🚧

Test d’intrusion

En attente d’une réponse d’autorisation de test sur le serveur OVH, les test seront menés sur une même version du site mais hébergée sur le NAS.
Les test effectués seront :

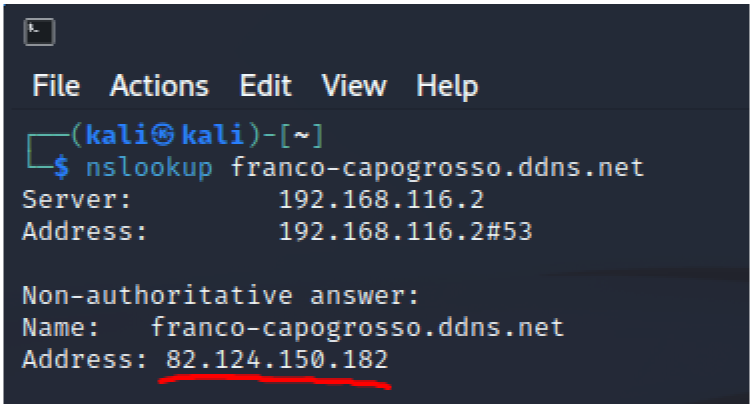
- Analyse de la configuration du serveur avec Nessus
- Analyse du site web avec Zaproxy
- Tentative d’injection SQL avec Sqlmap (se référer à la documentation d’Helmi)

<u>Analyse Nessus</u>

Nessus est un outil qui permet de scanner un serveur à la recherche de vulnérabilités (Ports ouverts, version des framework installés …).

Il nous faut tout d’abord l’IP du serveur, pour la trouver on va utiliser l’outil de résolution de DNS, nslookup

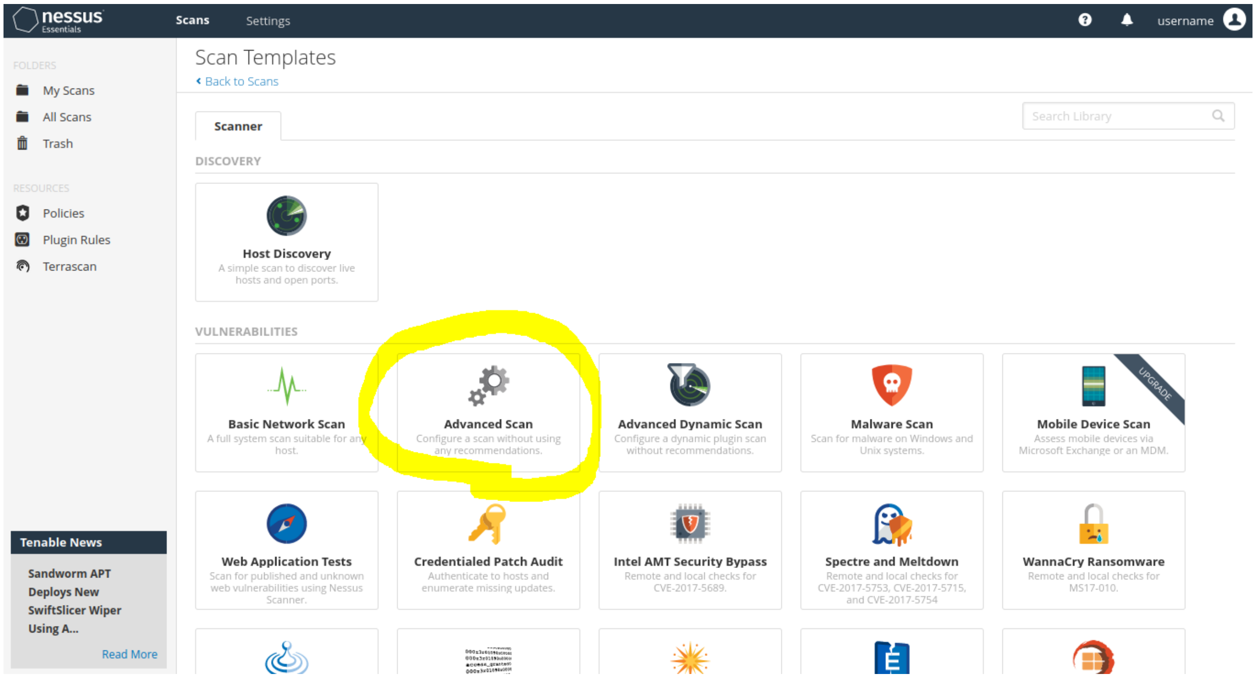
```
nslookup franco-capogrosso.ddns.net
```

