JKIICE Journal of the Korea Institute of Information and Communication Engineering

한국정보통신학회논문지 Vol. 23, No. 11: 1451~1461, Nov. 2019

DNS 스푸핑을 이용한 포털 해킹과 파밍의 위험성

최재원*

Web Server Hacking and Security Risk using DNS Spoofing and Pharming combined Attack

Jae-Won Choi*

*Professor, Department of Computer Engineering, Kyungsung University, Busan 48434, Korea

요 약

DNS 스푸핑은 공격자가 클라이언트와 DNS 서버 간 통신에 개입하여 실제 IP 주소가 아닌 가짜 IP 주소를 응답하여 DNS 서버를 속이는 공격이다. 웹 서버 초기화면 복제와 간단한 웹 프로그래밍으로 사용자 아이디와 비밀번호를 해킹하는 파밍 사이트 구현이 가능하다. 본 논문에서는 파밍사이트로 유도하는 DNS 스푸핑과 파밍사이트 구현을 결합한 웹 스푸핑 공격에 관해 연구하였다. 본 대학의 포털 서버를 대상으로 DNS 스푸핑 공격 방법과 절차 및 파밍 사이트 구현 방법에 관해 연구하였다. 경성포털의 경우 SSL에 의한 암호화와 보안인증이 이루어진 웹 서버임에도 우회 공격과 해킹이 가능하였다. 현재 많은 웹 서버가 보안조치가 이루어져 있지 않고, SSL에 의해 보안이 이루어진 웹 서버라 할지라도 이를 무력화 시킬 수 있으므로 이의 심각한 위험과 대응조치가 꼭 필요함을 알리고자 한다.

ABSTRACT

DNS spoofing is an attack in which an attacker intervenes in the communication between client and DNS server to deceive DNS server by responding to a fake IP address rather than actual IP address. It is possible to implement a pharming site that hacks user ID and password by duplicating web server's index page and simple web programming. In this paper we have studied web spoofing attack that combines DNS spoofing and pharming site implementation which leads to farming site. We have studied DNS spoofing attack method, procedure and farming site implementation method for portal server of this university. In the case of Kyungsung Portal, bypassing attack and hacking were possible even though the web server was SSL encrypted and secure authentication. Many web servers do not have security measures, and even web servers secured by SSL can be disabled. So it is necessary that these serious risks are to be informed and countermeasures are to be researched.

키워드 : DNS 스푸핑, ARP 스푸핑, Web 스푸핑, 네트워크보안

Key word : DNS Spoofing, ARP Spoofing, Web Spoofing, Network Security

Received 12 July 2019, **Revised** 22 August 2019, **Accepted** 20 September 2019

*** Corresponding Author** Jae-Won Choi(E-mail:choejw@ks.ac.kr, Tel:+82-51-663-4786)
Professor, Department of Computer Science and Engineering, Kyungsung University, Busan 48434, Korea

Open Access http://doi.org/10.6109/jkiice.2019.23.11.1451 print ISSN: 2234-4772 online ISSN: 2288-4165

Ⅰ. 서 론

국내에서 보안 문제의 심각성이 서서히 거론되던 5년 전에 본인이 겪었던 일이다. 농협 인터넷 뱅킹을 위해 네이버 검색창에 농협을 쳐서 농협 인터넷 뱅킹에 접속하였다. 평상시 보던 메인화면에 보안강화를 위한 조치로 추가 정보를 받겠다는 안내문이 떴다. 무의식적으로 보안카드의 숫자들을 모두 입력한 후 엔터키를 눌렀다. 동일한 안내문과 보안카드의 입력화면, 메인화면의 메뉴 클릭이 전혀 동작하지 않는 것을 확인하는 순간 해킹이라는 생각이 스쳐지나갔다. 그날은 일요일이었기에 농협과 관계 기관에 수없이 전화를 돌렸지만 연결되지 않았다. 30분이나 지나 겨우 당직자와 연결이 되었고 계좌폐쇄 등의 긴급조치로 다행히 인출은 막을 수 있었다. 만약 좀 더 정교한 파밍 사이트의 구현으로 파밍 사이트임을 전혀 눈치 챌 수 없도록 하였다면 어떠하였을까? 지금 생각해도 아찔한 생각이 든다.

최근 사이버위협과 개인정보 유출로 많은 사회적 문제가 되고 있다. 기존의 인터넷 사용자와 더불어 스마트폰을 이용한 인터넷 사용자의 대중화로 인터넷의 보안이 심각한 위험에 노출되어 있다. 웹 서버와 DNS 서버는 인터넷 기반의 정보시스템의 근간이 되며, 인터넷 서비스를 위한 핵심 서버이므로 이의 보안은 그 어느 때보다 중요한 시점에 있다.

해킹의 종류에는 여러 가지가 있지만 가장 대표적인 것이 스니핑(sniffing)과 스푸핑(spoofing)이다. 스니핑은 네트워크 상에서 자신이 아닌 다른 상대방들의 패킷을 '훔쳐보는 것'을 말하며, 스푸핑은 네트워크 상에서 거짓된 패킷을 발송하여 '속이는 것'을 말한다. DNS 서버는 인터넷에서 문자열로 된 도메인이름을 숫자로 된 IP 주소로 변환해 주는 네트워크 서버이다. DNS 스푸핑(DNS spoofing)은 DNS의 취약점을 악용하여 공격자가 사용자와 DNS 서버 간의 통신에 개입해서 실제 IP 주소가 아닌 다른 IP 주소를 반환하여 DNS 서버를 속이는 것을 말한다.

공격대상 PC의 사용자가 특정 웹 사이트를 접근하고자 할 때, 공격자의 DNS 스푸핑 공격으로 공격자가 만든 가짜 파밍 사이트로 유도하여 사용자의 아이디와 패스워드 등의 개인정보를 취득할 수 있다. DNS 스푸핑 공격과 원래 사이트와 완전히 동일한 가짜 사이트를 만드는 파밍(pharming) 사이트 구현 기술이 결합되면, 일반인은 물론이고 보안 전문가조차도 이를 전혀 인지할 수 없기에 심각한 보안 위험의 상태에 있다. 이로 인해 주요 포털 사이트를 대상으로 한 해킹과 많은 해킹 피해자들이 발생 할 수 있다. 그래서 본 논문에서는 DNS 스푸핑과 파밍사이트 구현 기술의 결합에 의한 웹 스푸핑 공격에 관해 연구하였다.

