Network Security

Project 1:
TLS Connection Hijacking

Chi-Yu Li (2024 Fall)
Computer Science Department
National Yang Ming Chiao Tung University

Goal

- Understand how to hijack a TLS connection

- You will learn about
  - Establish TLS connections with customized certificates
  - Handle multiple network connections
  - Importance of certificates and identity verification

Normal Network Connection

- Nowadays, most people use HTTPS to connect to the Internet
- Hypertext Transfer Protocol Secure (HTTPS) is an extension of the Hypertext Transfer Protocol (HTTP)
- In HTTPS, the communication protocol is encrypted using Transport Layer Security (TLS) or Secure Sockets Layer (SSL)

What is TLS?

- Transport Layer Security (TLS) is the successor to SSL (Secure Sockets Layer)
  - It is a protocol used to protect the security of network communications

- Key Features
  - Encryption: Protects data transmitted over the network from eavesdropping.
  - Authentication: Uses digital certificates to verify the identity of parties.
  - Data Integrity: Ensures that data has not been altered during transmission

TLS Primer: Certificate and CA

- TLS certificates are crucial for establishing secure connections
  - Containing public keys, identity information, and digital signature
  - Providing encryption, authentication, and data integrity

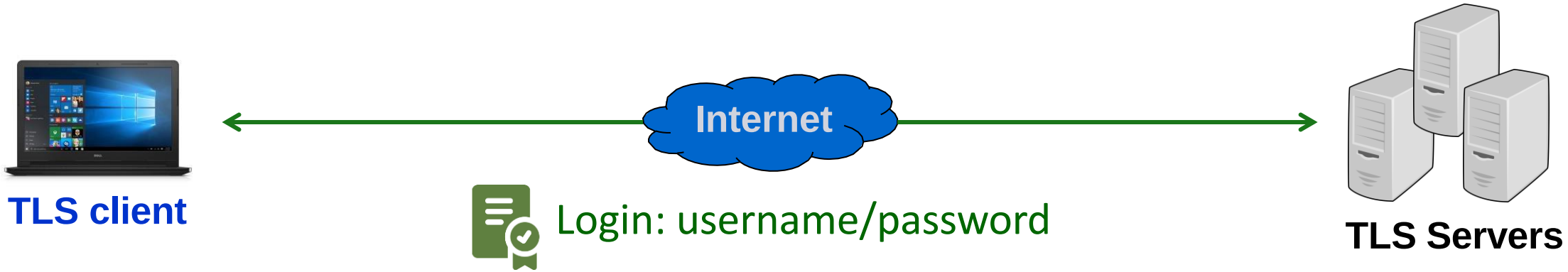
- A certificate authority (CA) is a trusted entity that issues certificates
  - verify the authenticity and trustworthiness of a website, domain and organization
  - users know they are connected with an official website, not a fake or spoofed website created by a attacker

TLS Primer: Cipher Suite

- Cipher Suites are sets of instructions that determine how TLS encrypts data
- Components of a Cipher Suite
  - Key Exchange Algorithm
    - Method for securely exchanging cryptographic keys between a client and a server
  - Encryption Algorithm
    - The cipher used to encrypt the data being transmitted
  - Hashing Algorithm
    - Used to ensure the integrity and authenticity of the message
  - E.g. TLS_RSA_WITH_AES_128_GCM_SHA256

