YALCIN Lorenzo

CR :Exploitation d'une faille applicative via Metasploit

Q1. Expliquer ce qu'est Metasploit et comment il fonctionne.

Metasploit est un logiciel open-source de test de pénétration utilisé pour identifier et exploiter les vulnérabilités des systèmes informatiques dans le but de tester leur sécurité.
Metasploit scanne d'abord le réseau cible pour détecter les machines et services actifs. Il identifie ensuite les failles de sécurité potentielles en comparant les résultats avec sa base de données de vulnérabilités. L'utilisateur choisit un exploit approprié, configure les paramètres nécessaires comme l'adresse IP cible, puis lance l'attaque.

Q2. Rechercher ce que signifie les termes suivants : payload, exploit, backdoor

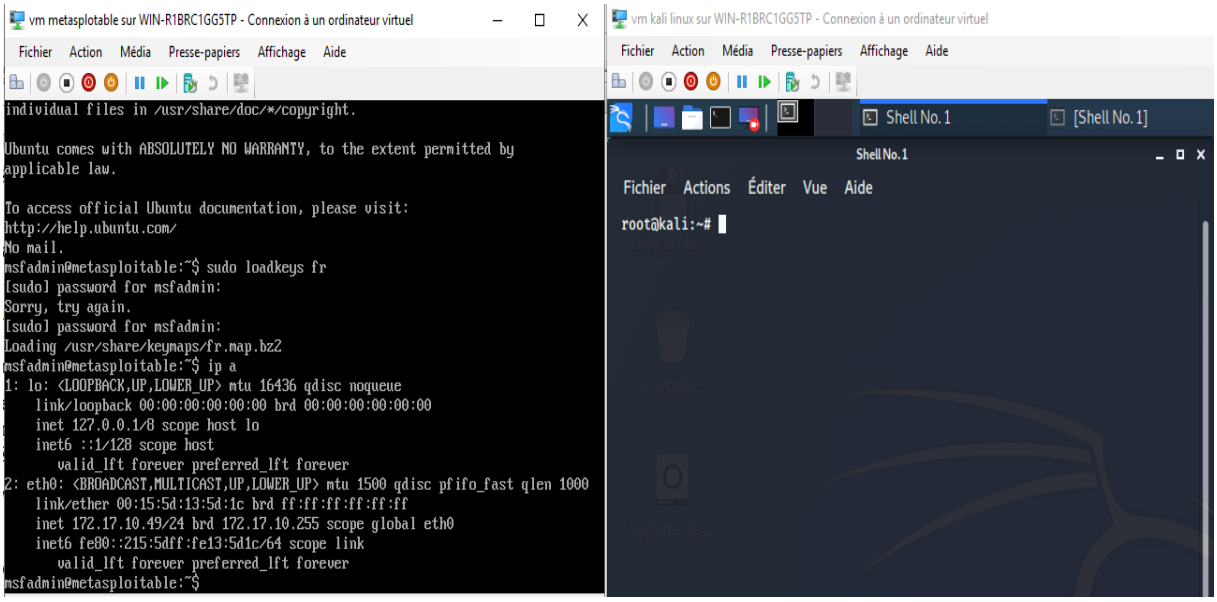
Payload : c'est un code malveillant qui s'exécute sur un système compromis après une attaque réussie. Il réalise l'action finale souhaitée par l'attaquant, comme ouvrir un accès distant, voler des données ou prendre le contrôle de la machine.

Exploit : ceci est un programme conçu pour profiter d'une faille de sécurité dans un logiciel ou un système. Il utilise cette vulnérabilité pour contourner les protections et exécuter des actions non autorisées, servant de passerelle pour délivrer le payload.

Backdoor : Mécanisme secret permettant d'accéder à un système en contournant les procédures d'authentification normales. Elle permet à un attaquant de maintenir un accès caché et persistant au système compromis sans être détecté.

Q3. Préparer votre environnement de travail en démarrant l'ensemble des machines du contexte.

Pour notre contexte nous aurons besoin d'un serveur metaspoitable linux et d'une machine debian kali :



Q4. Signification des variables RHOST et RPORT

RHOST (Remote Host) désigne l'a*dresse IP ou nom d'hôte de la machine cible à attaquer. C'est le système distant sur lequel l'exploit sera lancé. Exemple : RHOST=192.168.1.100*

RPORT (Remote Port) désigne le numéro du port réseau sur lequel le service vulnérable est en écoute sur la machine cible. Exemple : RPORT=21 pour un service FTP.

