**Computer Security Project 2**  **0716055 王耀德**

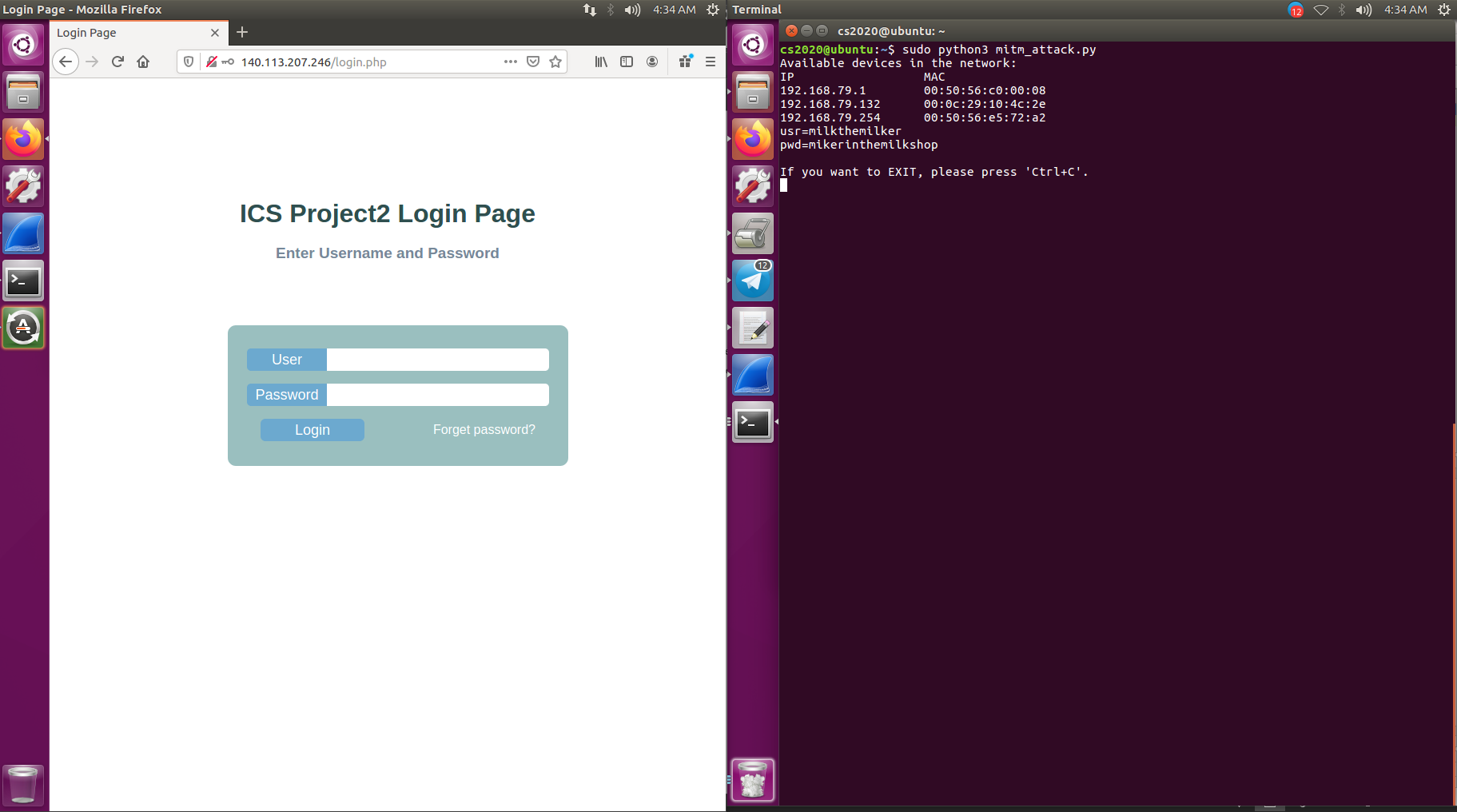
**0716074 蔡育呈**

**【Item1】**

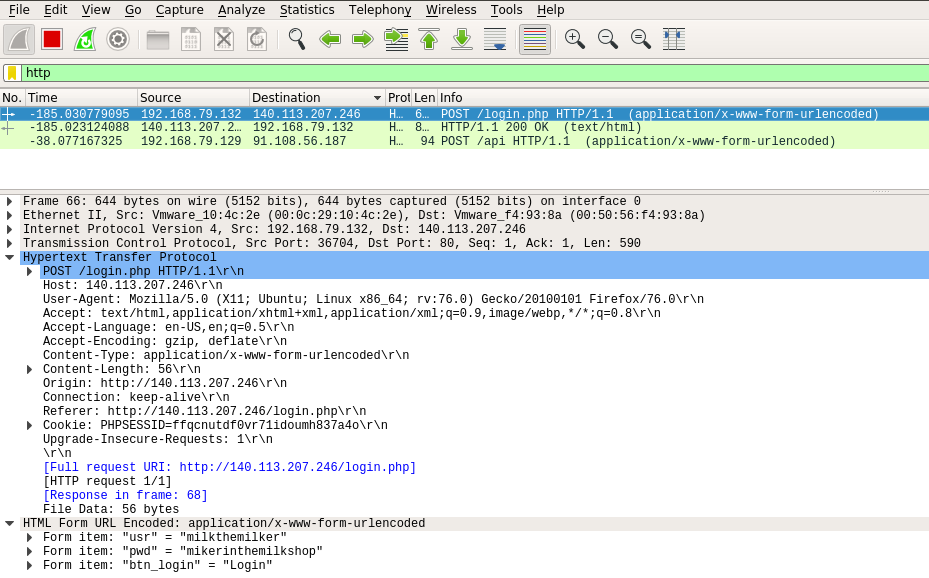
We implement the ARP spoofing with the scenario 2 which contains 2 virtual machines.

|  |  |  |  |
| --- | --- | --- | --- |
|  | **VM1 (Attacker)** | **VM2 (Victim)** | **AP** |
| **MAC** | 00:0c:29:4c:67:80 | 00:0c:29:10:4c:2e | 00:50:56:f4:93:8a |
| **IP** | 192.168.79.129 | 192.168.79.132 | 192.168.79.2 |

1. After submiting the user and password by the victim, the attacker would get them.



2. The attacker gets the HTTP packet(POST).



3.

|  |  |  |
| --- | --- | --- |
| **Packet** | **Source MAC** | **destination MAC** |
| **1** | 00:0c:29:10:4c:2e | 00:0c:29:4c:67:80 |
| **2** | 00:0c:29:4c:67:80 | 00:50:56:f4:93:8a |
| **3** | 00:50:56:f4:93:8a | 00:0c:29:4c:67:80 |
| **4** | 00:0c:29:4c:67:80 | 00:0c:29:10:4c:2e |