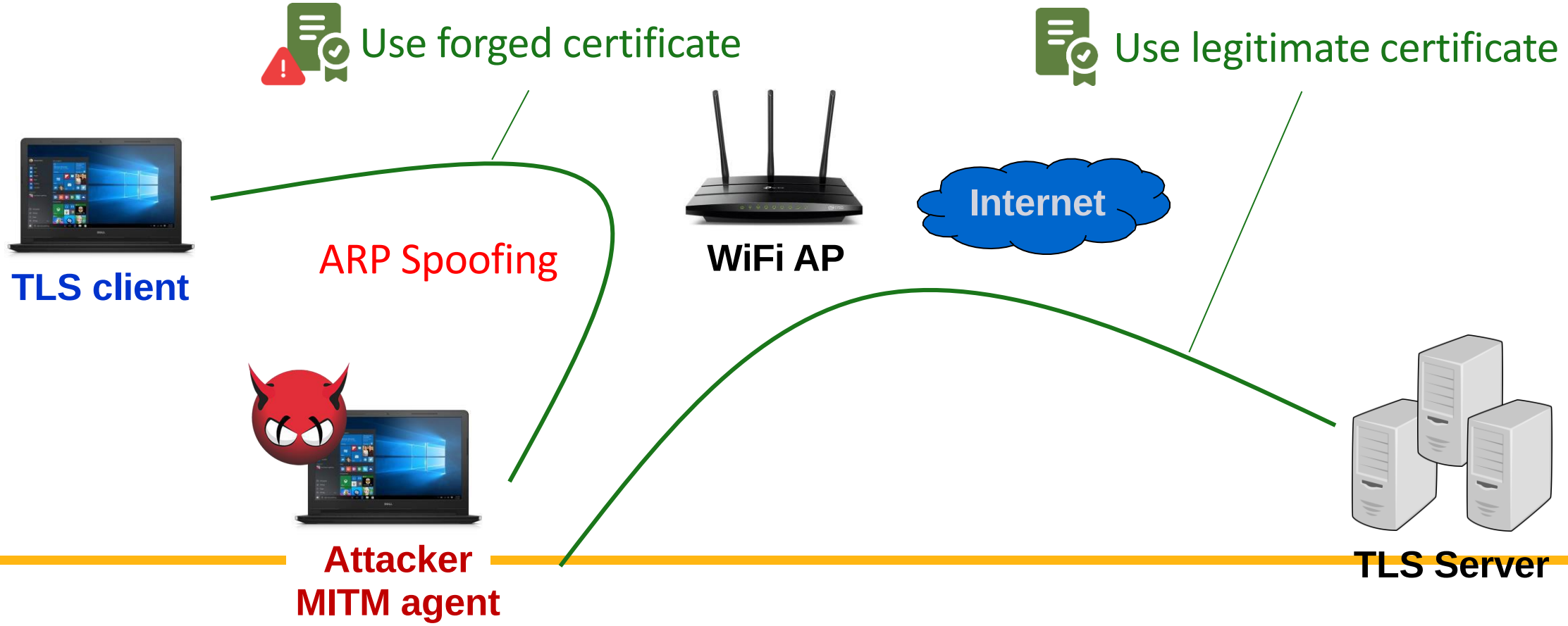
Normal TLS connection

- Establish a connection with a legitimate server certificate to ensure data security