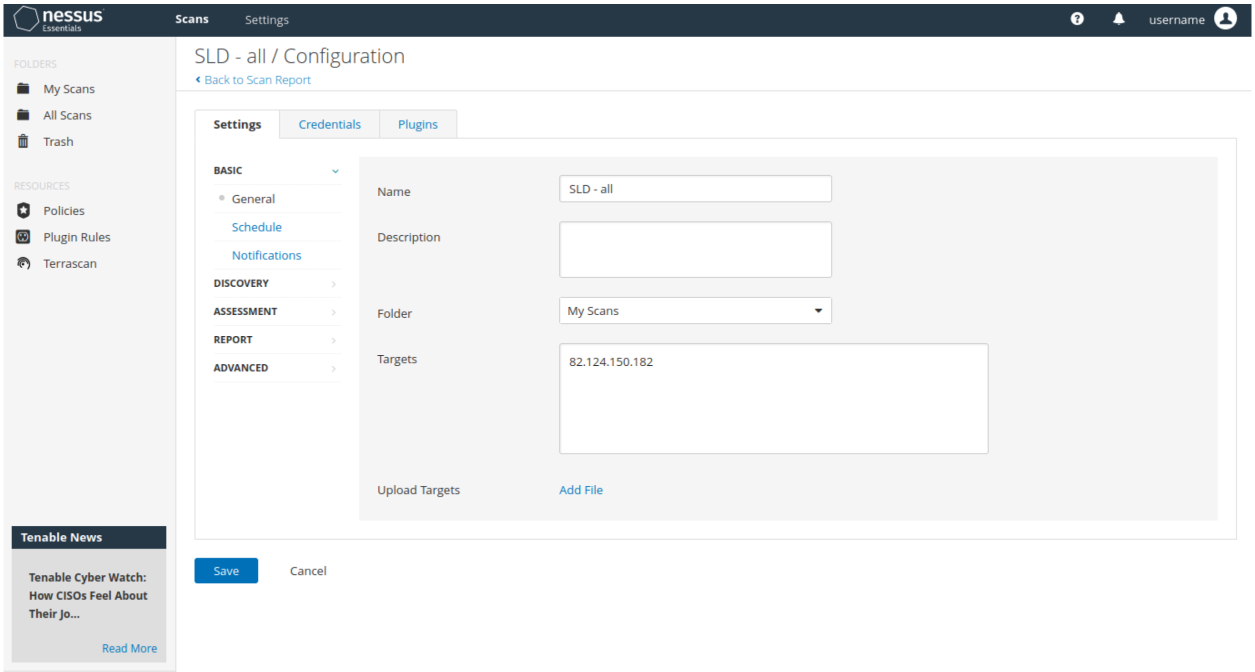


```
┌──(kali㉿kali)-[~]
└─$ nslookup franco-capogrosso.ddns.net
Server:         192.168.116.2
Address:        192.168.116.2#53

Non-authoritative answer:
Name:   franco-capogrosso.ddns.net
Address: 82.124.150.182
```

