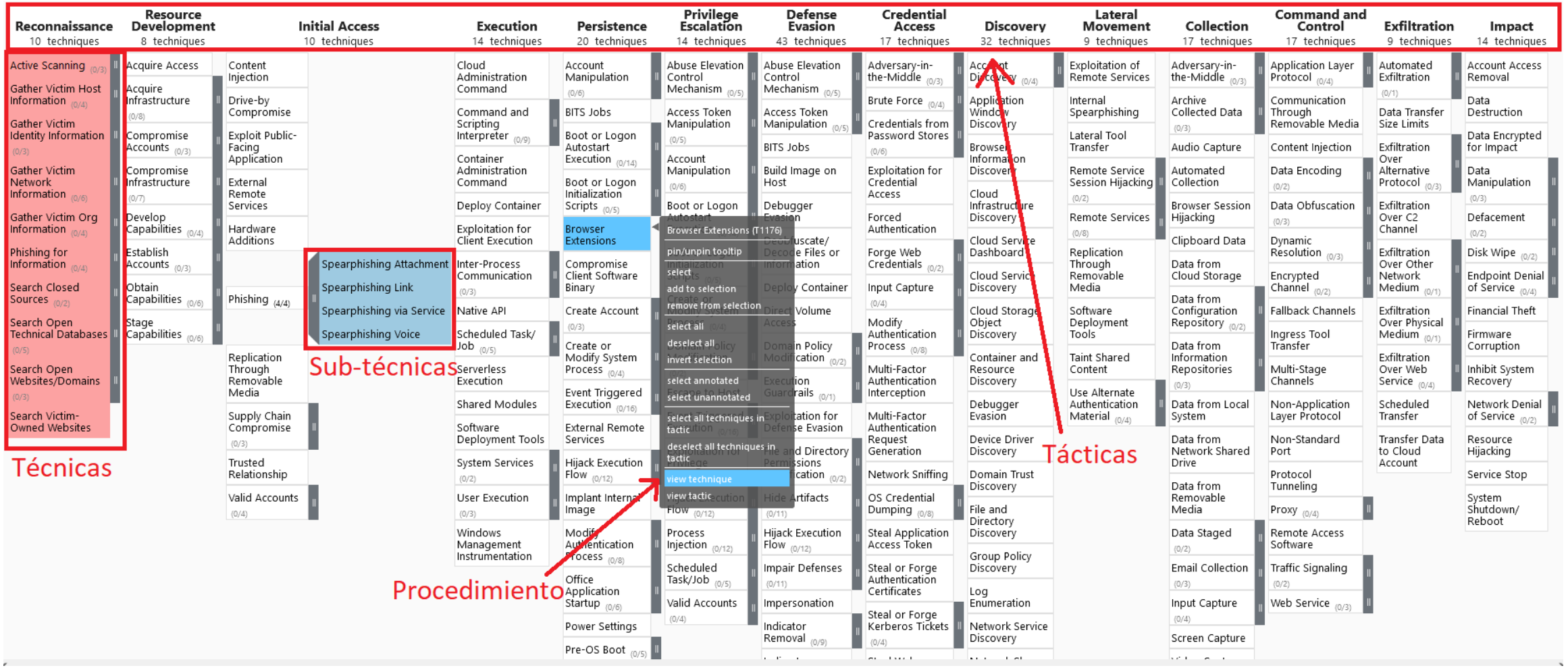
El nombre de cada columna de la matriz conforma la táctica; con un total de catorce, mientras que las técnicas y sub-técnicas se encuentran bajo el nombre de la columna a la que pertenecen e identificadas con su nombre o ID.

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®



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® Center for Internet Security®

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 in 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.

```yaml
---
# If you would like a report at the end accordin to OpenSCAP as to the report results
# then you should set ubtu18cis_oscap_scan to true/yes.
# NOTE: This requires the python_xmltojson package on the control host.
ubtu18cis_oscap_scan: false
ubtu18cis_report_dir: /tmp

ubtu18cis_section1_patch: true
ubtu18cis_section2_patch: true
ubtu18cis_section3_patch: true
ubtu18cis_section4_patch: true
ubtu18cis_section5_patch: true
ubtu18cis_section6_patch: true

# System will reboot if false, can give better audit results
ubtu18_skip_reboot: True

## Benchmark name used by auditing control role
# The audit variable found at the base
benchmark: UBUNTU18-CIS

### Audit Binary is required on the remote host
setup_audit: false
# How to retrieve audit binary
# Options are copy or download - detailed settings at the bottom of this file
# you will need to access to either github or the file already dowmloaded
get_audit_binary_method: download

# how to get audit files onto host options
# options are git/copy/get_url other e.g. if you wish to run from already downloaded conf
audit_content: git

# enable audits to run - this  runs the audit and get the latest content
run_audit: false
```

