SIEMs Attack Framework

Compromising Enterprise Networks from their own SIEM

Yamila Levalle
@ylevalle

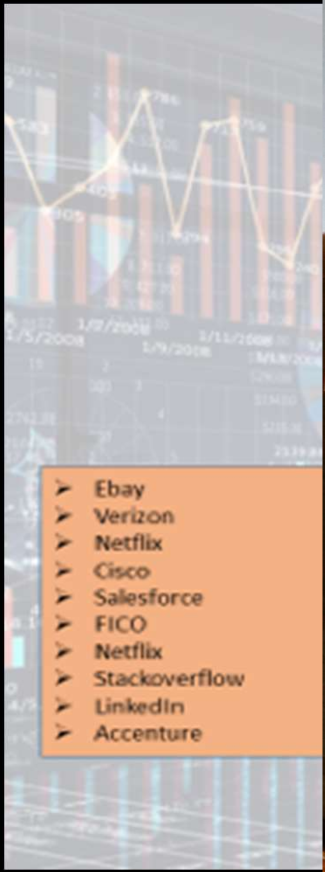
CySec by Women

Eleven Paths

Eleven Paths

@ylevalle

¿Quiénes usan SIEMs?



- Ebay
- Verizon
- Netflix
- Cisco
- Salesforce
- FICO
- Netflix
- Stackoverflow
- LinkedIn
- Accenture

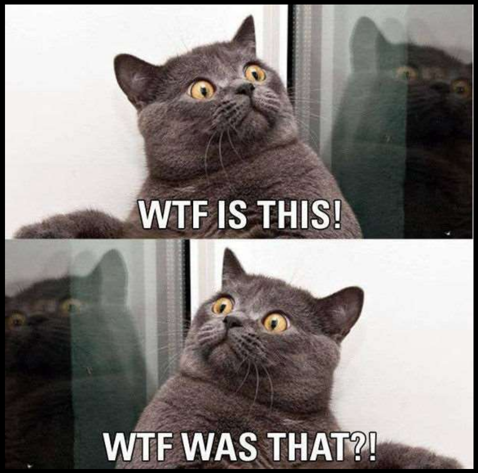
Eleven Paths

¿Por qué creamos esta herramienta?

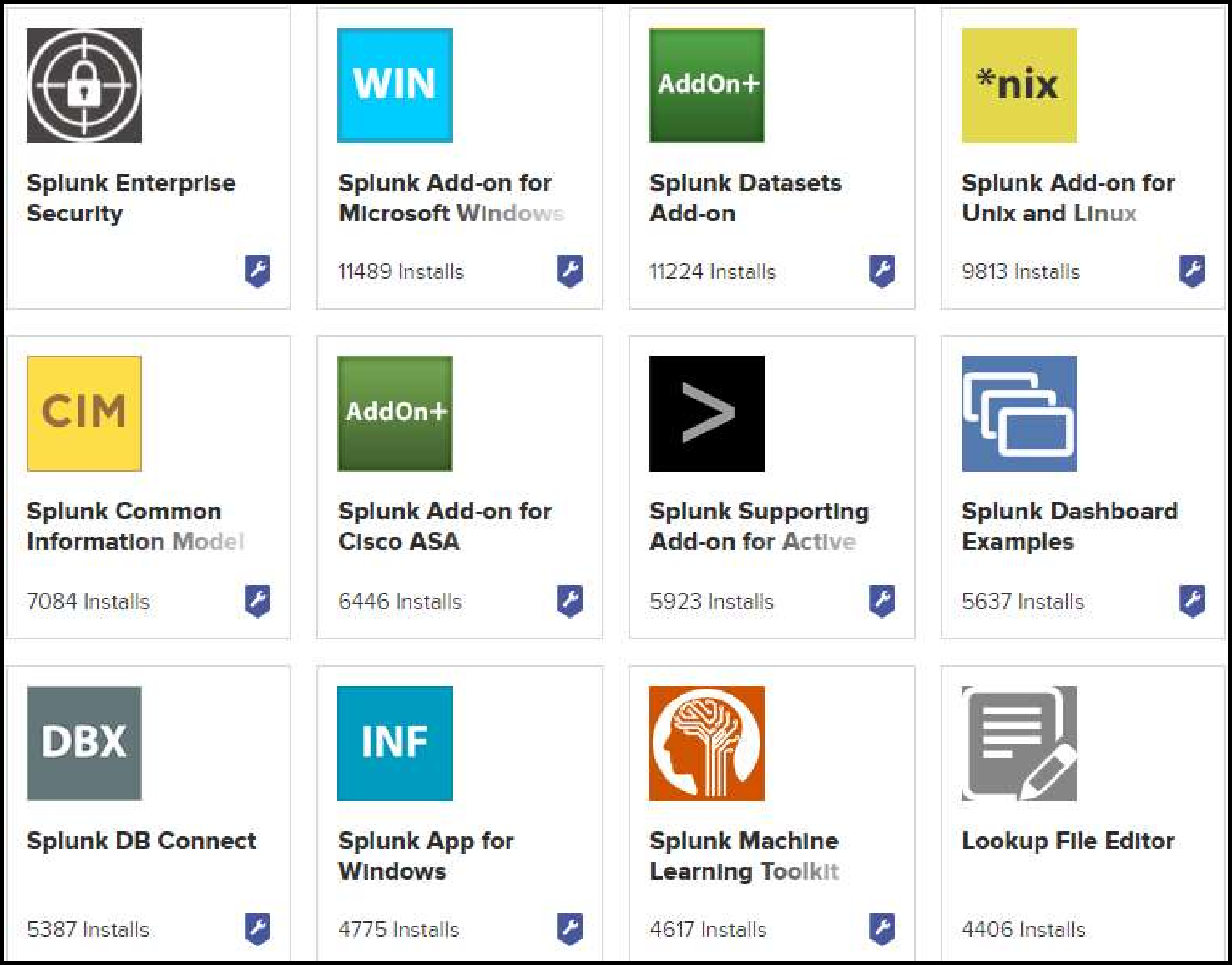
Desde el punto de vista del atacante los permisos que tienen los SIEMs sobre los equipos y cuentas de una red corporativa son muy amplios, y el acceso administrativo a un SIEM puede ser usado para obtener ejecución de código en el servidor donde se encuentra instalado el SIEM, y en algunos casos en los equipos "cliente" de los cuales el SIEM recolecta los eventos como servidores de Active Directory, Bases de Datos, Servidores AWS y dispositivos de red como Firewalls y Routers