On va maintenant créer un scan “Avancé” pour que Nessus analyse le plus d’éléments possible


nessus Essentials
Scans
Settings
username
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Terrascan
Tenable News
Sandworm APT Deploys New SwiftSlicer Wiper Using A...
Read More
Scan Templates
Back to Scans
Scanner
Search Library
DISCOVERY
Host Discovery
A simple scan to discover live hosts and open ports.
VULNERABILITIES
Basic Network Scan
A full system scan suitable for any host.
Advanced Scan
Configure a scan without using any recommendations.
Advanced Dynamic Scan
Configure a dynamic plugin scan without recommendations.
Malware Scan
Scan for malware on Windows and Unix systems.
Mobile Device Scan
Assess mobile devices via Microsoft Exchange or an MDM.
UPGRADE
Web Application Tests
Scan for published and unknown web vulnerabilities using Nessus Scanner.
Credentialed Patch Audit
Authenticate to hosts and enumerate missing updates.
Intel AMT Security Bypass
Remote and local checks for CVE-2017-5689.
Spectre and Meltdown
Remote and local checks for CVE-2017-5753, CVE-2017-5715, and CVE-2017-5754
WannaCry Ransomware
Remote and local checks for MS17-010.



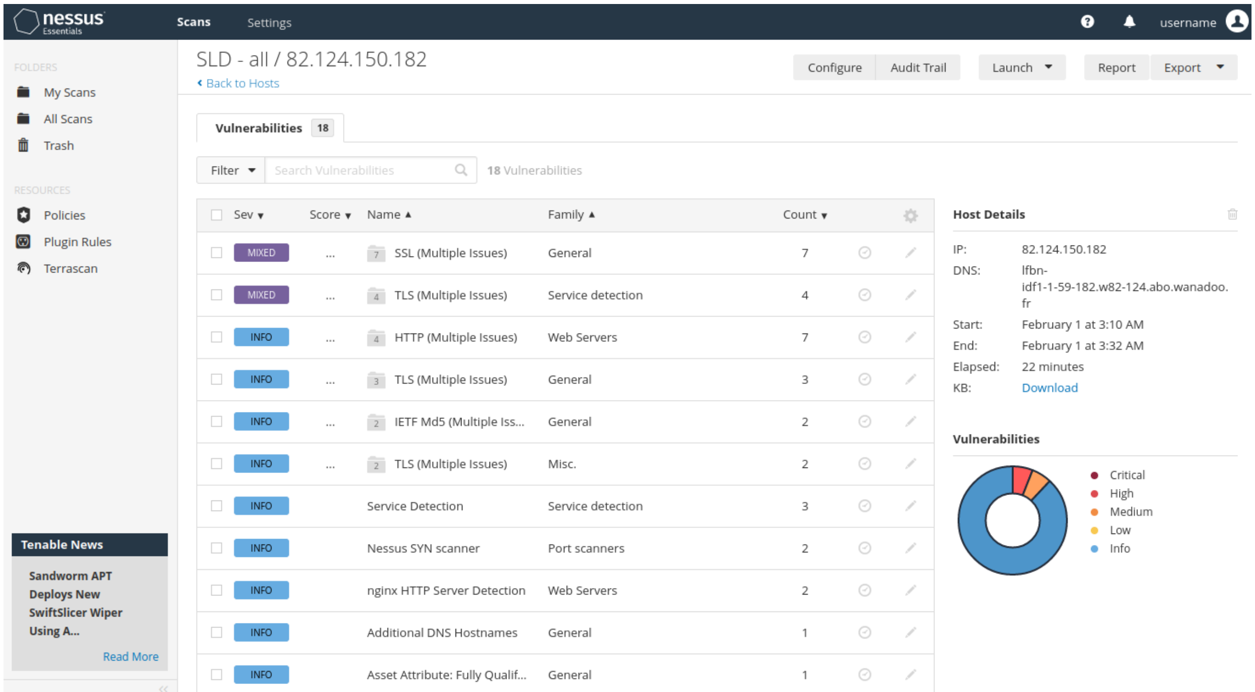
Name: SLD - all

Description:

