취약점 분석 보고서

Simple Web Server 2.2 rc2 Remote Buffer Overflow Exploit

2012-07-19

RedAlert Team 안상환

목 차

그림 목차

1. 개 요

1.1. 취약점 분석 추진 배경

본 취약성을 가진 프로그램은 간단한 설치만으로 웹 서버를 구축할 수 있는 프로그램입니다. 주로 일반 사용자들이 사용 하고 있습니다.
그렇기 때문에 본 취약성을 이용한 공격은 기업보다는 개인을 타깃으로 한 공격에 사용 될 수 있습니다.
일반 사용자는 해당 프로그램을 사용하여 간단하게 웹 서버를 구축 할 수 있지만, 취약한 프로그램을 포함한 이와 비슷한 종류의 프로그램들은 공격자로부터 전송된 공격코드에 유연하게 대처하지 못하는 실정입니다. 더욱이 피해자는 공격을 당하더라도 전문적인 지식 없이는 이를 인지하지 못하며, 공격자는 피해자 시스템을 기점으로 한 2 차,3 차 공격을 감행할 수 있습니다.

2. Simple Web Server 취약점

2.1. Simple Web Server 취약점 개요

취약점 이름	Simple Web Server 2.2 rc2 Remote Buffer Overflow Exploit		
최초 발표일	2012 년 07 월 19 일	문서 작성일	2012 년 7 월 19 일
제품	Simple Web Server (2.2)	벤더	personal
공격 범위	Remote / Network Access	공격 유형	Stack Buffer Overflow
취약한 OS	Windows	위험 등급	위험
취약점 영향	원격 코드 실행 및 서비스 거부 발생	CVE-ID	N/A

표 1 Simple Web Server 취약점 개요

Windows 기반의 웹 서버 구축 프로그램인 Simple Web Server 에서 발생한 Buffer Overflow 취약점입니다.
해당 취약점을 이용한 공격은 원격을 통해 가능하며 원격 공격자는 취약 웹 서버를 대상으로 특수하게 제작된 패킷을 전송함으로써 원격 코드 실행 및 서비스 거부를 발생 시킬 수 있습니다.

2.2. Simple Web Server 취약점 테스트 시스템 목록

Simple Web Server 취약점을 이용한 공격은 XP SP3 32bit 영문 버전에서 테스트 하였습니다.

- Microsoft Windows XP Professional SP3

표 2 취약한 시스템

2.3. Simple Web Server 취약점 공격 기법 원리

해당 취약점은 클라이언트로부터 전송된 웹 페이지 요청 구문을 웹 서버에서 분석하는 과정에서 발생하는 Buffer Overflow 취약점 입니다. 공격자는 특수하게 제작한 긴 요청구문을 서버로 전송하여 Buffer Overflow 를 발생 시킬 수 있으며, 이를 이용하여 공격자는 프로그램의 흐름을 원하는 주소로 변경 할 수 있습니다. 피해자 시스템은 해당 프로그램을 이용하여 웹 서버를 운용하기만 하여도 시스템의 최고 관리자 권한을 탈취 당할 뿐만 아니라, 임의의 코드 실행 및 서비스 거부가 발생 할 수 있습니다.