Splunk Version and Features

SPLUNK FREE	No Access Control or Authentication Run as Root / Admin by default Can upload custom apps and scripts
SPLUNK ENTERPRISE	Generally Admin/Password Optional Password Policies Run as Root / Admin by default Can upload custom apps and scripts
SPLUNK CLOUD	SAML, User/Password or LDAP No CLI or configuration file modification Can't upload custom apps and scripts



Splunkbase



- Splunk Enterprise Security
- Splunk Add-on for Microsoft Windows — 11489 Installs
- Splunk Datasets Add-on — 11224 Installs
- Splunk Add-on for Unix and Linux — 9813 Installs
- Splunk Common Information Model — 7084 Installs
- Splunk Add-on for Cisco ASA — 6446 Installs
- Splunk Supporting Add-on for Active — 5923 Installs
- Splunk Dashboard Examples — 5637 Installs
- Splunk DB Connect — 5387 Installs
- Splunk App for Windows — 4775 Installs
- Splunk Machine Learning Toolkit — 4617 Installs
- Lookup File Editor — 4406 Installs

¿Cómo?

Eleven Paths

@ylevalle

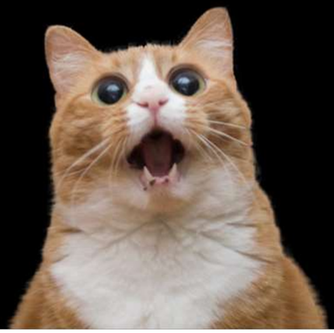
¿Qué podemos hacer?

- Obtener la configuración del SIEM e información relevante
- Realizar ataques de diccionario o fuerza bruta contra la interfaz web o la interfaz de management, o contra el software cliente de SIEM para obtener credenciales de administración
- Aprovechar las configuraciones por defecto de las imágenes virtuales OVA de los SIEMs para obtener credenciales de administración en el servidor donde está instalado el SIEM, la base de datos o la interfaz web

Eleven Paths

@ylevalle

- Leer archivos arbitrarios desde el servidor donde el SIEM está instalado
- Instalar aplicaciones maliciosos como Windows/Linux reverse y bind shells o scripts maliciosos para comprometer el servidor donde el SIEM está instalado
- Crear y aplicar políticas maliciosas, acciones o notificaciones que permitan ejecutar comandos cuando ocurra un evento determinado, con el objetivo de obtener un reverse shell en el servidor donde el SIEM está instalado



- Instalar aplicaciones maliciosos como un Windows/Linux reverse y bind shells o scripts maliciosos, con el objetivo de comprometer los clientes desde los cuales el SIEM recolecta los eventos
- Obtener las cuentas de usuario y contraseñas de sistemas críticos almacenadas en el SIEM (servidores LDAP/AD, bases de datos, dispositivos de red, servidores AWS)