본 논문에서는 공격자가 사용자와 DNS 서버 간의 통신에 개입해서 실제 IP 주소가 아닌 다른 IP 주소를 반환하여 파밍사이트로 유도하는 DNS 스푸핑 공격에 대해 연구한다. 그리고 경성대학의 포털인 경성포털을 대상으로 파밍 사이트 구현기술에 관해 연구한다. 이의 연구를 통해 DNS 스푸핑과 파밍사이트 구현 기술을 결합한 웹 스푸핑 공격에 웹 서버가 얼마나 심각한 해킹의 위험에 놓여 있는지에 대한 경각심을 일깨우고, 이에 대한 대처와 대응방안에 관한 연구가 꼭 필요함을 알리는데 그 목적이 있다.

본 논문에서는 먼저 DNS 스푸핑 공격에 관한 전반적인 소개와 DNS 스푸핑 공격을 위한 모의 해킹 환경과 공격 과정을 설명하였다. DNS 스푸핑 공격 툴의 설치와 파밍사이트 유도를 위한 공격 절차에 관해 연구하였다. 그리고 경성포털을 대상으로 파밍 사이트 구현 기술에 관해 연구하여 이의 위험성을 알리고, 대응방안에 관해 연구하였다.

Ⅱ. DNS 스푸핑 기술

DNS 스푸핑(DNS Spoofing)은 DNS 서버에서 전달되는 IP 주소를 변조하거나 DNS 서버를 장악하여 거짓 IP 주소를 응답하여 DNS 서버를 속이는 공격기법을 말한다. 먼저 DNS 스푸핑의 기본 개념을 설명하고, 이의 공격방법에 관해 연구하였다.

2.1. DNS 스푸핑 개요

DNS는 Domain Name Service/System의 약자로, 사용자가 원하는 사이트로 연결을 요청하면 도메인명을 해당 사이트의 IP 주소로 변환해주는 서비스를 말한다. DNS 스푸핑은 네트워크 해킹 공격 기법 중 하나로 DNS 서버에서 전달되는 IP 주소를 변조하거나 DNS 서버를 장악하여 사용자가 접속하고자 하는 서버의 IP 주소가 아닌 거짓 IP 주소를 반환하여 속이는 공격기법을 말한다.

DNS 서버로부터 도메인이름에 대한 IP 주소를 얻는 과정은 그림 1의 예와 같다[1]. ① 클라이언트는 먼저 자신의 로컬 DNS 캐시에 www.naver.com의 IP 주소가 존재하는지 확인하고, 캐시에 없으면 /etc/hosts 파일을 참조한다. 만약 hosts 파일에도 없으면 로컬 DNS 서버에게 질의한다. ② ~ ⑦ 로컬 DNS 서버에 해당 정보가 없으면 루트 DNS 서버를 거쳐 구한 naver.com의 권한 DNS(authoritative DNS) 서버로 DNS 질의(query)를 보내 www.naver.com에 대한 IP 주소를 얻는다. ⑧ 로컬 DNS 서버는 이의 주소를 자신의 DNS 캐시에 저장하고 클라이언트로 응답한다. 클라이언트도 자신의 DNS 캐시에 저장하여 이후 동일한 웹서버를 재접근할 경우 이의 DNS 캐시를 참조하여 빠른 주소 변환이 이루어지도록 한다.

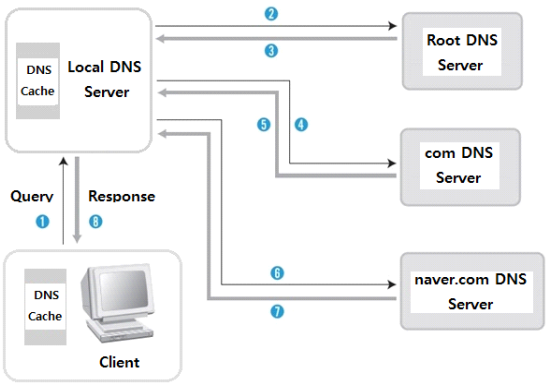

Fig. 1 DNS server's Address Resolution Procedure

DNS 스푸핑은 DNS 서버를 속여 실제 IP 주소가 아닌 거짓 IP 주소가 응답되도록 속이는 것인데, 여러 유형의 DNS 스푸핑 공격이 가능하다. 1) /etc/host 파일의 변경 2) 권한 DNS 서버의 존(zone) 파일을 직접 변경 3) 클라이언트 혹은 로컬 DNS 서버의 DNS 캐시를 오염(DNS cache poisoning)시킴으로써 DNS 스푸핑이 가능하다. 윈도우7 이후 보안조치로 /etc/host 파일의 변경은 관리자 권한이 주어진 경우에만 가능하고, 권한 DNS 서버의 직접 공격은 자체 보안으로 어려움이 있다.

DNS 시스템은 빠른 실시간 통신을 위해 UDP를 기반으로 구현되어 있어 TCP와 같은 연결 세션을 유지하지 않는다. 이로 인해 클라이언트는 요청한 DNS 쿼리에 대한 DNS 응답이 왔을 때 가장 먼저 도달한 DNS 응답만을 신뢰하고 늦게 도달한 DNS 응답은 버린다. 본 논문에서는 이러한 DNS 시스템의 취약점을 이용하여 공격자가 클라이언트와 DNS 서버 간의 통신에 직접 개입하여 권한 DNS 서버로 보내지는 DNS 질의를 가로채기 하여 가짜 IP 주소를 응답하여 클라이언트의 DNS 캐시를 오염시키는 DNS 스푸핑 공격에 관해 연구한다.

2.2. DNS 스푸핑 개념도

DNS 스푸핑은 공격자가 클라이언트와 DNS 서버 간의 통신에 개입해서 서버의 실제 IP 주소가 아닌 다른 IP 주소를 반환하여 DNS 서버를 속이는 것을 말한다.

1) DNS 쿼리 가로채기

DNS 스푸핑을 위해선 이의 준비단계로 ARP 스푸핑 공격을 먼저 수행해야 한다. ARP 스푸핑은 동일 LAN 상의 게이트웨이의 MAC 주소를 공격자의 MAC 주소로 속여 클라이언트와 서버 간의 모든 통신 패킷이 공격자를 거치도록 만든다[2]. 즉, 클라이언트가 공격자 컴퓨터를 게이트웨이로 잘못 알도록 속여 외부 서버 접근을 위해 게이트웨이를 거쳐야 하는 모든 패킷을 공격자 컴퓨터로 전송하게 만든다.

그림2와 같이 클라이언트가 외부망의 웹서버 접근을 위해 외부의 권한 DNS(authoritative DNS) 서버로 웹서버의 IP 주소를 물어볼 때 공격자가 이를 가로채어 파밍 사이트의 IP 주소를 클라이언트에게 응답한다.

