Tâche 7 Utilisation de scanneurs de vulnérabilité (13,5 points)

Liste des personnes impliquées avec pourcentage de répartition	
Etienne PAQUELET (100%)	25h-homme

Estimation du temps passé sur cette tâche en heure-homme :

Objectif : Réaliser plusieurs évaluations de la sécurité des serveurs

Sous-tâches	Evaluation prof
Installez dans la DMZ une machine/VM metasploitable	
Installez et utilisez SCNR	
Installez et utilisez Legion	
Installez et utilisez Nuclei	
Installez et utilisez Nikto	
Placez les scanners dans la DMZ, puis à l'extérieur	

Rapport

(Expliquez votre démarche, captures d'écrans des installations, listez le résultat des scans, etc.)

Legion : Ce scanner ne m'a pas posé problème, il a été simple d'utilisation puisqu'il est présent nativement dans kali. Il scan les vulnérabilités des services ainsi que les ports de la machine ciblée.

Son utilisation ressemble fortement à celle de nmap puisque son interface graphique ressemble à celle de zenmap.

Nuclei : Aucun problème d'utilisation ni d'installation.
Son utilisation est simpliste : *nuclei -u [host targetted]*

Il réalise plus particulièrement les analyses web mais scan également les vulnérabilités/failles de la machine.

Nikto : Présent également nativement dans kali, il ne m'a pas posé de problèmes pour son utilisation. Son utilisation est également simple *: nikto -host [host targetted]*

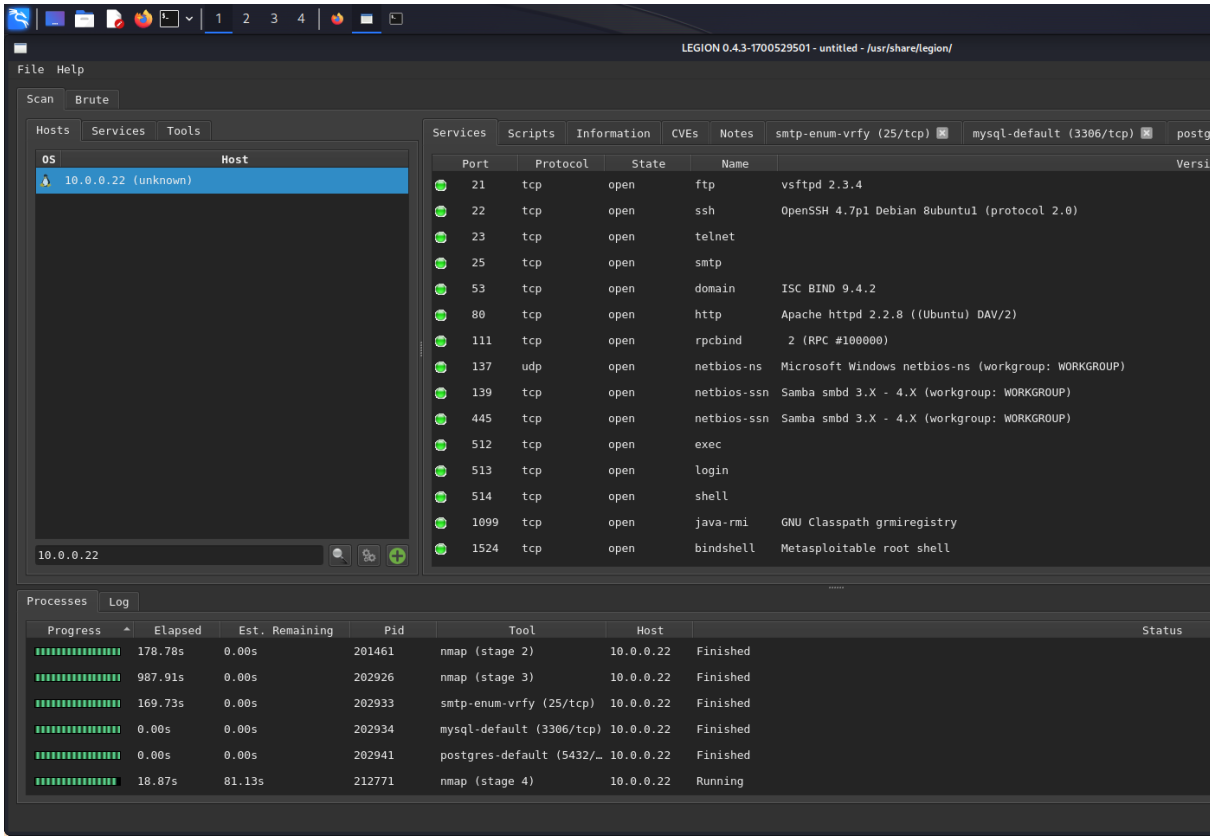
Nikto réalise principalement les scans web et XSS (Cross Site Scripting). Il m'a résumé les failles et informations qu'il a trouvé sur la cible.