Eleven Paths

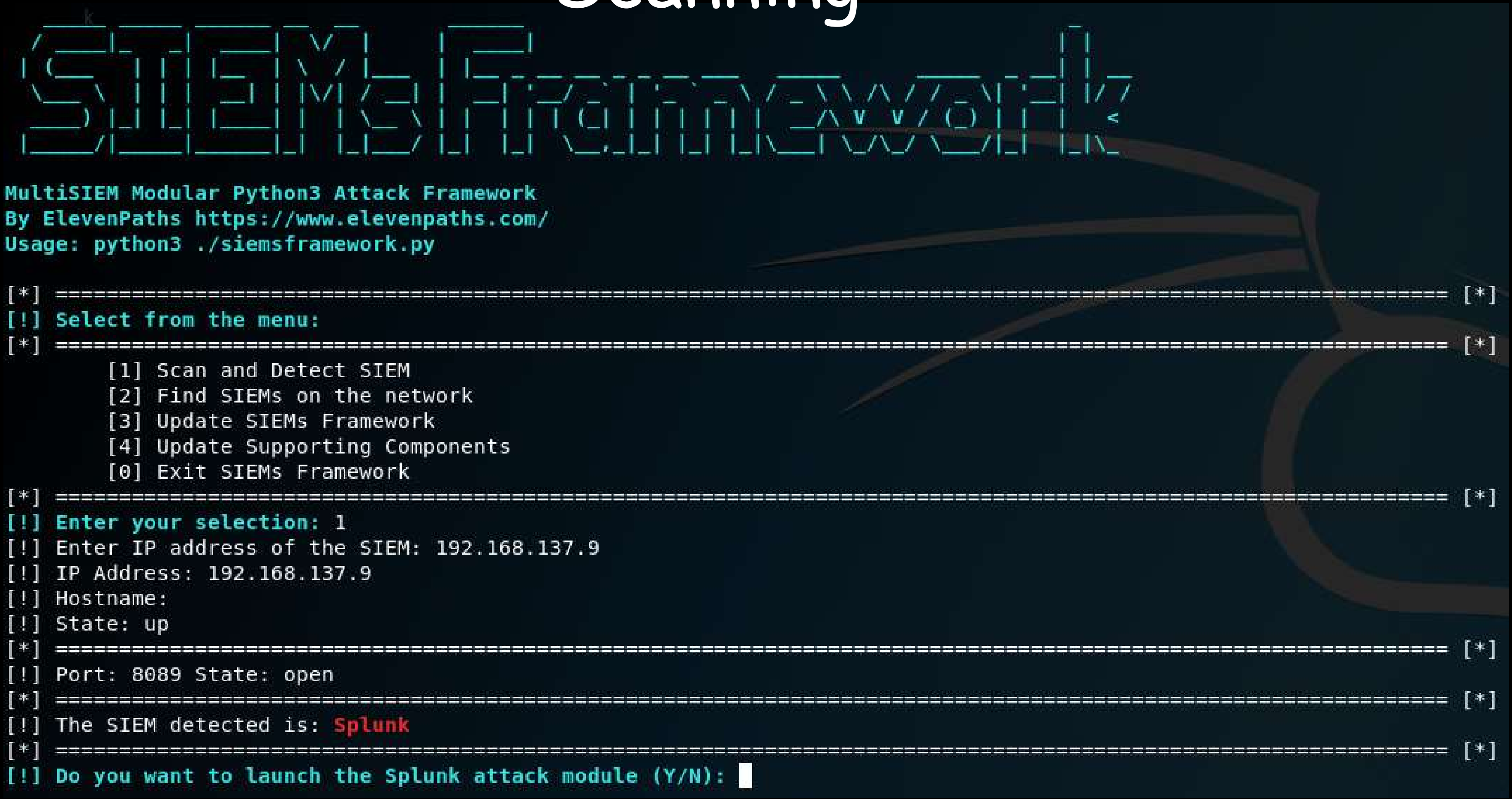
@ylevalle

SIEMs Framework Paquetes y Módulos

Eleven Paths

@ylevalle

Scanning



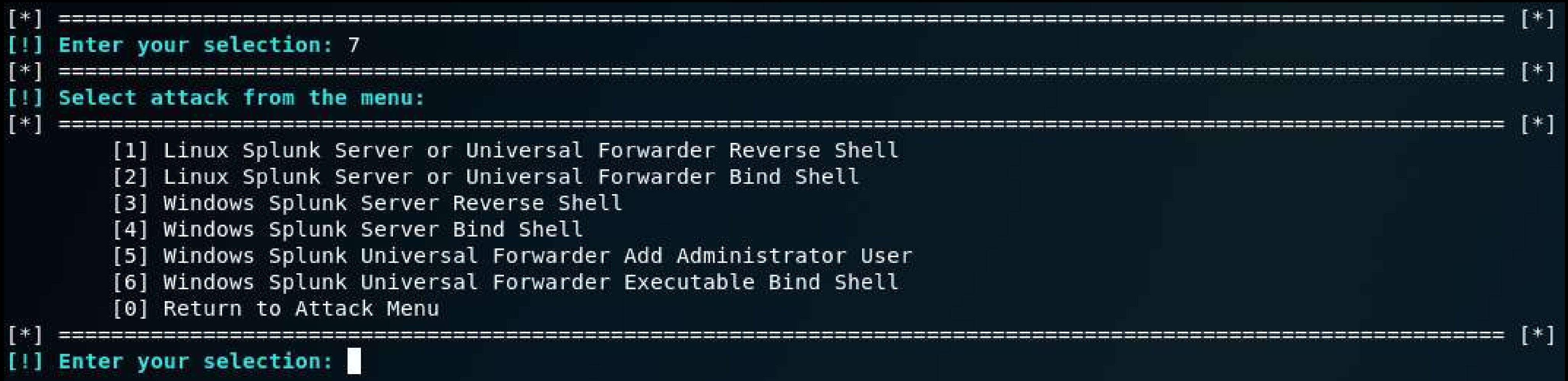
```
MultiSIEM Modular Python3 Attack Framework
By ElevenPaths https://www.elevenpaths.com/
Usage: python3 ./siemsframework.py

[*] ================================================================================================== [*]
[!] Select from the menu:
[*] ================================================================================================== [*]
        [1] Scan and Detect SIEM
        [2] Find SIEMs on the network
        [3] Update SIEMs Framework
        [4] Update Supporting Components
        [0] Exit SIEMs Framework
[*] ================================================================================================== [*]
[!] Enter your selection: 1
[!] Enter IP address of the SIEM: 192.168.137.9
[!] IP Address: 192.168.137.9
[!] Hostname:
[!] State: up
[*] ================================================================================================== [*]
[!] Port: 8089 State: open
[*] ================================================================================================== [*]
[!] The SIEM detected is: Splunk
[*] ================================================================================================== [*]
[!] Do you want to launch the Splunk attack module (Y/N):
```