Folder: My Scans

Targets: 82.124.150.182

Une fois ceci fait, on lance l’analyse et on patiente en attendant les résultats



SLD - all / 82.124.150.182

‹ Back to Hosts

18 Vulnerabilities

Sev	Score	Name	Family	Count
MIXED	...	7 SSL (Multiple Issues)	General	7
MIXED	...	4 TLS (Multiple Issues)	Service detection	4
INFO	...	4 HTTP (Multiple Issues)	Web Servers	7
INFO	...	3 TLS (Multiple Issues)	General	3
INFO	...	2 IETF Md5 (Multiple Iss...	General	2
INFO	...	2 TLS (Multiple Issues)	Misc.	2
INFO		Service Detection	Service detection	3
INFO		Nessus SYN scanner	Port scanners	2
INFO		nginx HTTP Server Detection	Web Servers	2
INFO		Additional DNS Hostnames	General	1
INFO		Asset Attribute: Fully Qualif...	General	1

Host Details

IP:	82.124.150.182
DNS:	lfbn-idf1-1-59-182.w82-124.abo.wanadoo.fr
Start:	February 1 at 3:10 AM
End:	February 1 at 3:32 AM
Elapsed:	22 minutes
KB:	Download

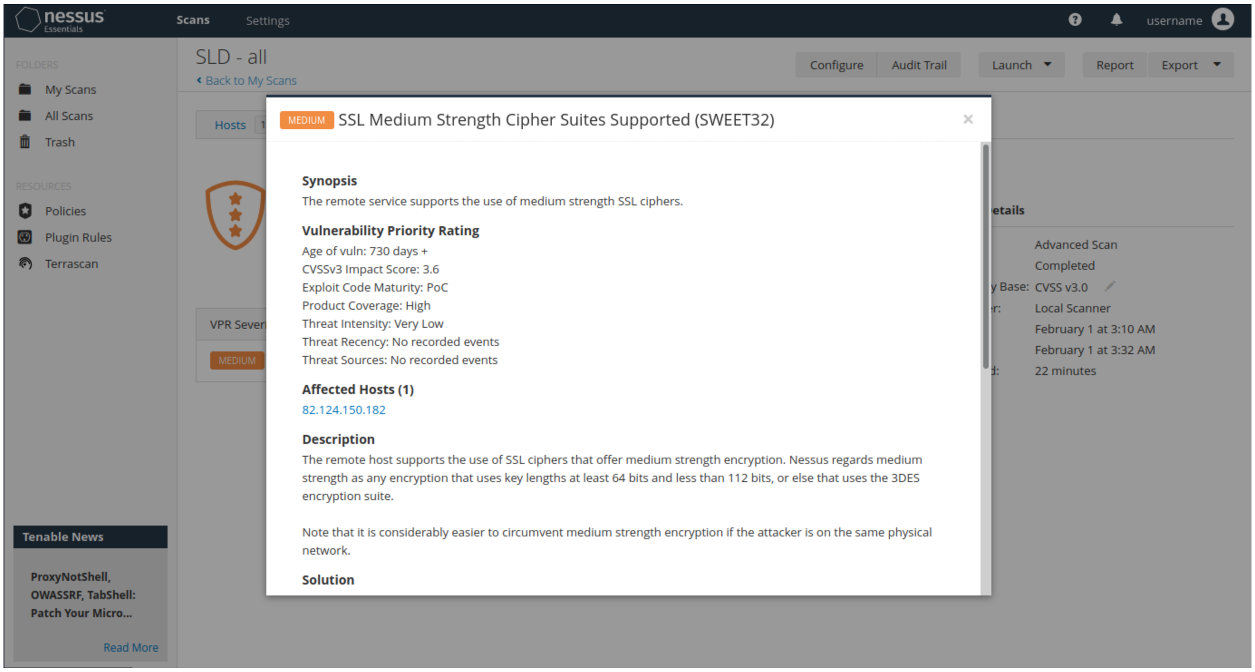
Vulnerabilities

Tenable News

Sandworm APT Deploys New SwiftSlicer Wiper Using A...