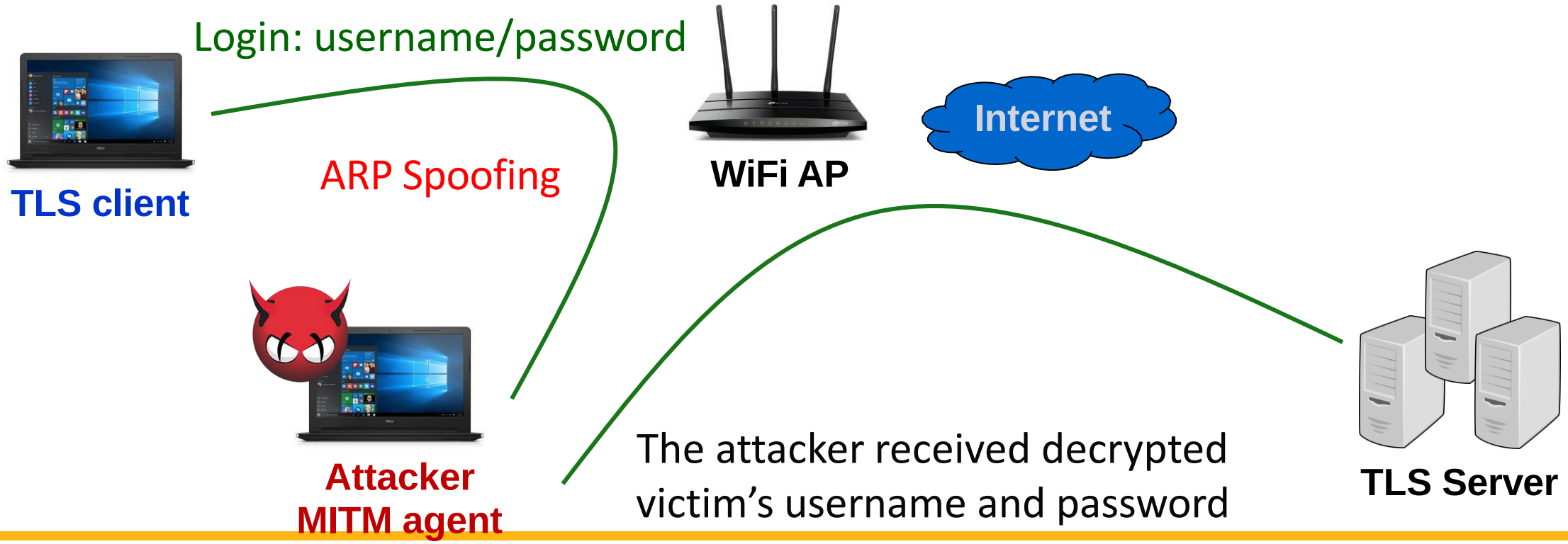
Attack Scenario

- How can Attacker steal Victim's user credentials?



Attack Scenario

- How can Attacker steal Victim's user credentials?



Major Ideas

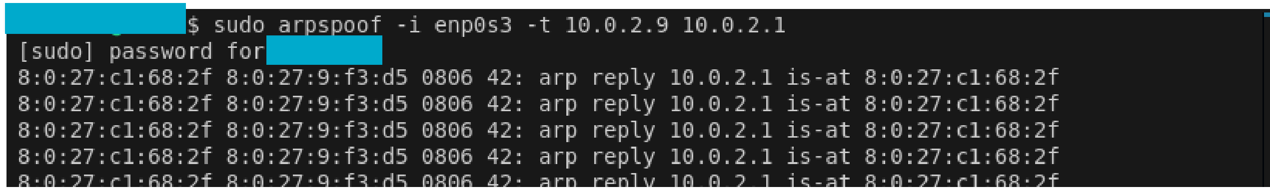
- Redirect Victim's traffic to Attacker
  - Man-in-the-middle based on ARP spoofing
- Dual Connection Establishment
  - What you need to implement in this project

Experimental Setting

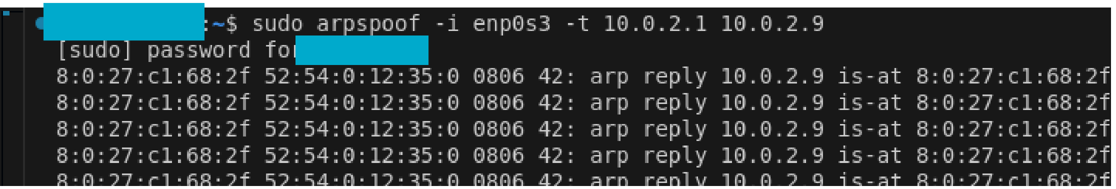
- The attacker VM executes the command below to redirect specific TLS packets to the MITM agent:
  - sudo ./setup.sh
- The victim VM should start the browser using the following command to establish a TLS connection with a forged certificate:
  - google-chrome --ignore-certificate-errors --user-data-dir=/tmp/chrome_dev
    - In real-life situations, such as IoT environments, where certificates are often not verified or when a certificate is injected into the browser, this type of attack can be justified.
  - recommend to open the browser in Incognito mode.

Experimental Setting: ARP Spoofing

- Attacker VM execute the command below in the MITM agent
  - ☐ sudo arpspoof -i INTERFACE -t GATEWAY_IP CLIENT_IP
  - ☐ sudo arpspoof -i INTERFACE -t CLIENT_IP GATEWAY_IP

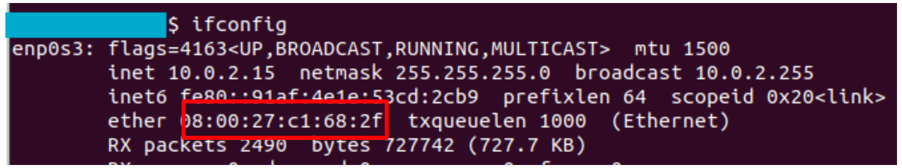


```
[redacted]$ sudo arpspoof -i enp0s3 -t 10.0.2.9 10.0.2.1
[sudo] password for [redacted]
8:0:27:c1:68:2f 8:0:27:9:f3:d5 0806 42: arp reply 10.0.2.1 is-at 8:0:27:c1:68:2f
8:0:27:c1:68:2f 8:0:27:9:f3:d5 0806 42: arp reply 10.0.2.1 is-at 8:0:27:c1:68:2f
8:0:27:c1:68:2f 8:0:27:9:f3:d5 0806 42: arp reply 10.0.2.1 is-at 8:0:27:c1:68:2f
8:0:27:c1:68:2f 8:0:27:9:f3:d5 0806 42: arp reply 10.0.2.1 is-at 8:0:27:c1:68:2f
8:0:27:c1:68:2f 8:0:27:9:f3:d5 0806 42: arp reply 10.0.2.1 is-at 8:0:27:c1:68:2f
```