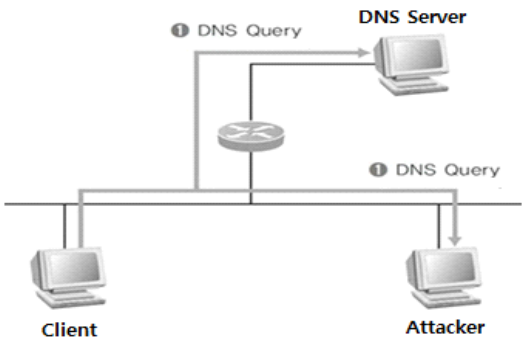

Fig. 2 Attacker's Interception of DNS Query

2) DNS 응답 위조

그림 3과 같이 외부망에 위치한 권한 DNS 서버가 올바른 DNS 응답을 보내기 전에, 지리적으로 가까운 곳에 위치한 공격자가 위조된 DNS 응답을 클라이언트로 먼저 보낸다. 클라이언트는 공격자가 보내준 가짜 IP를 자

신의 DNS 캐시에 저장하고, 뒤이어 날아온 올바른 DNS 응답은 이미 DNS 질의에 대한 응답이 이루어진 것으로 오인하여 버리게 된다.

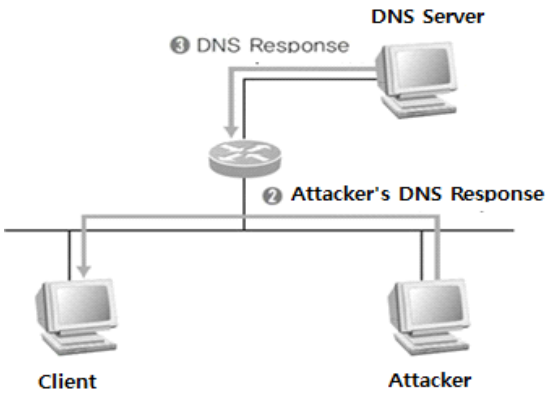

Fig. 3 Attacker's Fake of DNS Response

클라이언트는 공격자가 보낸 DNS 응답의 가짜 IP 주소의 파밍(pharming) 사이트로 접속하게 된다. 공격자가 만든 파밍 사이트는 사용자가 입력한 아이디와 패스워드 등의 사용자정보를 웹 프로그래밍으로 탈취하여 파일이나 데이터베이스에 저장할 수 있고, 사용자는 이를 전혀 인지하지 못하게 할 수 있다. 이의 구현방법은 Ⅳ장에서 자세히 다루었다.

2.3. 해킹 환경 구축

모의해킹을 위해 공격자는 VMware 상에 칼리(Kali) 리눅스를 장착하여 공격자의 기본 해킹 환경을 구축한다. 표 1의 해킹 환경 및 툴을 사용하였고, 모의해킹을 위한 네트워크 환경정보는 그림 4와 같다.

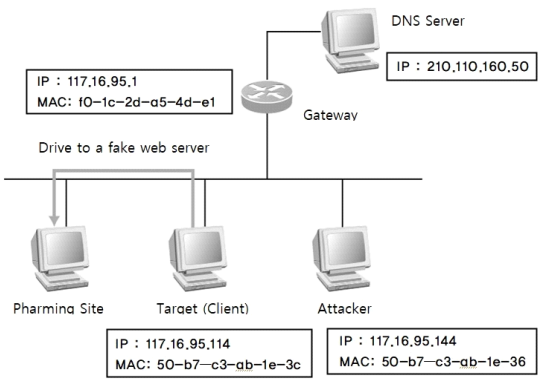

Fig. 4 Hacking Network Environment Information

Table. 1 Hacking Environment and Tools

Attacker System	VMware Workstation Pro 12 Kali Linux 2.0
Target System	Windows 10
Hacking Tools	Ettercap, Wireshark Fragrouter 1.6 Dsniff. i686 2.4 - 0.7.b1.fc12

Ⅲ. DNS 스푸핑 이용한 경성포털 해킹

DNS 스푸핑 공격을 위한 공격자 환경 구축과 파밍사이트로의 유도를 위한 DNS 스푸핑 공격의 방법 및 절차에 관해 연구하였다. 모의 해킹을 위한 웹 서버는 본 대학의 보안 취약점 분석을 위해 경성포털로 하였다. 경성포털은 별도의 외부 인증서버를 통한 SSL 암호화와 보안인증이 강화된 웹 서버이다.

3.1. 공격자 환경 구축

공격자는 VMware 상에 칼리(Kali) 리눅스를 설치하여 아래의 절차를 따라 기본 해킹 환경을 구축한다.

1) 공격자 가상머신 생성

공격자의 해킹 환경 구축을 위해 먼저 공격자 PC에 VMware를 설치한다. VMware Workstation Pro 12 버전을 설치하였다. VMware 가상머신 상에 공격자 머신을 생성하고, 다양한 해킹 툴이 제공되는 Kali 리눅스를 장착한다. 이의 자세한 설치과정은 생략하였다.

2) 공격자 네트워크 설정

네트워크 설정을 위해선 VMware를 마우스 우클릭하여 관리자 권한으로 실행해야 한다. [Edit]→[Virtual Network Editor...]를 클릭하여, 그림 5와 같이 [Add Network...]을 누르고 VMnet2를 추가한 후 Bridged 모드로 설정한다. 브리지(bridge) 모드는 실제 네트워크의 IP 주소로 동작하기 위한 모드이고, 그림 6과 같이 공격자의 IP 주소와 로컬 DNS의 IP 주소를 설정한다.