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

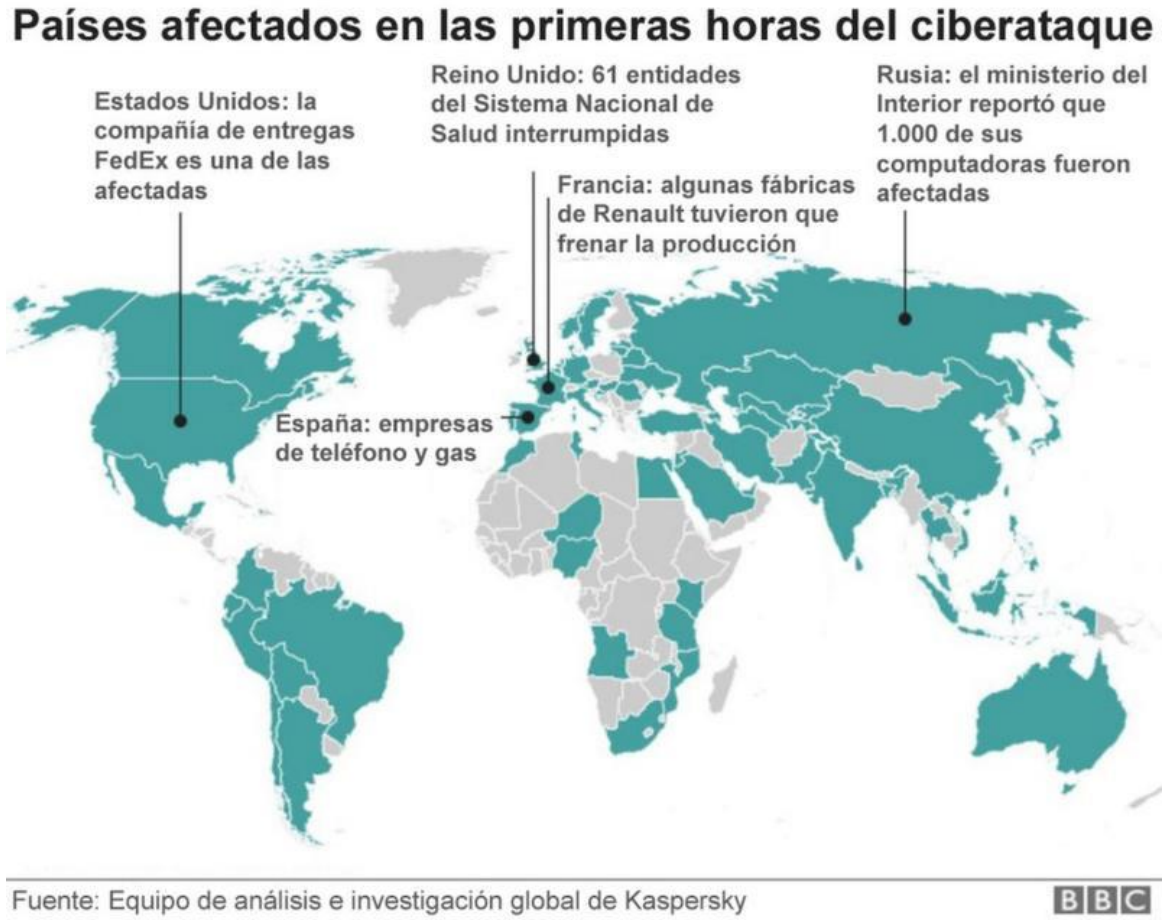
Grupo Lazarus

Introducción

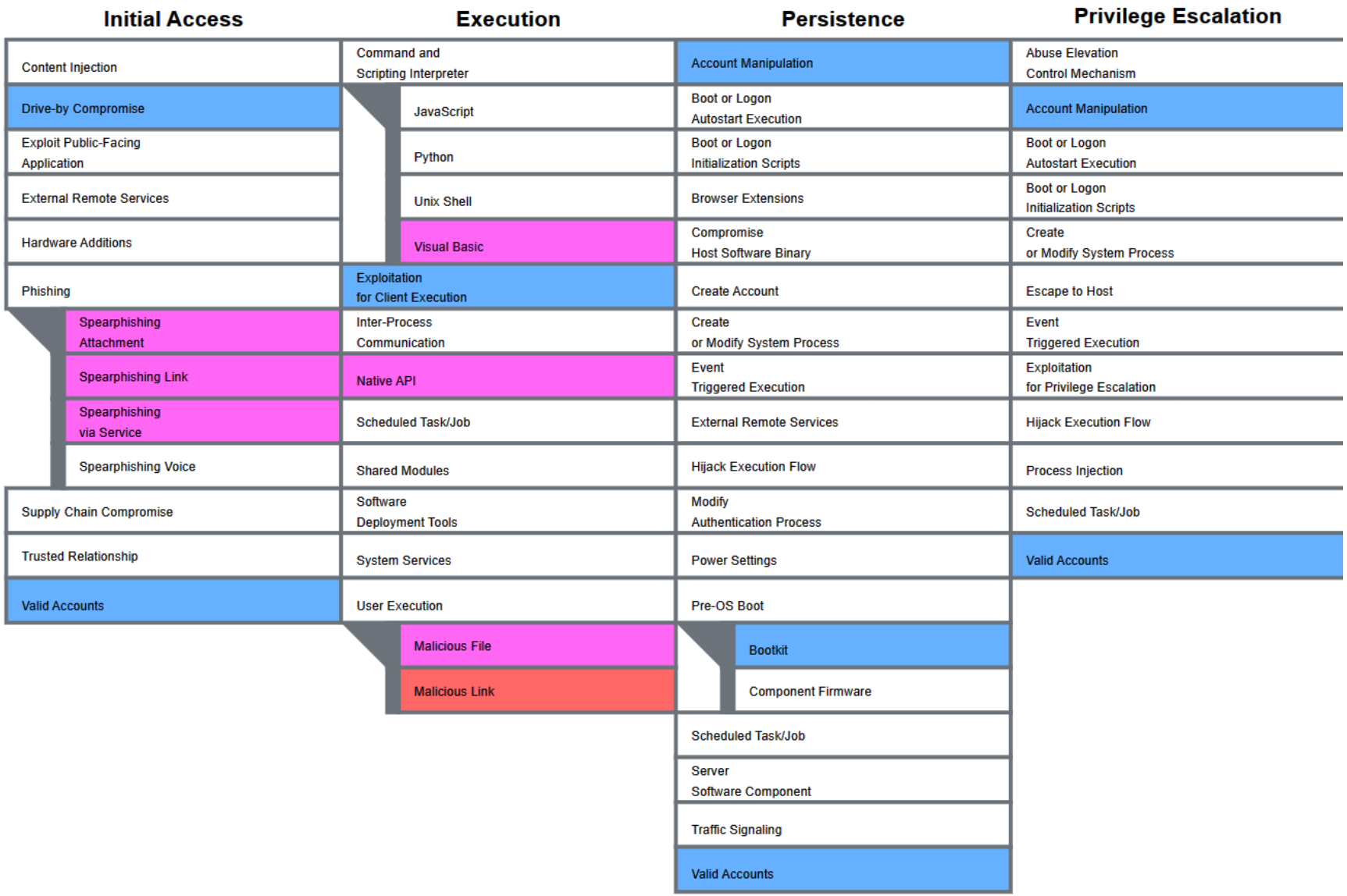
¿Qué es el grupo Lazarus?