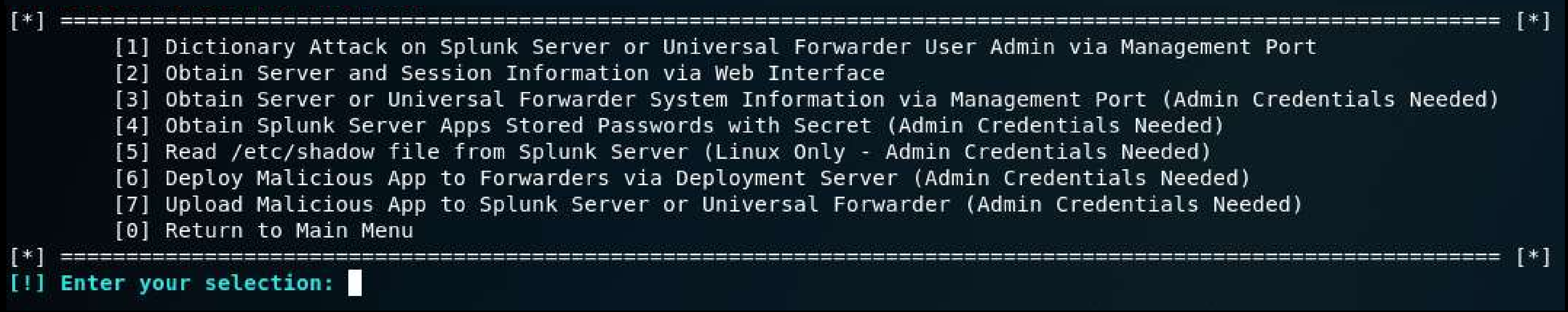
Eleven Paths

@ylevalle

Splunk

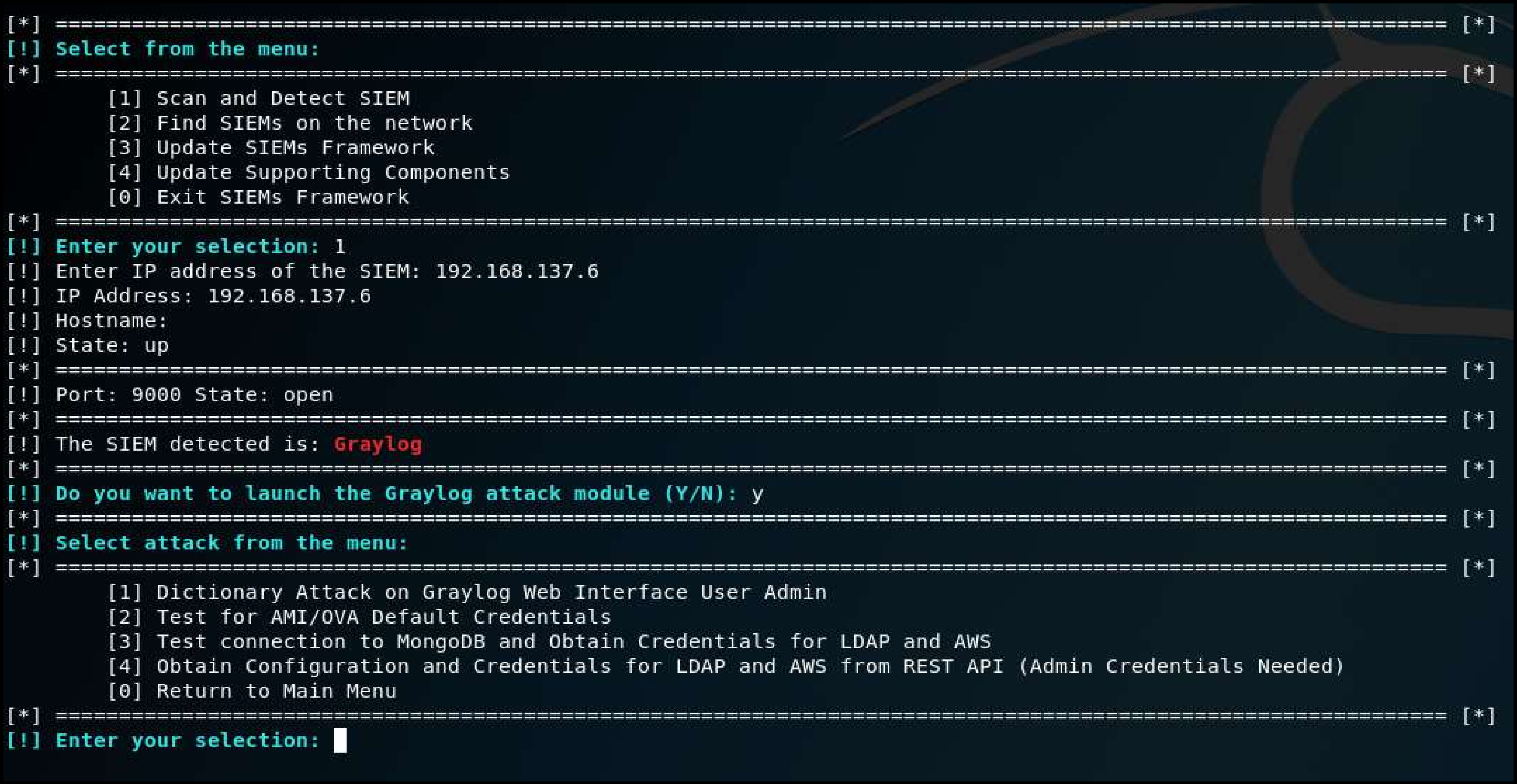


```
[*] ============================================================================================ [*]
[!] Enter your selection: 7
[*] ============================================================================================ [*]
[!] Select attack from the menu:
[*] ============================================================================================ [*]
        [1] Linux Splunk Server or Universal Forwarder Reverse Shell
        [2] Linux Splunk Server or Universal Forwarder Bind Shell
        [3] Windows Splunk Server Reverse Shell
        [4] Windows Splunk Server Bind Shell
        [5] Windows Splunk Universal Forwarder Add Administrator User
        [6] Windows Splunk Universal Forwarder Executable Bind Shell
        [0] Return to Attack Menu
[*] ============================================================================================ [*]
[!] Enter your selection: 
```



```
[*] ============================================================================================ [*]
        [1] Dictionary Attack on Splunk Server or Universal Forwarder User Admin via Management Port
        [2] Obtain Server and Session Information via Web Interface
        [3] Obtain Server or Universal Forwarder System Information via Management Port (Admin Credentials Needed)
        [4] Obtain Splunk Server Apps Stored Passwords with Secret (Admin Credentials Needed)
        [5] Read /etc/shadow file from Splunk Server (Linux Only - Admin Credentials Needed)
        [6] Deploy Malicious App to Forwarders via Deployment Server (Admin Credentials Needed)
        [7] Upload Malicious App to Splunk Server or Universal Forwarder (Admin Credentials Needed)
        [0] Return to Main Menu
[*] ============================================================================================ [*]
[!] Enter your selection: 
```

Graylog

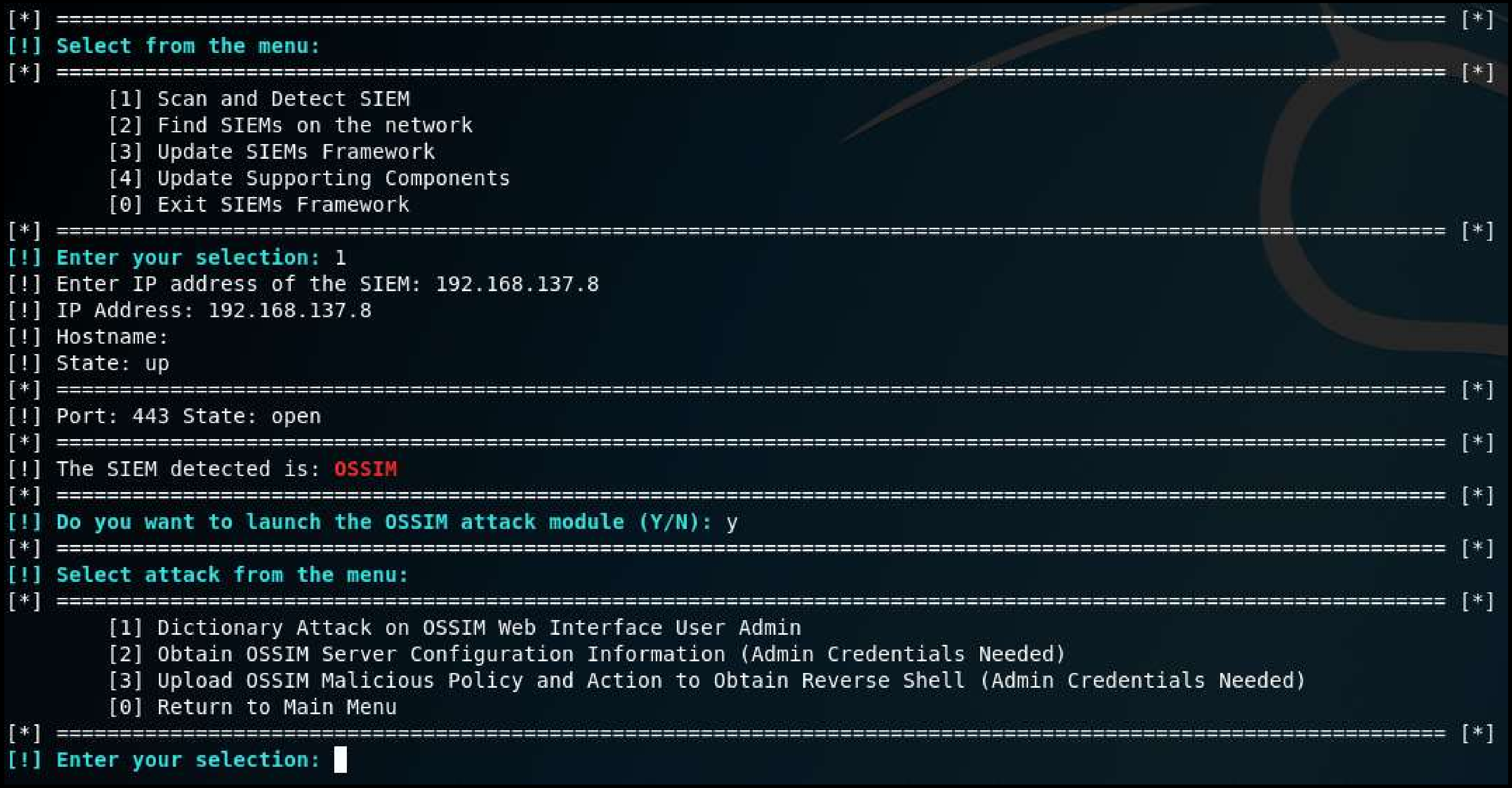


```
[*] ========================================================================================= [*]
[!] Select from the menu:
[*] ========================================================================================= [*]
        [1] Scan and Detect SIEM
        [2] Find SIEMs on the network
        [3] Update SIEMs Framework
        [4] Update Supporting Components
        [0] Exit SIEMs Framework
[*] ========================================================================================= [*]
[!] Enter your selection: 1
[!] Enter IP address of the SIEM: 192.168.137.6
[!] IP Address: 192.168.137.6
[!] Hostname:
[!] State: up
[*] ========================================================================================= [*]
[!] Port: 9000 State: open
[*] ========================================================================================= [*]
[!] The SIEM detected is: Graylog
[*] ========================================================================================= [*]
[!] Do you want to launch the Graylog attack module (Y/N): y
[*] ========================================================================================= [*]
[!] Select attack from the menu:
[*] ========================================================================================= [*]
        [1] Dictionary Attack on Graylog Web Interface User Admin
        [2] Test for AMI/OVA Default Credentials
        [3] Test connection to MongoDB and Obtain Credentials for LDAP and AWS
        [4] Obtain Configuration and Credentials for LDAP and AWS from REST API (Admin Credentials Needed)
        [0] Return to Main Menu
[*] ========================================================================================= [*]
[!] Enter your selection: 
```