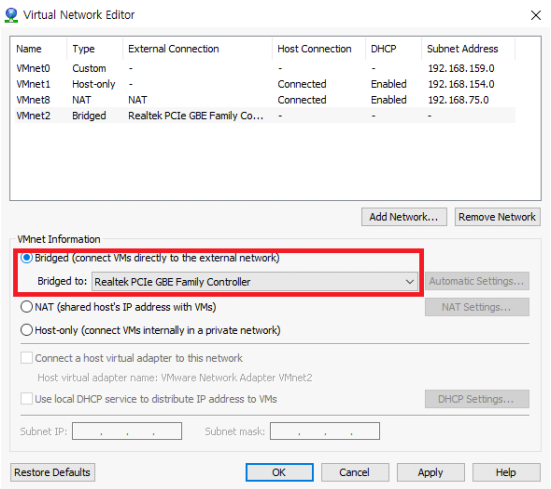

Fig. 5 Set to Bridged Mode

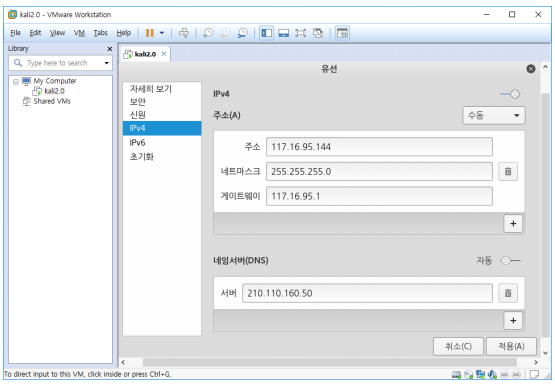

Fig. 6 Set Attacker's Network Address

3) 기본 해킹 툴의 설치 확인

Kail 리눅스에는 그림 7과 같이 Arpspoof, Fragrouter, Ettercap, Wireshark 등의 해킹 도구가 기본적으로 설치되어 있다[3]. Ettercap은 LAN상에서 '중간자 공격(MITM)'을 쉽게 할 수 있게 하는 해킹 툴로 그래픽 인터페이스를 제공한다. Wireshark는 네트워크에 오가는 패킷을 캡처해 분석할 수 있는 패킷분석기이다. Arpspoof는 Dsniff 패키지에 포함되어 있는 ARP 스푸핑을 위한 공격 툴이고, Fragrouter는 스니핑을 보조하는 도구로 포워딩 기능을 수행한다[4].

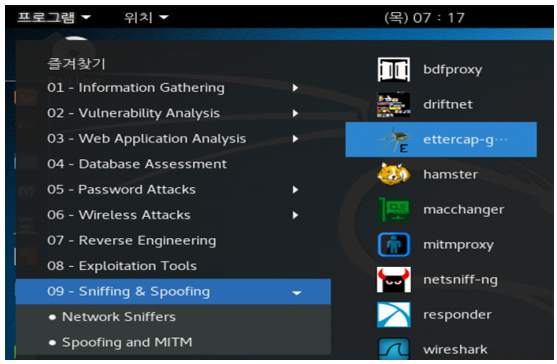

Fig. 7 Hacking Tools supplied on Kali Linux

3.2. 공격 방법 및 절차

공격자는 ARP 스푸핑을 통해 클라이언트의 모든 패킷을 스니핑 하고, DNS 스푸핑을 통해 클라이언트가 경성포털(portal.ks.ac.kr)을 접근할 때 공격자가 만든 가짜 파밍 사이트로 유도(117.16.95.144)한다. 이의 공격 방법 및 세부절차는 다음과 같다.

3.2.1. ARP 스푸핑 공격

DNS 스푸핑을 위해선 이의 준비단계로 ARP 스푸핑 공격을 먼저 수행하여야 한다[5-6].

1) 공격대상의 ARP Cache 확인 (공격전)

ARP 스푸핑 공격전 그림 8과 같이 공격대상 PC의 ARP Cache를 확인한다. 게이트웨이의 IP 주소는 117.16.95.1 이고, MAC 주소는 f0-1c-2d-a5-4d-e1 이다. 공격자의 IP 주소는 117.16.95.144 이고, MAC 주소는 50-b7-c3-ab-1e-36 이다.

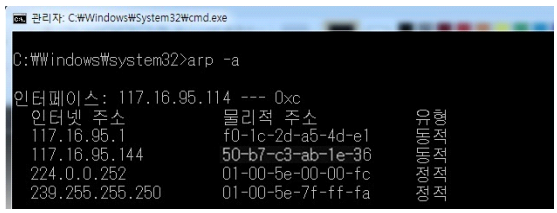

Fig. 8 ARP Cache of Target Client (Before Attack)

2) Ettercap 실행

Ettercap을 실행하고 그림 9와 같이 [Sniff]→[Unified sniffing]을 선택한다.

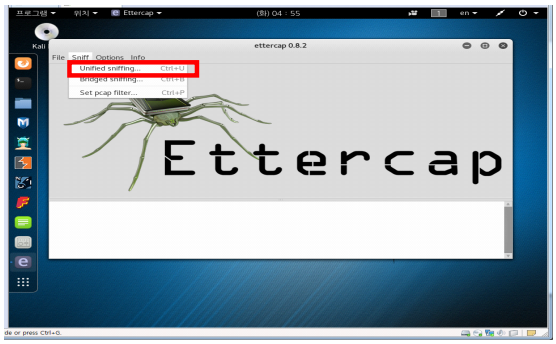

Fig. 9 Execute Ettercap

3) 공격대상 설정

먼저 그림 10과 같이 [Hosts]→[Scan for hosts]와 [Hosts list]를 순서대로 클릭하여 로컬 LAN 상에 동작 중인 컴퓨터를 리스트업 한다. 리스트에서 그림 11과 같이 공격대상을 선택한다. 그림 12와 같이 Target1에는 클라이언트 PC를 등록하고, Target2에는 Default 게이트웨이를 등록한다.

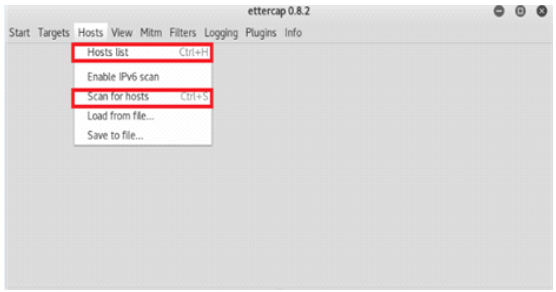

Fig. 10 Scan for Hosts on Local LAN

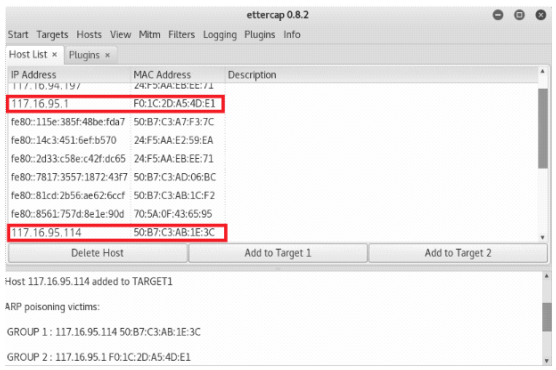

Fig. 11 Scanned Hosts List

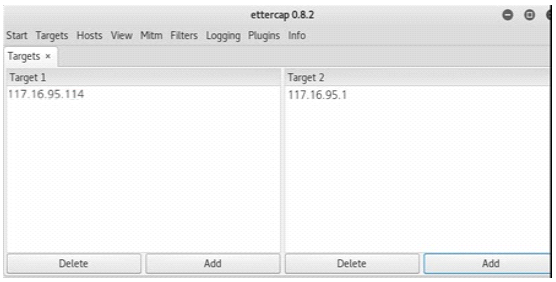

Fig. 12 Register ARP Spoofing Targets

4) ARP 스푸핑 공격 시행

ARP 스푸핑 공격 유형 선택을 위해 그림 13과 같이 [Mitm]→[ARP poisoning]을 클릭하여 [Sniff remote connections]를 체크한다. 이는 클라이언트와 GW 양쪽 모두에게 상대방의 MAC 주소를 공격자의 MAC 주소로 속이는 ARP Reply를 전송한다. 이로 인해 클라이언트와 GW간의 모든 통신 패킷이 공격자를 거치게 되어 스니핑 할 수 있다. 그림 14와 같이 [Start]→[Start sniffing]을 클릭하여 ARP 스푸핑 공격을 실행하여 스니핑을 시작한다.