SCNR : Ce scanner a été quelque peu plus problématique au niveau de l'installation. J'ai du crée une nouvelle VM Kali puisqu'il refusait de s'installer sur la première VM Kali. De plus, j'ai utilisé un script fourni sur github afin de l'installer plus facilement que montré sur le site officiel.

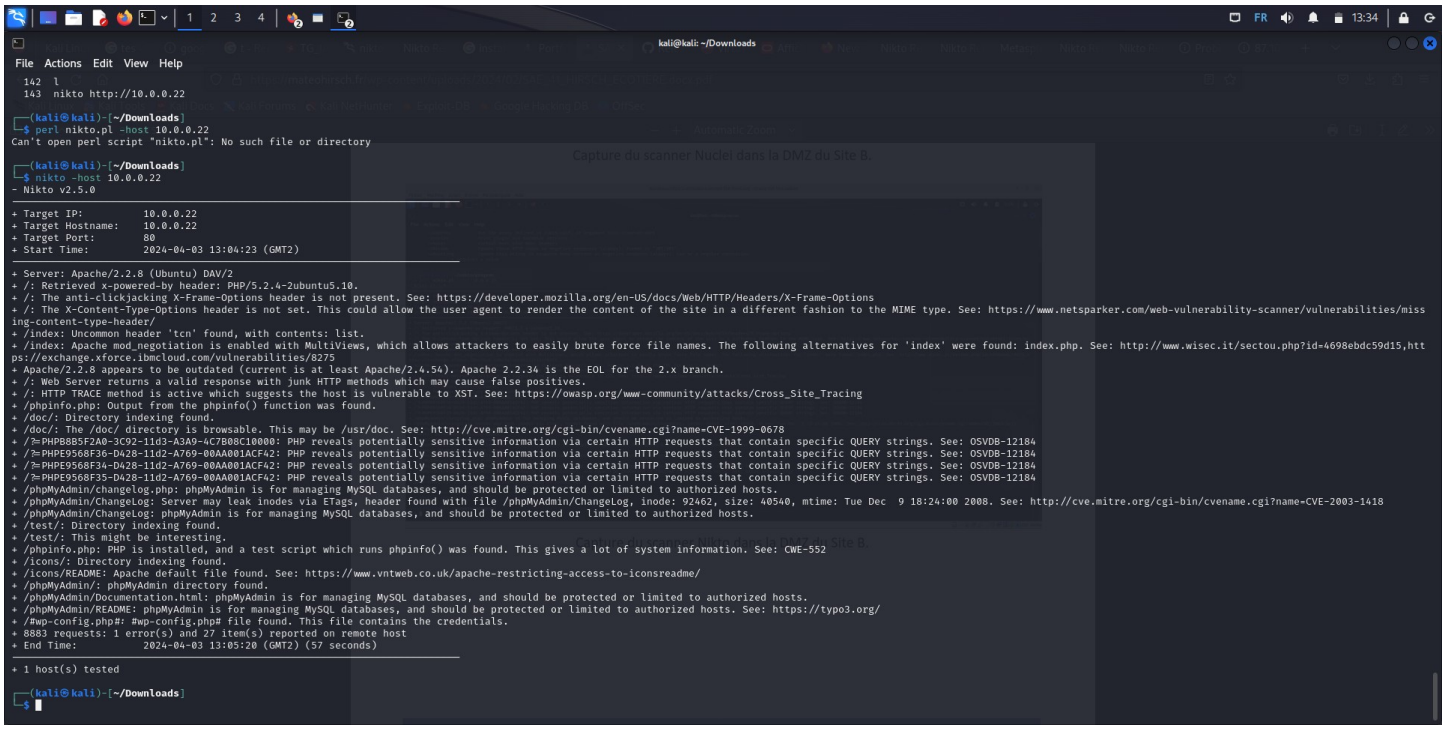
Son utilisation est plutôt simple : *./scnr-v4.1/bin/scnr [host targetted]*

