夏課題の報告

菊池研 B3 住友孝彰

夏課題の予定

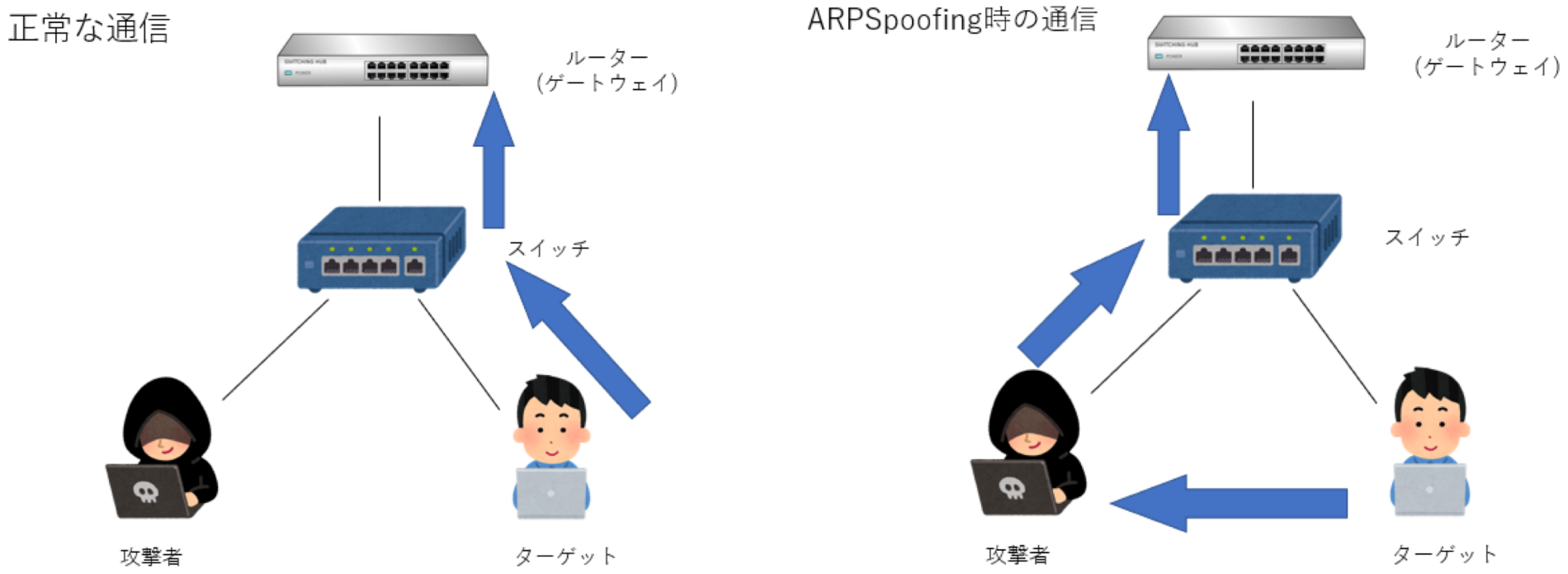
- 松本さんに行っていただいた実験環境の再現
- Ubuntuのコマンドを用いて行えるARPSpoofingの観測
- ScapyをもちいてARPSpoofingを行うプログラムの作成
- Win7, 10, Android, ios, router, kali linuxの6種類の環境でARP通信の間隔と初期接続の際のシーケンスを集める

実際に行ったこと

- 松本さんに行っていただいた実験環境の再現
  - 有線ネットワークの構築
- UbuntuのコマンドをもちいてARPSpoofingの観測
- ScapyをもちいてARPSpoofingを行うプログラムの作成
- Win7, 10, Android, ios, router, kali linuxの6種類の環境でARP通信の間隔または接続時の最初のARP通信を観測する

Ubuntuのコマンドを用いて行えるARPSpoofingの観測

- Ubuntuのコマンドで行えるARPSpoofingを行うための通信をwiresharkで観測し、どのような通信で攻撃しているか調べた
- arpspoof –I [インターフェース] –t [ターゲットIP][ゲートウェイIP]で行える



ARPSpoofingを行う通信の中身

正しいARPreply

```
Address Resolution Protocol (reply)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: reply (2)
    Sender MAC address: Yamaha_6a:61:45 (ac:44:f2:6a:61:45)
    Sender IP address: 192.168.100.1
    Target MAC address: Microsof_00:66:7b (28:16:a8:00:66:7b)
    Target IP address: 192.168.100.3
```

不正なARPreply

```
Address Resolution Protocol (reply)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: reply (2)
    Sender MAC address: Sony_38:9d:d0 (54:53:ed:38:9d:d0)
    Sender IP address: 192.168.100.1
    Target MAC address: Microsof_00:66:7b (28:16:a8:00:66:7b)
    Target IP address: 192.168.100.3
```

Wiresharkを用いて通信の中身を見比べてみると、”Sender MAC address”の中身が異なっていることが分かる。
これは通信を送る側のMACアドレスを表すものである。
これよりARPSpoofingは偽のMACアドレスをターゲットに認識させて行う攻撃であることが分かった。
また、通信の間隔は2秒であった

Scapyを用いてARPSpoofingを行うプログラムの作成

- 「Ubuntuのコマンドを用いて行えるARPSpoofingの観測」で得られた情報をもとにpythonのライブラリ「scapy」でARPSpoofingを行うプログラムを作成した。

- 必要な情報はubuntuのコマンドで行うときと同じようにターゲットのIPアドレスとゲートウェイのIPアドレスとした。

- 入力されたIPアドレスに対してARPrequestを送ることでIPアドレスに対応したMACアドレスを得る、その後、偽造ARPreplyを2秒間隔で送るプログラムである。

結果

```
admin1005@d:~$ arp
アドレス                 HWタイプ  HWアドレス           フラグ マスク インタフェース
192.168.100.2            ether   28:16:a8:00:66:7b   C                     enp14
s0
192.168.100.3            ether   54:53:ed:38:9d:d0   C                     enp14
s0
_gateway                 ether   ac:44:f2:6a:61:45   C                     enp14
s0
admin1005@d:~$ arp
アドレス                 HWタイプ  HWアドレス           フラグ マスク インタフェース
192.168.100.2            ether   28:16:a8:00:66:7b   C                     enp14
s0
192.168.100.3            ether   54:53:ed:38:9d:d0   C                     enp14
s0
_gateway                 ether   28:16:a8:00:66:7b   C                     enp14
s0
admin1005@d:~$
```

```
157 52.865418     192.168.100.5        192.168.100.1
158 53.867674     192.168.100.5        192.168.100.1
163 54.891692     192.168.100.5        192.168.100.1
167 55.915523     192.168.100.5        192.168.100.1
172 56.939605     192.168.100.5        192.168.100.1
173 57.963715     192.168.100.5        192.168.100.1
```

このプログラムを作動させた機体のIPアドレスは”192.168.100.2”、
ターゲットの機器のIPアドレスは”192.168.100.5である。
上のARPテーブルが攻撃前と下のARPテーブルが攻撃後であるが、比べるとgatewayのHWアドレスが書き変わっていることが分かる。
また本来観測できないターゲットからゲートウェイへの通信も観測できた。

Win7, 10, Android, ios, router, kali linuxの6種類の環境でARP通信の間隔または接続時の最初のARP通信を観測する

- ルーターからのARPRequestの間隔
  - 約30秒
- 接続した際の最初の最初のARP通信
  - Win7, 10, ios
    - 自分のIPアドレスを誰も使っていないか確かめるARPRequest
  - Kali linux, android
    - ゲートウェイのMACアドレスを要求するARPRequest