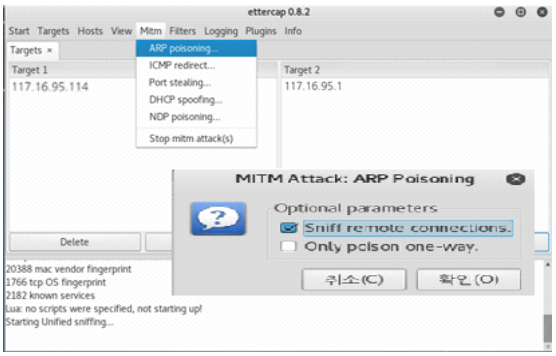

Fig. 13 Select ARP Spoofing Attack

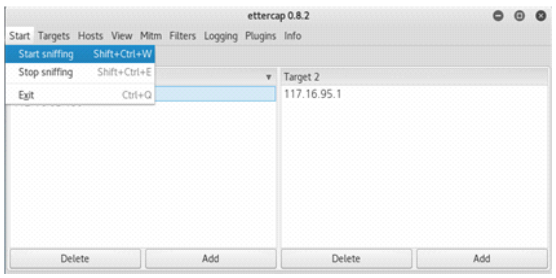

Fig. 14 Execute ARP Spoofing Attack

5) 공격대상의 ARP Cache 변경 (공격후)

ARP 스푸핑 공격으로 그림 15와 같이 게이트웨이의 MAC 주소가 공격자의 MAC 주소 50-b7-c3-ab-1e-36으로 변경된 것을 확인할 수 있다.

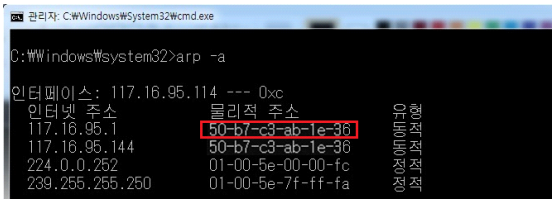

Fig. 15 ARP Cache of Target Client (After Attack)

3.2.2. DNS 스푸핑 공격

DNS 스푸핑을 공격을 통해 경성포털의 접근시 파밍 사이트로 유도한다.

1) DNS 환경 파일 수정

/etc/ettercap/etter.dns 파일을 그림 16과 같이 수정하여 클라이언트가 경성포털(portal.ks.ac.kr)을 접근하고자 하면 파밍사이트(117.16.95.144)로 유도되도록 한다.

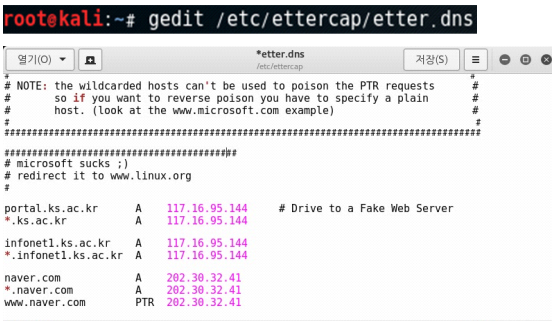

Fig. 16 Modify etter.dns for driving to pharming site

2) DNS 스푸핑 공격 시행

DNS 스푸핑 공격은 2가지 방법의 실행이 가능한데, 그림 17과 같이 [Plugins]→[Manage the plugins]를 클릭하여 목록 중 dns_spoof 항목을 더블클릭 하면 DNS 스푸핑 공격이 시행된다.

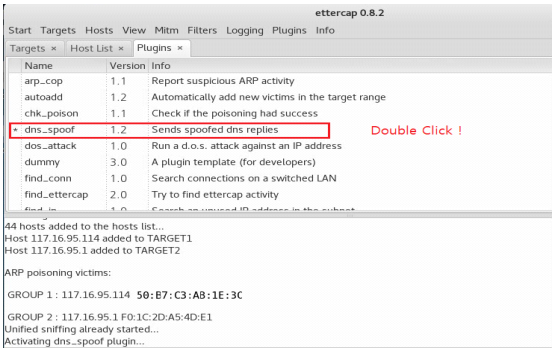

Fig. 17 Execute DNS Spoofing Attack (graphic mode)

3) DNS 스푸핑 공격 성공

ping 명령을 통해 DNS 스푸핑 공격의 성공을 확인 할 수 있다. portal.ks.ac.kr의 IP 주소가 그림 18과 같이 공격자가 응답한 파밍사이트의 주소(117.16.95.144)로 바뀐 것을 알 수 있다.

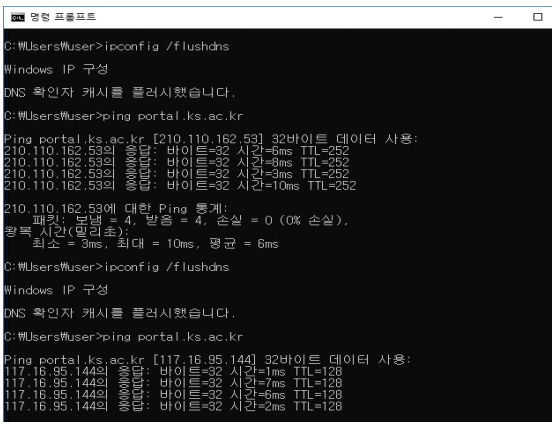

Fig. 18 Success of DNS Spoofing Attack

3.3. 경성포털 해킹

공격자의 DNS 스푸핑 공격으로 공격자가 만든 가짜 파밍 사이트로 유도하여 사용자의 아이디와 패스워드 등의 개인정보를 취득할 수 있다. 경성포털의 해킹을 위해 그림 19와 같이 원래 사이트와 완전히 동일한 경성포털의 초기화면을 어렵지 않게 만들 수 있다.