Cependant, vu que cet outil est très « curieux », il scan chaque page et ainsi, le scan est long (22 heures environ pour le scan interne et externe), mais fournit beaucoup d'information sur chaque vulnérabilité découverte sur la machine cible dans le rapport.

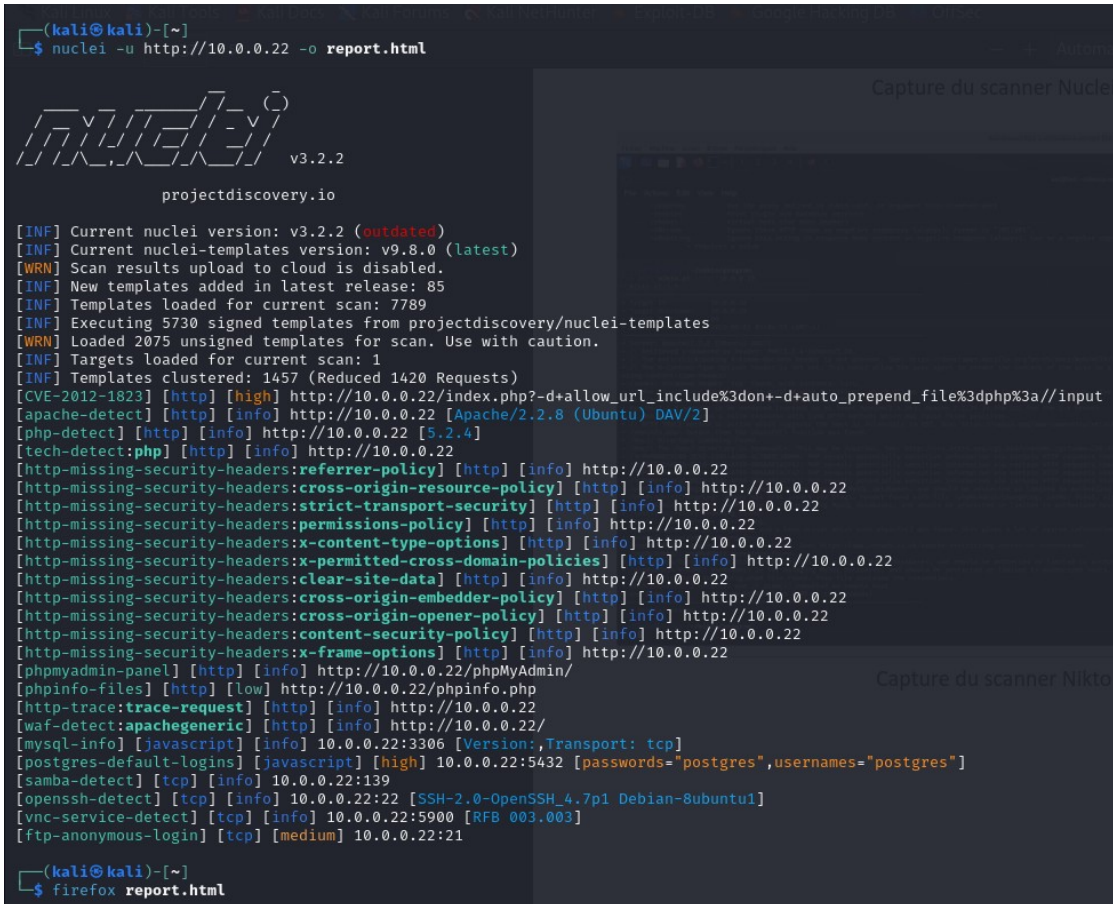
J'ai tout d'abord configuré la VM Metasploitable en bridge sur l'interface DMZ du pare feu A. Puis, j'ai effectué un scan interne en utilisant les scanner Legion, Nuclei, Nikto et Codename SCNR. Il n'y a pas eu trop de difficulté à installer ces outils hormis pour SCNR. Ensuite, j'ai scanné cette même machine depuis l'extérieur du réseau, c'est à dire, depuis « internet ». J'ai pu remarqué qu'il y avait une différence entre le scan interne et externe. Cela peut s'expliquer par le pare feu qui bloque et ou ralentit via le filtrage certains scans depuis l'extérieur. Ce pare feu rend les attaques plus difficiles pour les attaquants vu que via le filtrage, les recherches lors de la phase d'énumération sont ralenties.