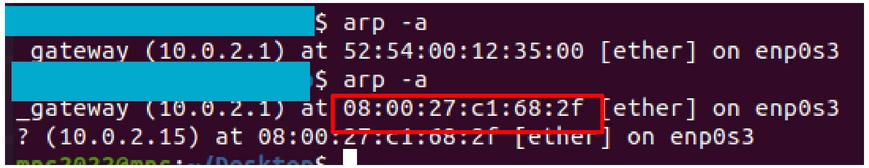
```
[redacted]:~$ sudo arpspoof -i enp0s3 -t 10.0.2.1 10.0.2.9
[sudo] password fo[redacted]
8:0:27:c1:68:2f 52:54:0:12:35:0 0806 42: arp reply 10.0.2.9 is-at 8:0:27:c1:68:2f
8:0:27:c1:68:2f 52:54:0:12:35:0 0806 42: arp reply 10.0.2.9 is-at 8:0:27:c1:68:2f
8:0:27:c1:68:2f 52:54:0:12:35:0 0806 42: arp reply 10.0.2.9 is-at 8:0:27:c1:68:2f
8:0:27:c1:68:2f 52:54:0:12:35:0 0806 42: arp reply 10.0.2.9 is-at 8:0:27:c1:68:2f
8:0:27:c1:68:2f 52:54:0:12:35:0 0806 42: arp reply 10.0.2.9 is-at 8:0:27:c1:68:2f
```

- Victim VM execute arp -a to check ARP table
  - ☐ If the gateway's mac address is the same with that of the attacker, ARP spoofing is successful



```
[redacted]$ ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.2.15  netmask 255.255.255.0  broadcast 10.0.2.255
        inet6 fe80::91af:4e1e:53cd:2cb9  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:c1:68:2f  txqueuelen 1000  (Ethernet)
        RX packets 2490  bytes 727742 (727.7 KB)
```

MITM Agent



```
[redacted]$ arp -a
 gateway (10.0.2.1) at 52:54:00:12:35:00 [ether] on enp0s3
[redacted]$ arp -a
_gateway (10.0.2.1) at 08:00:27:c1:68:2f [ether] on enp0s3
? (10.0.2.15) at 08:00:27:c1:68:2f [ether] on enp0s3
```

TLS Client

Task I: Establishing TLS Connections

- TLS Client to MITM Agent:
  - The MITM agent can use a forged certificate to establish a TLS connection.
    - Configure the server settings (TLS version, check mode, etc.) so that the victim accepts the TLS connection.

- MITM Agent to TLS server:
  - The MITM agent can retrieve the destination address from the victim's packet
  - The MITM agent uses this address to connect to the TLS server.
    - A fixed address for the TLS server connection is not allowed.
      - should be able to connect to different websites.

Task II: Establish multiple TLS connections

- The program should still works normally when opening another website
  - Handling concurrency
    - Ensure the program can manage multiple simultaneous TLS connections efficiently
    - Consider using threading, fork(), or asynchronous I/O (select(), epoll()) to avoid blocking connections
  - Session management
    - Each connection should maintain its own independent TLS session context
    - Avoid session interference between multiple websites being accessed simultaneously

Verification Steps

- 1. MITM agent can correctly establish two TLS connection (60%)
  - TLS client to MITM agent / MITM agent to TLS server
- 2. Fetch the username/password and show in the terminal (20%)
  - MITM agent should print the hijacked data from portal
- 3. The attacker program can establish multiple TLS connections (20%)
  - Handle requests for other TLS connections as normal

Verification Steps

- 1. MITM agent can correctly establish two TLS connection (60%)
  - When executing the attack program, the client can successfully connect to the school's portal webpage.
  - The program should also print the destination IP and port.

```
:~/project1$ sudo python3 attack.py 10.0.2.9 enp0s3
[sudo] password for
TLS Connection Established : [140.113.41.157:443]
```