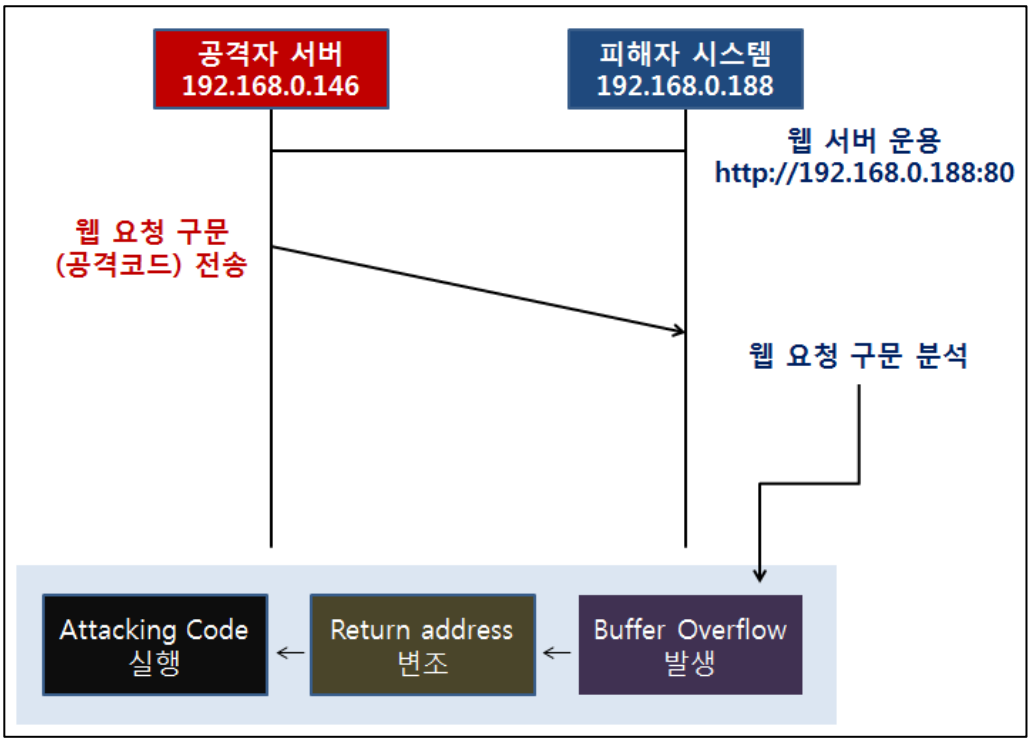

그림 1 Simple Web Server Buffer Overflow 공격 개요도

첫째, 공격자는 피해자 시스템으로부터 운용중인 웹 서버로 공격코드가 삽입된 웹 요청 구문을 전송합니다.
둘째, 취약한 웹 서버에서는 공격자로부터 전송된 패킷을 분석하기 시작하는데, 이 과정에서 Buffer Overflow 가 발생합니다.
셋째, Buffer Overflow 가 발생하여 인접 스택의 데이터 및 return address 를 변조하여, 프로그램의 흐름을 변경 / Attacking Code 를 실행 합니다.

3. 분 석

3.1. 공격 테스트

<그림 2>은 해당 취약점을 가진 프로그램을 실행시킨 화면입니다. <그림 3>은 취약한 웹 서버 메인 페이지입니다. 공격자는 해당 웹 서버가 동작 할 때 공격 할 수 있습니다.