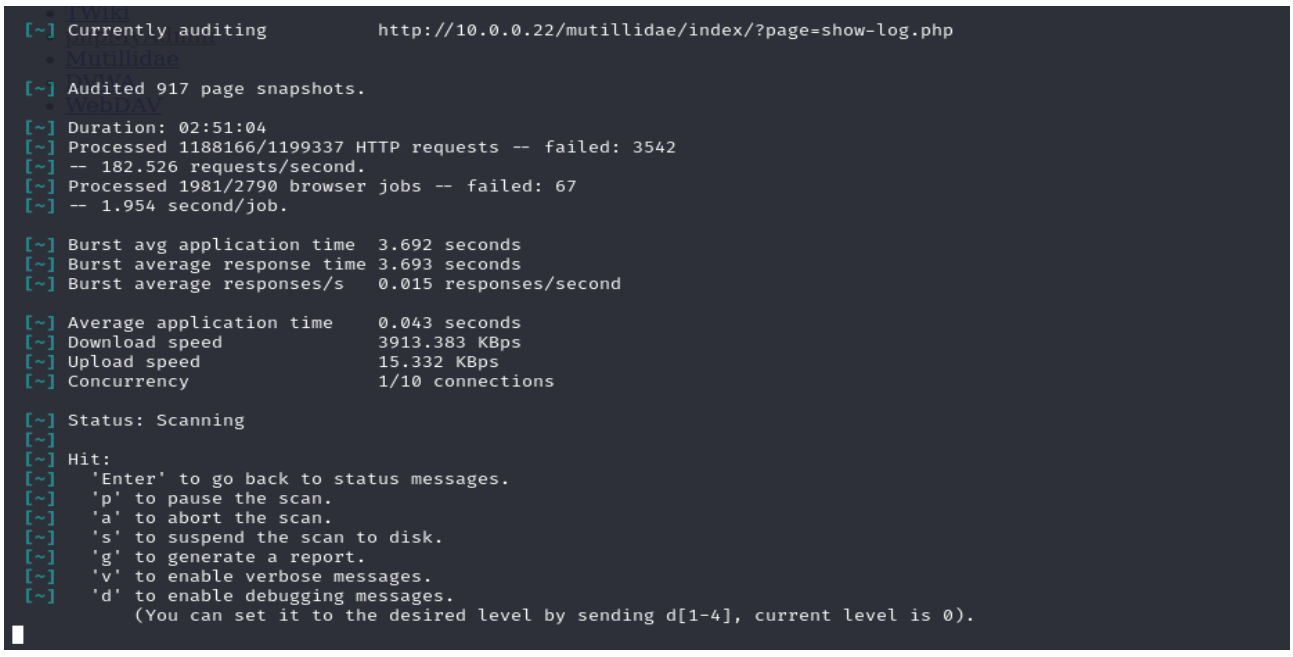
Scan Legion dans la DMZ



Scan Nikto dans la DMZ



Scan nuclei dans la DMZ



Scan SCNR dans la DMZ.