사용자가 아이디와 비밀번호를 입력 후 로그인 버튼을 누르면, 공격자의 해킹 프로그램이 실행되고, 사용자 아이디와 비밀번호를 입력받아 파일에 기록한 후, 사용자에게는 그림 20의 비밀번호 입력 오류메시지를 띄운

다. 사용자가 확인버튼을 클릭하면, 이번에는 원래의 경성포털로 접속하여 사용자 아이디와 비밀번호를 입력받아 정상적인 로그인이 이루어지도록 한다.

사용자 측에서 볼 때는 자신의 실수로 비밀번호 입력 오류가 발생하였던 것으로만 인지하지만 해킹 프로그램에 의해 그림 21과 같이 사용자 아이디와 비밀번호를 탈취할 수 있다. 이와 같이 가짜 초기화면과 웹 프로그래밍으로 파밍사이트를 만들고, DNS 스푸핑으로 유도하면 사용자는 이를 전혀 인지할 수 없기에 심각한 보안의 위험이 있다.

현재 대부분의 웹 서버는 보안조치가 이루어져 있지 않은 상태이다. 경성포털의 경우 SSL(Secure Socket Layer)에 의한 암호화와 보안인증이 이루어진 웹 서버임에도 불구하고 이를 무력화시키는 회피공격이 가능하다는 것이다. 그리고 암호 통신을 하지 않는 웹 서버의 경우에는 Wireshark를 이용한 패킷 분석만으로도 사용자의 아이디와 비밀번호를 읽어낼 수 있다.

Fig. 19 Pharming Site of Kysungsung Portal

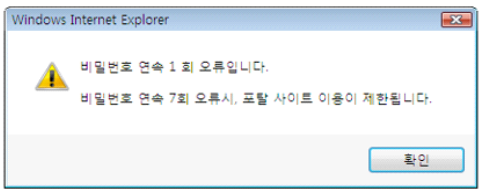

Fig. 20 Login Error Message

```
id : qweqweqw
passwd : eqweqweqweqwe
ip : 202.30.32.160
등록일자 : 2019년 05월 08일 06시 06분 00초
================================================

id : 5235
passwd : 12341234
ip : 210.110.180.187
등록일자 : 2019년 05월 08일 06시 07분 51초
================================================

id : kdw3479
passwd : apfhd
ip : 202.30.32.160
등록일자 : 2019년 05월 08일 06시 28분 07초
================================================
```

Fig. 21 Hacking of User's ID and Password

Ⅳ. 파밍 사이트 구현과 위험성

파밍 사이트의 구현 방법과 해킹 프로그램의 구현에 관해 연구하였고, 이의 위험성과 대응방안에 관해 연구하였다.

4.1. 파밍 사이트 구현 방법

원래 사이트와 완전히 동일한 경성포털의 초기화면은 어렵지 않게 만들 수 있다.

1) 초기화면 웹페이지 복사하기

웹페이지의 소스는 해당 브라우저의 '소스보기' 기능을 이용해 볼 수 있고 이를 복사할 수 있다. Kali에서 Firefox를 실행 후 경성포털에 접속한다. 그림 22와 같이 웹브라우저의 [File]→[Save Page As...]를 선택하여 /var/www/html/index.html 경로에 그림23과 같이 저장한다.

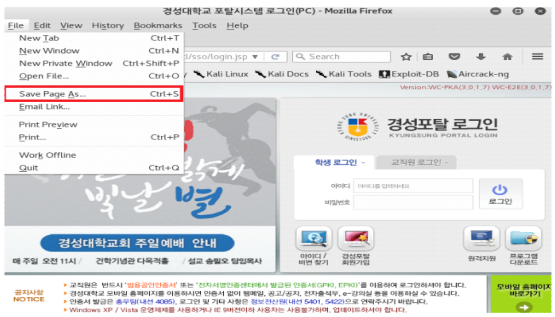

Fig. 22 Click 'Source View' menu on Index Page

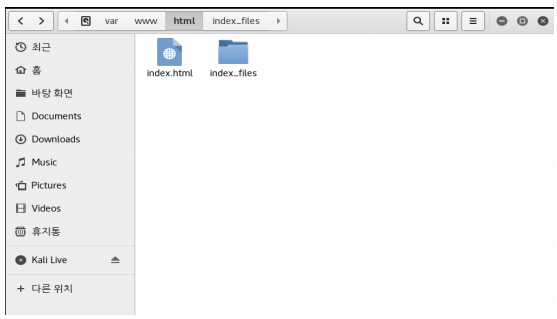

Fig. 23 Save Source of Index Page to index.html

'Save Page As' 기능을 이용하면 해당 웹페이지에 포함된 그림들을 한꺼번에 다운받아 그림 24와 같이 저장할 수 있다.

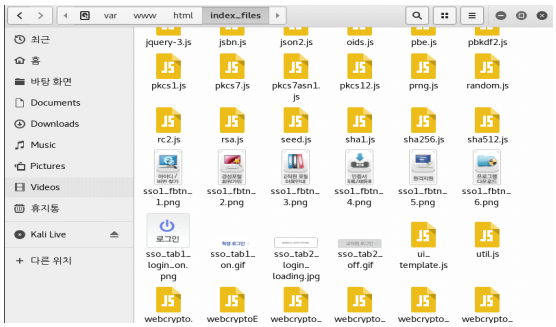

Fig. 24 Download and Save Sources of Index Page

2) URL 접근 이미지 저장하기

그림 25와 같이 인터넷에서 URL로 접근하는 배경 이미지는 직접 URL로 접근해서 마우스 우클릭을 통해 이미지를 저장한다. 이의 이미지는 소스의 경로와 동일하게 /var/www/html/_res 폴더를 만들어 저장한다.

Fig. 25 Save Source of Index Page to index.html

4.2. 파밍 사이트 구현 프로그램

사용자가 로그인 버튼을 눌렀을 때, 사용자 아이디와 비밀번호를 탈취하는 해킹 프로그램을 분석하였다.