Ces deux variables définissent précisément la cible de l'attaque dans Metasploit.

Q5. A quoi sert la commande nmap ? Et l'option -A ?

Nmap est un outil de scan réseau qui permet de découvrir les machines actives, identifier les ports ouverts et détecter les services en cours d'exécution sur un réseau. Il est utilisé pour analyser la sécurité des systèmes informatiques. Ensuite l'option -A active le scan qui fournit un maximum d'informations sur la cible. Elle détecte automatiquement le système d'exploitation et les versions des services en une seule commande.

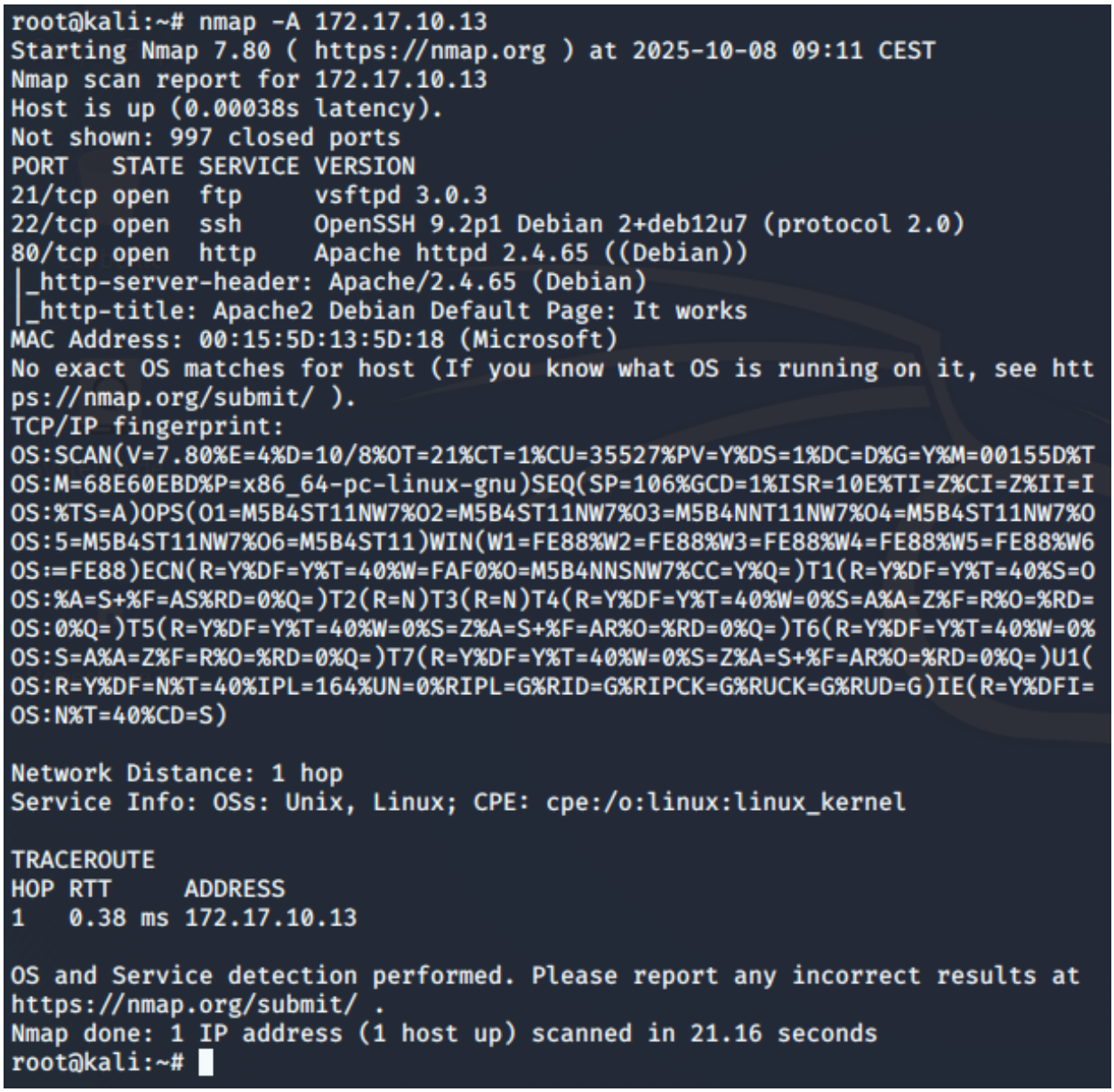
Q6. Expliquer le résultat de la commande nmap -A @IPDeVotreServeurMetasploitable

Elle a permis de scanner la machine 172.17.10.13 et de découvrir les services actifs (FTP, SSH, HTTP), leurs versions exactes, et de collecter des indices sur le système d'exploitation.

