

2018 컴퓨터 보안 PROJECT

패킷 분석을 통한 사용자 계정 탈취

무사완성하조

201511784 권신영

201511815 박성수

201511867 조희진

201511874 홍지민

CONTENTS

01 주제

02 설계

03 동작 방식

04 시연 영상

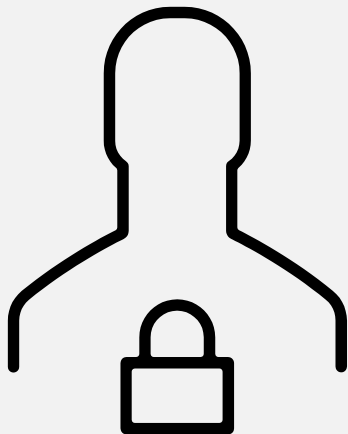
05 보안 조치

01 주제 주제 선정

패킷 분석을 통한 사용자 계정 탈취

```
170 0.669638 203.249.22.91 203.249.3.239 TCP 662 63149 → 80 [PSH, ACK] Seq=1 Ack=1 Win=65535 Len=608 [TCP segment of a reassembled PDU]
171 0.669781 203.249.22.91 203.249.3.239 HTTP 95 POST /login/method!logincheck.action HTTP/1.1 (application/x-www-form-urlencoded)

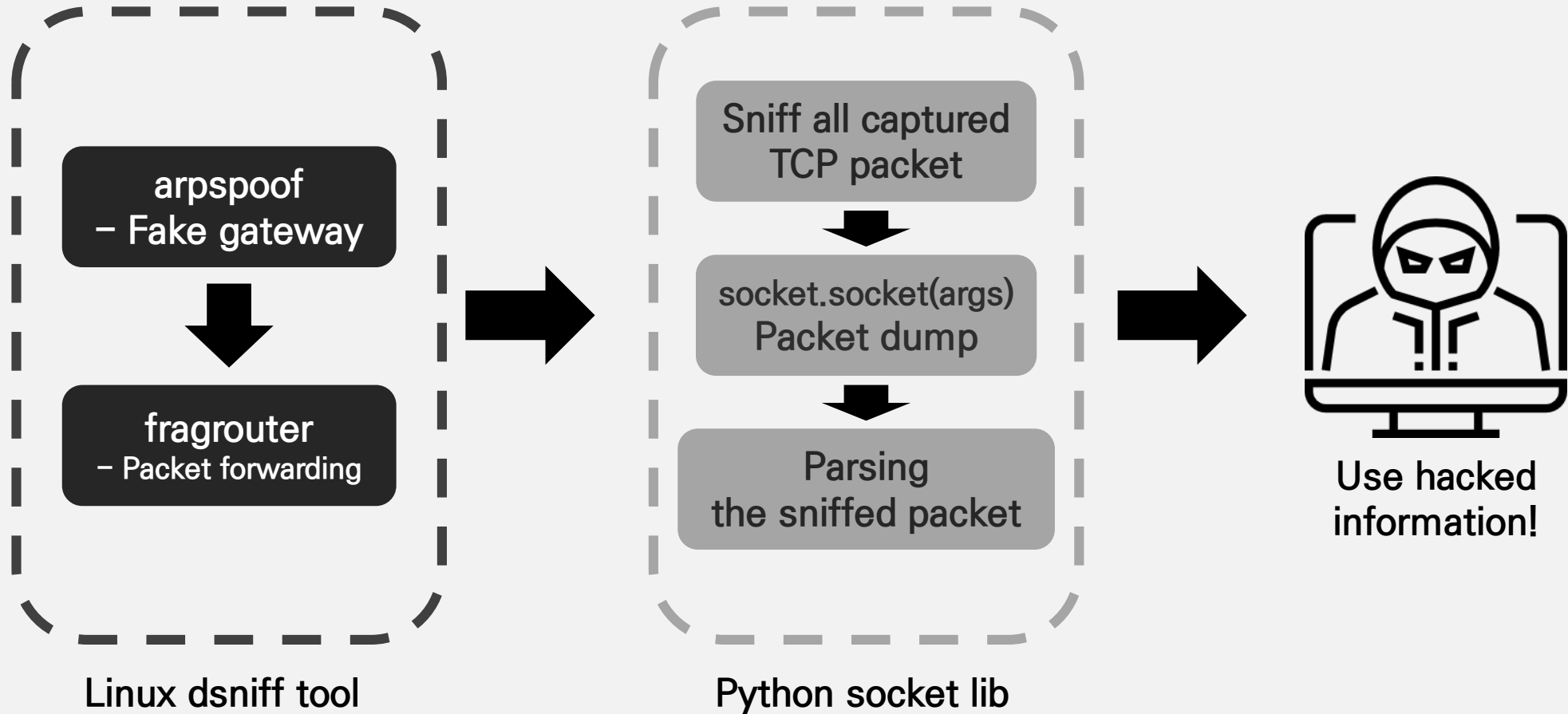
> Frame 171: 95 bytes on wire (760 bits), 95 bytes captured (760 bits) on interface 0
> Ethernet II, Src: SamsungE_7f:e0:93 (98:83:89:7f:e0:93), Dst: PrimaryA_6b:32:88 (00:20:9c:6b:32:88)
> Internet Protocol Version 4, Src: 203.249.22.91, Dst: 203.249.3.239
> Transmission Control Protocol, Src Port: 63149, Dst Port: 80, Seq: 609, Ack: 1, Len: 41
> [2 Reassembled TCP Segments (649 bytes): #170(608), #171(41)]
> Hypertext Transfer Protocol
> HTML Form URL Encoded: application/x-www-form-urlencoded
  > Form item: "login_id" = "201511874"
  > Form item: "login_pwd" = "ASDFqwer1234"
```