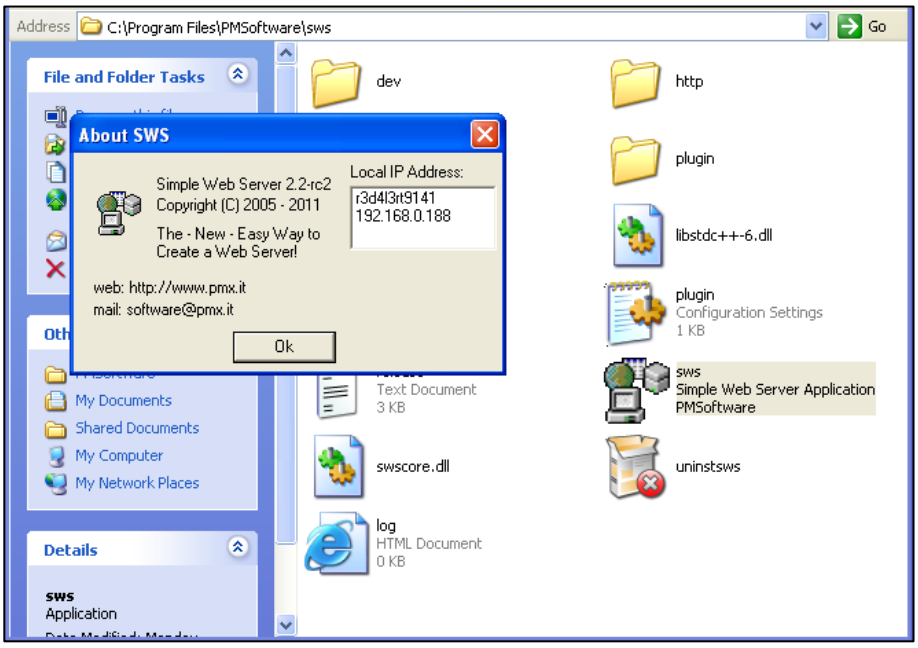

그림 2 취약한 프로그램

그림 3 운용중인 웹 서버

공격코드는 아래 <그림 3>과 같습니다.

메모리 내 삽입된 Shellcode 를 검색해 실행하는 Egg Hunter 기법을 사용하고 있으며, 직접적으로 Return Address 를 변조하여 Egg Hunter Code 로 이동 하도록 합니다.

그림 4 공격코드

피해자 시스템의 대상 프로그램을 타깃으로 공격코드를 실행하여 피해자 시스템의 관리자 권한을 획득 한 것을 <그림 5>를 통해 확인 할 수 있습니다.
공격이 완료 된 후 대상 프로그램은 종료 되지 않고 정상 동작하며, 공격자가 Session 을 종료 시킬 때 대상 프로그램은 종료 됩니다. 이는 피해자가 전문적 지식이 있지 않고서 자신의 시스템 관리자 권한이 탈취당한 것을 인지 할 수 없습니다.