1) 로그인 버튼 클릭시 실행 함수 찾기

먼저 그림 26과 같이 index.html 소스를 분석하여 로그인 버튼을 클릭시 실행되는 로그인 함수 idpwLogin()을 찾는다.

```
<div class="btn1" id="btn1Area">
    <input width="63" height="63" id="tabArea1Img" onclick="idpwLogin(this.form);
    return false;" type="image" alt="경성포탈에 로그인합니다." src="./_res/sso_tab1_
    login_on.png" />
</div>
```

Fig. 26 idpwLogin() Function called on Click Login

2) 웹서버 인증 프로그램 호출 변경

idpwLogin() 함수를 분석하여 그림 27과 같이 웹서버의 인증 프로그램을 호출하는 부분을 찾아 해킹 프로그램(Login.jsp)이 호출되도록 변경한다. 경성포털의 경우 SSL에 의한 암호화와 보안인증이 이루어진 웹 서버임에도 불구하고, 이를 우회하여 해킹 프로그램의 실행이 가능하다. 아이디와 패스워드를 암호화 통신을 하는 경우에도 이를 주석처리한 후 우회 실행이 가능하다. 즉, 현재 많은 웹 서버가 보안조치가 이루어져 있지 않고, SSL에 의한 암호화와 보안인증이 이루어진 웹 서버라 할지라도 무력화 시킬 수 있는 점에 보안 문제의 심각성이 있다.

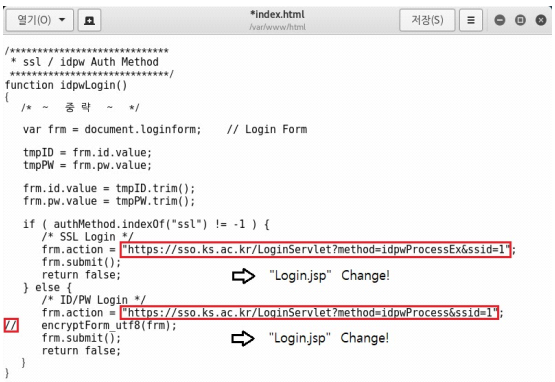

Fig. 27 Change Authentication Program's Name

3) 해킹 프로그램 구현

해킹 프로그램은 그림 28과 같이 JSP(혹은 PHP) 웹 프로그램으로 간단히 구현할 수 있다. 사용자가 입력한 아이디와 비밀번호를 입력받아 파일에 기록한 후, 사용자에게는 그림 20과 같은 비밀번호 입력 오류메시지를 띄운다. 사용자가 확인버튼을 클릭하면, 이번에는 원래의 경성포털로 포워딩하여 사용자 아이디와 비밀번호를 입력받아 정상적인 로그인이 이루어지도록 한다. 본 해킹 프로그램의 일부 소스는 보안 위험의 심각성을 고려하여 공개하지 않도록 한다.

```
<%
try {
    String [] params = request.getParameterValues("params");

    FileWriter b=new FileWriter("KSParmingdata.txt",true);
    BufferedWriter a=new BufferedWriter(b);

    Timestamp now = new Timestamp(System.currentTimeMillis());
    SimpleDateFormat format = new SimpleDateFormat("yyyy년 MM월 dd일 hh시 mm분 ss초");
    String strDate = format.format(now);


    a.write("id : "+ params[0]+"\r\n");
    a.write("passwd : "+ params[1]+"\r\n");
    a.write("ip : "+ params[2]+"\r\n");
    a.write("등록일자 : "+strDate+"\r\n");

    a.write("==========\r\n\r\n");
    a.flush();
    a.close();

}
catch(Exception e) {
    e.printStackTrace();
}
%>
```

Source Hidden Due to a Security Risk Reason !

Fig. 28 Implementation of Hacking Program

4.3. DNS 스푸핑 공격 패킷 분석

DNS 스푸핑 공격으로 클라이언트의 portal.ks.ac.kr 접근을 위한 DNS 쿼리에 대한 공격자가 조작한 DNS 응답에 파밍사이트의 주소(117.16.95.144)가 실린 것을 그림 29의 패킷 분석을 통해 확인할 수 있다. 이러한 네트워크 프로토콜 패킷은 Raw Socket을 이용하여 전송할 수 있으며, socket() 함수의 두 번째 매개변수를 SOCK_RAW로 설정하면 된다.

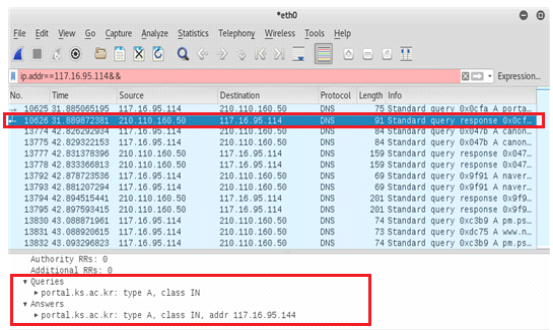

Fig. 29 Packet Analysis of DNS Spoofing Program

4.4. 웹 스푸핑의 위험성과 대응방안

DNS 스푸핑과 파밍사이트 구현이 결합된 웹 스푸핑 공격의 위험성과 대응방안에 관해 연구하였다.

1) 웹 스푸핑의 위험성

DNS 스푸핑과 파밍사이트 구현이 결합된 웹 스푸핑 공격은 사용자가 이를 전혀 인지하지 못하게 할 수 있다. DNS 스푸핑은 DNS 취약점을 이용하여 공격자가 클라이언트와 DNS 서버간 통신에 개입하여 가짜 IP 주소를 응답하여 파밍 사이트로 유도한다. 이의 공격은 클라이언트의 DNS 캐시를 오염시킬 뿐만 아니라 동일한 방식으로 로컬 DNS 서버의 DNS 캐시를 오염시킬 수도 있다. 또한 원래 사이트와 완전히 동일한 초기화면은 어렵지 않게 만들 수 있다. 그리고 간단한 웹 프로그래밍 기술을 사용하여 첫 로그인 시에는 사용자에게는 비밀번호 입력 오류를 알리고, 재 로그인 시에는 원래 사이트로 포워딩하여 정상 로그인이 이루어지도록 하여 이를 전혀 인지하지 못하게 할 수 있다.

경성포털의 경우 SSL에 의한 암호화와 보안인증이 이루어진 웹 서버임에도 불구하고, 이를 우회하여 해킹 프로그램의 실행이 가능하고, 암호화 통신을 하는 경우에도 이를 주석처리한 후 우회 공격이 가능하다. 현재 많은 웹 서버가 보안조치가 이루어져 있지 않은 상태이고, SSL에 의한 암호화와 보안인증이 이루어진 웹 서버라 할지라도 이를 무력화 시킬 수 있다는 점에서 보안 문제의 심각성이 있다. 주요 포털을 대상으로 한 해킹이 많이 발생 할 수 있으므로 이의 대응방안에 관한 연구와 조치가 꼭 이루어져야 하는 상황에 있다.