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.

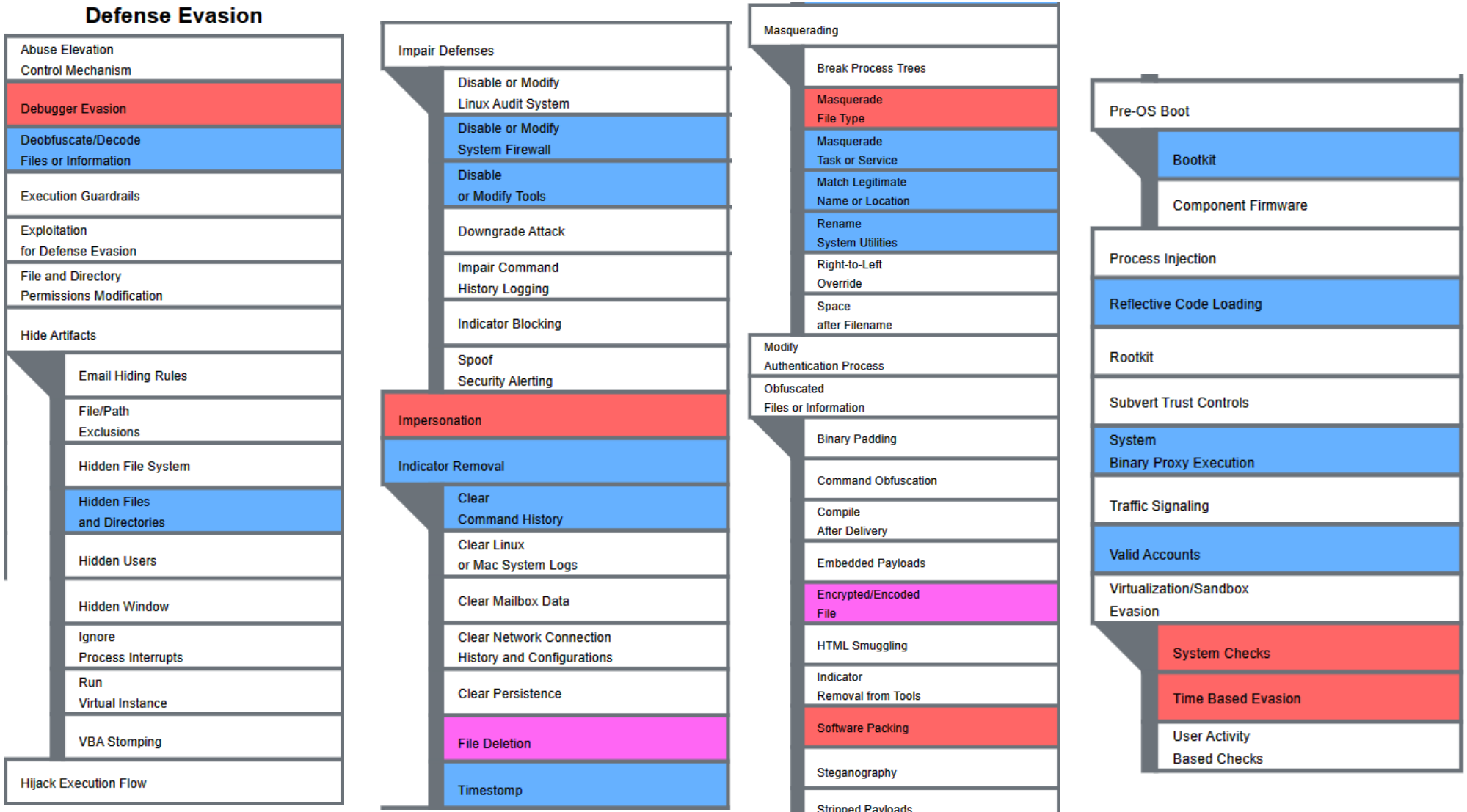
Llevan operando desde 2009 y han participado en numerosos ataques, varios de ellos enfocados en Corea del Sur, hasta el famoso ataque de WannaCry en 2017.