Eleven Paths

@ylevalle

Ossim

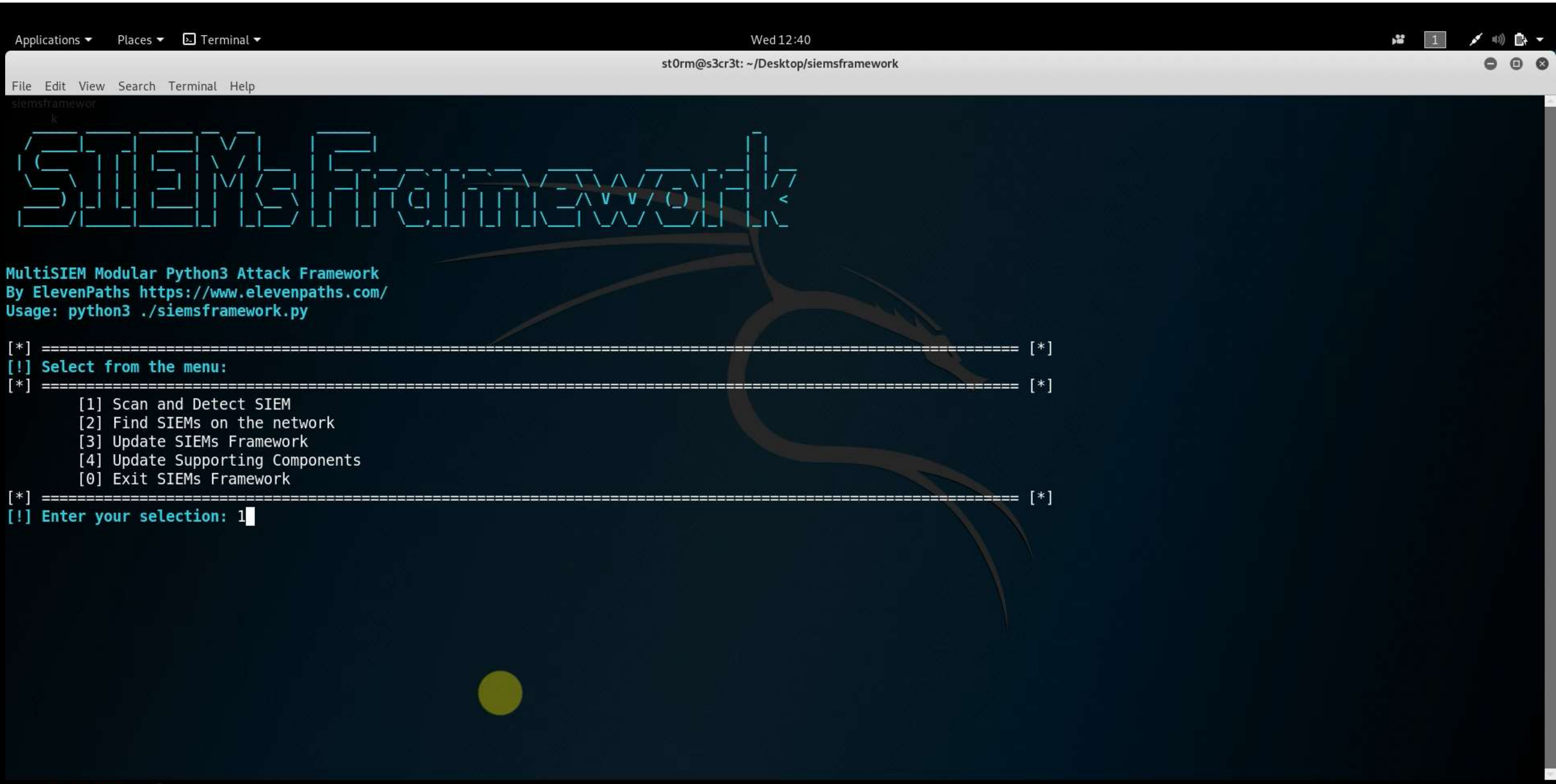


```
[*] ============================================================================================================ [*]
[!] Select from the menu:
[*] ============================================================================================================ [*]
    [1] Scan and Detect SIEM
    [2] Find SIEMs on the network
    [3] Update SIEMs Framework
    [4] Update Supporting Components
    [0] Exit SIEMs Framework
[*] ============================================================================================================ [*]
[!] Enter your selection: 1
[!] Enter IP address of the SIEM: 192.168.137.8
[!] IP Address: 192.168.137.8
[!] Hostname:
[!] State: up
[*] ============================================================================================================ [*]
[!] Port: 443 State: open
[*] ============================================================================================================ [*]
[!] The SIEM detected is: OSSIM
[*] ============================================================================================================ [*]
[!] Do you want to launch the OSSIM attack module (Y/N): y
[*] ============================================================================================================ [*]
[!] Select attack from the menu:
[*] ============================================================================================================ [*]
    [1] Dictionary Attack on OSSIM Web Interface User Admin
    [2] Obtain OSSIM Server Configuration Information (Admin Credentials Needed)
    [3] Upload OSSIM Malicious Policy and Action to Obtain Reverse Shell (Admin Credentials Needed)
    [0] Return to Main Menu
[*] ============================================================================================================ [*]
[!] Enter your selection:
```