사용자 계정 탈취

02 설계
구체적인 설계 내용

ARP Spoofing을 이용 중간자 공격으로 패킷 sniffing, dump



03 동작 방식

패킷 분석을 통한 사용자 계정 탈취

```
D:\Users\WTS140>arp -a

인터페이스: 192.168.1.177 --- 0xb
인터네트 주소      물리적 주소
192.168.1.1         38-2c-4a-f4-21-40
192.168.1.2         54-bd-79-e7-fb-10
192.168.1.4         00-15-5d-58-e6-01
192.168.1.11        a4-c4-94-50-b4-82
192.168.1.46        f8-e6-1a-bc-ff-48
192.168.1.111       00-26-66-a3-18-62
192.168.1.167       f8-0d-60-ce-db-65
192.168.1.255       ff-ff-ff-ff-ff-ff
224.0.0.2           01-00-5e-00-00-02
224.0.0.7           01-00-5e-00-00-07
224.0.0.22          01-00-5e-00-00-16
224.0.0.251         01-00-5e-00-00-fb
224.0.0.252         01-00-5e-00-00-fc
224.0.1.187         01-00-5e-00-01-bb
239.192.152.143     01-00-5e-40-98-8f
239.255.255.250     01-00-5e-7f-ff-fa
255.255.255.255     ff-ff-ff-ff-ff-ff

인터페이스: 172.20.174.1 --- 0xc
인터네트 주소      물리적 주소
224.0.0.2           01-00-5e-00-00-02
224.0.0.7           01-00-5e-00-00-07
224.0.0.22          01-00-5e-00-00-16
224.0.0.251         01-00-5e-00-00-fb
224.0.0.252         01-00-5e-00-00-fc
224.0.1.187         01-00-5e-00-01-bb
239.192.152.143     01-00-5e-40-98-8f
239.255.255.250     01-00-5e-7f-ff-fa
255.255.255.255     ff-ff-ff-ff-ff-ff
```

```
D:\Users\WTS140>arp -a

인터페이스: 192.168.1.177 --- 0xb
인터네트 주소      물리적 주소
192.168.1.1         00-15-5d-58-e6-02
192.168.1.2         54-bd-79-e7-fb-10
192.168.1.4         00-15-5d-58-e6-01
192.168.1.5         00-15-5d-58-e6-02
192.168.1.11        a4-c4-94-50-b4-82
192.168.1.46        f8-e6-1a-bc-ff-48
192.168.1.111       00-26-66-a3-18-62
192.168.1.167       f8-0d-60-ce-db-65
192.168.1.255       ff-ff-ff-ff-ff-ff
224.0.0.2           01-00-5e-00-00-02
224.0.0.7           01-00-5e-00-00-07
224.0.0.22          01-00-5e-00-00-16
224.0.0.251         01-00-5e-00-00-fb
224.0.0.252         01-00-5e-00-00-fc
224.0.1.187         01-00-5e-00-01-bb
239.192.152.143     01-00-5e-40-98-8f
239.255.255.250     01-00-5e-7f-ff-fa
255.255.255.255     ff-ff-ff-ff-ff-ff

인터페이스: 172.20.174.1 --- 0xc
인터네트 주소      물리적 주소
224.0.0.2           01-00-5e-00-00-02
224.0.0.7           01-00-5e-00-00-07
224.0.0.22          01-00-5e-00-00-16
224.0.0.251         01-00-5e-00-00-fb
224.0.0.252         01-00-5e-00-00-fc
224.0.1.187         01-00-5e-00-01-bb
239.192.152.143     01-00-5e-40-98-8f
239.255.255.250     01-00-5e-7f-ff-fa
255.255.255.255     ff-ff-ff-ff-ff-ff
```