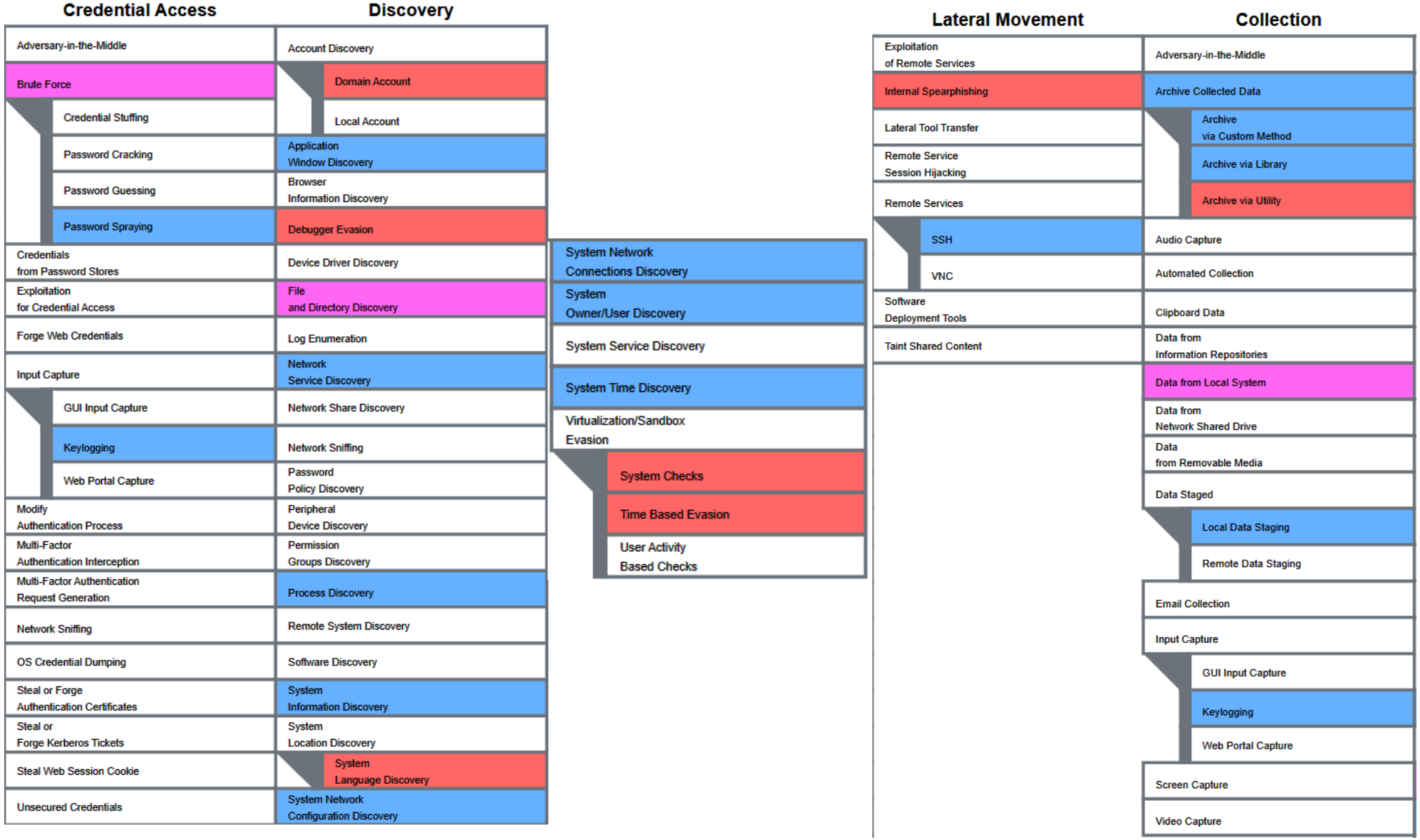
Matriz con sus TTPs - I



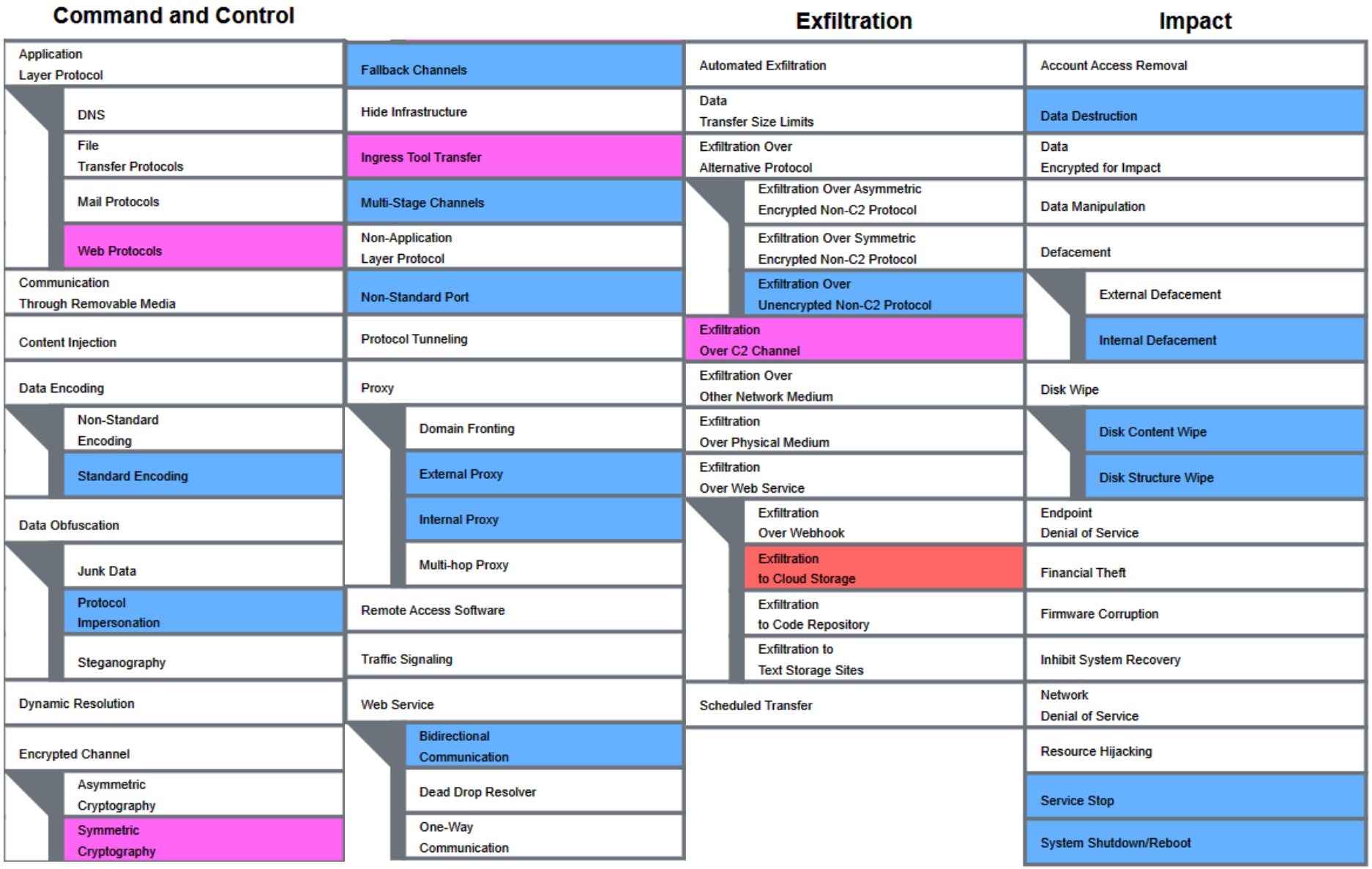
Matriz con sus TTPs - II