Show Time!

Eleven Paths

@ylevalle

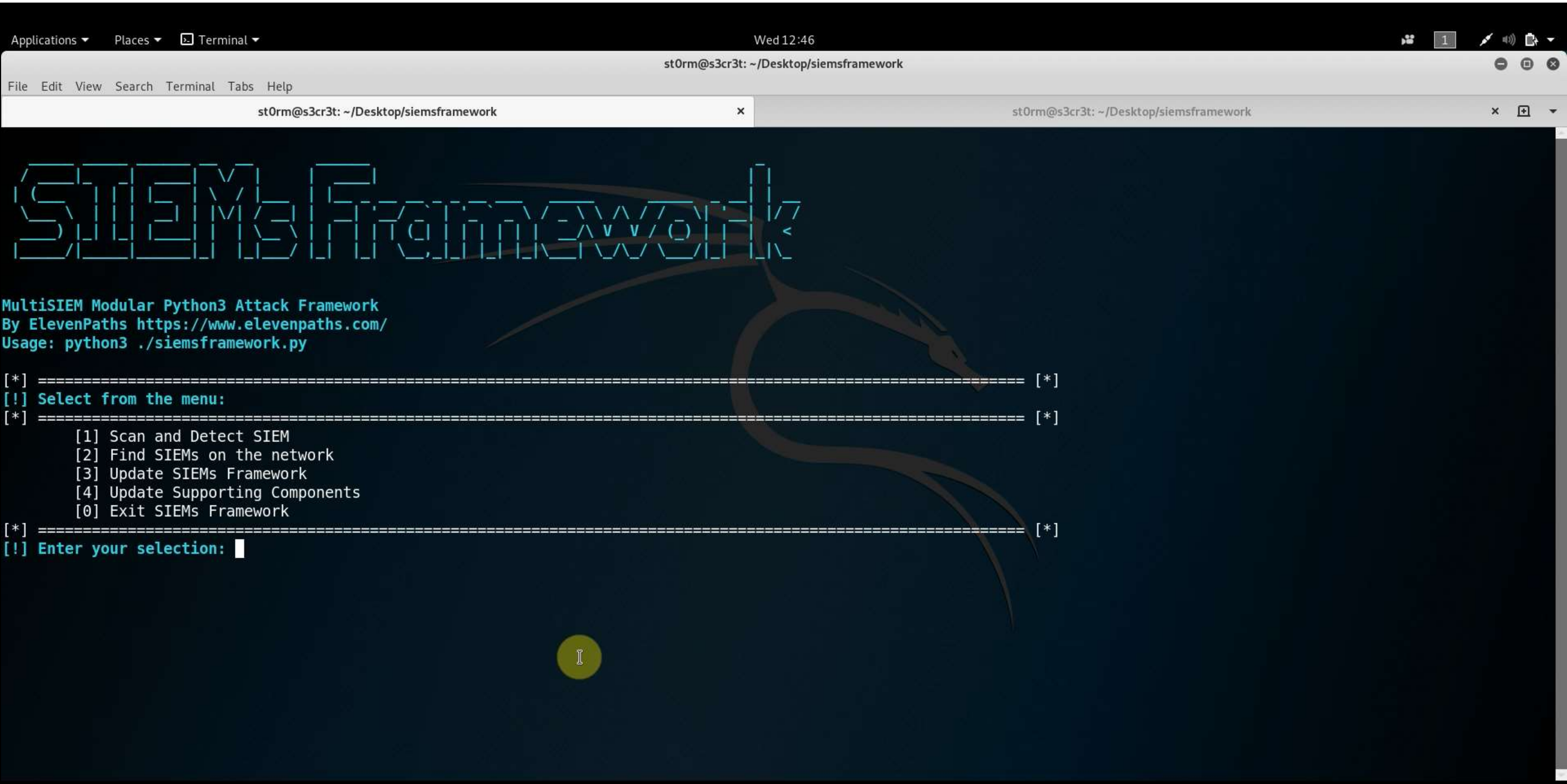


```
MultiSIEM Modular Python3 Attack Framework
By ElevenPaths https://www.elevenpaths.com/
Usage: python3 ./siemsframework.py

[*] ========================================================================================================== [*]
[!] Select from the menu:
[*] ========================================================================================================== [*]
        [1] Scan and Detect SIEM
        [2] Find SIEMs on the network
        [3] Update SIEMs Framework
        [4] Update Supporting Components
        [0] Exit SIEMs Framework
[*] ========================================================================================================== [*]
[!] Enter your selection: 1
```