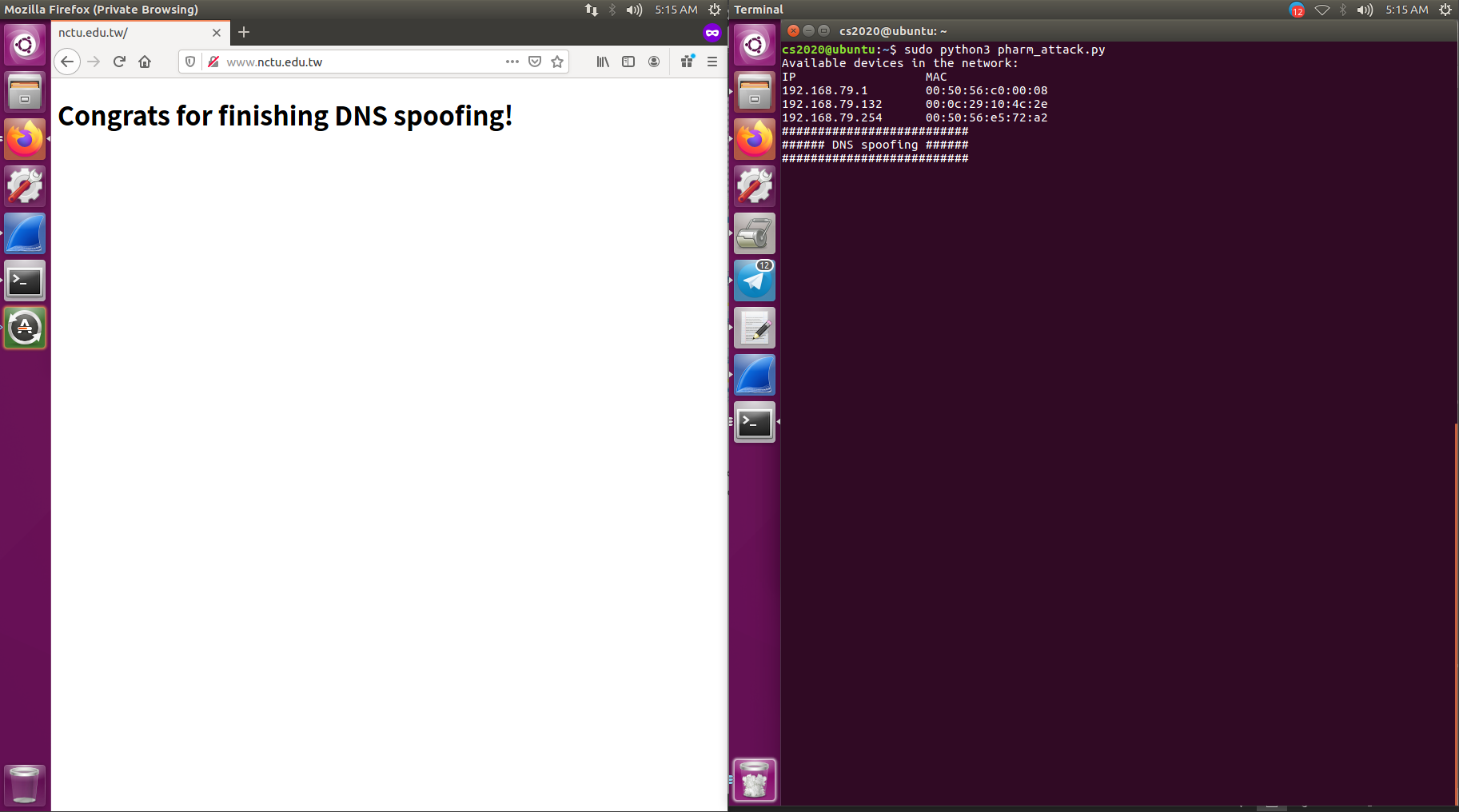
|  |
| --- |
|  |
|  |
|  |
|  |

**【Item2】**

We implement the ARP spoofing with the scenario 2 which contains 2 virtual machines.

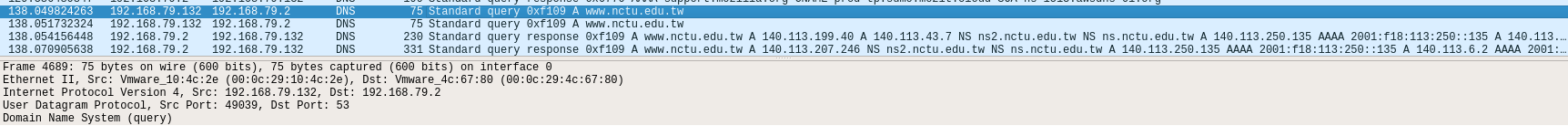
|  |  |  |  |
| --- | --- | --- | --- |
|  | **VM1 (Attacker)** | **VM2 (Victim)** | **AP** |
| **MAC** | 00:0c:29:4c:67:80 | 00:0c:29:10:4c:2e | 00:50:56:f4:93:8a |
| **IP** | 192.168.79.129 | 192.168.79.132 | 192.168.79.2 |