Matriz con sus TTPs - III

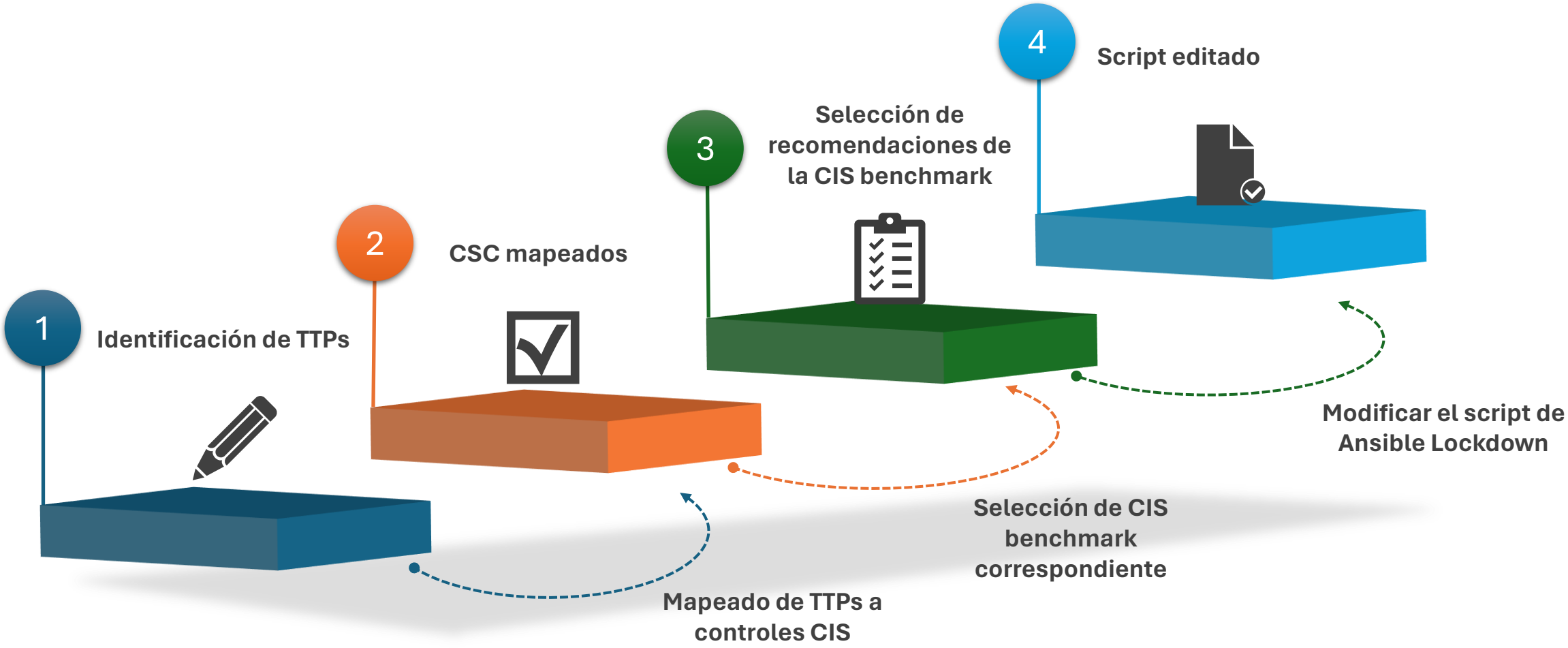


Matriz con sus TTPs - IV



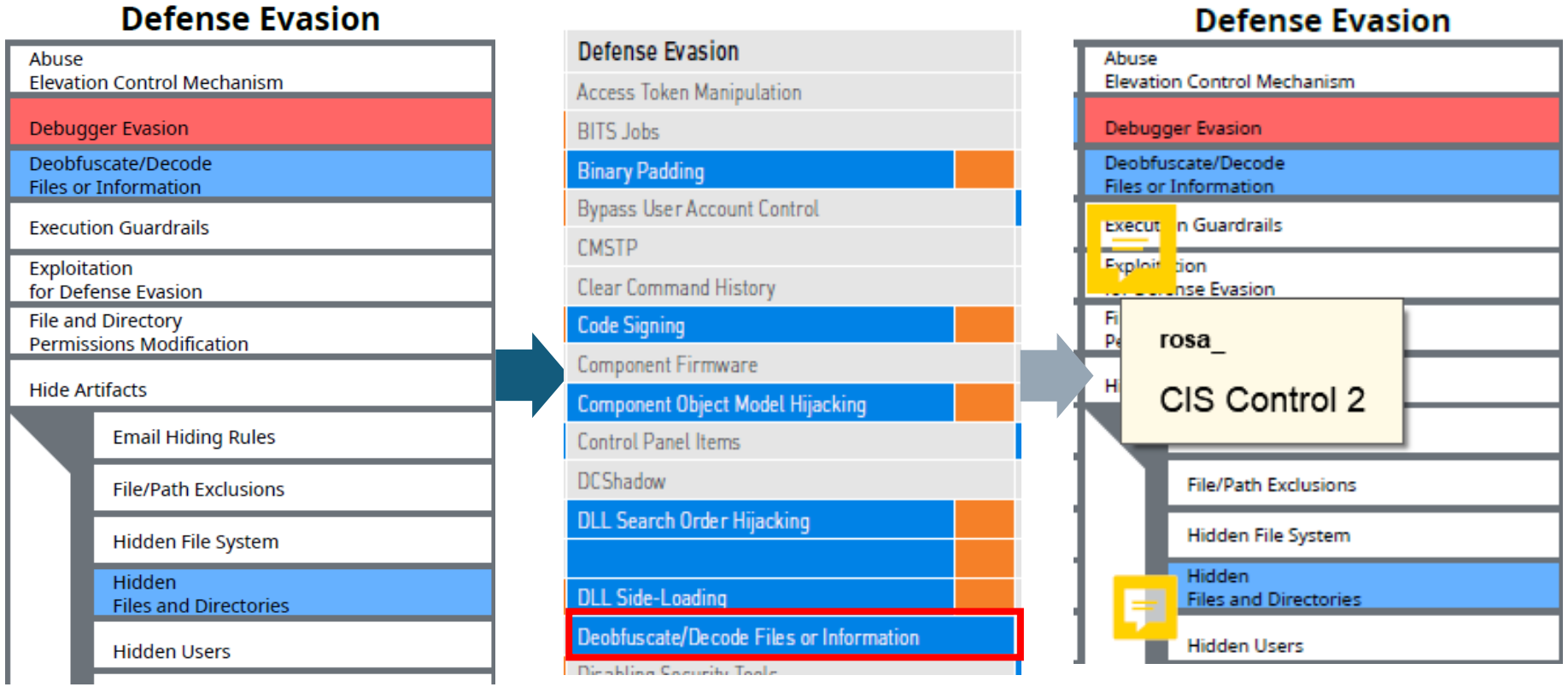
Procedimiento

