Rex0519 Update CR1.md — Latest commit a7b6ed1 now — History

1 contributor

166 lines (130 sloc) 5.52 KB — Raw Blame

CR1

Flow des notions

- Type de Hackers

BLACK HAT Malicious hacker

WHITE HAT Ethical hacker

GREY HAT Not malicious, but not always ethical

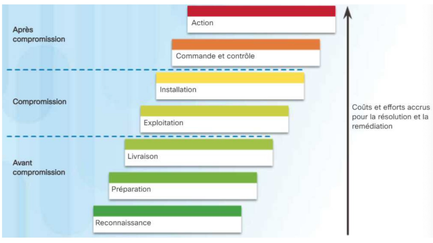
GREEN HAT New, unskilled hacker

BLUE HAT Vengeful hacker

RED HAT Vigilante hacker

- Evolution des outils de securite et d'attaque

- TYPES D'ATTAQUES RÉSEAU
  - Attaques de reconnaissance
  - Attaques d'accès
  - Attaques DoS
- LA CHAÎNE DE FRAPPE DANS LA CYBERDÉFENSE



Plateforme KALI

preparation d'exploitation

'service postgresql start'

'msfconsole' outil pour exploiter kali

'help' -- manual.

'use exploit/chemin/something'

'show options' montrer tous les prarametres de la methode

'show info'

nmap.org

'nmap -sV -T4 -O -F --version-light 192.168.1.1'

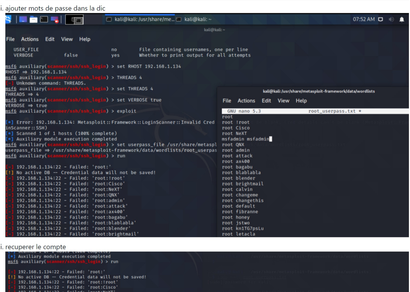
▶ show more

hacked de quelques ports

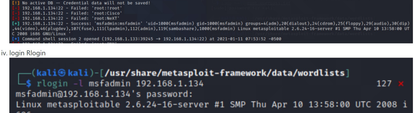
1. FTP
2. SSH
   i. l'installation du systeme vunerable

```
msfadmin@metasploitable:~$
msfadmin@metasploitable:~$
msfadmin@metasploitable:~$
msfadmin@metasploitable:~$
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:30:cb:56
          inet addr:192.168.1.134  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe30:cb56/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:400210 errors:0 dropped:0 overruns:0 frame:0
          TX packets:303832 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:104795625 (176.2 MB)  TX bytes:23423328 (22.3 MB)
          Interrupt:17 Base address:0x2000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:1216 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1216 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:564925 (551.6 KB)  TX bytes:564925 (551.6 KB)

msfadmin@metasploitable:~$ _
```

   ii. ajouter mots de passe dans la dic



   iii. recuperer le compte



   iv. login Rlogin

```
┌──(kali㉿kali)-[/usr/share/metasploit-framework/data/wordlists]
└─$ rlogin -l msfadmin 192.168.1.134                                    127 ⨯
msfadmin@192.168.1.134's password:
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i
686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
Last login: Mon Jan 11 04:48:12 2021
msfadmin@metasploitable:~$
```

3. SMB

secu de routeur

crack mot de passe de routeur (kali)

'enable password cisco'

'service password-encryption' This command obscures all clear-text passwords in the configuration using a Vigenere cipher.

'git clone https://github.com/theevilbit/ciscot7.git' c'est pour un logiciel linux de craquer le mdp de routeur cisco 7. Excuter la commande suivant dans le terminal, 'python ciscot7.py -d -p lechainchiffre'

AUGMENTER LA SÉCURITÉ D'ACCÈS

'line console 0' pour configurer le mode de console qui est connecté directement sur le routeur

vty aka virtual teletype cest pour la tele-connexion telnet ou SSH.