01 arpspoof으로 gateway MAC 변조 확인

ARP Spoofing

- ARP를 누가 보냈는지 알 수 없는 ARP 프로토콜의 취약점을 이용한 공격 기법
- 네트워크 상의 호스트는 자신이 보낸 ARP request에 대한 응답이 아니더라도 자신에게 들어오는 ARP reply를 보고 자신의 ARP캐시 테이블을 업데이트
←ARP reply는 source에 대한 검증 절차 X, arp table에 바로 반영

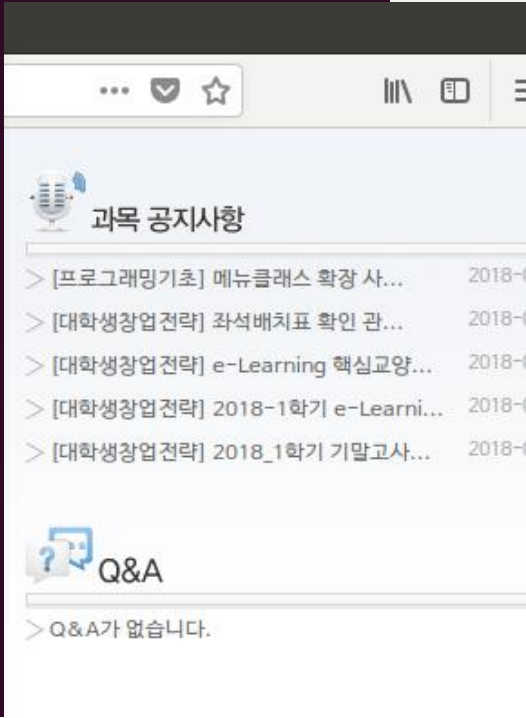
Arpspoof

- 타겟 PC에게 게이트 웨이는 공격자 PC라는 거짓 ARP reply 메시지를 보내 타겟 PC의 ARP 캐시 테이블 조작
- ✓ 타겟 PC의 ARP 캐시 정보에서 정상적인 라우터의 MAC 주소 38-2c-4a-f4-21-40
- ✓ 공격자가 ARP reply 패킷을 지속적으로 전송하여 타겟 PC에서 ARP 캐시가 공격자 PC의 MAC 주소인 00-15-5d-58-e6-02 로 변경

03 동작 방식

패킷 분석을 통한 사용자 계정 탈취

```
ts140v2@ts140v2-Virtual-Machine: ~/sniff
ts140v2@ts140v2-Virtual-Machine:~/sniff$ sudo python3 tcp_sniffer.py
id : 201511815
pw : 
id : 201511815
pw : 
^CTraceback (most recent call last):
  File "tcp_sniffer.py", line 26, in <module>
    packet = s.recvfrom(4096)
KeyboardInterrupt
ts140v2@ts140v2-Virtual-Machine:~/sniff$
```



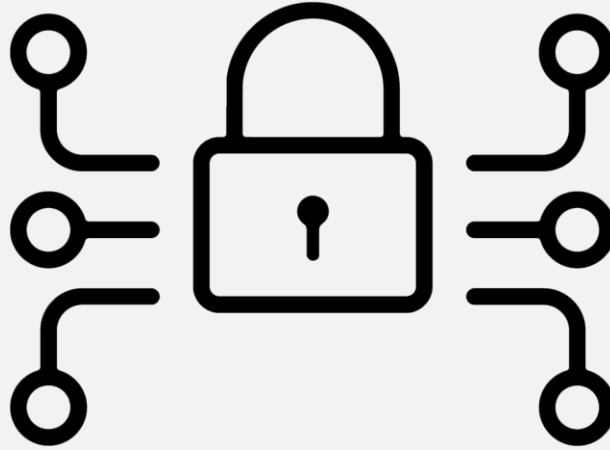
02 ubuntu에서 arpspoof 시도로 login packet capture , sniff 성공

arpspoof를 통해 사용자가 보낸 패킷을 확인
이후 바로fragrouter을 통해 포워딩하기 때문에 사용자의
의심 피함

→공격자는 arpspoof를 통해 얻은 패킷 분석으로
원하는 login packet capture,sniff 가능

attacer : ubuntu (192.168.1.5)
target : windows 10 (192.168.1.177)
gateway : ASUS AC87U (192.168.1.1)

04 시연 영상



Arp Spoofing 보안 조치

arp spoofing 기법은 ARP캐쉬가 dynamic(동적)으로 설정되어 있을 때, 공격자에 의해 변경되는 점 이용
→ 기본게이트웨이의 주소를 arp -s 명령을 사용하여 ARP캐쉬에 static(정적)으로 등록하여
arp spoofing으로 인한 MAC주소 변조 무효화

Thank you
Q&A