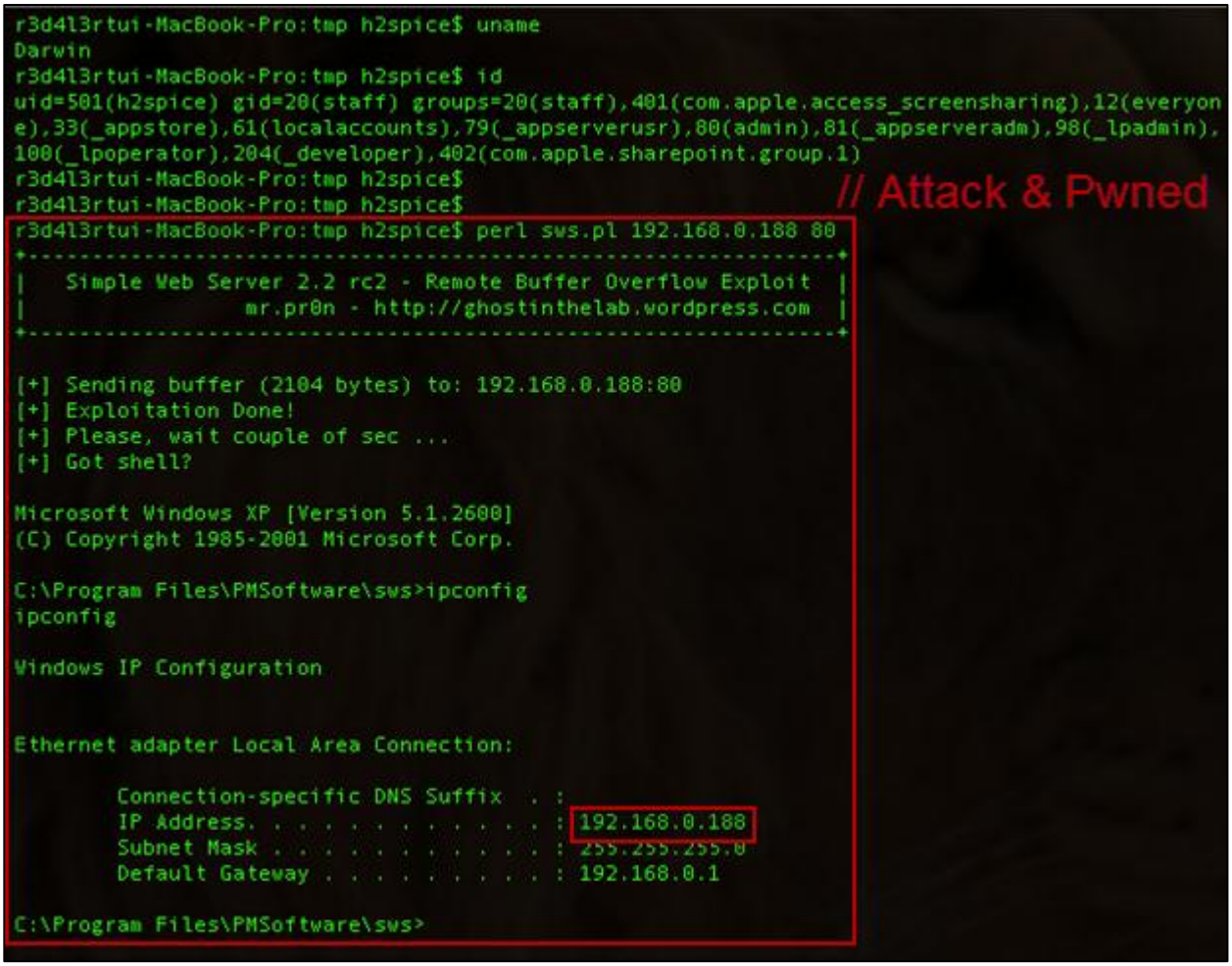

그림 5 피해자 시스템 권한 탈취

피해자는 아래 명령이나 netstat –an 과 같은 Session 연결 상태를 확인 하는 명령을 사용하여 해킹 여부를 확인 할 수 있습니다.

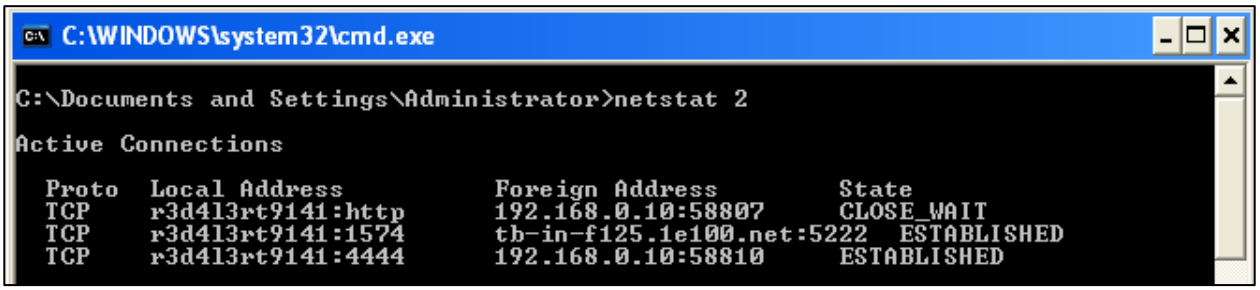

그림 6 피해자 시스템 네트워크 연결 상태

3.2. 공격 기법 분석

본인은 immunity Debugger 를 이용하여 분석하였습니다..

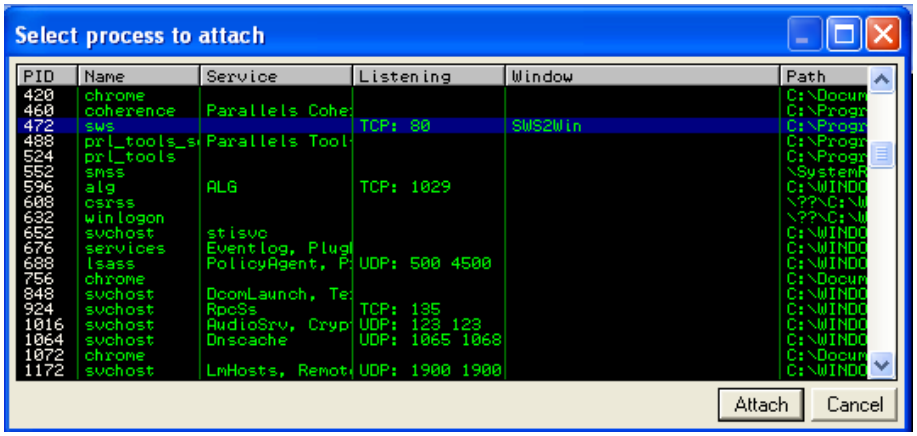

그림 7 immunity Debugger 를 이용하여 디버깅

공격자로부터 공격코드가 삽입된 패킷이 전송되면 대상 프로그램은 해당 요청 구문을 분석하는 과정에서 Buffer Overflow 가 발생하게 됩니다.