Eleven Paths

@ylevalle

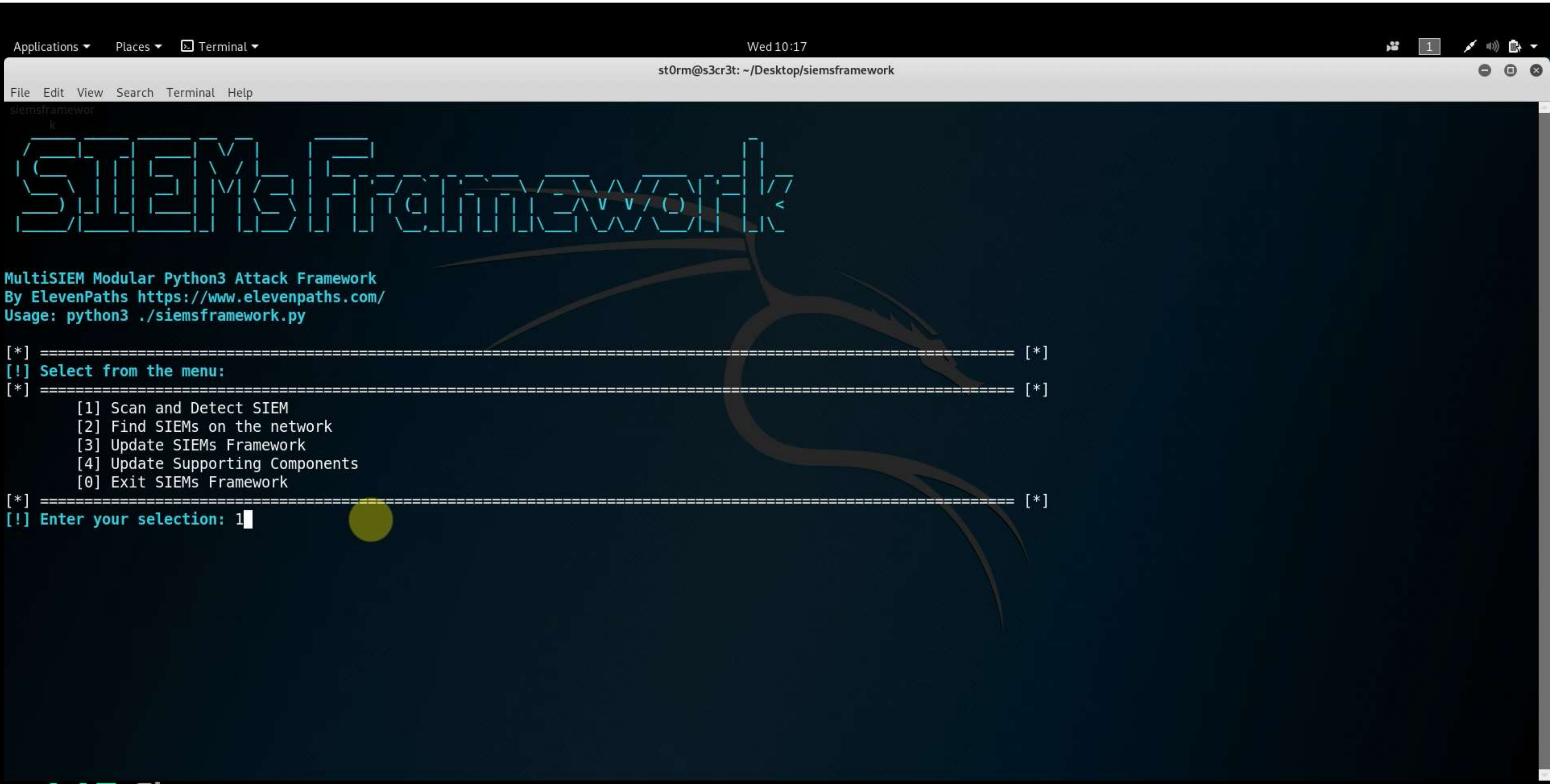

Applications
Places
Terminal
Wed 12:46
st0rm@s3cr3t: ~/Desktop/siemsframework
File Edit View Search Terminal Tabs Help
st0rm@s3cr3t: ~/Desktop/siemsframework
st0rm@s3cr3t: ~/Desktop/siemsframework

```
MultiSIEM Modular Python3 Attack Framework
By ElevenPaths https://www.elevenpaths.com/
Usage: python3 ./siemsframework.py

[*] ============================================================================================= [*]
[!] Select from the menu:
[*] ============================================================================================= [*]
       [1] Scan and Detect SIEM
       [2] Find SIEMs on the network
       [3] Update SIEMs Framework
       [4] Update Supporting Components
       [0] Exit SIEMs Framework
[*] ============================================================================================= [*]
[!] Enter your selection:
```

Eleven Paths

@ylevalle

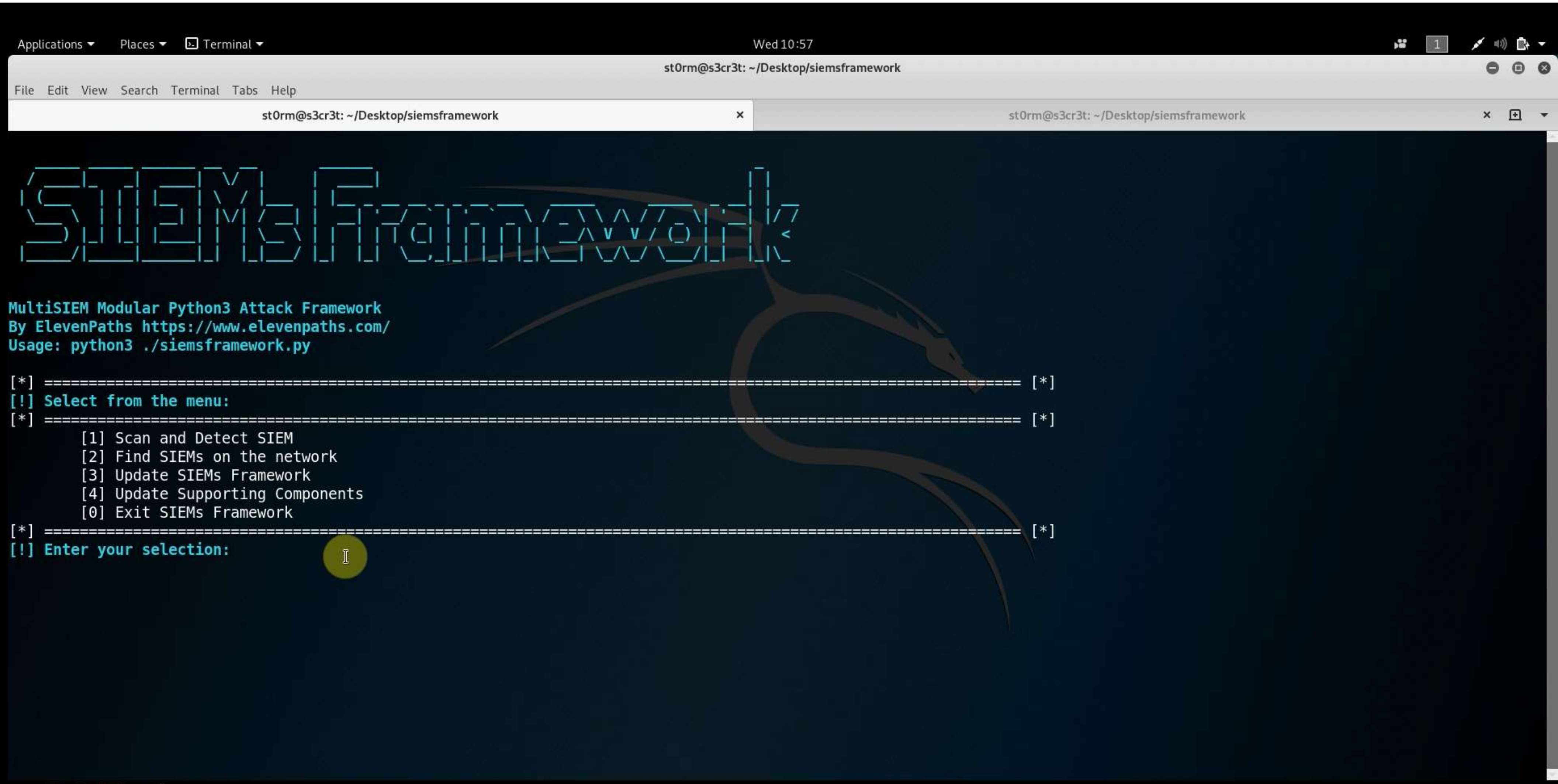


```
MultiSIEM Modular Python3 Attack Framework
By ElevenPaths https://www.elevenpaths.com/
Usage: python3 ./siemsframework.py

[*] ============================================================================================================== [*]
[!] Select from the menu:
[*] ============================================================================================================== [*]
        [1] Scan and Detect SIEM
        [2] Find SIEMs on the network
        [3] Update SIEMs Framework
        [4] Update Supporting Components
        [0] Exit SIEMs Framework
[*] ============================================================================================================== [*]
[!] Enter your selection: 1
```