Q7. A l'aide des informations de l'exploit, expliquer quelle est la faille utilisée ?

La faille exploitée est une backdoor qui a été volontairement introduite dans l'archive de téléchargement du serveur ftp vsftpd version 2.3.4 entre le 30 juin et le 1er juillet 2011. Un attaquant avait compromis la version officielle du logiciel en y ajoutant du code malveillant.

Cette backdoor permet d'exécuter des commandes système à distance sur le serveur sans avoir besoin d'authentification, donnant ainsi un accès complet à la machine compromise. Il s'agit d'une faille d'exécution de commandes à distance (Remote Command Execution) particulièrement dangereuse car elle contourne totalement les mécanismes de sécurité. La backdoor a été retirée le 3 juillet 2011 après sa découverte.



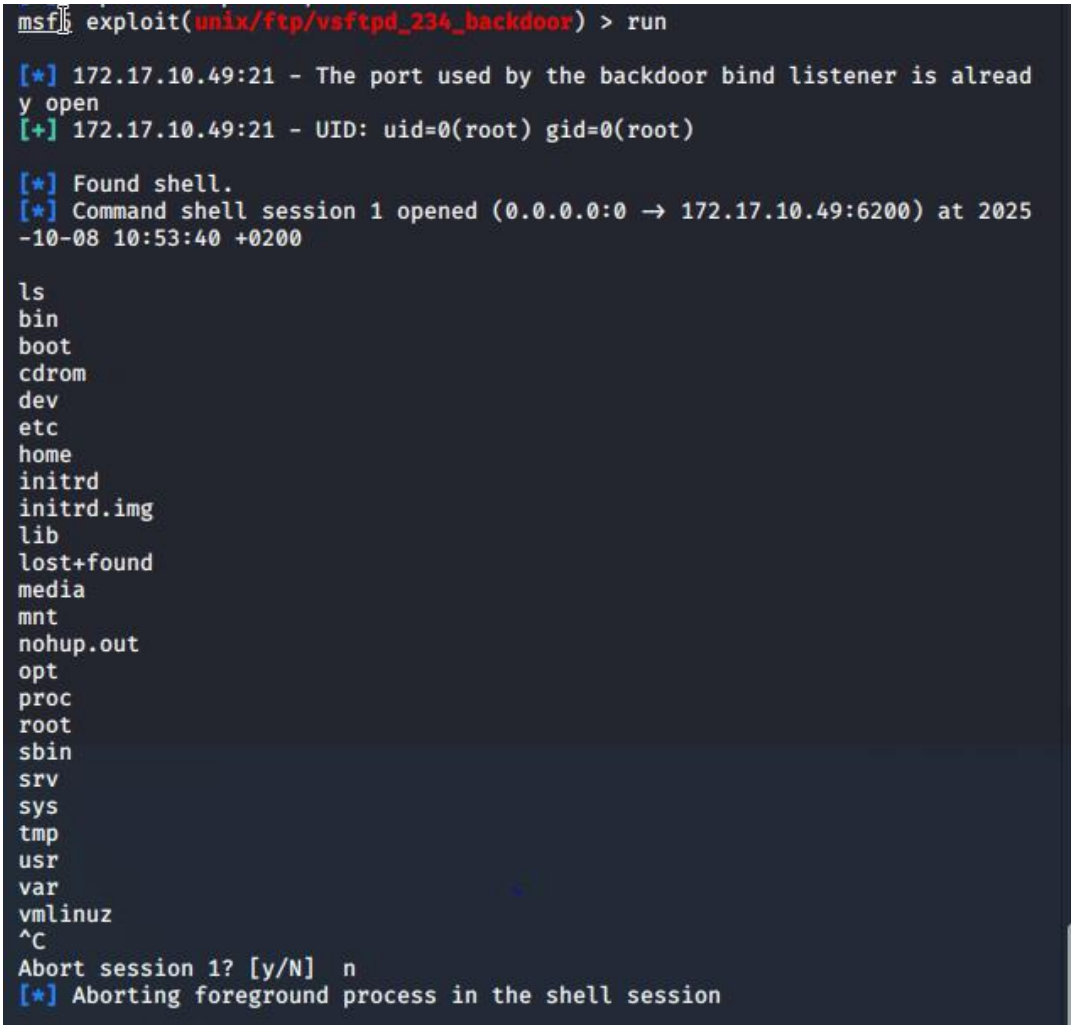
Sur un autre terminal lancer le programme Metasploit puis sélectionner l'exploit associé :