Read More

Ici, sans surprises étant donné que l’on a scanné un Serveur NAS Synology déjà sécurisé, il n’y a pas de faille majeure repérée.



SLD - all

‹ Back to My Scans

MEDIUM SSL Medium Strength Cipher Suites Supported (SWEET32)

Synopsis

The remote service supports the use of medium strength SSL ciphers.

Vulnerability Priority Rating

Age of vuln: 730 days +
CVSSv3 Impact Score: 3.6
Exploit Code Maturity: PoC
Product Coverage: High
Threat Intensity: Very Low
Threat Recency: No recorded events
Threat Sources: No recorded events

Affected Hosts (1)

82.124.150.182

Description

The remote host supports the use of SSL ciphers that offer medium strength encryption. Nessus regards medium strength as any encryption that uses key lengths at least 64 bits and less than 112 bits, or else that uses the 3DES encryption suite.

Note that it is considerably easier to circumvent medium strength encryption if the attacker is on the same physical network.

Solution

etails

Advanced Scan
Completed
y Base: CVSS v3.0
r: Local Scanner
February 1 at 3:10 AM
February 1 at 3:32 AM
d: 22 minutes

Tenable News

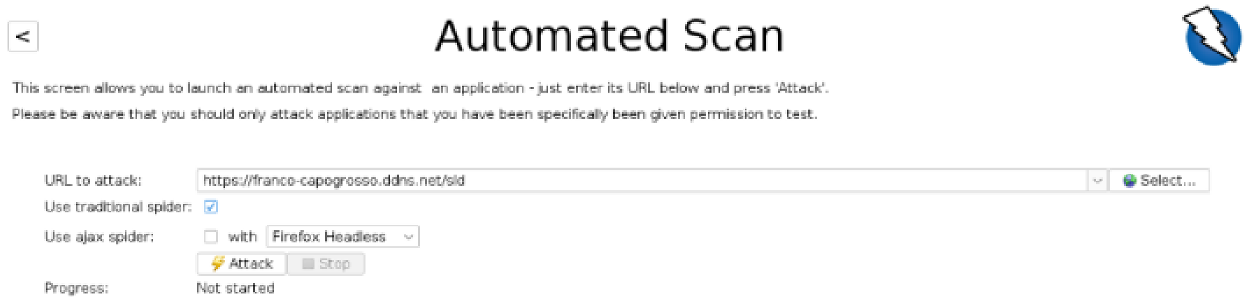
ProxyNotShell, OWASSRF, TabShell: Patch Your Micro...

Read More

Le plus gros problème trouvé par Nessus est la force de chiffrement de la clé SSL, ce qui n’est rien de grave.

Analyse Zaproxy

Zaproxy est un outil qui permet l’analyse du code source d’un site web dans le but d’y trouver des vulnérabilités.