Eleven Paths

@ylevalle


Applications
Places
Terminal
Wed 10:57
st0rm@s3cr3t: ~/Desktop/siemsframework
File
Edit
View
Search
Terminal
Tabs
Help
st0rm@s3cr3t: ~/Desktop/siemsframework
st0rm@s3cr3t: ~/Desktop/siemsframework
SIEMs Framework

```
MultiSIEM Modular Python3 Attack Framework
By ElevenPaths https://www.elevenpaths.com/
Usage: python3 ./siemsframework.py

[*] ========================================================================================== [*]
[!] Select from the menu:
[*] ========================================================================================== [*]
        [1] Scan and Detect SIEM
        [2] Find SIEMs on the network
        [3] Update SIEMs Framework
        [4] Update Supporting Components
        [0] Exit SIEMs Framework
[*] ========================================================================================== [*]
[!] Enter your selection:
```

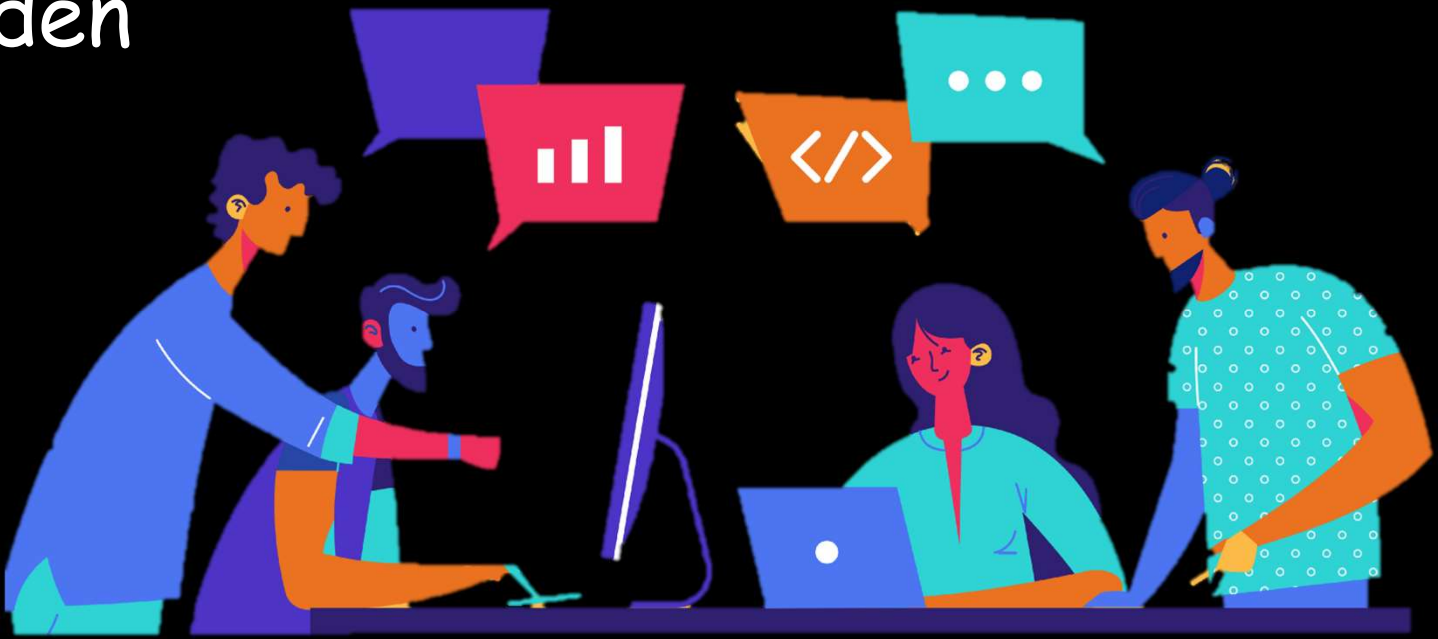
Eleven
Paths

@ylevalle

Próximos Pasos

- Agregar paquetes para más SIEMs: McAfee, SIEMonster, ElasticSIEM
- Agregar Módulo para Graylog Reverse Shell desde un Alarm Callback
- Agregar Módulo para Análisis de Inputs en Graylog para obtener más credenciales
- Agregar módulo para Splunk Vmware OVA
- Agregar escaneo y detección de SIEMs en puertos no default
- Continuar el research y descubrir nuevos vectores de ataque

Gracias! Y pueden contribuir <3



Eleven Paths

CySec by Women

https://github.com/ElevenPaths/siemframework