# Computer Security  Project 2

0816146 Yung-Hsiang Wei

## (1) The evidence that I have finished the MITM attack

Attempt to login NYCU E3 using curl, and the attacker can see the username and password.

```
➜  ~ ip a
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 fq_codel state UP group default qlen 1000
    link/ether 08:00:27:eb:ec:e0 brd ff:ff:ff:ff:ff:ff
    inet 10.42.42.2/28 brd 10.42.42.15 scope global enp0s3
       valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:feeb:ece0/64 scope link
       valid_lft forever preferred_lft forever
➜  ~ hostname
comp-sec-2
➜  ~ make
curl -k 'https://e3.nycu.edu.tw/login/index.php' \
        -H 'User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:88.0) Gecko/20100101 Firefox/88.0' \
        -H 'Content-Type: application/x-www-form-urlencoded' \
        -H 'Referer: https://e3.nycu.edu.tw/login/index.php' \
        -H 'Cookie: MoodleSession=d9pi0iqrmu6p936d19mahjnnv4; PHPSESSID=aev1i7nn8v7mfdb6uecnrgsv52' \
        -d 'username=Sean' \
        -d 'password=FLAG{p@ssw0rd}' \
        -d 'captcha_code=2048'
<!DOCTYPE html>
<html  lang="zh-tw" xml:lang="zh-tw">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />

<title>重新導向</title>
</head><body><div style="margin-top: 3em; margin-left:auto; margin-right:auto; text-align:center;">本頁面會自動重新導向。如果什麼都沒發生，請點選下面的"繼續"連結。<br /><a href="https://e3.nycu.edu.tw/">繼續</a></div></body></html>%
```

Fig 1. Victim side, login to E3

```
➜  Project2-MITM-and-Pharming ip a
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 fq_codel state UP group default qlen 1000
    link/ether 08:00:27:e3:8e:b1 brd ff:ff:ff:ff:ff:ff
    inet 10.42.42.3/28 brd 10.42.42.15 scope global noprefixroute enp0s3
       valid_lft forever preferred_lft forever
    inet6 fe80::b847:e04e:753a:b69a/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
➜  Project2-MITM-and-Pharming hostname
comp-sec-3
➜  Project2-MITM-and-Pharming sudo ./mitm_attack
Available devices
+-----------------+-------------------+
| IP Address      | MAC Address       |
+-----------------+-------------------+
| 10.42.42.2      | 08:00:27:eb:ec:e0 |
| 10.42.42.14     | 08:00:27:76:48:7c |
+-----------------+-------------------+

Username: Sean
Password: FLAG{p@ssw0rd}
```

Fig 2. Attacker side, captured the password

## (2) The evidence that I have finished the pharming attack

The DNS request is forged using NF queue and scapy library.

```
➜  ~ ip a
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 fq_codel state UP group default qlen 1000
    link/ether 08:00:27:eb:ec:e0 brd ff:ff:ff:ff:ff:ff
    inet 10.42.42.2/28 brd 10.42.42.15 scope global enp0s3
       valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:feeb:ece0/64 scope link
       valid_lft forever preferred_lft forever
➜  ~ hostname
comp-sec-2
➜  ~ curl http://www.nycu.edu.tw
<!DOCTYPE html>
<html>
<body>

<h1>Congrats for finishing DNS spoofing!</h1>

</body>
</html>
```

Fig 3. Victim side, browse NYCU homepage

```
➜  Project2-MITM-and-Pharming ip a
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 fq_codel state UP group default qlen 1000
    link/ether 08:00:27:e3:8e:b1 brd ff:ff:ff:ff:ff:ff
    inet 10.42.42.3/28 brd 10.42.42.15 scope global noprefixroute enp0s3
       valid_lft forever preferred_lft forever
    inet6 fe80::b847:e04e:753a:b69a/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
➜  Project2-MITM-and-Pharming hostname
comp-sec-3
➜  Project2-MITM-and-Pharming sudo ./pharm_attack
Available devices
+------------------+--------------------+
| IP Address       | MAC Address        |
+------------------+--------------------+
| 10.42.42.2       | 08:00:27:eb:ec:e0  |
| 10.42.42.14      | 08:00:27:76:48:7c  |
+------------------+--------------------+
NYCU homepage is redirected to 140.113.207.246
```

Fig 4. Attacker side, modified DNS response

## (3) Solution to defend against ARP spoofing attack

- Separate end users to different VLANs.
- Only allow one IP address for each MAC address, or block the MAC address / physical port.
- Send gateway ARP packet to end devices periodically.