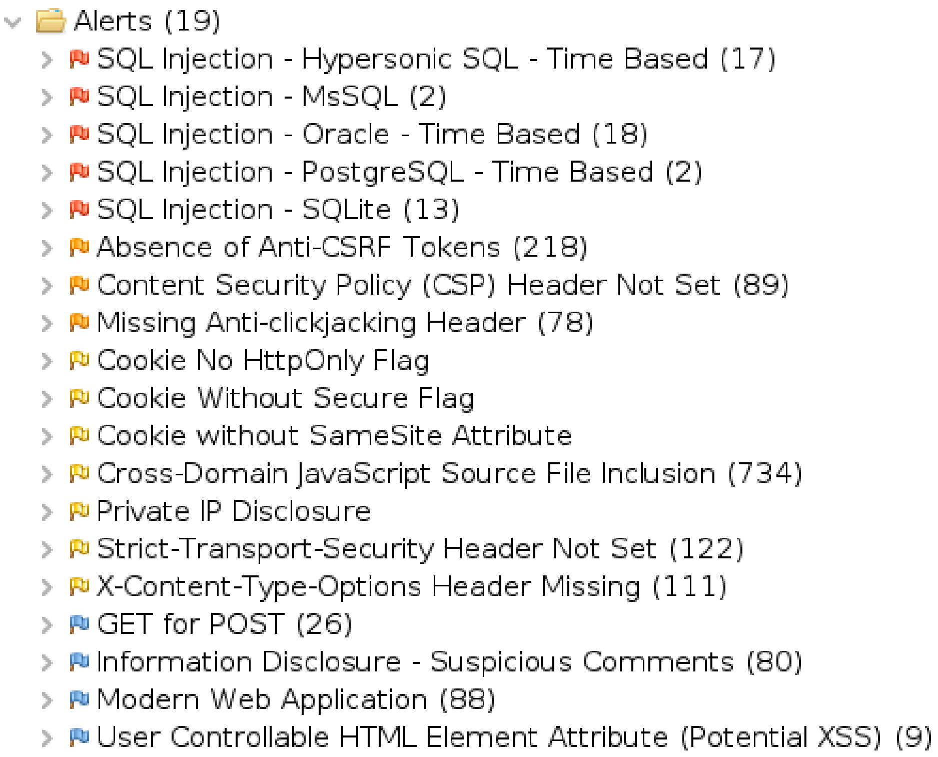


Automated Scan

This screen allows you to launch an automated scan against an application - just enter its URL below and press 'Attack'.
Please be aware that you should only attack applications that you have been specifically been given permission to test.

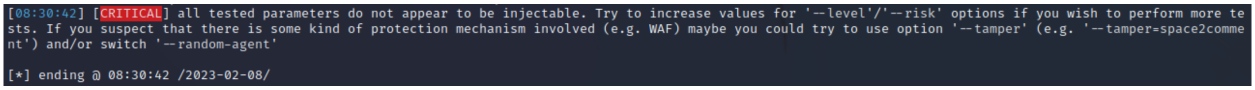
URL to attack: https://franco-capogrosso.ddns.net/sld
Use traditional spider: ☑
Use ajax spider: □ with Firefox Headless
Progress: Not started

Une fois le scan lancé, voici les résultats :



```
Alerts (19)
  SQL Injection - Hypersonic SQL - Time Based (17)
  SQL Injection - MsSQL (2)
  SQL Injection - Oracle - Time Based (18)
  SQL Injection - PostgreSQL - Time Based (2)
  SQL Injection - SQLite (13)
  Absence of Anti-CSRF Tokens (218)
  Content Security Policy (CSP) Header Not Set (89)
  Missing Anti-clickjacking Header (78)
  Cookie No HttpOnly Flag
  Cookie Without Secure Flag
  Cookie without SameSite Attribute
  Cross-Domain JavaScript Source File Inclusion (734)
  Private IP Disclosure
  Strict-Transport-Security Header Not Set (122)
  X-Content-Type-Options Header Missing (111)
  GET for POST (26)
  Information Disclosure - Suspicious Comments (80)
  Modern Web Application (88)
  User Controllable HTML Element Attribute (Potential XSS) (9)
```

Les alertes ici sont des potentielles vulnérabilités, rien de confirmé. Nous allons donc tenter d’effectuer des injections SQL sur les pages concernées.



```
[08:30:42] [CRITICAL] all tested parameters do not appear to be injectable. Try to increase values for '--level'/'--risk' options if you wish to perform more te
sts. If you suspect that there is some kind of protection mechanism involved (e.g. WAF) maybe you could try to use option '--tamper' (e.g. '--tamper=space2comme
nt') and/or switch '--random-agent'

[*] ending @ 08:30:42 /2023-02-08/
```

Après des test effectués avec SQLmap on observe qu’aucun des champs n’est réellement vulnérable à une injection SQL.

Pour ce qui est des autres alertes signalées par Zaproxy il s’agit de conventions de code qui ne sont pas respectées pour la plupart. Il n’y a rien d’inquiétant.