Pasos del procedimiento



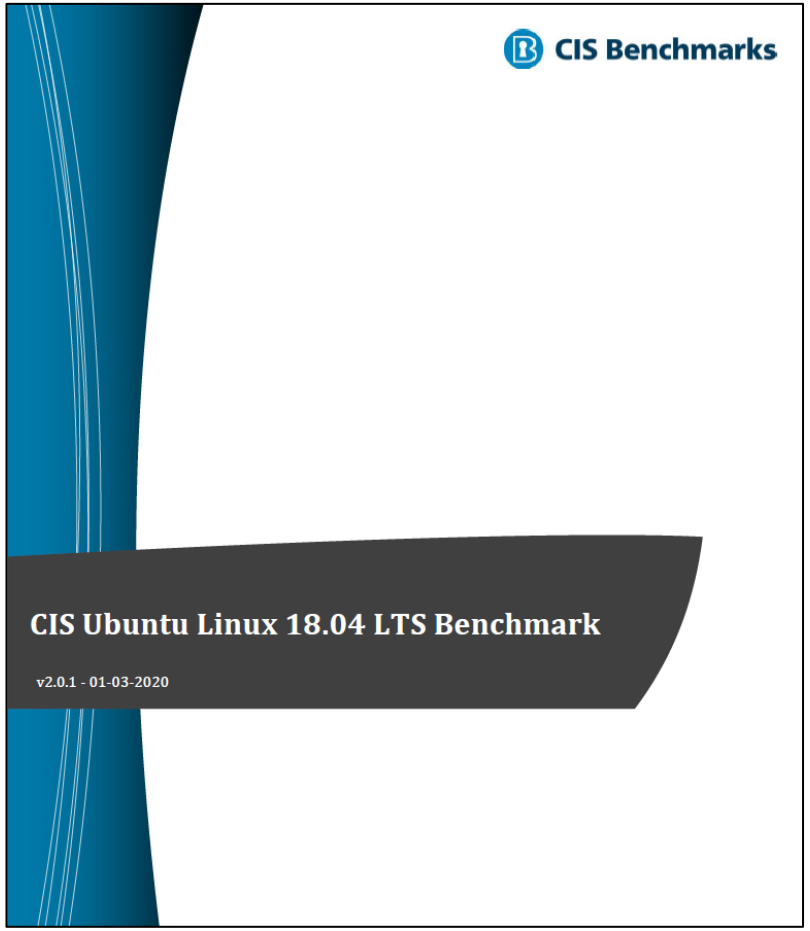
1. Mapeo de TTPs a CSC

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.