<그림 8>을 통해 Stack 의 데이터들이 변조 된 것을 확인 할 수 있습니다.

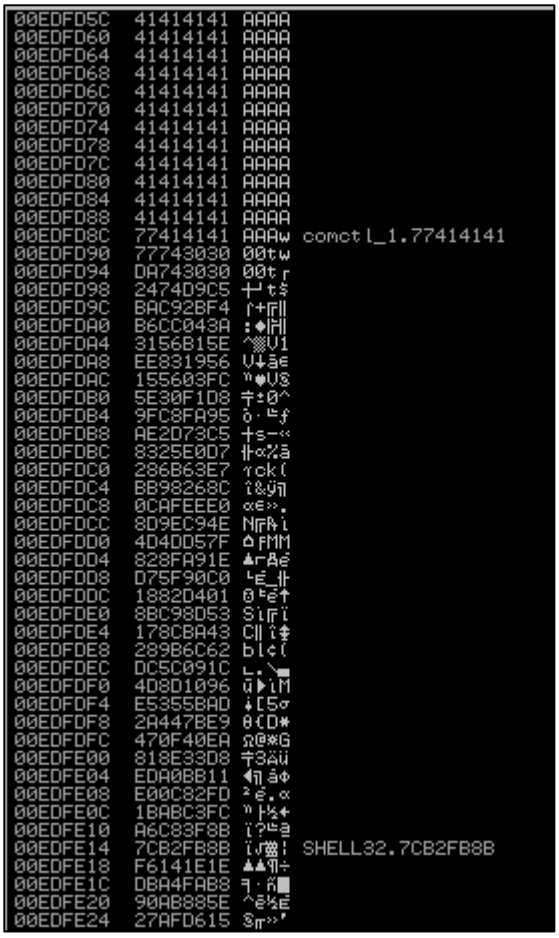

그림 8 Stack 에 삽입된 공격코드

Buffer Overflow 로 인해 인접 스택의 데이터 침범 및 변조가 발생하여 Return Address 의 본 주소도 변조 된 것을 확인 할 수 있습니다. 변조된 Return Address 의 주소는 kernel32 의 JMP ESP 주소로써, 메모리에 삽입된 Egg Hunter Code 로 이동하도록 합니다.

그림 9 Return Address 변조

JMP ESP 코드가 동작하고 Attacking Code 인근 Nop sled 로 이동하게 됩니다.
Nop sled 를 타고 Egg Hunter Code 가 실행됩니다.