Verification Steps

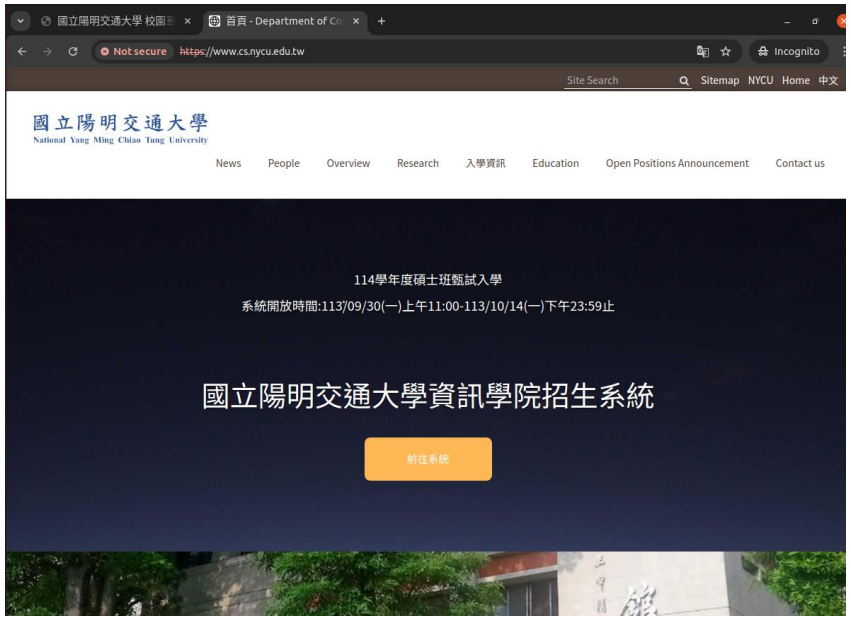
- 2. Fetch the username/password and show in the terminal (20%)
  - MITM agent should check hijacked data and print the account and password

```
[redacted]~/project1$ sudo python3 attack.py 10.0.2.9 enp0s3
[sudo] password for [redacted]
TLS Connection Established : [140.113.41.157:443]
id: 312[redacted] password:[redacted]
```

Verification Steps

- 3. The attacker program can interact with the server with multiple handshakes (20%)
  - The program still works normally when opening another website

```
[redacted]~/project1$ sudo python3 attack.py 10.0.2.9 enp0s3
[sudo] password for [redacted]
TLS Connection Established : [140.113.41.157:443]
id: 312[redacted], password: [redacted]
TLS Connection Established : [140.113.24.241:443]
```



Important: How to Prepare Your Attack Programs?

- You need to develop and run your program in the provided virtual machine.
  - **VM Image**: Please download it from the provided link
    - Username/password: ns2024/ns2024
  - Network setting: NAT Network
- Do not hardcode the network interface. You are allowed to assign it during execution.
  - During the demo, the program may be run on either VMware or VirtualBox, so ensure that no fixed values are used.
- Only Python is allowed for the development.

Important: How to Prepare Your Attack Programs?

- Must provide an attack program named **attack.py** (Missing: -20%)
- Test requirements for the program
  - Due to the environment settings, this project focuses on hijacking websites within the school's IP domain (140.113.*.*)
    - You can use the nslookup command to verify if a specific host is within the school IP domain
  - During the demo, all certificates will be provided by the TA and will be located in the ../certificates/ directory
- The program must work with the following test commands:
  - sudo ./attack.py <victim ip> or sudo ./attack.py <victim ip> <interface>
- You are allowed to team up. Each team has at most 3 students.
  - Teams: discussions are allowed, but no collaboration

Project Submission

- Due date: 10/30
- Makeup submission (75 points at most): TBA (After the final)
- Submission rules
  - Put your source code files into a directory and name it using your student ID(s)
    - If your team has two members, please concatenate your IDs separated by "-"
  - Zip the directory and upload the zip file to New E3 (only upload python files)
  - A sample of the zip file: 01212112-02121221.zip
    - attack.py
    - bbb.py
  - If files are not in a directory after unzip, 10 points will be deducted.

Online Project Demo

- Demo date: 11/1
- TA will prepare your zip file and run your programs for the demo on behalf of you
  - TA will run your program in the same given virtual environment
- You will
  - be asked to launch a TLS hijacking attack
  - be not allowed to modify your codes or scripts in the demo
  - be asked some questions
  - be responsible to show and explain the outcome to TA

Questions?