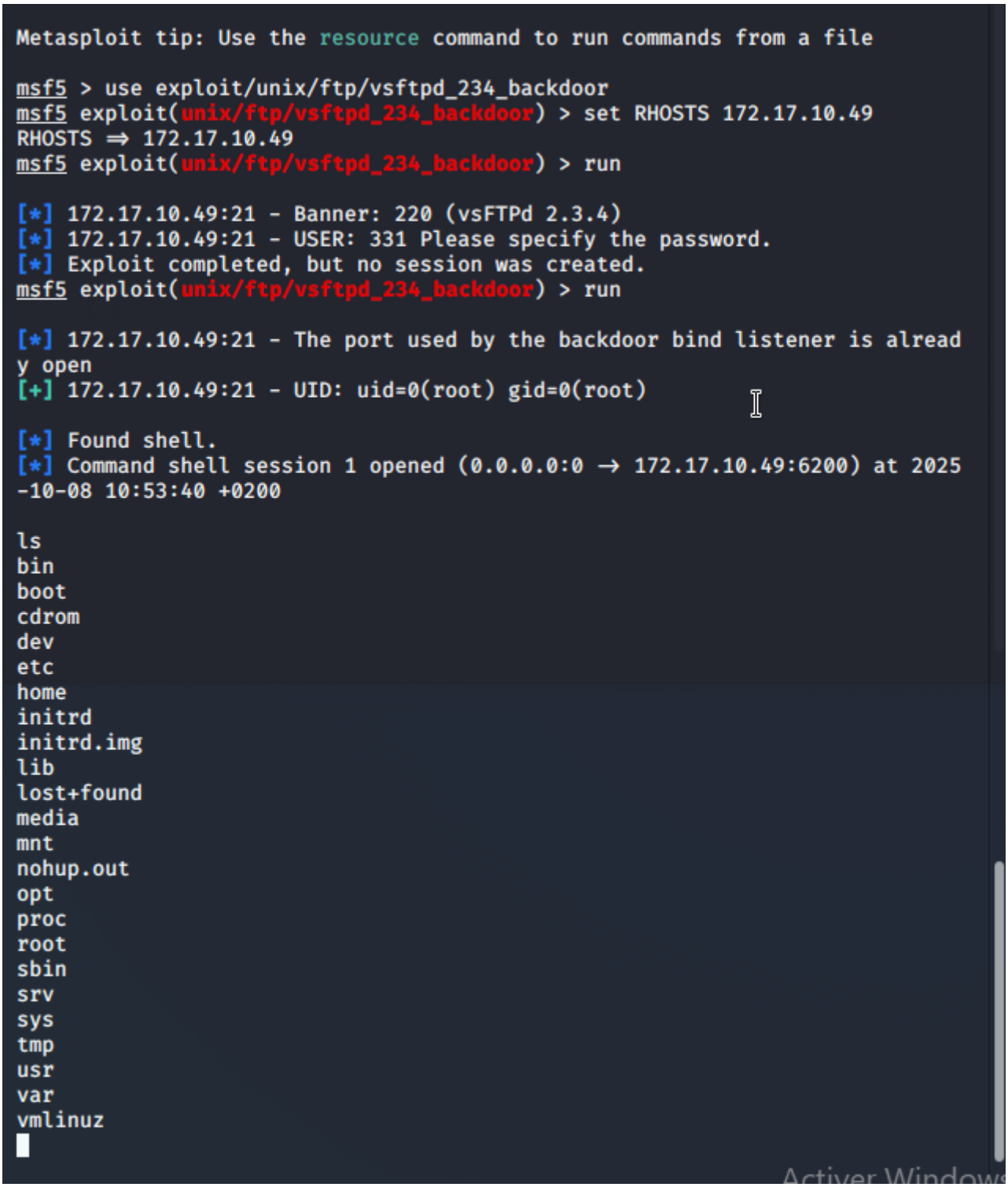
```
msf5 > use exploit/unix/ftp/vsftpd_234_backdoor
msf5 exploit(unix/ftp/vsftpd_234_backdoor) > show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS                   yes       The target host(s), range CIDR identi
fier, or hosts file with syntax 'file:<path>'
   RPORT   21               yes       The target port (TCP)


Exploit target:

   Id  Name
   --  ----
   0   Automatic
```