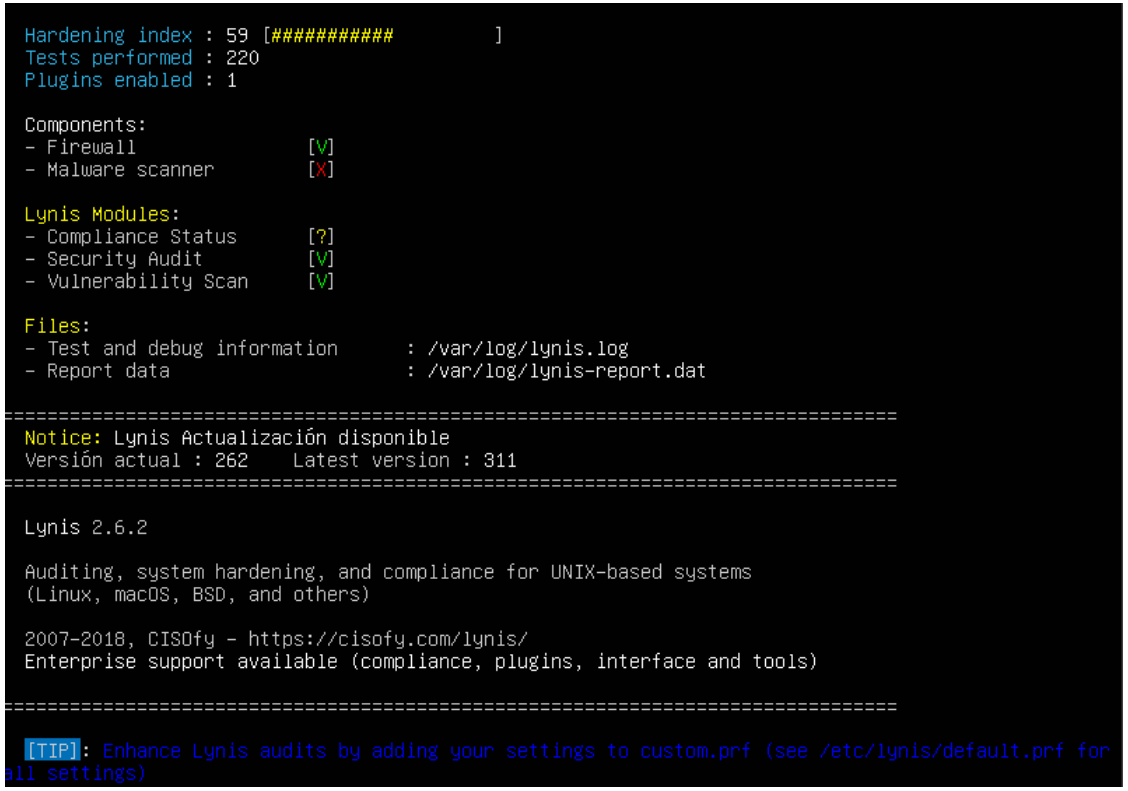
```
# Section 2 Fixes
# Section 2 is Services (Special
ubtu18cis_rule_2_1_1_1: false
ubtu18cis_rule_2_1_1_2: false
ubtu18cis_rule_2_1_1_3: true
ubtu18cis_rule_2_1_1_4: true
ubtu18cis_rule_2_1_2: true
ubtu18cis_rule_2_1_3: false
ubtu18cis_rule_2_1_4: false
ubtu18cis_rule_2_1_5: false
ubtu18cis_rule_2_1_6: 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

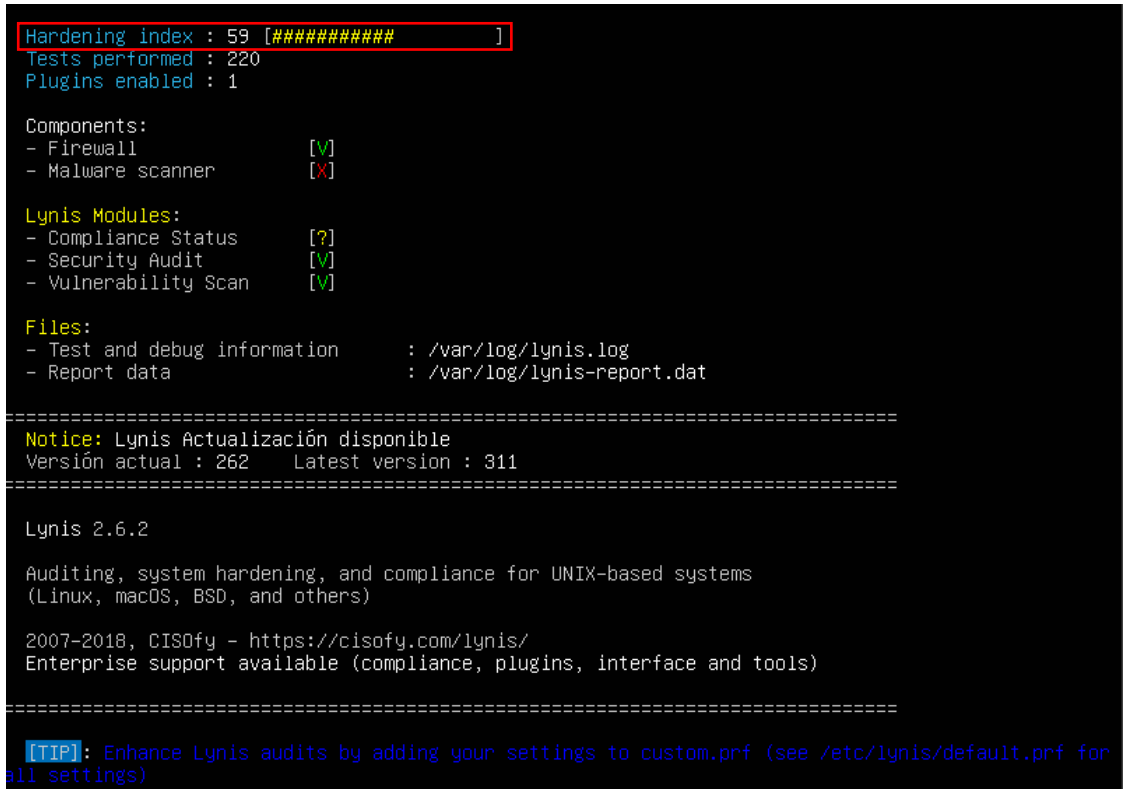