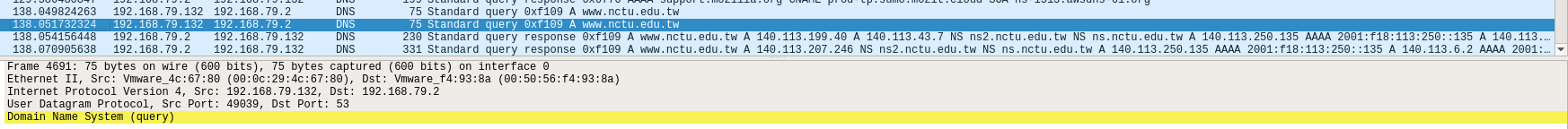
1. After directing to the [**www.nctu.edu.tw**](http://www.nctu.edu.tw), we actually get the content of **140.113.207.246**.

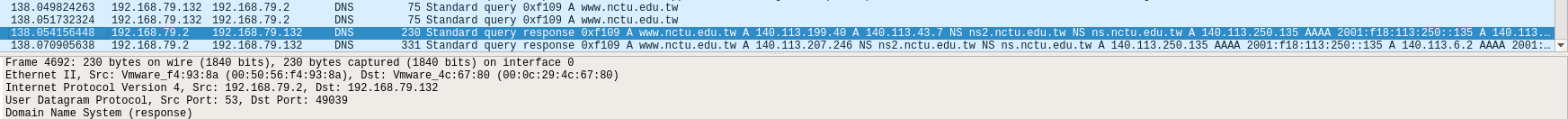
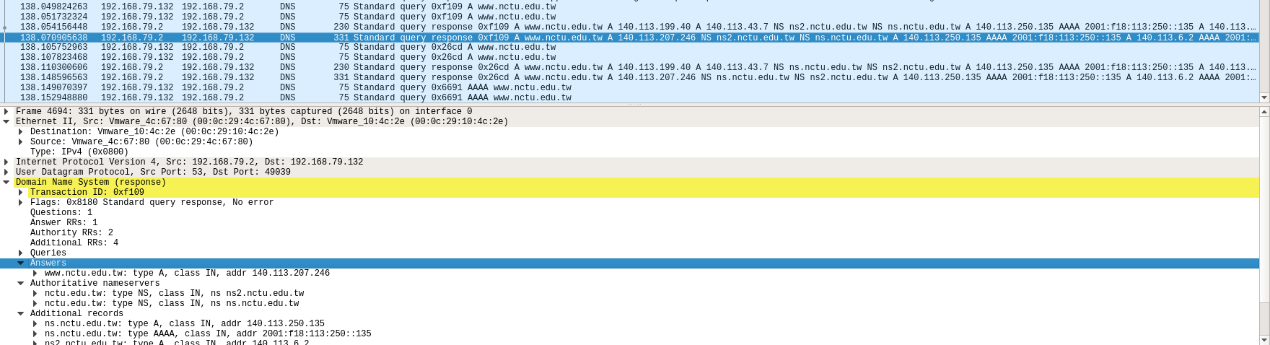


2.

|  |  |  |
| --- | --- | --- |
| **Packet** | **Source MAC** | **destination MAC** |
| **1** | 00:0c:29:10:4c:2e | 00:0c:29:4c:67:80 |
| **2** | 00:0c:29:4c:67:80 | 00:50:56:f4:93:8a |
| **3** | 00:50:56:f4:93:8a | 00:0c:29:4c:67:80 |
| **4** | 00:0c:29:4c:67:80 | 00:0c:29:10:4c:2e |







!!!

**【Item3】**

Creating a static ARP entry in your server can help reduce the risk of spoofing. If you have two hosts that regularly communicate with one another, setting up a static ARP entry creates a permanent entry in your ARP cache that can help add a layer of protection from spoofing.