A la suite faire un « set RHOSTS 172.17.10.48 » donc de l'ip qu'on veut attaquer (machine metaspoitable dans notre cas) et faire un run pour appliquer la commande :

```
msf5 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 172.17.10.49
RHOSTS ⇒ 172.17.10.49
msf5 exploit(unix/ftp/vsftpd_234_backdoor) > run
```

Voici une vue d'ensemble de toutes les commandes appliqué et leurs utilités





1. Sélection et configuration de l'exploit :

Nous avons utilisé l'exploit : exploit/unix/ftp/vsftpd_234_backdoor qui cible la backdoor malveillante présente dans VSFTPD version 2.3.4 puis nous avons configuré la cible avec set RHOSTS 172.17.10.49 pour définir l'adresse IP du serveur cible.

2. Lancement de l'attaque :

En exécutant la commande run, Metasploit a lancé l'exploit contre le serveur FTP cible. L'exploit a réussi à identifier et activer la backdoor cachée dans le service VSFTPD.

3. Exploitation de la backdoor :

Le système indique que "le port utilisé par le backdoor bind listener est déjà ouvert" et qu'il a trouvé un shell. La backdoor a ouvert un port d'écoute (6200) permettant une connexion directe sans authentification. L'exploit a automatiquement livré le payload qui établit une session shell à distance.

4. Accès root obtenu :

Le message « UID: uid=0(root) gid=0(root) » confirme que vous avez obtenu un accès avec les privilèges root (administrateur) sur le système cible.

5. Contrôle total du système :

La liste des répertoires affichée (ls, bin, boot, etc, home, root, etc.) prouve que vous avez maintenant un shell de commande complet sur le serveur compromis et pouvez exécuter n'importe quelle commande système comme si vous étiez physiquement connecté en tant qu'administrateur.

En résumé :

L'exploit a activé la backdoor préexistante, qui a permis de délivrer le payload (shell distant), vous donnant un accès root complet au serveur vulnérable.

Q8. Consulter le site https://www.cvedetails.com et expliquer en quoi ce site peut être utile pour un analyste en cybersécurité.

Le site CVEDetails est une base données en ligne qui permet de répertoires pour toutes les vulnérabilités de sécurité informatiques connues, il permet pour un analyste en cybersécurité de pouvoir faire :
- des recherches et trouver rapidement des informations sur une faille de sécurité
- une évaluation de la gravité de la faille pour permettant de hiérarchiser les correctifs à appliquer en priorité
- un identification des exploits indique donc si des exploits publics ou des modules Metasploit existent pour exploiter la vulnérabilité
- une veille de sécurité donc se tenir informé de toutes les nouvelles vulnérabilité apparentes

Q9. Les développeurs peuvent-ils être concernés par une faille sur un serveur FTP ? Justifier.

Oui, les développeurs peuvent être concernés par une faille sur un serveur FTP, car elle peut entraîner le vol ou la modification de leur code source, l'exposition de données personnelles et sensibles ou l'altération de fichiers qu'ils transfèrent. Même s'ils ne gèrent pas le serveur, ils doivent utiliser des protocoles sécurisés comme SFTP ou FTPS pour protéger leurs échanges.

Q10.Conclure sur l'intérêt de disposer de logiciels mis à jour régulièrement dans le cadre du contexte étudié.

Disposer de logiciels régulièrement mis à jour est essentiel pour corriger les failles de sécurité, comme celles pouvant affecter un serveur FTP. Les mises à jour permettent de renforcer la protection des données, de prévenir les intrusions et d'assurer la stabilité et la fiabilité des outils utilisés par les développeurs. Cela permet en parallèle d'éviter des attaques ou intrusion inconnu.

Q11.A partir du moment où vous avez accès à un shell sur le serveur, quelle pourrait être la suite de l'attaque ?

Si un attaquant obtient un shell sur le serveur, il peut chercher à élever ses privilèges, établir une persistance, se déplacer dans le réseau et extraire du code, des fichiers de configuration ou des secrets. Les conséquences possibles sont le vol ou l'altération du code source, la compromission de données sensibles, l'impact sur la disponibilité des services et des coûts importants de remise en état et de réputation.

Il est donc impératif d'isoler immédiatement l'hôte compromis, de préserver les preuves (journaux, image disque), de révoquer les accès compromis (comptes, clés), et de lancer une investigation pour déterminer l'étendue de la compromission. Après identification et nettoyage, restaurer les services depuis des sauvegardes fiables, durcir les configurations (authentification forte, segmentation réseau) et appliquer les mises à jour.