- **Lynis** es una herramienta de auditoría de seguridad automatizada para sistemas basados en UNIX. Realiza un análisis de seguridad en profundidad y se ejecuta localmente.

- Su objetivo principal es probar las defensas de seguridad y proporcionar consejos para reforzar aún más el sistema.

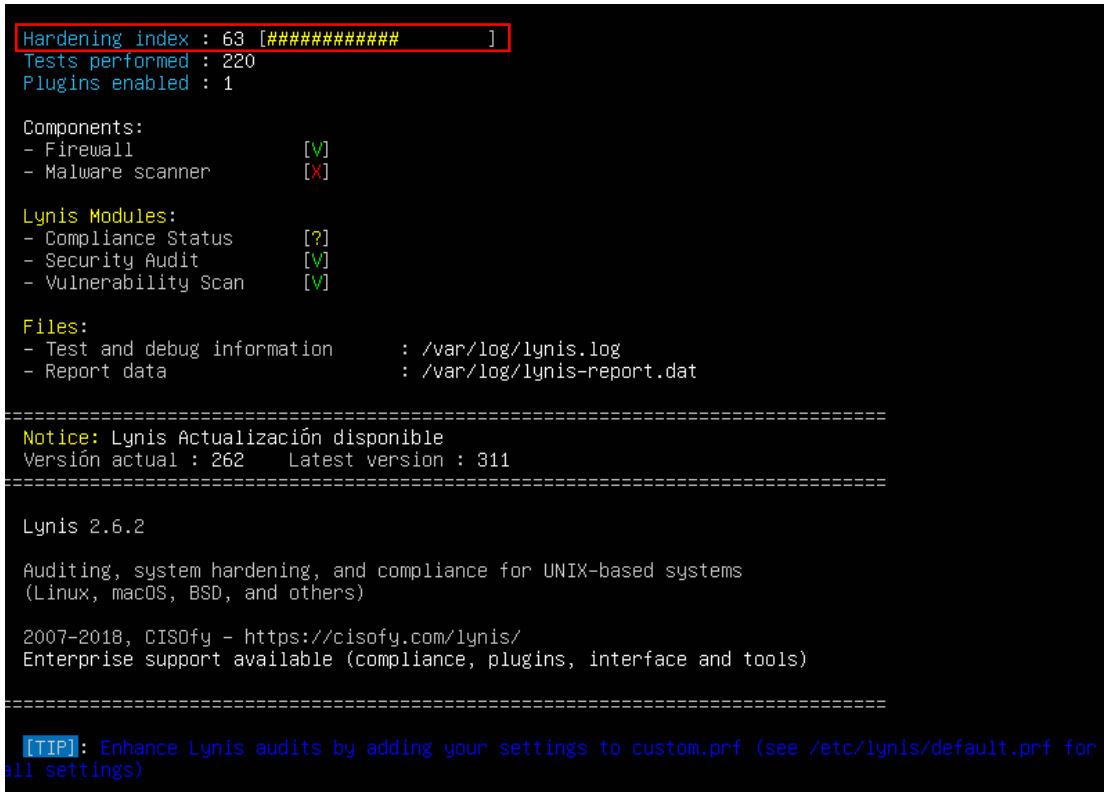


Al final de la ejecución nos proporciona un resumen con, entre otras cosas, una puntuación de 0 a 100

Ejecución y auditoría



Salida de lynis antes de utilizar Ansible Lockdown



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