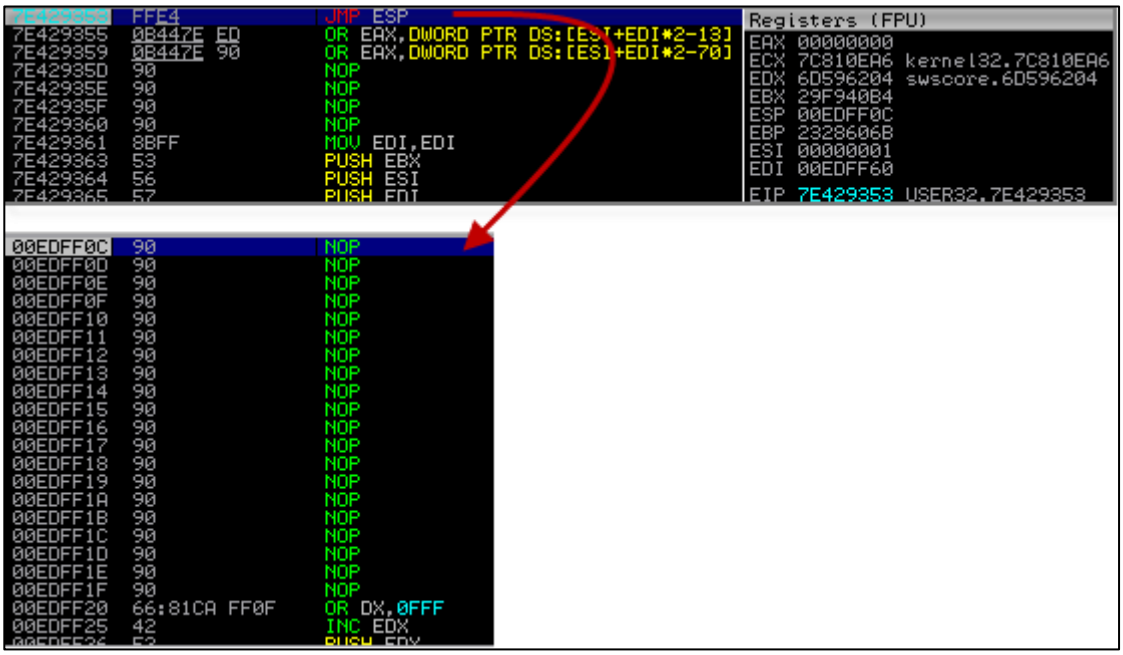

그림 10 JMP ESP 동작

<그림 11>은 Egg Hunter Code 가 실행되는 모습입니다.

Egg Hunter Code 는 메모리 내 위치한 Shellcode 를 검색하여 실행하는 역할을 하고 있습니다.

그림 11 Egg Hunter Code 실행

Egg Hunter 코드가 Shellcode 를 검색하는 알고리즘은 간단한 검색 알고리즘으로 Shellcode 앞에 위치한 Tag 로 불리는 유니크한 문자열을 검색하여 Shellcode 의 위치를 찾고 해당 위치로 이동하게 됩니다.

아래 <그림 12>는 Egg Hunter Code 가 정상적으로 동작하여 Shellcode 로 이동한 화면이며 Shellcode 가 실행 됩니다.