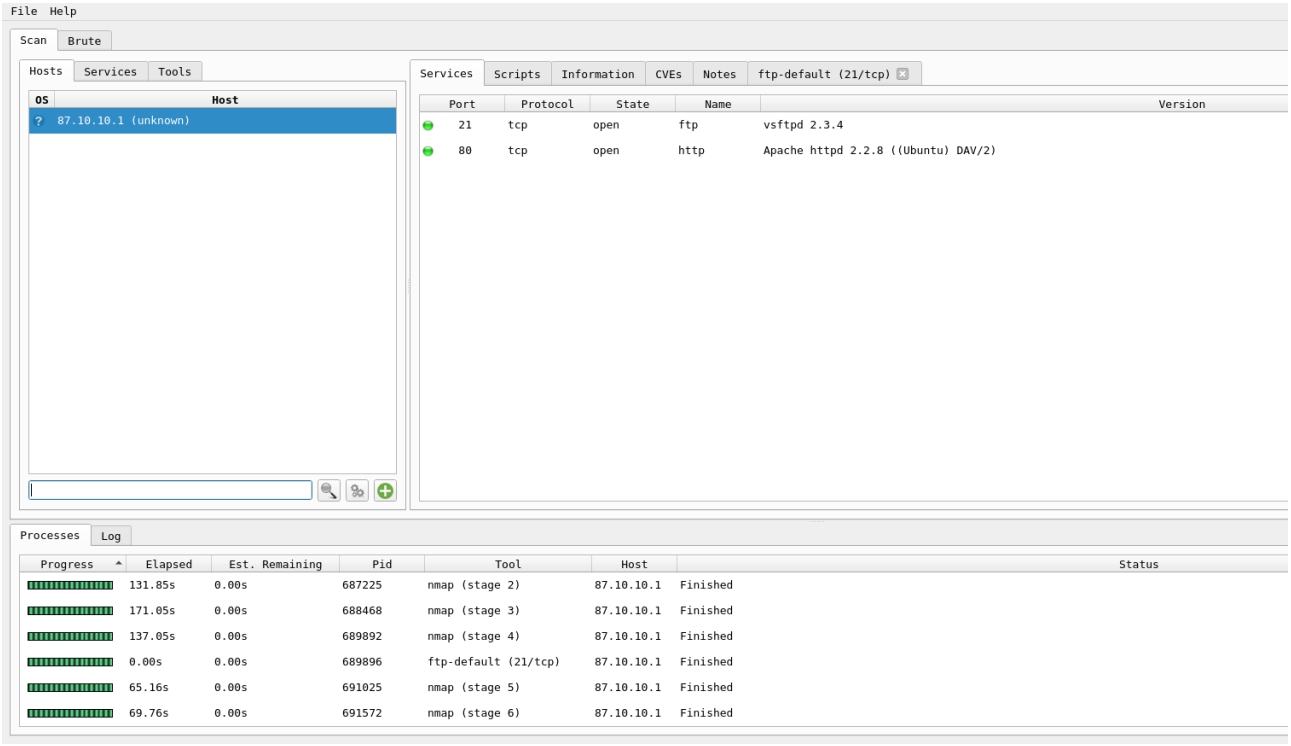
Scan externe sur http://87.10.10.1

```
┌──(kali㉿kali)-[~/Downloads]
└─$ nuclei -u http://87.10.10.1 -o report.html

                     __     _
   ____  __  _______/ /__  (_)
  / __ \/ / / / ___/ / _ \/ /
 / / / / /_/ / /__/ /  __/ /
/_/ /_/\__,_/\___/_/\___/_/   v3.2.2

                projectdiscovery.io

[INF] Current nuclei version: v3.2.2 (outdated)
[INF] Current nuclei-templates version: v9.8.0 (latest)
[WRN] Scan results upload to cloud is disabled.
[INF] New templates added in latest release: 85
[INF] Templates loaded for current scan: 7789
[INF] Executing 5730 signed templates from projectdiscovery/nuclei-templates
[WRN] Loaded 2075 unsigned templates for scan. Use with caution.
[INF] Targets loaded for current scan: 1
[INF] Templates clustered: 1457 (Reduced 1420 Requests)
[CVE-2012-1823] [http] [high] http://87.10.10.1/index.php?-d+allow_url_include%3don+-d+auto_prepend_file%3dphp%3a//input
[apache-detect] [http] [info] http://87.10.10.1 [Apache/2.2.8 (Ubuntu) DAV/2]
[php-detect] [http] [info] http://87.10.10.1 [5.2.4]
[tech-detect:php] [http] [info] http://87.10.10.1
[http-missing-security-headers:permissions-policy] [http] [info] http://87.10.10.1
[http-missing-security-headers:x-frame-options] [http] [info] http://87.10.10.1
[http-missing-security-headers:x-permitted-cross-domain-policies] [http] [info] http://87.10.10.1
[http-missing-security-headers:referrer-policy] [http] [info] http://87.10.10.1
[http-missing-security-headers:clear-site-data] [http] [info] http://87.10.10.1
[http-missing-security-headers:cross-origin-embedder-policy] [http] [info] http://87.10.10.1
[http-missing-security-headers:cross-origin-opener-policy] [http] [info] http://87.10.10.1
[http-missing-security-headers:content-security-policy] [http] [info] http://87.10.10.1
[http-missing-security-headers:x-content-type-options] [http] [info] http://87.10.10.1
[http-missing-security-headers:cross-origin-resource-policy] [http] [info] http://87.10.10.1
[http-missing-security-headers:strict-transport-security] [http] [info] http://87.10.10.1
[phpmyadmin-panel] [http] [info] http://87.10.10.1/phpMyAdmin/
[phpinfo-files] [http] [low] http://87.10.10.1/phpinfo.php
[http-trace:trace-request] [http] [info] http://87.10.10.1
[waf-detect:apachegeneric] [http] [info] http://87.10.10.1/
[ftp-anonymous-login] [tcp] [medium] 87.10.10.1:21
```