2) 대응방안

ARP 스푸핑은 대부분의 스니핑에 근간되는 공격이므로 이를 차단하는 것이다. 이를 위한 방법은 여러 가지가 있으나 가장 좋은 방법은 데이터를 암호화 하는 것이다. SSL을 이용한 어플리케이션 레벨의 데이터 암호화는 본 논문에서 다룬 바와 같이 우회 공격이 가능하므로, ARP 프로토콜 레벨의 암호화가 이루어지도록 하여야 한다. 그러므로 하드웨어 스위치 장치에서 ARP 스푸핑을 차단하는 방법이 효과적인 방법이 될 수 있다. 침입방지탐지시스템(IPS)의 도입으로 ARP 스푸핑을 패턴을 탐지하여 이를 차단하는 방법이나 OS 레벨(ARP 레벨)에서 ARP 스푸핑을 패턴을 탐지하여 이를 차단하는 보안패치도 대안이 될 수 있다.

DNS 스푸핑은 공격자가 클라이언트와 DNS 서버 간의 통신에 개입해서 실제 IP가 아닌 다른 IP를 반환하거나, DNS 서버의 IP 스푸핑으로 파밍 DNS 서버에 의해 다른 IP를 반환하는 공격이다. 이를 위한 방법은 여러 가지가 있으나 가장 효율적인 방법은 클라이언트의 웹 브라우저에 DNS 보안 에이전트를 설치하여 브라우저와 DNS 서버간의 인증과 암호화를 하는 방법이다. 그리고 보안 DNS에 의한 DNS 서버간의 인증과 암호화가 이루

어지도록 하는 방법도 가능하다[7-8].

HSTS(HTTP Strict Transport Security)란 웹 브라우저가 HTTPS 프로토콜만을 사용해서 서버와 통신하도록 강제하는 보안기능이다[9]. 이는 최초 접속시부터 https로만 접속하도록 강제함으로써 SSL 우회를 통한 웹 스푸핑 공격을 차단할 수 있도록 한다.

Ⅴ. 결 론

DNS 스푸핑은 DNS 취약점을 이용하여 공격자가 클라이언트와 DNS 서버간 통신에 개입하여 가짜 IP 주소를 응답하여 파밍 사이트로 유도하는 공격이다. DNS 스푸핑과 파밍사이트 구현이 결합된 웹 스푸핑 공격이 이루어지면 사용자 아이디와 비밀번호 탈취를 사용자는 전혀 인지하지 할 수 없다. 이에 파밍사이트로 유도하는 DNS 스푸핑과 파밍사이트 구현을 결합한 웹 스푸핑 공격에 관해 연구하였다.

경성포털은 별도의 외부 인증서버를 통한 SSL 암호화와 보안인증이 강화된 웹 서버이고, 본 대학의 보안 취약점 분석을 위해 모의해킹 대상을 경성포털로 하였다. VMware에 Kali 리눅스를 설치하여 공격자 환경을 구축하고, DNS 스푸핑 공격 방법과 절차에 관해 연구하였다. 그리고 경성포털을 대상으로 파밍 사이트 구현에 관해 연구를 하였다. 동일한 초기화면의 제작과 웹 프로그래밍으로 어렵지 않게 파밍 사이트의 구현과 사용자 아이디와 비밀번호 해킹이 가능함을 확인하였다.

경성포털의 경우 SSL에 의한 암호화와 보안인증이 이루어진 웹 서버임에도 불구하고, 우회 공격이 가능하였다. 사용자가 로그인 시 비밀번호 입력 오류창을 띄워 단순 입력 실수로 인지하게 한 후, 아이디와 비밀번호를 해킹한 후 원래 사이트로 포워딩하여 재 로그인을 하게 하여 해킹을 전혀 인지 못한다. 현재 많은 웹 서버가 보안조치가 이루어져 있지 않은 상태이고, SSL에 의한 암호화와 보안인증이 이루어진 웹 서버라 할지라도 이를 무력화 시킬 수 있다는 점에서 보안 문제의 심각성이 있다. 주요 포털을 대상으로 한 해킹이 많이 발생 할 수 있으므로 이의 대응방안에 관한 연구와 조치가 꼭 이루어져야 하는 상황에 있다. 향후 DNS 스푸핑과 파밍사이트 구현이 결합된 웹 스푸핑 공격의 대응방안에 관한 후속 연구를 계속할 것이다.

ACKNOWLEDGEMENT

This research was supported by Kyungsung University Research Grants in 2018.

REFERENCES

[1] D. I. Yang, *Network Hacking and Security*, Seoul, Korea: Hanbit Media Inc., ch. 3, pp. 128-129, 2016.

[2] J. W. Choi, “Research on Network Hacking and Implementation Techniques using ARP Redirect Method according to Server Types,” *Jounal of Kysungsung Univ. RIET*, vol. 23, pp. 1-11, Feb. 2017.

[3] S. H. Moon, *Learning hacking and security with Kali Linux*, Seoul, Korea: BPAN Books Pub., ch. 1, pp.10-11, 2016.

[4] Naver Blog. Introduction to the sniffing tools Dsniff [Internet]. Available: http://kkn1220.tistory.com/72.

[5] J. W. Choi, “Network Hacking and Implementation Techniques using Faked ARP Reply Unicast Spoofing according to various Server Types,” *Journal of Korea Institute of Information and Communication Engineering*, vol. 21, no. 1, pp. 61-71, Jan. 2017.

[6] Deepak Devanand, ARP Cache in Windows [Internet]. Available:https://windowswizardry.wordpress.com/2017/05 /22/arp-cache-in-windows, May 22, 2017.

[7] KISA, DNSSEC (Domain Name System Security Extension) Concept [Internet]. Available:https://kisa.kr/jsp/resources/dns/dnssecInfo/dnssecInfo.jsp, 2019.

[8] V. Bhavana, “Data Security in Cloud environments,” Asia-pacific Journal of Convergent Research Interchange, HSST, ISSN : 2508-9080, vol.1, no.4, (2015,December). pp. 25-31, [Internet]. Available: http://dx.doi.org/10.21742/APJCRI.2015.12.04.

[9] RSEC.KR, HSTS (HTTP Strict Transport Security) Concept and Setup[Internet]. Available: https://rsec.kr/?p=315, Jul. 28, 2017.

최재원(Jae-Won Choi)

1988년 2월 고려대학교 컴퓨터공학과(공학사)
1990년 8월 미시간주립대학교 컴퓨터공학과 (공학석사)
1995년 8월 건국대학교 전자공학과 (공학박사)
1990년 10월 ~ 1997년 8월 삼성전자 통신연구소 선임연구원
1997년 9월 ~ 2019년 現 경성대학교 컴퓨터공학과 교수
※관심분야 : 정보통신, 정보보안, 인터넷응용, 모바일앱