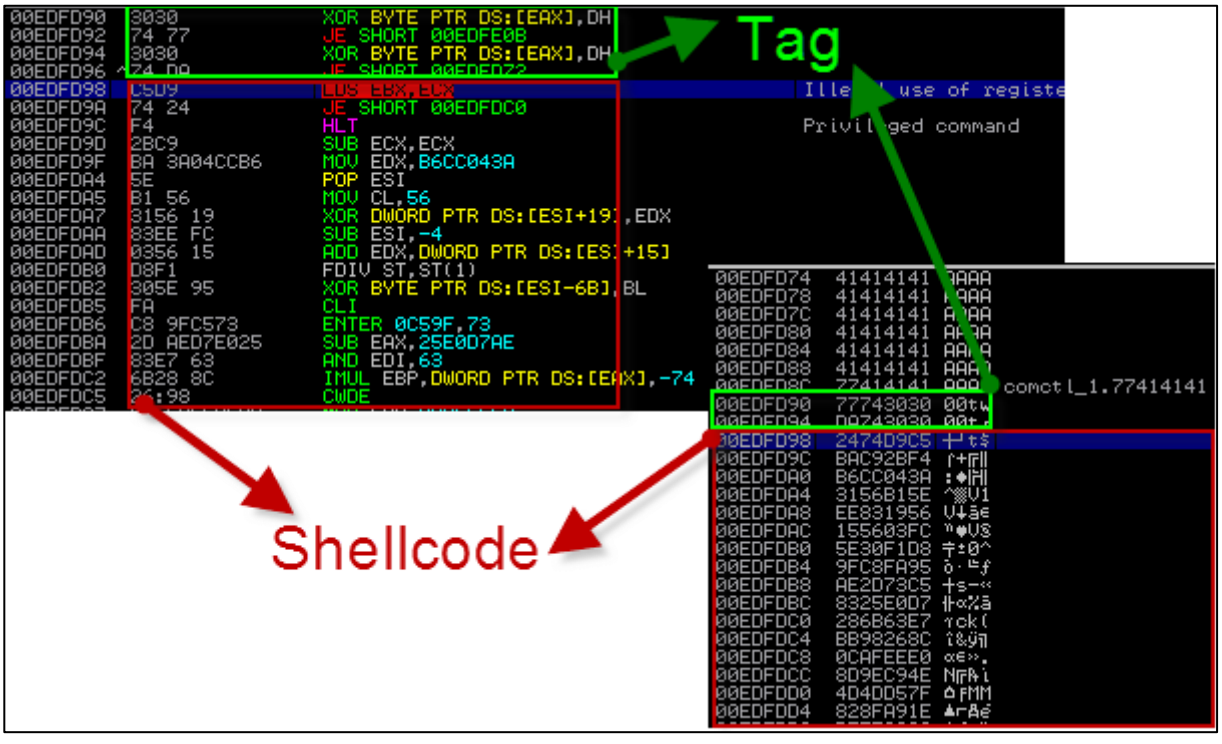

그림 12 Shellcode 실행

Shellcode 가 정상적으로 실행되고 공격자 시스템과 Session 이 연결된 것을 확인 할 수 있습니다.

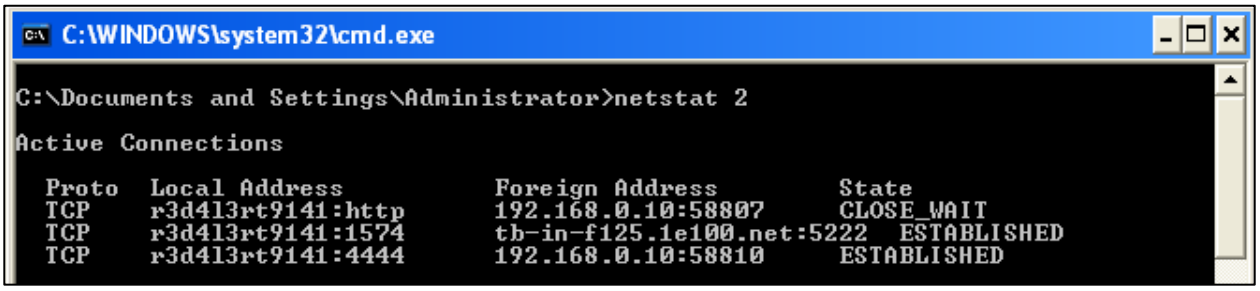

그림 13 공격자 시스템과 Session 연결

4. 결 론

대상 프로그램은 간단한 방법으로 Attacking code 를 실행 시킬 수 있었습니다.
위에서 테스트한 공격은 고급 기술을 요구하지 않고 간단한 Buffer Overflow 지식만으로도 해당 공격을 수행 할 수 있습니다. 간단한 지식만으로 할 수 있는 공격치고는 너무나 위협적인 결과를 보여주며, 해당 공격을 통해 2 차, 3 차 공격을 감행 하여 더 큰 피해를 입힐 수 있습니다.
이러한 부분으로 인하여 사용자뿐만 아니라 개발사 또한 큰 피해를 입을 수 있으며, 개발사에서는 제품 출시 전에 제품 내 모든 입력 값에 대한 무결성 검증을 할 필요가 있으며, 기타 보안 검사 후 출시 하여야 합니다.

5. 대응 방안

해당 취약점은 제한된 버퍼 내 입력 값에 대한 제한이 없기 때문에 발생한 취약점입니다. 그러므로 사용자 입력 값의 길이 제한을 두어 인접 스택 영역을 침범하지 못하게 할 수 있습니다. 사용자는 방화벽 사용을 철저히 하여야 하고 수시로 의심스러운 네트워크와 연결되어 있지는 않은지 확인 하여야 합니다.

6. 참고 자료

6.1. 참고 문헌

6.2. 참고 웹 문서

http://www.exploit-db.com/exploits/19937/