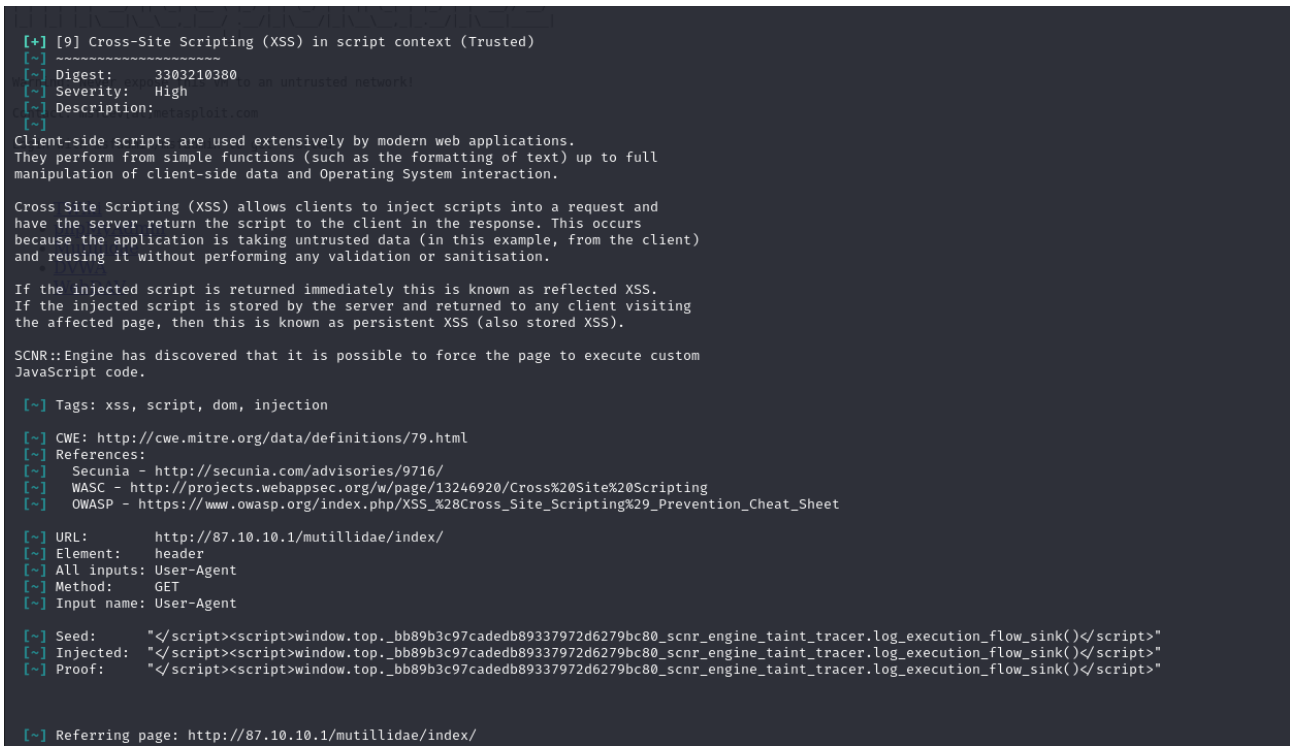
scan depuis « internet » avec Nuclei

```
┌──(kali㉿kali)-[~/Downloads]
└─$ nikto -host 87.10.10.1
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          87.10.10.1
+ Target Hostname:    87.10.10.1
+ Target Port:        80
+ Start Time:         2024-04-04 11:27:32 (GMT2)
---------------------------------------------------------------------------
+ Server: Apache/2.2.8 (Ubuntu) DAV/2
+ /: Retrieved x-powered-by header: PHP/5.2.4-2ubuntu5.10.
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ /index: Uncommon header 'tcn' found, with contents: list.
+ /index: Apache mod_negotiation is enabled with MultiViews, which allows attackers to easily brute force file names. The following alternatives for 'index' were found: index.php. See: http://www.wisec.it/sectou.php?id=4698ebdc59d15,https://exchange.xforce.ibmcloud.com/vulnerabilities/8275
+ Apache/2.2.8 appears to be outdated (current is at least Apache/2.4.54). Apache 2.2.34 is the EOL for the 2.x branch.
+ /: Web Server returns a valid response with junk HTTP methods which may cause false positives.
+ /: HTTP TRACE method is active which suggests the host is vulnerable to XST. See: https://owasp.org/www-community/attacks/Cross_Site_Tracing
+ /phpinfo.php: Output from the phpinfo() function was found.
+ /doc/: Directory indexing found.
+ /doc/: The /doc/ directory is browsable. This may be /usr/doc. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0678
+ /?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See: OSVDB-12184
+ /?=PHPE9568F36-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See: OSVDB-12184
+ /?=PHPE9568F34-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See: OSVDB-12184
+ /?=PHPE9568F35-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See: OSVDB-12184
+ /phpMyAdmin/changelog.php: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
+ /phpMyAdmin/ChangeLog: Server may leak inodes via ETags, header found with file /phpMyAdmin/ChangeLog, inode: 92462, size: 40540, mtime: Tue Dec  9 18:24:00 2008. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-1418
+ /phpMyAdmin/ChangeLog: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
+ /test/: Directory indexing found.
+ /test/: This might be interesting.
+ /phpinfo.php: PHP is installed, and a test script which runs phpinfo() was found. This gives a lot of system information. See: CWE-552
+ /icons/: Directory indexing found.
+ /icons/README: Apache default file found. See: https://www.vntweb.co.uk/apache-restricting-access-to-iconsreadme/
+ /phpMyAdmin/: phpMyAdmin directory found.
+ /phpMyAdmin/Documentation.html: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
+ /phpMyAdmin/README: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts. See: https://typo3.org/
+ /#wp-config.php#: #wp-config.php# file found. This file contains the credentials.
+ 8883 requests: 1 error(s) and 27 item(s) reported on remote host
+ End Time:           2024-04-04 11:28:36 (GMT2) (64 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested

┌──(kali㉿kali)-[~/Downloads]
```

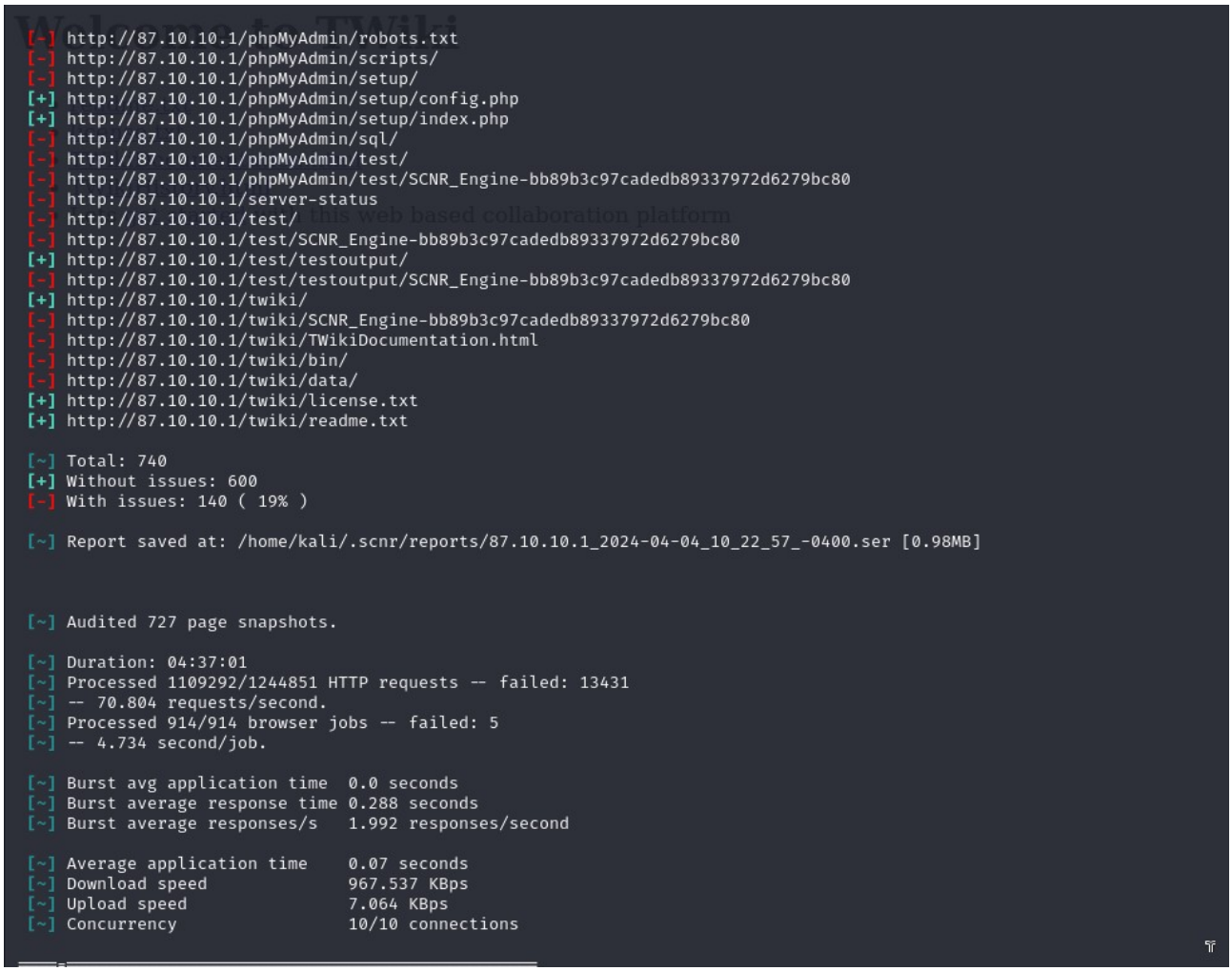
scan depuis « internet » avec Nikto



scan depuis « internet » avec Legion



Scan depuis « internet » avec Codename SCNR



Scan depuis « internet » avec Codename SCNR